Cisco IOS Service Selection Gateway Command Reference

October 2009

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 Service Selection Gateway Command Reference
© 2009 Cisco Systems, Inc. All rights reserved.

CONTENTS

About Cisco IOS Software Documentation ix

Documentation Objectives ix

Audience ix

Documentation Conventions ix

Typographic Conventions x

Command Syntax Conventions x

Software Conventions xi

Reader Alert Conventions xi

Documentation Organization xi

Cisco IOS Documentation Set xii

Cisco IOS Documentation on Cisco.com xii

Configuration Guides, Command References, and Supplementary Resources xiii

Additional Resources and Documentation Feedback xx

Using the Command-Line Interface in Cisco IOS Software xxi

Initially Configuring a Device xxi

Using the CLI xxii

Understanding Command Modes xxii

Using the Interactive Help Feature xxv

Understanding Command Syntax xxvi

Understanding Enable and Enable Secret Passwords xxvii

Using the Command History Feature xxviii

Abbreviating Commands xxix

Using Aliases for CLI Commands xxix

Using the no and default Forms of Commands xxx

Using the debug Command xxx

Filtering Output Using Output Modifiers xxx

Understanding CLI Error Messages xxxi

Saving Changes to a Configuration xxxi

Additional Information xxxii

Introduction SSG- 1

Service Selection Gateway Commands SSG- 3

address-pool SSG- 4
attribute SSG- 6
authorization list SSG- 9
authorization pending maximum SSG- 10
authorization rate-limit SSG- 11
clear ssg connection SSG- 12
clear ssg host SSG- 13
clear ssg next-hop SSG- 16
clear ssg open-garden SSG- 17
clear ssg pass-through-filter SSG- 19
clear ssg pending-command SSG- 20
clear ssg prepaid default-quota SSG- 21
clear ssg radius-proxy client-address SSG- 22
clear ssg radius-proxy nas-address SSG- 23
clear ssg service SSG- 25
clear ssg user transparent all SSG- 27
clear ssg user transparent passthrough SSG- 28
clear ssg user transparent suspect SSG- 29
clear ssg user transparent unidentified SSG- 30
client-address SSG- 31
destination access-list SSG- 33
destination range SSG- 35
dnis-prefix all service SSG- 37
download exclude-profile (SSG dial-out) SSG- 39
download exclude-profile (SSG PTA-MD) SSG- 41
download exclude-profile (SSG-auto-domain) SSG- 43
exclude SSG- 45
exclude (SSG PTA-MD) SSG- 47
exclude dnis-prefix SSG- 50
forward accounting-on-off SSG- 52
forward accounting-start-stop SSG- 53
hand-off SSG- 55
home-agent (SSG-radius-proxy) SSG- 57

host overlap **SSG- 59**
idle (SSG-radius-proxy-timers) **SSG- 60**
idle-timeout (SSG) **SSG- 62**
ip-address (SSG-radius-proxy-timers) **SSG- 64**
key (SSG-radius-proxy-client) **SSG- 66**
length (SSG) **SSG- 68**
local-profile **SSG- 70**
max-sessions host **SSG- 72**
mode extended **SSG- 74**
msid (SSG-radius-proxy-timers) **SSG- 76**
nat user-address **SSG- 78**
network (ssg-redirect) **SSG- 80**
network-list **SSG- 82**
port (ssg-redirect) **SSG- 84**
port-list **SSG- 86**
query ip dhcp **SSG- 88**
redirect access-list **SSG- 89**
redirect captivate advertising default group **SSG- 91**
redirect captivate initial default group **SSG- 93**
redirect permanent http to **SSG- 95**
redirect prepaid-user to **SSG- 97**
redirect smtp group **SSG- 99**
redirect to **SSG- 101**
redirect unauthenticated-user to **SSG- 103**
redirect unauthorized-service service to **SSG- 105**
redirect unauthorized-service to **SSG- 107**
remove vsa **SSG- 109**
select **SSG- 111**
server (SSG) **SSG- 113**
server-group **SSG- 115**
server-port **SSG- 117**
session-identifier **SSG- 119**
sessions auto cleanup **SSG- 121**
show ssg auto-domain exclude-profile **SSG- 123**
show ssg binding **SSG- 125**

show ssg connection SSG- 127
show ssg dial-out exclude-list SSG- 131
show ssg direction SSG- 132
show ssg host SSG- 133
show ssg interface SSG- 139
show ssg multidomain ppp exclude-list SSG- 140
show ssg next-hop SSG- 142
show ssg open-garden SSG- 144
show ssg pass-through-filter SSG- 145
show ssg pending-command SSG- 147
show ssg port-map ip SSG- 148
show ssg port-map status SSG- 150
show ssg prepaid default-quota SSG- 152
show ssg radius-proxy SSG- 154
show ssg service SSG- 158
show ssg summary SSG- 162
show ssg tcp-redirect group SSG- 163
show ssg user transparent SSG- 166
show ssg user transparent authorizing SSG- 167
show ssg user transparent passthrough SSG- 168
show ssg user transparent suspect SSG- 169
show ssg user transparent unidentified SSG- 171
show ssg vc-service-map SSG- 173
source ip SSG- 174
ssg aaa group prepaid SSG- 176
ssg accounting SSG- 178
ssg attribute 44 suffix host ip SSG- 180
ssg auto-domain SSG- 181
ssg auto-logoff arp SSG- 183
ssg auto-logoff icmp SSG- 185
ssg bind direction SSG- 187
ssg bind service SSG- 190
ssg default-network SSG- 192
ssg dfp ip SSG- 193
ssg dfp weight SSG- 195

ssg dial-out SSG- 197
ssg direction SSG- 199
ssg enable SSG- 201
ssg intercept dhcp SSG- 203
ssg local-forwarding SSG- 205
ssg login transparent SSG- 206
ssg maximum host SSG- 207
ssg maximum service SSG- 208
ssg maxservice SSG- 209
ssg multidomain ppp SSG- 210
ssg next-hop download SSG- 212
ssg open-garden SSG- 214
ssg pass-through SSG- 216
ssg port-map SSG- 218
ssg port-map destination access-list SSG- 220
ssg port-map destination range SSG- 222
ssg port-map enable SSG- 224
ssg port-map length SSG- 226
ssg port-map source ip SSG- 228
ssg prepaid reauthorization drop-packet SSG- 230
ssg prepaid threshold SSG- 232
ssg profile-cache SSG- 234
ssg qos police SSG- 236
ssg query mac dhcp SSG- 239
ssg radius-helper SSG- 240
ssg radius-proxy SSG- 242
ssg service-cache SSG- 244
ssg service-cache refresh SSG- 246
ssg service-password SSG- 248
ssg service-search-order SSG- 249
ssg tcp-redirect SSG- 251
ssg vc-service-map SSG- 253
ssg wlan reconnect SSG- 255
timeouts (SSG-radius-proxy) SSG- 257
user passthrough maximum SSG- 258

user suspect maximum **SSG- 259**
user suspect timeout **SSG- 260**
user unidentified timeout **SSG- 261**
user unidentified traffic permit **SSG- 262**
username mac **SSG- 263**

About Cisco IOS Software Documentation

Last Updated: October 14, 2009

This document describes the objectives, audience, conventions, and organization used in Cisco IOS 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 ix
- Audience, page ix
- Documentation Conventions, page ix
- Documentation Organization, page xi
- Additional Resources and Documentation Feedback, page xx

Documentation Objectives

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

Audience

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

Documentation Conventions

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

This section contains the following topics:

- Typographic Conventions, page x
- Command Syntax Conventions, page x
- Software Conventions, page xi
- Reader Alert Conventions, page xi

Typographic Conventions

Cisco IOS documentation uses the following typographic conventions:

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

Command Syntax Conventions

Cisco IOS documentation uses the following command syntax conventions:

Convention	Description
bold	Bold text indicates commands and keywords that you enter as shown.
italic	Italic text indicates arguments for which you supply values.
[x]	Square brackets enclose an optional keyword or argument.
...	An ellipsis (three consecutive nonbolded periods without spaces) after a syntax element indicates that the element can be repeated.
|	A vertical line, called a pipe, that is enclosed within braces or square brackets 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 software uses the following program code conventions:

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

Reader Alert Conventions

Cisco IOS 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 documentation set, how it is organized, and how to access it on Cisco.com. It also lists the configuration guides, command references, and supplementary references and resources that comprise the documentation set. It contains the following topics:

- Cisco IOS Documentation Set, page xii
- Cisco IOS Documentation on Cisco.com, page xii
- Configuration Guides, Command References, and Supplementary Resources, page xiii

Cisco IOS Documentation Set

The Cisco IOS 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 select severity 3 (moderate) defects in released Cisco IOS 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 release.
  - Configuration guides—Compilations of documents that provide conceptual and task-oriented descriptions of Cisco IOS features.
  - Command references—Compilations of command pages in alphabetical order that provide detailed information about the commands used in the Cisco IOS features and the processes that comprise the related configuration guides. For each technology, there is a single command reference that supports all Cisco IOS releases and that is updated at each standard release.
- Lists of all the commands in a specific release and all commands that are new, modified, removed, or replaced in the release.
- Command reference book for **debug** commands. Command pages are listed in alphabetical order.
- Reference book for system messages for all Cisco IOS releases.

Cisco IOS Documentation on Cisco.com

The following sections describe the organization of the Cisco IOS documentation set and how to access various document types.

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

New Features List

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

Feature Guides

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

Configuration Guides

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

Command References

Command reference books contain descriptions of Cisco IOS 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 commands, use the Command Lookup Tool at http://tools.cisco.com/Support/CLILookup or the *Cisco IOS Master Command List, All Releases*, at http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html.

Cisco IOS Supplementary Documents and Resources

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

Configuration Guides, Command References, and Supplementary Resources

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

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

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 Configuration Guides and Command References

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

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

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
• *Cisco IOS Bridging and IBM Networking Configuration Guide* • *Cisco IOS Bridging Command Reference* • *Cisco IOS IBM Networking Command Reference*	Transparent and source-route transparent (SRT) bridging, source-route bridging (SRB), Token Ring Inter-Switch Link (TRISL), and token ring route switch module (TRRSM). Data-link switching plus (DLSw+), serial tunnel (STUN), block serial tunnel (BSTUN); logical link control, type 2 (LLC2), synchronous data link control (SDLC); IBM Network Media Translation, including Synchronous Data Logical Link Control (SDLLC) and qualified LLC (QLLC); downstream physical unit (DSPU), Systems Network Architecture (SNA) service point, SNA frame relay access, advanced peer-to-peer networking (APPN), native client interface architecture (NCIA) client/server topologies, and IBM Channel Attach.
• *Cisco IOS Broadband Access Aggregation and DSL Configuration Guide* • *Cisco IOS Broadband Access Aggregation and DSL Command Reference*	PPP over ATM (PPPoA) and PPP over Ethernet (PPPoE).
• *Cisco IOS Carrier Ethernet Configuration Guide* • *Cisco IOS Carrier Ethernet Command Reference*	Connectivity fault management (CFM), Ethernet Local Management Interface (ELMI), IEEE 802.3ad link bundling, Link Layer Discovery Protocol (LLDP), media endpoint discovery (MED), and Operation, Administration, and Maintenance (OAM).
• *Cisco IOS Configuration Fundamentals Configuration Guide* • *Cisco IOS Configuration Fundamentals Command Reference*	Autoinstall, Setup, Cisco IOS command-line interface (CLI), Cisco IOS file system (IFS), Cisco IOS web browser user interface (UI), basic file transfer services, and file management.
• *Cisco IOS DECnet Configuration Guide* • *Cisco IOS DECnet Command Reference*	DECnet protocol.
• *Cisco IOS Dial Technologies Configuration Guide* • *Cisco IOS Dial Technologies Command Reference*	Asynchronous communications, dial backup, dialer technology, dial-in terminal services and AppleTalk remote access (ARA), dial-on-demand routing, dial-out, ISDN, large scale dial-out, modem and resource pooling, Multilink PPP (MLP), PPP, and virtual private dialup network (VPDN).
• *Cisco IOS Flexible NetFlow Configuration Guide* • *Cisco IOS Flexible NetFlow Command Reference*	Flexible NetFlow.
• *Cisco IOS High Availability Configuration Guide* • *Cisco IOS High Availability Command Reference*	A variety of high availability (HA) features and technologies that are available for different network segments (from enterprise access to service provider core) to facilitate creation of end-to-end highly available networks. Cisco IOS HA features and technologies can be categorized in three key areas: system-level resiliency, network-level resiliency, and embedded management for resiliency.
• *Cisco IOS Integrated Session Border Controller Command Reference*	A VoIP-enabled device that is deployed at the edge of networks. An SBC is a toolkit of functions, such as signaling interworking, network hiding, security, and quality of service (QoS).

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

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
• *Cisco IOS Intelligent Services Gateway Configuration Guide* • *Cisco IOS Intelligent Services Gateway Command Reference*	Subscriber identification, service and policy determination, session creation, session policy enforcement, session life-cycle management, accounting for access and service usage, and session state monitoring.
• *Cisco IOS Interface and Hardware Component Configuration Guide* • *Cisco IOS Interface and Hardware Component Command Reference*	LAN interfaces, logical interfaces, serial interfaces, virtual interfaces, and interface configuration.
• *Cisco IOS IP Addressing Services Configuration Guide* • *Cisco IOS IP Addressing Services Command Reference*	Address Resolution Protocol (ARP), Network Address Translation (NAT), Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), and Next Hop Address Resolution Protocol (NHRP).
• *Cisco IOS IP Application Services Configuration Guide* • *Cisco IOS IP Application Services Command Reference*	Enhanced Object Tracking (EOT), Gateway Load Balancing Protocol (GLBP), Hot Standby Router Protocol (HSRP), IP Services, Server Load Balancing (SLB), Stream Control Transmission Protocol (SCTP), TCP, Web Cache Communication Protocol (WCCP), User Datagram Protocol (UDP), and Virtual Router Redundancy Protocol (VRRP).
• *Cisco IOS IP Mobility Configuration Guide* • *Cisco IOS IP Mobility Command Reference*	Mobile ad hoc networks (MANet) and Cisco mobile networks.
• *Cisco IOS IP Multicast Configuration Guide* • *Cisco IOS IP Multicast Command Reference*	Protocol Independent Multicast (PIM) sparse mode (PIM-SM), bidirectional PIM (bidir-PIM), Source Specific Multicast (SSM), Multicast Source Discovery Protocol (MSDP), Internet Group Management Protocol (IGMP), and Multicast VPN (MVPN).
• *Cisco IOS IP Routing Protocols Configuration Guide* • *Cisco IOS IP Routing Protocols Command Reference*	Border Gateway Protocol (BGP), multiprotocol BGP, multiprotocol BGP extensions for IP multicast, bidirectional forwarding detection (BFD), Enhanced Interior Gateway Routing Protocol (EIGRP), Interior Gateway Routing Protocol (IGRP), Intermediate System-to-Intermediate System (IS-IS), On-Demand Routing (ODR), Open Shortest Path First (OSPF), and Routing Information Protocol (RIP).
• *Cisco IOS IP Routing: BFD Configuration Guide*	Bidirectional forwarding detection (BFD).
• *Cisco IOS IP Routing: BGP Configuration Guide* • *Cisco IOS IP Routing: BGP Command Reference*	Border Gateway Protocol (BGP), multiprotocol BGP, multiprotocol BGP extensions for IP multicast.
• *Cisco IOS IP Routing: EIGRP Configuration Guide* • *Cisco IOS IP Routing: EIGRP Command Reference*	Enhanced Interior Gateway Routing Protocol (EIGRP).
• *Cisco IOS IP Routing: ISIS Configuration Guide* • *Cisco IOS IP Routing: ISIS Command Reference*	Intermediate System-to-Intermediate System (IS-IS).
• *Cisco IOS IP Routing: ODR Configuration Guide* • *Cisco IOS IP Routing: ODR Command Reference*	On-Demand Routing (ODR).

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

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
• *Cisco IOS IP Routing: OSPF Configuration Guide* • *Cisco IOS IP Routing: OSPF Command Reference*	Open Shortest Path First (OSPF).
• *Cisco IOS IP Routing: Protocol-Independent Configuration Guide* • *Cisco IOS IP Routing: Protocol-Independent Command Reference*	IP routing protocol-independent features and commands. Generic policy-based routing (PBR) features and commands are included.
• *Cisco IOS IP Routing: RIP Configuration Guide* • *Cisco IOS IP Routing: RIP Command Reference*	Routing Information Protocol (RIP).
• *Cisco IOS IP SLAs Configuration Guide* • *Cisco IOS IP SLAs Command Reference*	Cisco IOS IP Service Level Agreements (IP SLAs).
• *Cisco IOS IP Switching Configuration Guide* • *Cisco IOS IP Switching Command Reference*	Cisco Express Forwarding, fast switching, and Multicast Distributed Switching (MDS).
• *Cisco IOS IPv6 Configuration Guide* • *Cisco IOS IPv6 Command Reference*	For IPv6 features, protocols, and technologies, go to the IPv6 "Start Here" document.
• *Cisco IOS ISO CLNS Configuration Guide* • *Cisco IOS ISO CLNS Command Reference*	ISO Connectionless Network Service (CLNS).
• *Cisco IOS LAN Switching Configuration Guide* • *Cisco IOS LAN Switching Command Reference*	VLANs, Inter-Switch Link (ISL) encapsulation, IEEE 802.10 encapsulation, IEEE 802.1Q encapsulation, and multilayer switching (MLS).
• *Cisco IOS Mobile Wireless Gateway GPRS Support Node Configuration Guide* • *Cisco IOS Mobile Wireless Gateway GPRS Support Node Command Reference*	Cisco IOS Gateway GPRS Support Node (GGSN) in a 2.5-generation general packet radio service (GPRS) and 3-generation universal mobile telecommunication system (UMTS) network.
• *Cisco IOS Mobile Wireless Home Agent Configuration Guide* • *Cisco IOS Mobile Wireless Home Agent Command Reference*	Cisco Mobile Wireless Home Agent, an anchor point for mobile terminals for which mobile IP or proxy mobile IP services are provided.
• *Cisco IOS Mobile Wireless Packet Data Serving Node Configuration Guide* • *Cisco IOS Mobile Wireless Packet Data Serving Node Command Reference*	Cisco Packet Data Serving Node (PDSN), a wireless gateway that is between the mobile infrastructure and standard IP networks and that enables packet data services in a code division multiple access (CDMA) environment.
• *Cisco IOS Mobile Wireless Radio Access Networking Configuration Guide* • *Cisco IOS Mobile Wireless Radio Access Networking Command Reference*	Cisco IOS radio access network products.
• *Cisco IOS Multiprotocol Label Switching Configuration Guide* • *Cisco IOS Multiprotocol Label Switching Command Reference*	MPLS Label Distribution Protocol (LDP), MPLS Layer 2 VPNs, MPLS Layer 3 VPNs, MPLS traffic engineering (TE), and MPLS Embedded Management (EM) and MIBs.

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

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
• *Cisco IOS Multi-Topology Routing Configuration Guide* • *Cisco IOS Multi-Topology Routing Command Reference*	Unicast and multicast topology configurations, traffic classification, routing protocol support, and network management support.
• *Cisco IOS NetFlow Configuration Guide* • *Cisco IOS NetFlow Command Reference*	Network traffic data analysis, aggregation caches, and export features.
• *Cisco IOS Network Management Configuration Guide* • *Cisco IOS Network Management Command Reference*	Basic system management; system monitoring and logging; troubleshooting, logging, and fault management; Cisco Discovery Protocol; Cisco IOS Scripting with Tool Control Language (Tcl); Cisco networking services (CNS); DistributedDirector; Embedded Event Manager (EEM); Embedded Resource Manager (ERM); Embedded Syslog Manager (ESM); HTTP; Remote Monitoring (RMON); SNMP; and VPN Device Manager Client for Cisco IOS software (XSM Configuration).
• *Cisco IOS Novell IPX Configuration Guide* • *Cisco IOS Novell IPX Command Reference*	Novell Internetwork Packet Exchange (IPX) protocol.
• *Cisco IOS Optimized Edge Routing Configuration Guide* • *Cisco IOS Optimized Edge Routing Command Reference*	Optimized edge routing (OER) monitoring; Performance Routing (PfR); and automatic route optimization and load distribution for multiple connections between networks.
• *Cisco IOS Quality of Service Solutions Configuration Guide* • *Cisco IOS Quality of Service Solutions Command Reference*	Traffic queueing, traffic policing, traffic shaping, Modular QoS CLI (MQC), Network-Based Application Recognition (NBAR), Multilink PPP (MLP) for QoS, header compression, AutoQoS, Resource Reservation Protocol (RSVP), and weighted random early detection (WRED).
• *Cisco IOS Security Command Reference*	Access control lists (ACLs); authentication, authorization, and accounting (AAA); firewalls; IP security and encryption; neighbor router authentication; network access security; network data encryption with router authentication; public key infrastructure (PKI); RADIUS; TACACS+; terminal access security; and traffic filters.
• *Cisco IOS Security Configuration Guide: Securing the Data Plane*	Access Control Lists (ACLs); Firewalls: Context-Based Access Control (CBAC) and Zone-Based Firewall; Cisco IOS Intrusion Prevention System (IPS); Flexible Packet Matching; Unicast Reverse Path Forwarding (uRPF); Threat Information Distribution Protocol (TIDP) and TMS.
• *Cisco IOS Security Configuration Guide: Securing the Control Plane*	Control Plane Policing, Neighborhood Router Authentication.
• *Cisco IOS Security Configuration Guide: Securing User Services*	AAA (includes 802.1x authentication and 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.

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

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
• *Cisco IOS Security Configuration Guide: Secure Connectivity*	Internet Key Exchange (IKE) for IPsec VPNs; IPsec Data Plane features; IPsec Management features; Public Key Infrastructure (PKI); Dynamic Multipoint VPN (DMVPN); Easy VPN; Cisco Group Encrypted Transport VPN (GETVPN); SSL VPN.
• *Cisco IOS Service Advertisement Framework Configuration Guide* • *Cisco IOS Service Advertisement Framework Command Reference*	Cisco Service Advertisement Framework.
• *Cisco IOS Service Selection Gateway Configuration Guide* • *Cisco IOS Service Selection Gateway Command Reference*	Subscriber authentication, service access, and accounting.
• *Cisco IOS Software Activation Configuration Guide* • *Cisco IOS Software Activation Command Reference*	An orchestrated collection of processes and components to activate Cisco IOS software feature sets by obtaining and validating Cisco software licenses.
• *Cisco IOS Software Modularity Installation and Configuration Guide* • *Cisco IOS Software Modularity Command Reference*	Installation and basic configuration of software modularity images, including installations on single and dual route processors, installation rollbacks, software modularity binding, software modularity processes, and patches.
• *Cisco IOS Terminal Services Configuration Guide* • *Cisco IOS Terminal Services Command Reference*	DEC, local-area transport (LAT), and X.25 packet assembler/disassembler (PAD).
• *Cisco IOS Virtual Switch Command Reference*	Virtual switch redundancy, high availability, and packet handling; converting between standalone and virtual switch modes; virtual switch link (VSL); Virtual Switch Link Protocol (VSLP). **Note** For information about virtual switch configuration, see the product-specific software configuration information for the Cisco Catalyst 6500 series switch or for the Metro Ethernet 6500 series switch.
• *Cisco IOS Voice Configuration Library* • *Cisco IOS Voice Command Reference*	Cisco IOS support for voice call control protocols, interoperability, physical and virtual interface management, and troubleshooting. The library includes documentation for IP telephony applications.
• *Cisco IOS VPDN Configuration Guide* • *Cisco IOS VPDN Command Reference*	Layer 2 Tunneling Protocol (L2TP) dial-out load balancing and redundancy; L2TP extended failover; L2TP security VPDN; multihop by Dialed Number Identification Service (DNIS); timer and retry enhancements for L2TP and Layer 2 Forwarding (L2F); RADIUS Attribute 82 (tunnel assignment ID); shell-based authentication of VPDN users; tunnel authentication via RADIUS on tunnel terminator.

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

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
• *Cisco IOS Wide-Area Networking Configuration Guide* • *Cisco IOS Wide-Area Networking Command Reference*	Frame Relay; Layer 2 Tunnel Protocol Version 3 (L2TPv3); L2VPN Pseudowire Redundancy; L2VPN Interworking; Layer 2 Local Switching; Link Access Procedure, Balanced (LAPB); and X.25.
• *Cisco IOS Wireless LAN Configuration Guide* • *Cisco IOS Wireless LAN Command Reference*	Broadcast key rotation, IEEE 802.11x support, IEEE 802.1x authenticator, IEEE 802.1x local authentication service for Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST), Multiple Basic Service Set ID (BSSID), Wi-Fi Multimedia (WMM) required elements, and Wi-Fi Protected Access (WPA).

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

Table 2 Cisco IOS Supplementary Documents and Resources

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

Additional Resources and Documentation Feedback

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

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

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

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, 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, and Flip Gift Card 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 Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, 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. (0908R)

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

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

Using the Command-Line Interface in Cisco IOS Software

Last Updated: October 14, 2009

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

- Initially Configuring a Device, page xxi
- Using the CLI, page xxii
- Saving Changes to a Configuration, page xxxi
- Additional Information, page xxxii

For more information about using the CLI, see the "Using the Cisco IOS Command-Line Interface" section of the *Cisco IOS Configuration Fundamentals Configuration Guide*.

For information about the software documentation set, see the "About Cisco IOS 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/Technologies 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 changes that you can make to a console port and an AUX port:

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

Note The AUX port on the Route Processor (RP) installed in a Cisco 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 xxii
- Using the Interactive Help Feature, page xxv
- Understanding Command Syntax, page xxvi
- Understanding Enable and Enable Secret Passwords, page xxvii
- Using the Command History Feature, page xxviii
- Abbreviating Commands, page xxix
- Using Aliases for CLI Commands, page xxix
- Using the no and default Forms of Commands, page xxx
- Using the debug Command, page xxx
- Filtering Output Using Output Modifiers, page xxx
- Understanding CLI Error Messages, page xxxi

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 3 lists common command modes with associated CLI prompts, access and exit methods, and a brief description of how each mode is used.

Table 3 CLI Command Modes

Command Mode	Access Method	Prompt	Exit Method	Mode Usage
User EXEC	Log in.	`Router>`	Issue the **logout** or **exit** command.	• Change terminal settings. • Perform basic tests. • Display device status.
Privileged EXEC	From user EXEC mode, issue the **enable** command.	`Router#`	Issue the **disable** command or the **exit** command to return to user EXEC mode.	• Issue **show** and **debug** commands. • Copy images to the device. • Reload the device. • Manage device configuration files. • Manage device file systems.
Global configuration	From privileged EXEC mode, issue the **configure terminal** command.	`Router(config)#`	Issue the **exit** command or the **end** command to return to privileged EXEC mode.	Configure the device.
Interface configuration	From global configuration mode, issue the **interface** command.	`Router(config-if)#`	Issue the **exit** command to return to global configuration mode or the **end** command to return to privileged EXEC mode.	Configure individual interfaces.
Line configuration	From global configuration mode, issue the **line vty** or **line console** command.	`Router(config-line)#`	Issue the **exit** command to return to global configuration mode or the **end** command to return to privileged EXEC mode.	Configure individual terminal lines.

Table 3 CLI Command Modes (continued)

Command Mode	Access Method	Prompt	Exit Method	Mode Usage
ROM monitor	From privileged EXEC mode, issue the **reload** command. Press the **Break** key during the first 60 seconds while the system is booting.	`rommon # >` The # symbol represents the line number and increments at each prompt.	Issue the **continue** command.	• Run as the default operating mode when a valid image cannot be loaded. • Access the fall-back procedure for loading an image when the device lacks a valid image and cannot be booted. • Perform password recovery when a Ctrl-Break sequence is issued within 60 seconds of a power-on or reload event.
Diagnostic (available only on Cisco ASR 1000 series routers)	The router boots or enters diagnostic mode in the following scenarios. When a Cisco IOS process or processes fail, in most scenarios the router will reload. • A user-configured access policy was configured using the **transport-map** command, which directed the user into diagnostic mode. • The router was accessed using an RP auxiliary port. • A break signal (**Ctrl-C**, **Ctrl-Shift-6**, or the **send break** command) was entered, and the router was configured to enter diagnostic mode when the break signal was received.	`Router(diag)#`	If a Cisco IOS process failure is the reason for entering diagnostic mode, the failure must be resolved and the router must be rebooted to exit diagnostic mode. If the router is in diagnostic mode because of a transport-map configuration, access the router through another port or use a method that is configured to connect to the Cisco IOS CLI. If the RP auxiliary port was used to access the router, use another port for access. Accessing the router through the auxiliary port is not useful for customer purposes.	• Inspect various states on the router, including the Cisco IOS state. • Replace or roll back the configuration. • Provide methods of restarting the Cisco IOS software or other processes. • Reboot hardware (such as the entire router, an RP, an ESP, a SIP, a SPA) or other hardware components. • Transfer files into or off of the router using remote access methods such as FTP, TFTP, and SCP.

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

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

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

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

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

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

Using the Interactive Help Feature

The CLI includes an interactive Help feature. Table 4 describes the purpose of the CLI interactive Help commands.

Table 4 CLI Interactive Help Commands

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

The following examples show how to use the help commands:

help

```
Router> help

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

Two styles of help are provided:

1. Full help is available when you are ready to enter a command argument (e.g. 'show ?')
and describes each possible argument.

2. Partial help is provided when an abbreviated argument is entered and you want to know
what arguments match the input (e.g. 'show pr?'.)
```

?

```
Router# ?
Exec commands:
  access-enable        Create a temporary access-List entry
  access-profile       Apply user-profile to interface
  access-template      Create a temporary access-List entry
  alps                 ALPS exec commands
  archive              manage archive files
<snip>
```

partial command?

```
Router(config)# zo?
zone  zone-pair
```

partial command<Tab>

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

command ?

```
Router(config-if)# pppoe ?
  enable        Enable pppoe
  max-sessions  Maximum PPPOE sessions
```

command keyword ?

```
Router(config-if)# pppoe enable ?
  group  attach a BBA group
  <cr>
```

Understanding Command Syntax

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

Specific conventions convey information about syntax and command elements. Table 5 describes these conventions.

Table 5 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 numeral. 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 numeral for the first character of your password followed by a space, the system will read the number as if it were the numeric keyword and not as part of your password.

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

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

For more information about password recovery procedures for Cisco products, see http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00801746e6.shtml.

Using the Command History Feature

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

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

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

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

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

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

- Press Ctrl-P or the Up Arrow key—Recalls commands beginning with the most recent command. Repeat the key sequence to recall successively older commands.
- Press Ctrl-N or the Down Arrow key—Recalls the most recent commands in the history buffer after they have been recalled using Ctrl-P or the Up Arrow key. Repeat the key sequence to recall successively more recent commands.

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

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

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

Abbreviating Commands

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

Using Aliases for CLI Commands

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

Table 6 shows the default command aliases.

Table 6 Default Command Aliases

Command Alias	Original Command
h	help
lo	logout
p	ping
s	show
u or **un**	undebug
w	where

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

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

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

For more information about the **alias** command, see http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_a1.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 software. Some **debug** commands are **debug all**, **debug aaa accounting**, and **debug mpls packets**. To use **debug** commands during a Telnet session with a device, you must first enter the **terminal monitor** command. To turn off debugging completely, you must enter the **undebug all** command.

For more information about **debug** commands, see the *Cisco IOS Debug Command Reference* at http://www.cisco.com/en/US/docs/ios/debug/command/reference/db_book.html.

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

Filtering Output Using Output Modifiers

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

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 7 shows the common CLI error messages.

Table 7 Common CLI Error Messages

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

For more system error messages, see the following document:

- *Cisco IOS Release 12.4T System Message Guide*

Saving Changes to a Configuration

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

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

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

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

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

Additional Information

- "Using the Cisco IOS Command-Line Interface" section of the *Cisco IOS Configuration Fundamentals Configuration Guide*

  http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/cf_cli-basics.html
- Cisco Product/Technology Support

  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 software

  http://www.cisco.com/pcgi-bin/Support/Errordecoder/index.cgi
- Command Lookup Tool, a tool to help you find detailed descriptions of Cisco IOS commands (requires Cisco.com user ID and password)

  http://tools.cisco.com/Support/CLILookup
- Output Interpreter, a troubleshooting tool that analyzes command output of supported **show** commands

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

---

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, 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, and Flip Gift Card 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 Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, 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. (0908R)

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

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

Introduction

Service Selection Gateway (SSG) is a switching solution for service providers who offer intranet, extranet, and Internet connections to subscribers who use broadband access technology, such as digital subscriber lines (DSL), cable modems, and wireless. SSG allows simultaneous access to network services.

The *Cisco IOS Service Selection Gateway Command Reference* contains commands for configuring SSG. The commands in this document are organized alphabetically.

Some commands required for configuring SSG may be found in other Cisco IOS command references. Use the master list of commands or search online to find these commands.

For information about how to configure SSG, consult the *Cisco IOS Service Selection Gateway Configuration Guide*.

Service Selection Gateway Commands

This chapter presents commands for configuring and maintaining Cisco IOS Service Selection Gateway (SSG) applications. The commands are presented in alphabetical order.

address-pool

Note Effective with Cisco IOS Release 15.0(1)M, the **address-pool** command is not available in Cisco IOS software.

To define local IP pools that are to be used by Service Selection Gateway (SSG) to assign IP addresses to users for which SSG is acting as a RADIUS client, use the **address-pool** command in SSG-radius-proxy configuration mode. To remove a local IP pool, use the **no** form of this command.

address-pool *start-ip end-ip* [**domain** *domain-name*]

no address-pool *start-ip end-ip* [**domain** *domain-name*]

Syntax Description

start-ip	First IP address of the local IP address pool.
end-ip	Last IP address of the local IP address pool.
domain	(Optional) IP address pool for a specific domain.
domain-name	(Optional) Name of the domain.

Defaults

SSG does not assign IP addresses from a local IP pool.

Command Modes

SSG-radius-proxy configuration

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2 T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to configure SSG to assign an IP address taken from a local pool to a user for which SSG is acting as a RADIUS client. SSG assigns an IP address from a local pool only when one has not been assigned by one of the following methods:

- Assignment in the Access-Accept from the AAA server
- Assignment in the Access-Request received from the client
- Assignment from an Autodomain service (tunnel or proxy) that does not have the **auto-domain nat user-address** configuration enabled

Note You must have SSG the AutoDomain configured in order for an IP address to be assigned from an Autodomain tunnel.

You can use this command to define a global local IP address pool or an IP address pool for a specific domain by using the **domain** keyword. You cannot create pools with more than 20,000 addresses.

Note Using IP address pools within SSG is completely standalone and unrelated to Cisco IOS IP local pools.

Examples

The following example shows how to configure a local IP address pool for SSG:

```
address-pool 172.16.16.0 172.16.20.0
```

The following example shows how to configure a local IP address pool for the domain named “cisco”.

```
address-pool 172.21.21.0 172.21.25.0 domain cisco
```

Related Commands

Command	Description
clear ssg radius-proxy client-address	Clears all hosts connected to a specific RADIUS client.
clear ssg radius-proxy nas-address	Clears all hosts connected to a specific NAS.
forward accounting-start-stop	Proxies accounting start, stop, and update packets generated by any RADIUS clients to the AAA server.
idle-timeout (SSG)	Configures a host object timeout value.
server-port	Defines the ports for the SSG RADIUS proxy.
show ssg tcp-redirect group	Displays the pool of IP addresses configured for a router or a specific domain.
ssg enable	Enables SSG.
ssg radius-proxy	Enables SSG RADIUS Proxy.
ssg tcp-redirect	Configures the RADIUS proxy IP address and shared secret.

attribute

Note Effective with Cisco IOS Release 15.0(1)M, the **attribute** command is not available in Cisco IOS software.

To configure an attribute in a local service profile, use the **attribute** command in profile configuration mode. To delete an attribute from a service profile, use the **no** form of this command.

attribute *radius-attribute-id* [*vendor-id*] [*cisco-vsa-type*] *attribute-value*

no attribute *radius-attribute-id* [*vendor-id*] [*cisco-vsa-type*] *attribute-value*

Syntax Description

radius-attribute-id	RADIUS attribute ID to be configured.
vendor-id	(Optional) Vendor ID. Required if the RADIUS attribute ID is 26, indicating a vendor-specific attribute (VSA). The Cisco vendor ID is 9.
cisco-vsa-type	(Optional) Cisco VSA type. Required if the vendor ID is 9, indicating a Cisco VSA.
attribute-value	Attribute value. The following optional attribute values are also supported: • **L***interval*—Required to change an interim accounting interval. Specifies the new accounting interval in seconds. • **Q**—Configures the token bucket parameters for the Service Selection Gateway (SSG) Hierarchical Policing feature.

Defaults

For the **L***interval* option: If the L option is not defined, the accounting records for a service profile will be sent at the interval configured by the **ssg accounting interval** command. If the **ssg accounting interval** command is not set, the accounting records are sent every 600 seconds.

Otherwise, no default behavior or values are set.

Command Modes

Profile configuration

Command History

Release	Modification
12.0(3)DC	This command was introduced on the Cisco 6400 NRP.
12.2(4)B	The L and Q attributes were introduced as an *attribute-value*.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(13)T	This command was modified for Cisco IOS Release 12.2(13)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to configure attributes in local service profiles.

For the SSG Open Garden feature, use this command to configure the Service Route, DNS Server Address, and Domain Name attributes in a local service profile before adding the service to the open garden.

To change the SSG accounting interval for a service profile, use the **L***interval* option in the **attribute** command. For example, if L80 is entered as the attribute value, the service profile sends accounting information every 80 seconds. Interim accounting can be disabled by entering the value (in seconds) as 0 (for instance, L0). When interim accounting is disabled, the normal accounting stops and starts are still sent.

For the SSG Hierarchical Policing feature, use the Q option to configure the token bucket parameters (token rate, normal burst, and excess burst). The syntax for the Q option is as follows:

Router(config-prof)# **attribute** radius-attribute-id vendor-id cisco-vsa-type
"**QU**;upstream-committed-rate;upstream-normal-burst;
[upstream-excess-burst];**D**;downstream-committed-rate;
downstream-normal-burst;[downstream-excess-burst]"

The variables are used to configure upstream (U) and downstream (D) policing. The upstream traffic is the traffic that travels from the subscriber to the network, and the downstream traffic is the traffic that travels from the network to the subscriber.

Examples

In the following example, the Cisco AV pair Upstream Access Control List (inacl) attribute is configured in the local service profile called "cisco.com":

```
Router(config)# local-profile cisco.com
Router(config-prof)# attribute 26 9 1 "ip:inacl#101=deny tcp 10.2.1.0 0.0.0.255 any eq 21"
```

In the following example, the Session-Timeout attribute is deleted from the local service profile called "cisco.com":

```
Router(config)# local-profile cisco.com
Router(config-prof)# no attribute 27 600
```

In the following example, the local profile "cisco.com" is configured to send an interim accounting update every 90 seconds:

```
Router(config)# local-profile cisco.com
Router(config-prof)# attribute 26 9 1 "L90"
```

In the following example, the SSG Hierarchical Policing parameters are set for upstream and downstream traffic:

```
Router(config)# local-profile cisco.com
Router(config-prof)# attribute 26 9 251 "QU:8000:16000:20000:D10000:20000:30000"
```

In the following example, an open garden service called "opencisco.com" is defined.

```
Router(config)# local-profile opencisco.com
Router(config-prof)# attribute 26 9 251 "Oopengarden1.com"
Router(config-prof)# attribute 26 9 251 "D10.13.1.5"
Router(config-prof)# attribute 26 9 251 "R10.1.1.0;255.255.255.0"
Router(config-prof)# exit
Router(config)# ssg open-garden opencisco.com
```

Related Commands

Command	Description
debug ssg data	Displays SSG QoS information.
local-profile	Configures a local service profile.
show ssg connection	Displays information about a particular SSG connection, including the policing parameters.
show ssg host	Displays information about an SSG host, including whether policing is enabled or disabled and the policing configurations of a particular host.
show ssg open-garden	Displays a list of all configured open garden services.
ssg accounting interval	Specifies the interval at which accounting updates are sent to the server.
ssg open-garden	Designates a service, defined in a local service profile, to be an open garden service.
ssg qos police	Enables SSG Hierarchical Policing on a router.

authorization list

Note Effective with Cisco IOS Release 15.0(1)M, the **authorization list** command is not available in Cisco IOS software.

To specify the server group that Service Selection Gateway (SSG) uses for authorization of transparent autologon users, use the **authorization list** command in transparent auto-logon configuration mode. To remove the server group specification, use the **no** form of this command.

authorization list *list-name*

no authorization list *list-name*

Syntax Description

list-name	Name of the server group that will be used for authorization of transparent autologon users.

Defaults

The default server group is used for user authorization.

Command Modes

Transparent auto-logon configuration

Command History

Release	Modification
12.3(1a)BW	This command was introduced.
12.3(3)B	This command was integrated into Cisco IOS Release 12.3(3)B.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
15.0(1)M	This command was removed.

Usage Guidelines

The server group must be configured using authentication, authorization, and accounting (AAA) commands.

Examples

The following example configures SSG to use the server group named “alpha” for authorization of transparent autologon users:

```
Router(config-login-transparent)# authorization list alpha
```

Related Commands

Command	Description
ssg login transparent	Enables the SSG Transparent Autologon feature.

authorization pending maximum

Note Effective with Cisco IOS Release 15.0(1)M, the **authorization pending maximum** command is not available in Cisco IOS software.

To specify the maximum number of Service Selection Gateway (SSG) transparent autologon access requests that can be pending at a given time, use the **authorization pending maximum** command in transparent auto-logon configuration mode. To remove the specification, use the **no** form of this command.

authorization pending maximum *number*

no authorization pending maximum *number*

Syntax Description

number	Maximum number of access requests that can be pending at a given time. Range is 1 to 5000.

Defaults

No maximum limit is set.

Command Modes

Transparent auto-logon configuration

Command History

Release	Modification
12.3(1a)BW	This command was introduced.
12.3(3)B	This command was integrated into Cisco IOS Release 12.3(3)B.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
15.0(1)M	This command was removed.

Usage Guidelines

When the number of SSG transparent autologon access requests reaches the configured maximum, SSG issues a system logging message. Any received packets that cause SSG to send a new RADIUS request are dropped at the Cisco Express Forwarding (CEF) path.

Examples

The following example specifies that the maximum number of access requests that can be pending is 10:

```
Router(config-login-transparent)# authorization pending maximum 10
```

Related Commands

Command	Description
ssg login transparent	Enables the SSG Transparent Autologon feature.

authorization rate-limit

Note Effective with Cisco IOS Release 15.0(1)M, the **authorization rate-limit** command is not available in Cisco IOS software.

To specify the maximum number of Service Selection Gateway (SSG) transparent autologon authorization requests sent per second to the authentication, authorization, and accounting (AAA) server, use the **authorization rate-limit** command in transparent auto-logon configuration mode. To remove the specification, use the **no** form of this command.

authorization rate-limit *number*

no authorization rate-limit *number*

Syntax Description

number	Maximum number of authorization requests sent per second. Range is from 1 to 10000.

Defaults

No rate limit is set.

Command Modes

Transparent auto-logon configuration

Command History

Release	Modification
12.3(1a)BW	This command was introduced.
12.3(3)B	This command was integrated into Cisco IOS Release 12.3(3)B.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
15.0(1)M	This command was removed.

Usage Guidelines

This command must be configured on the basis of the number of requests that the AAA server can handle per second. When the number of authorization requests per second reaches the configured rate limit, SSG issues a syslog message. A syslog message is generated only once for each time the rate-limit value is reached.

Examples

The following example specifies that the maximum number of authorization requests is 10:

```
Router(config-login-transparent)# authorization rate-limit 10
```

Related Commands

Command	Description
ssg login transparent	Enables the SSG Transparent Autologon feature.

clear ssg connection

Note Effective with Cisco IOS Release 15.0(1)M, the **clear ssg connection** command is not available in Cisco IOS software.

To remove the connections of a given host and a service name, use the **clear ssg connection** command in privileged EXEC mode.

clear ssg connection *ip-address service-name* [*interface*]

Syntax Description

ip-address	IP address of an active Service Selection Gateway (SSG) connection.
service-name	Name of an active SSG connection.
interface	(Optional) Interface to which the host is connected.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(3)DC	This command was introduced on the Cisco 6400 node route processor.
12.2(2)B	The *interface* argument was added.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Examples

The following example shows how to remove the service connection for “Service1” to host 192.168.1.1, connected through Fast Ethernet:

```
Router# clear ssg connection 192.168.1.1 fastethernet Service1
```

Related Commands

Command	Description
show ssg connection	Displays the connections of a given host and a service name.

clear ssg host

Note Effective with Cisco IOS Release 15.0(1)M, the **address-pool** command is not available in Cisco IOS software.

To remove a Service Selection Gateway (SSG) host object or a range of host objects, use the **clear ssg host** command in privileged EXEC mode. The command syntax of the **clear ssg host** command depends on whether the SSG port-bundle host key has been enabled with the **ssg port-map** global configuration command.

SSG Host Key Is Not Enabled

clear ssg host {**all** | **range** *start-ip-address end-ip-address*}

SSG Host Key Is Enabled

clear ssg host {**all** | *ip-address* | **range** [*start-ip-address end-ip-address* [*interface*]]}

Syntax Description

all	Clears all SSG host objects.
ip-address	Clears the specified SSG host object. This option is available only when SSG host key functionality is enabled.
range	Clears a specified range of SSG host objects.
start-ip-address	Host IP address. This argument specifies the beginning of an IP address range if it is followed by an *end-ip-address* value.
end-ip-address	(Optional) Host IP address that is used with the *ip-address* argument to specify a range of host objects.
interface	(Optional) SSG downlink interface through which the host or subscriber is connected, such as ATM, Fast Ethernet, or Virtual-Access. For more information, use the question mark (?) online help function.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(3)DC	This command was introduced on the Cisco 6400 node route processor.
12.2(2)B	The *interface* argument was added for the SSG Host Key feature.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(15)B	This command was modified by the introduction of • Syntax dependence on SSG host key • The *start-ip-address* and *end-ip-address* arguments • The **all** keyword
12.3(4)T	The modifications made in release 12.2(15)B were integrated into Cisco IOS Release 12.3(4)T.

Release	Modification
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to remove one, all, or a range of SSG host objects. You can specify the host objects to remove by entering the host IP addresses or the SSG downlink interface through which the subscriber is connected.

Note The system deletes the specified host objects that exist *at the time* that you enter this command. The system may not delete host objects that are created *after* you enter the command or while the system is executing the command. Enter the **show ssg host** command to confirm that all specified host objects have been deleted.

You can specify the SSG downlink interface only when the SSG Host Key feature is enabled. To enable the host key, enter the **ssg port-map** command in global configuration mode. To disable the host key, enter the **no ssg port-map** command.

Note The **ssg port-map** command does not take effect until after the router is reloaded.

Examples

SSG Port-Bundle Host Key Is Not Enabled

The following example shows how to delete host objects for a range of IP addresses:

```
Router# clear ssg host range 10.0.0.2 10.0.0.20
```

The following example shows how to delete all host objects:

```
Router# clear ssg host all
```

SSG Port-Bundle Host Key Is Enabled

The following example shows how to delete all host objects:

```
Router# clear ssg host all
```

The following example shows how to delete all host objects for subscribers connected through IP address 10.0.0.2:

```
Router# clear ssg host 10.0.0.2
```

The following example shows how to delete host objects for a specific range of IP addresses:

```
Router# clear ssg host range 10.0.0.2 10.0.0.20
```

The following example shows how to delete host objects for a specific IP address range and interface:

```
Router# clear ssg host range 10.0.0.2 10.0.0.20 FastEthernet 0/0
```

Related Commands

Command	Description
show ssg host	Displays information about a subscriber and current connections of the subscriber.
ssg port-map	Enables the SSG port-bundle host key.

clear ssg next-hop

Note Effective with Cisco IOS Release 15.0(1)M, the **clear ssg next-hop** command is not available in Cisco IOS software.

To remove a next-hop table, use the **clear ssg next-hop** command in privileged EXEC mode.

clear ssg next-hop

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(3)DC	This command was introduced on the Cisco 6400 node route processor.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

If you use this command to clear the next-hop table, nothing appears when you use the **show ssg next-hop** command. However, the next-hop table will still appear in the running configuration. To remove the next-hop table from the running configuration, use the **no** form of the **ssg next-hop download** command.

Examples

The following example shows how to remove the next-hop table:

```
Router# clear ssg next-hop
```

Related Commands

Command	Description
show ssg next-hop	Displays the next-hop table.
ssg next-hop download	Downloads the next-hop table from a RADIUS server.

clear ssg open-garden

Note Effective with Cisco IOS Release 15.0(1)M, the **clear ssg open-garden** command is not available in Cisco IOS software.

To remove open garden configurations and all open garden service objects, use the **clear ssg open-garden** command in privileged EXEC mode.

clear ssg open-garden

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(5)DC	This command was introduced on the Cisco 6400 series node route processor.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

This command removes the open garden configuration by deleting all instances of the **ssg open-garden** global configuration command. This command also removes the service object of all the open garden services. The local service profiles of the open garden services are not deleted from the configuration.

Examples

In the following example, all open garden services are displayed and then removed:

```
Router# show ssg open-garden

nrp1-nrp2_og1
nrp1-nrp2_og2
nrp1-nrp2_og3
nrp1-nrp2_og4

Router# clear ssg open-garden
Router# show ssg open-garden
Router#
```

Related Commands

Command	Description
local-profile	Configures a local service profile.

Command	Description
show ssg open-garden	Displays a list of all configured open garden services.
ssg open-garden	Designates a service, defined in a local service profile, as an open garden service.

clear ssg pass-through-filter

Note Effective with Cisco IOS Release 15.0(1)M, the **clear ssg pass-through-filter** command is not available in Cisco IOS software.

To remove the downloaded filter for transparent pass-through, use the **clear ssg pass-through-filter** command in privileged EXEC mode.

clear ssg pass-through-filter

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(3)DC	This command was introduced on the Cisco 6400 node route processor.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Removing the filter allows unauthenticated traffic to pass through the Service Selection Gateway in either direction without modification. If you use this command to clear the downloaded transparent pass-through filter, nothing will be displayed when you use the **show ssg pass-through-filter** command. However, the transparent pass-through filter will still appear in the running configuration. To remove the transparent pass-through filter from the running configuration, use the **no** form of the **ssg pass-through** command.

Examples

The following example shows how to remove the downloaded transparent pass-through filter:

```
Router# clear ssg pass-through-filter
```

Related Commands

Command	Description
show ssg pass-through-filter	Displays the downloaded filter for transparent pass-through.
ssg pass-through	Enables transparent pass-through.

clear ssg pending-command

Note Effective with Cisco IOS Release 15.0(1)M, the **clear ssg pending-command** command is not available in Cisco IOS software.

To remove all pending commands, use the **clear ssg pending-command** command in privileged EXEC mode.

clear ssg pending-command

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(3)DC	This command was introduced on the Cisco 6400 node route processor.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to clear pending commands.

Examples

The following example shows how to clear pending commands:

```
Router# clear ssg pending-command
```

Related Commands

Command	Description
show ssg pending-command	Displays current pending commands.

clear ssg prepaid default-quota

Note Effective with Cisco IOS Release 15.0(1)M, the **clear ssg prepaid default-quota** command is not available in Cisco IOS software.

To clear the Service Selection Gateway (SSG) prepaid default quota counters, use the **clear ssg prepaid default-quota** command in privileged EXEC mode.

clear ssg prepaid default-quota

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(11)T	This command was introduced.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

SSG maintains two counters to keep track of the number of times the SSG prepaid default quota has been allotted. One counter is for the total number of default quotas allotted by SSG (irrespective of how many times the prepaid server has become available and unavailable). The other counter keeps track of the number of default quotas allotted by SSG during the latest instance of prepaid server unavailability. The **clear ssg prepaid default-quota** command clears the SSG default quota counters.

The **show ssg prepaid default-quota** command displays the number of default quotas that SSG has allocated since the last time the **clear ssg prepaid default-quota** command was entered.

Examples

The following example shows how to clear the default quota counter for all quotas allocated by SSG:

```
Router# clear ssg prepaid default-quota
```

Related Commands

Command	Description
show ssg prepaid default-quota	Displays the values of the SSG prepaid default quota counters.

clear ssg radius-proxy client-address

Note Effective with Cisco IOS Release 15.0(1)M, the **clear ssg radius-proxy client-address** command is not available in Cisco IOS software.

To clear all hosts connected to a specific RADIUS client, use the **clear ssg radius-proxy client-address** command in privileged EXEC mode.

client ssg radius-proxy client-address *ip-address*

Syntax Description

ip-address	IP address of a RADIUS client.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to clear all hosts connected to a specific RADIUS client. This command deactivates and destroys all host objects associated with the specified RADIUS client.

Examples

The following example shows how to clear all hosts connected to the RADIUS client that has the IP address 172.16.0.0:

```
clear ssg radius-proxy client-address 172.16.0.0
```

Related Commands

Command	Description
address-pool	Defines local IP pools to be used by SSG to assign IP addresses to users for which SSG is acting as a RADIUS client.
clear ssg radius-proxy nas-address	Clears all hosts connected to a specific NAS.
idle-timeout (SSG)	Configures a host object timeout value.
show ssg tcp-redirect group	Displays the pool of IP addresses configured for a router or for a specific domain.
ssg enable	Enables SSG.
ssg radius-proxy	Enables SSG RADIUS Proxy.
ssg tcp-redirect	Configures the RADIUS proxy IP address and shared secret.

clear ssg radius-proxy nas-address

Note Effective with Cisco IOS Release 15.0(1)M, the **clear ssg radius-proxy has-address** command is not available in Cisco IOS software.

To clear all hosts connected to a specific network access server (NAS), use the **clear ssg radius-proxy nas-address** command in privileged EXEC mode.

client ssg radius-proxy nas-address *ip-address*

Syntax Description

ip-address	IP address of a RADIUS client.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to clear all hosts connected to a specific NAS. This command deactivates and destroys all host objects associated with the specified NAS client.

Note Service Selection Gateway (SSG) does not currently notify RADIUS clients when a host object is removed from the SSG.

Examples

The following example shows how to clear all hosts connected to the NAS with IP address 172.16.0.0:

```
clear ssg radius-proxy nas-address 172.16.0.0
```

Related Commands

Command	Description
address-pool	Defines local IP pools to be used by SSG to assign IP addresses to users for which SSG is acting as a RADIUS client.
clear ssg radius-proxy nas-address	Clears all hosts connected to a specific RADIUS client.
forward accounting-start-stop	Proxies accounting start, stop, and update packets generated by any RADIUS clients to the AAA server.
idle-timeout (SSG)	Configures a host object timeout value.

server-port	Defines the ports for the SSG RADIUS proxy.
show ssg tcp-redirect group	Displays the pool of IP addresses configured for a router or for a specific domain.
ssg enable	Enables SSG.
ssg radius-proxy	Enables SSG RADIUS Proxy.
ssg tcp-redirect	Configures the RADIUS proxy IP address and shared secret.

clear ssg service

Note Effective with Cisco IOS Release 15.0(1)M, the **clear ssg service** command is not available in Cisco IOS software.

To remove a service object and all connection objects of the service, use the **clear ssg service** command in privileged EXEC mode.

clear ssg service {*service-name* | **all**}

Syntax Description

service-name	Service name.
all	Clears all service objects.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(3)DC	This command was introduced on the Cisco 6400 node route processor.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(15)B	The **all** keyword was added.
12.3(4)T	The **all** keyword was integrated into Cisco IOS Release 12.3(4)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to remove one or all service objects and all connection objects of the services.

Note When you use the **all** keyword, the system deletes all service objects that exist *at the time* that you enter this command. The system may not delete service objects that are created *after* you enter the command or while the system is executing the command. Enter the **show ssg service** command to confirm that all service objects have been deleted.

Examples

The following example show how to remove all service objects and connections:

```
Router# clear ssg service all
```

The following example shows how to remove a service called “Perftest”:

```
Router# clear ssg service Perftest
```

Related Commands

Command	Description
show ssg binding	Displays service names that have been bound to interfaces and the interfaces to which they have been bound.
show ssg service	Displays the information for a service.
ssg bind service	Specifies the interface for a service.

clear ssg user transparent all

Note Effective with Cisco IOS Release 15.0(1)M, the **clear ssg user transparent all** command is not available in Cisco IOS software.

To delete all Service Selection Gateway (SSG) transparent autologon transparent pass-through (TP), suspect (SP), unidentified (NR), and authorizing (WA) users, use the **clear ssg user transparent all** command in privileged EXEC mode.

clear ssg user transparent all

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(1a)BW	This command was introduced.
12.3(3)B	This command was integrated into Cisco IOS Release 12.3(3)B.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to clear all SSG transparent autologon users, including pass-through (TP), suspect (SP), unidentified (NR), and authorizing (WA) users.

Examples

The following example deletes all TP, SP, NR, and WA users:

```
Router# clear ssg user transparent all
```

Related Commands

Command	Description
ssg login transparent	Enables the SSG Transparent Autologon feature.

clear ssg user transparent passthrough

Note Effective with Cisco IOS Release 15.0(1)M, the **clear ssg user transparent passthrough** command is not available in Cisco IOS software.

To delete Service Selection Gateway (SSG) transparent autologon transparent pass-through (TP) users, use the **clear ssg user transparent passthrough** command in privileged EXEC mode.

clear ssg user transparent passthrough {**all** | *ip-address*}

Syntax Description

all	Deletes all pass-through user entries.
ip-address	Deletes the entry for the specified IP address.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(1a)BW	This command was introduced.
12.3(3)B	This command was integrated into Cisco IOS Release 12.3(3)B.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Examples

The following example deletes all pass-through user entries:

```
Router# clear ssg user transparent passthrough all
```

Related Commands

Command	Description
ssg login transparent	Enables the SSG Transparent Autologon feature.

clear ssg user transparent suspect

Note Effective with Cisco IOS Release 15.0(1)M, the **clear ssg user transparent suspect** command is not available in Cisco IOS software.

To delete Service Selection Gateway (SSG) transparent autologon suspect (SP) user entries, use the **clear ssg user transparent suspect** command in privileged EXEC mode.

clear ssg user transparent suspect {**all** | *ip-address*}

Syntax Description

all	Deletes all suspect user entries.
ip-address	Deletes the entry for the specified IP address.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(1a)BW	This command was introduced.
12.3(3)B	This command was integrated into Cisco IOS Release 12.3(3)B.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

An SSG transparent autologon suspect (SP) user is a user whose authentication, authorization, and accounting (AAA) authorization resulted in an Access Reject.

Examples

The following example deletes all suspect user entries:

```
Router# clear ssg user transparent suspect
```

Related Commands

Command	Description
ssg login transparent	Enables the SSG Transparent Autologon feature.

clear ssg user transparent unidentified

Note Effective with Cisco IOS Release 15.0(1)M, the **clear ssg user transparent unidentified** command is not available in Cisco IOS software.

To delete all Service Selection Gateway (SSG) transparent autologon unidentified user (NR) entries, use the **clear ssg user transparent unidentified** command in privileged EXEC mode.

clear ssg user transparent unidentified {**all** | *ip-address*}

Syntax Description

all	Deletes all unidentified user entries.
ip-address	Deletes the entry for the specified IP address.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(1a)BW	This command was introduced.
12.3(3)B	This command was integrated into Cisco IOS Release 12.3(3)B.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Examples

The following example clears all unidentified user entries:

```
Router# clear ssg user transparent unidentified all
```

Related Commands

Command	Description
ssg login transparent	Enables the SSG Transparent Autologon feature.

client-address

Note Effective with Cisco IOS Release 15.0(1)M, the **client-address** command is not available in Cisco IOS software.

To configure a RADIUS client to proxy requests from a specified IP address to a RADIUS server and to enter SSG-radius-proxy-client configuration mode, use the **client-address** command in SSG-radius-proxy configuration mode. To remove a client from the client list, use the **no** form of this command.

client-address *ip-address* [**vrf** *vrf-name*]

no client-address *ip-address*

Syntax Description

ip-address	IP address of a RADIUS client.
vrf *vrf-name*	(Optional) Associates a configured VPN routing/forwarding (VRF) instance with a RADIUS client.

Defaults

No default behavior or values.

Command Modes

SSG-radius-proxy configuration

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(15)B	This command was modified to enter SSG-radius-proxy-client mode.
12.3(4)T	The modifications from 12.2(15)B were integrated into Cisco IOS Release 12.3(4)T.
12.3(11)T	The **vrf** *vrf-name* option was introduced.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to configure the RADIUS client to proxy requests from a specified IP address to a RADIUS server. You can also use this command to enter SSG-radius-proxy-client mode.

Examples

The following example shows how to enter SSG-radius-proxy-client mode:

```
client-address 172.16.0.0
```

The following example shows how to configure a RADIUS client to proxy all requests from IP address 172.16.0.0 to the RADIUS server and assigns the shared secret "cisco" to the client:

```
client-address 172.16.0.0
 key cisco
```

The following example defines a RADIUS client that is connected to SSG through a VRF called "BLUE":

```
ip vrf BLUE
 rd 1:1
!
ssg radius-proxy
 client-address 10.1.1.1 vrf BLUE
  key cisco
!
```

Related Commands

Command	Description
address-pool	Defines local IP pools to be used by SSG to assign IP addresses to users for whom SSG is acting as a RADIUS client.
clear ssg radius-proxy client-address	Clears all hosts connected to a specific RADIUS client.
host-route insert	Inserts a host route via the RADIUS client address into the VRF configured for the RADIUS client.
key (SSG-radius-proxy-client)	Configures the shared secret between SSG and a RADIUS client.
server-port	Configures the ports on which SSG listens for RADIUS-requests from configured RADIUS clients.
session-identifier (SSG-radius-proxy-client)	Overrides SSG's automatic RADIUS client session identification.
show ssg radius-proxy	Displays the pool of IP addresses configured for a router or for a specific domain.
ssg radius-proxy	Enables SSG RADIUS Proxy and enters SSG-radius-proxy mode.

destination access-list

Note Effective with Cisco IOS Release 15.0(1)M, the **destination access-list** command is not available in Cisco IOS software.

To specify packets for port-mapping by specifying an access list to compare against subscriber traffic, use the **destination access-list** command in SSG portmap configuration mode. To remove this specification, use the **no** form of this command.

destination access-list *access-list-number*

no destination access-list *access-list-number*

Syntax Description

access-list-number	Integer from 100 to 199 that is the number or name of an extended access list.

Defaults

SSG does not use an access list when port-mapping subscriber traffic.

Command Modes

SSG portmap configuration

Command History

Release	Modification
12.2(16)B	This command was introduced. This command replaces the **ssg port-map destination access-list** command.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

When the **destination access-list** command is configured, any traffic going to the default network and matching the access list will be port-mapped.

Note A default network must be configured and routable from SSG in order for this command to be effective.

You can use multiple entries of the **destination access-list** command. The access lists are checked against the subscriber traffic in the order in which they are defined.

Examples

In the following example, SSG will port-map packets that are permitted by access list 100:

```
ssg port-map
 destination access-list 100
 source ip Ethernet0/0/0
!
```

```
.
.
.
!
access-list 100 permit ip 10.0.0.0 0.255.255.255 host 70.13.6.100
access-list 100 deny   ip any any
```

Related Commands

Command	Description
destination range	Identifies packets for port-mapping by specifying the TCP port range to compare against the subscriber traffic.
ssg port-map	Enables the SSG port-bundle host key and enters SSG portmap configuration mode.

destination range

Note Effective with Cisco IOS Release 15.0(1)M, the **destination range** command is not available in Cisco IOS software.

To identify packets for port-mapping by specifying the TCP port range to compare against the subscriber traffic, use the **destination range** command in SSG portmap configuration mode. To remove this specification, use the **no** form of this command.

destination range *port-range-start* **to** *port-range-end* [**ip** *ip-address*]

no destination range *port-range-start* **to** *port-range-end* [**ip** *ip-address*]

Syntax Description

port-range-start	Port number at the start of the TCP port range.
to	Specifies higher end of TCP port range.
port-range-end	Port number at the end of TCP port range.
ip *ip-address*	(Optional) Destination IP address in the packets.

Defaults

A TCP port range is not used in port-mapping subscriber traffic.

Command Modes

SSG portmap configuration

Command History

Release	Modification
12.2(16)B	This command was introduced. This command replaces the **ssg port-map destination range** command.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

If a destination IP address is not configured, a default network must be configured and routable from SSG in order for this command to be effective.

If the destination IP address is not configured, any traffic going to the default network whose destination port falls within the destination port range will be port-mapped.

You can use multiple entries of the **destination range** command. The port ranges are checked against the subscriber traffic in the order in which they were defined.

Examples

In the following example, SSG will port-map any packets that are going to the default network and have a destination port within the range from 8080 to 8081:

```
ssg port-map
 destination range 8080 to 8081
```

Related Commands

Command	Description
destination access-list	Specifies packets for port-mapping by specifying an access list to compare against the subscriber traffic.
ssg port-map	Enables the SSG port-bundle host key and enters SSG portmap configuration mode.

dnis-prefix all service

Note Effective with Cisco IOS Release 15.0(1)M, the **dnis-prefix all service** command is not available in Cisco IOS software.

To configure the dial-out global service, use the **dnis-prefix all service** command in SSG dial-out configuration mode. To remove a service name and prevent further connections to the specified service, use the **no** form of this command.

dnis-prefix all service *service-name*

no dnis-prefix all service [*service-name*]

Syntax Description

service-name	Name of the dial-out global service.

Defaults

Dial-out global service is not configured.

Command Modes

SSG dial-out configuration

Command History

Release	Modification
12.2(15)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to configure the dial-out global service used for users who are doing account logon with a structured username (*user@DNIS*). The service profile is downloaded when the user connects to the dial-out service. You can specify only one dial-out global service. If you configure this command more than once and use different service names each time, the previously configured service name is removed from the configuration.

If SSG is operating in SSG Autodomain basic mode, you should configure the dial-out tunnel service profile as the dial-out global service. If SSG is operating in SSG Autodomain extended mode, you should configure the virtual-user profile as the dial-out global service and configure dial-out tunnel service as an Autologon service within SSG Autodomain extended mode.

Examples

The following example shows how to configure a global dial-out service profile named “profile1” as the global dial-out service profile:

```
dnis-prefix all service profile1
```

The following example shows how to configure a global dial-out service profile when SSG is operating in SSG Autodomain basic mode:

```
dnis-prefix all service dialout_tunnel
```

The following example shows how to configure a global dial-out service profile when SSG is operating in SSG Autodomain extended mode:

```
dnis-prefix all service virtual-user
```

Related Commands

Command	Purpose
download exclude-profile (ssg dial-out)	Downloads the DNIS exclusion list locally or from a AAA server.
exclude dnis-prefix	Configures the DNIS filter by adding a DNIS prefix to the DNIS exclusion list.
show ssg dial-out exclude-list	Displays information about the DNIS prefix profile and the DNIS exclusion list.
ssg dial-out	Enters SSG dial-out configuration mode.

download exclude-profile (SSG dial-out)

Note Effective with Cisco IOS Release 15.0(1)M, the **download exclude-profile** (SSG dial-out) command is not available in Cisco IOS software.

To download the Dialed Number Identification Service (DNIS) exclusion list locally or from a authentication, authorization, and accounting (AAA) server, use the **download exclude-profile** command in SSG dial-out configuration mode. To remove the DNIS exclusion list from the configuration, use the **no** form of this command.

download exclude-profile *profile-name* [*password*]

no download exclude-profile *profile-name* [*password*]

Syntax Description

profile-name	Name of the DNIS exclusion list.
password	(Optional) Password of the DNIS exclusion list.

Defaults

A DNIS exclusion list is not downloaded.

Command Modes

SSG dial-out configuration

Command History

Release	Modification
12.2(15)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to download a DNIS exclusion list from the local profile configured in Service Selection Gateway (SSG) or from a AAA server. If you do not specify a profile name and password, SSG attempts to download the profile with the previously configured profile name and password. If there is no previously configured profile name and password, the DNIS exclusion list is not downloaded.

You can download only one DNIS exclusion list. If you attempt to use the **download exclude-profile** command more than once with different profile names, only the last profile name is downloaded, and the previously downloaded profiles are removed from the configuration.

Use the **no download exclude-profile** command to remove the downloaded DNIS exclusion list from the configuration.

You can configure the order in which SSG searches for the DNIS exclusion list using the **ssg service-search-order** command.

Examples

The following example shows how to download a DNIS exclusion list with a profile name of "dnisprofile1" and a password of "abc":

```
download exclude-profile dnisprofile1 abc
```

Related Commands

Command	Description
dnis-prefix all service	Configures the dial-out global service.
exclude dnis-prefix	Configures the DNIS filter by adding a DNIS prefix to the DNIS exclusion list.
show ssg dial-out exclude-list	Displays information about the DNIS exclusion list.
ssg dial-out	Enters SSG dial-out configuration mode.
ssg service-search-order	Specifies the order in which SSG searches for a service profile.

download exclude-profile (SSG PTA-MD)

Note Effective with Cisco IOS Release 15.0(1)M, the **download exclude-profile** (SSG PTA-MD) command is not available in Cisco IOS software.

To download a PPP Termination Aggregation-Multidomain (PTA-MD) exclusion list from the authentication, authorization, and accounting (AAA) server to the router, use the **download exclude-profile** command in SSG PTA-MD configuration mode. To remove all domains in the specified PTA-MD exclusion list, use the **no** form of this command.

download exclude-profile *profile-name* [*password*]

no download exclude-profile *profile-name* [*password*]

Syntax Description

profile-name	Name of the exclusion list to download.
password	(Optional) Password required to download the PTA-MD exclusion list from the AAA server. If no password is entered, the password used in the previous exclusion list download will be used to download the exclusion list.

Defaults

A PTA-MD exclusion list is not downloaded.

Command Modes

SSG PTA-MD configuration

Command History

Release	Modification
12.2(15)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

A PTA-MD exclusion list provides the option of passing the entire structured username in the form *user@service* to PPP for authenticating an SSG request. The entire structured username can be passed to PPP through the use of a PTA-MD exclusion list; if an entire structured username should be passed to PPP, the domain (the *@servic*e portion of the structured username) should be added to a PTA-MD exclusion list. The **download exclude-profile** command is used to download an exclusion list from the AAA server as part of the process for adding domains to an exclusion list using the router command-line interface (CLI).

PTA-MD exclusion lists can also be configured directly on the AAA server.

Examples

In the following example, a PTA-MD exclusion list that already includes “cisco”, “motorola”, “nokia”, and “voice-stream” is downloaded from the AAA server. After the exclusion list is downloaded, “microsoft” and “sun” are added to the exclusion list.

The exclusion list currently on the AAA server includes “cisco”, “motorola”, “nokia”, and “voice-stream”:

```
user = pta_md{
profile_id = 119
profile_cycle = 2
member = SSG-DEV
radius=6510-SSG-v1.1 {
check_items= {
2=cisco
}
reply_attributes= {
9,253="XPcisco"
9,253="XPmotorola"
9,253="XPnokia"
9,253="XPvoice-stream"
```

The PTA-MD exclusion list is then downloaded to the router from the AAA server. The password to download the exclusion list is “cisco”. After the PTA-MD exclusion list is downloaded, “microsoft” and “sun” are added to the list using the router CLI:

```
ssg multidomain ppp
 download exclude-profile pta_md cisco
 exclude domain microsoft
 exclude domain sun
```

The enhancements to the exclusion list are then verified:

```
Router# show ssg multidomain ppp exclude-list

Profile name :pta_md
1   cisco
2   motorola
3   nokia
4   voice-stream

Domains added via CLI :
1   microsoft
2   sun
```

Related Commands

Command	Description
exclude (SSG PTA-MD)	Adds a domain name to the existing PTA-MD exclusion list.
show ssg multidomain ppp exclude-list	Displays the contents of the PTA-MD exclusion list.
ssg multidomain ppp	Enters PTA-MD configuration mode.

download exclude-profile (SSG-auto-domain)

Note Effective with Cisco IOS Release 15.0(1)M, the **downoad exclude-profile** (SSG-auto-domain) command is not available in Cisco IOS software.

To add domain names or Access Point Names (APNs) to the Service Selection Gateway (SSG) Autodomain exclusion list, use the **download exclude-profile** command in SSG-auto-domain configuration mode. To remove a name from the Autodomain exclusion list, use the **no** form of this command.

download exclude-profile *profile-name password*

no download exclude-profile *profile-name password*

Syntax Description

profile-name	Name for a list of excluded names that may be downloaded from the authentication, authorization, and accounting (AAA) server.
password	Password for a list of excluded names that may be downloaded from the AAA server.

Defaults

No default behavior or values.

Command Modes

SSG-auto-domain configuration

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use the **download exclude-profile** command to specify the name and password for a list of names that are excluded from being downloaded from the AAA server. Downloads from the AAA server occur at the time of entering the configuration and also on subsequent Route Processor reloads. By reentering the configuration command, you can synchronize with a modified table on the AAA server by forcing a new download. For every successful exclude-profile download, Service Selection Gateway (SSG) deletes the exclude entries added by the previous exclude-profile download and adds the new downloaded entries to the Autodomain exclusion list. The excluded name list introduces the following new attributes to the SSG Control-Info vendor-specific attributes (VSAs):

X—Excluded name list entry.

A—Add this name to the APN exclusion list.

D—Add this name to the domain name exclusion list.

The following is an example profile using the new exclusion list attributes:

```
abc Password = "cisco" Service-Type = Outbound
  Control-Info = XAapn1.gprs
  Control-Info = XAapn2.com
  Control-Info = XDcisco.com
  Control-Info = XDcompany.com
```

Examples

The following example shows how to add a list of names called “abc” with the password “cisco” to the Autodomain exclusion list:

```
download exclude-profile abc cisco
```

Related Commands

Command	Description
exclude	Configures the Autodomain exclusion list.
mode extended	Enables extended mode for SSG Autodomain.
nat user-address	Enables Network Address Translation (NAT) on Autodomain tunnel service.
select	Configures the Autodomain selection mode.
show ssg auto-domain exclude-profile	Displays the contents of an Autodomain exclude-profile downloaded from the AAA server.
ssg enable	Enables SSG functionality.

exclude

Note Effective with Cisco IOS Release 15.0(1)M, the **exclude** command is not available in Cisco IOS software.

To add Access Point Names (APNs) and domain names to a Service Selection Gateway (SSG) Autodomain exclusion list, use the **exclude** command in SSG-auto-domain mode. To remove an APN or domain name from the Autodomain exclusion list, use the **no** form of this command.

exclude {**apn** | **domain**} *name*

no exclude {**apn** | **domain**} *name*

Syntax Description

apn	Adds an APN to the exclusion list.
domain	Adds a domain to the exclusion list.
name	Name of the APN or domain to be added to the exclusion list.

Command Default

No default behavior or values.

Command Modes

SSG-auto-domain

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use the **exclude** command to add an APN or a domain to the Autodomain exclusion list. APN and domain names that are not on an exclusion list are used to perform Autodomain for a user. You can use the **no download exclude-profile** command to remove a domain or APN name that is downloaded from the AAA server.

Examples

The following example shows how to add the APN named “abc” to the exclusion list:

```
exclude apn abc
```

The following example shows how to add the domain named “xyz” to the exclusion list:

```
exclude domain xyz
```

Related Commands

Command	Description
exclude	Adds to the Autodomain download exclusion list.
mode extended	Enables extended mode for SSG Autodomain.
nat user-address	Enables NAT on Autodomain tunnel service.
select	Configures the Autodomain selection mode.
show ssg auto-domain exclude-profile	Displays the contents of an Autodomain exclude-profile downloaded from the AAA server.
ssg enable	Enables SSG functionality.

exclude (SSG PTA-MD)

Note Effective with Cisco IOS Release 15.0(1)M, the **exclude** (SSG PTA-MD) command is not available in Cisco IOS software.

To add a domain to a PPP Termination Aggregation-Multidomain (PTA-MD) exclusion list, use the **exclude** command in SSG PTA-MD configuration mode. To remove a domain from the PTA-MD exclusion list, use the **no** form of this command.

exclude [**domain** *name* | **all-domains**]

no exclude [**domain** *name* | **all-domains**]

Syntax Description

domain	(Optional) Adds a domain to the exclusion list.
name	(Optional) Name of the domain to be added to the exclusion list.
all-domains	(Optional) Excludes all domains; in effect, disables parsing of PPP structured usernames.

Defaults

A domain is not included in a PTA-MD exclusion list.

Command Modes

SSG PTA-MD configuration

Command History

Release	Modification
12.2(15)B	This command was introduced in PTA-MD configuration mode.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

A PTA-MD exclusion list provides the option of passing an entire structured username in the form *user@service* to PPP for authenticating a Service Selection Gateway (SSG) request. The entire structured username can be passed to PPP through the use of a PTA-MD exclusion list; if an entire structured username should be passed to PPP, the domain (the *@service* portion of the structured username) should be added to a PTA-MD exclusion list. The **exclude** command is used to add a domain to the exclusion list as part of the process for adding domains to an exclusion list using the router command-line interface (CLI).

PTA-MD exclusion lists can also be configured directly on the authentication, authorization, and accounting (AAA) server.

To disable all parsing of PPP structured usernames during authentication, use the **exclude all-domains** command.

Examples

Adding Domains to an Existing PTA-MD Exclusion List

In the following example, a PTA-MD exclusion list that already includes “cisco”, “motorola”, “nokia”, and “voice-stream” is downloaded from the AAA server. After the exclusion list is downloaded, “microsoft” and “sun” are added to the exclusion list.

The exclusion list currently on the AAA server includes “cisco”, “motorola”, “nokia”, and “voice-stream”:

```
user = pta_md{
profile_id = 119
profile_cycle = 2
member = SSG-DEV
radius=6510-SSG-v1.1 {
check_items= {
2=cisco
}
reply_attributes= {
9,253="XPcisco"
9,253="XPmotorola"
9,253="XPnokia"
9,253="XPvoice-stream"
```

In the following example, the PTA-MD exclusion list is downloaded to the router from the AAA server. The password to download the exclusion list is “cisco”. After the PTA-MD exclusion list is downloaded, “microsoft” and “sun” are added to the list using the router CLI:

```
ssg multidomain ppp
 download exclude-profile pta_md cisco
 exclude domain microsoft
 exclude domain sun
```

The enhancements to the exclusion list are then verified:

```
Router# show ssg multidomain ppp exclude-list

Profile name :pta_md
1   cisco
2   motorola
3   nokia
4   voice-stream

Domains added via CLI :
1   microsoft
2   sun
```

Disabling Parsing of PPP Structured Usernames

In the following example, parsing of PPP structured usernames is disabled:

```
exclude all-domains
```

Related Commands

Command	Description
download exclude-profile (SSG PTA-MD)	Downloads the PTA-MD exclusion list from the AAA server to the router.

Command	Description
show ssg multidomain ppp exclude-list	Displays the contents of the PTA-MD exclusion list.
ssg multidomain ppp	Enters PTA-MD configuration mode.

exclude dnis-prefix

Note Effective with Cisco IOS Release 15.0(1)M, the **exclude dnis-prefix** command is not available in Cisco IOS software.

To configure the Dialed Number Identification Service (DNIS) filter by adding a DNIS prefix to the DNIS exclusion list, use the **exclude dnis-prefix** command in SSG dial-out configuration mode. To remove a DNIS prefix from the DNIS exclusion list, use the **no** form of this command.

exclude dnis-prefix *dnis-prefix*

no exclude dnis-prefix *dnis-prefix*

Syntax Description

dnis-prefix	DNIS prefix to be added to the DNIS exclusion list.

Defaults

No DNIS prefix is added to the DNIS exclusion list.

Command Modes

SSG dial-out configuration

Command History

Release	Modification
12.2(15)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to add a DNIS prefix to the DNIS exclusion list. You can use this command to add multiple DNIS prefixes to the DNIS exclusion list. When a user dials with a DNIS whose prefix is in the DNIS exclusion list, the service logon for that user is rejected.

Examples

The following example adds the DNIS prefix “1122334455” to the DNIS exclusion list:

```
exclude dnis-prefix 1122334455
```

Related Commands

Command	Description
dnis-prefix all service	Configures the dial-out global service.
download exclude-profile (SSG dial-out)	Downloads the DNIS exclusion list locally or from a AAA server.

Command	Description
show ssg dial-out exclude-list	Displays information about the DNIS prefix profile and the DNIS exclusion list.
ssg dial-out	Enters SSG dial-out configuration mode.

forward accounting-on-off

Note Effective with Cisco IOS Release 15.0(1)M, the **forward accounting-on-off** command is not available in Cisco IOS software.

To allow forwarding of accounting-on-off packets generated by any RADIUS clients to the authentication, authorization, and accounting (AAA) server, use the **forward accounting-on-off** command in SSG radius-proxy mode. To suppress forwarding of accounting-on-off packets, use the **no** form of this command.

forward accounting-on-off

no forward accounting-on-off

Syntax Description

This command has no arguments or keywords.

Command Default

Accounting-on-off packets generated by RADIUS clients are not sent to the AAA server.

Command Modes

SSG radius-proxy configuration (config-radius-proxy)

Command History

Release	Modification
12.4(15)T	This command was introduced.
15.0(1)M	This command was removed.

Examples

The following example shows how to allow packet forwarding from the RADIUS client to the AAA server:

```
Router(config)# ssg enable
Router(config)# ssg radius-proxy
Router(config-radius-proxy)# forward accounting-on-off
```

Related Commands

Command	Description
forward accounting-start-stop	Allows accounting start, stop, and update packets generated by any RADIUS clients to the AAA server.

forward accounting-start-stop

Note Effective with Cisco IOS Release 15.0(1)M, the **forward accounting-start-stop** command is not available in Cisco IOS software.

To proxy accounting start, stop, and update packets generated by any RADIUS clients to the authentication, authorization, and accounting (AAA) server, use the **forward accounting-start-stop** command in SSG-radius-proxy configuration mode. To stop forwarding accounting start, stop, and update packets, use the **no** form of this command.

forward accounting-start-stop

no forward accounting-start-stop

Syntax Description

This command has no arguments or keywords.

Defaults

Forward accounting-start-stop is disabled by default.

Command Modes

SSG-radius-proxy configuration

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to proxy accounting start, stop, and update packets generated by all RADIUS clients to the AAA server. Disabling this command reduces RADIUS packet traffic and processing for deployments where the billing server is not using these packets for billing purposes.

Note The **forward accounting-start-stop** command does not affect accounting on and off packets, which are forwarded regardless of this command.

Examples

The following example shows how to proxy accounting packets generated by all RADIUS clients to the AAA server:

```
ssg radius-proxy
 server-port auth 1645 acct 1646
 client-address 10.1.2.2 key secret1
 client-address 10.2.25.90 key secret2
 client-address 10.0.0.1 key secret3
```

```
client-address 10.23.3.2 key secret4
idle-timeout 30
forward accounting-start-stop
address-pool 10.1.1.1 10.1.40.250
address-pool 10.1.5.1 10.1.5.30 domain ssg.com
```

Related Commands

Command	Description
address-pool	Defines local IP pools to be used by SSG to assign IP addresses to users for which SSG is acting as a RADIUS client.
clear ssg radius-proxy client-address	Clears all hosts connected to a specific RADIUS client.
clear ssg radius-proxy nas-address	Clears all hosts connected to a specific NAS.
idle-timeout (SSG)	Configures a host object timeout value.
server-port	Defines the ports for the SSG RADIUS proxy.
show ssg tcp-redirect group	Displays the pool of IP addresses configured for a router or for a specific domain.
ssg enable	Enables SSG.
ssg radius-proxy	Enables SSG RADIUS Proxy.

hand-off

Note Effective with Cisco IOS Release 15.0(1)M, the **hand-off** command is not available in Cisco IOS software.

To configure a Service Selection Gateway (SSG) RADIUS proxy handoff timeout, use the **hand-off** command in SSG-radius-proxy-timers configuration mode. To disable the handoff timeout, use the **no** form of this command.

hand-off *timeout*

no hand-off *timeout*

Syntax Description

timeout	Timeout value, in seconds. Valid range is 1 to 30 seconds. The default is 5 seconds.

Defaults

The handoff timeout is set to 5 seconds.

Command Modes

SSG-radius-proxy-timers

Command History

Release	Modification
12.2(15)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to configure an SSG RADIUS proxy handoff timeout. You can use this command when a PPP session is not disabled and the host object remains active after a base station controller (BSC) handoff.

A Session-Continue vendor-specific attribute (VSA) with a value of 1 in an Accounting-Stop packet indicates that a BSC/packet control function (PCF) handoff is in progress. When SSG detects the BSC/PCF handoff, it keeps the host object and begins the configured handoff timeout. If SSG does not receive an Accounting-Start for this host object before the handoff timeout expires, it deletes the host object.

Examples

The following example shows how to configure a handoff timeout value of 25 seconds:

```
ssg radius-proxy
 ssg timeouts
 hand-off 25
```

Related Commands

Command	Description
idle (SSG-radius-proxy-timers)	Configures a host object timeout value.
ip-address (SSG-radius-proxy-timers)	Configures an SSG RADIUS proxy IP address timeout.
key (SSG-radius-proxy-client)	Configures a shared secret between SSG and a RADIUS client.
ssg radius-proxy	Enables SSG RADIUS Proxy and enters SSG-radius-proxy mode.
timeouts (SSG-radius-proxy)	Enters SSG-radius-proxy-timeouts mode.

home-agent (SSG-radius-proxy)

Note Effective with Cisco IOS Release 15.0(1)M, the **home-agent** (SSG-radius-proxy) command is not available in Cisco IOS software.

To configure an IP address or domain for a Home Agent (HA) in a CDMA2000 network, use the **home-agent** command in SSG-radius-proxy configuration mode. To remove an HA address or domain, use the **no** form of this command.

home-agent {**address** *HA-ip-address* | **domain** *domain-name* [**address** *domain-ip-address*]}

no home-agent {**address** *HA-ip-address* | **domain** *domain-name* [**address** *domain-ip-address*]}

Syntax Description

address *ip-address*	IP address of the local Home Agent.
domain *domain-name*	Domain of the local Home Agent.
address *ip-address*	(Optional) IP address of the domain of the Home Agent.

Defaults

No default behavior or values.

Command Modes

SSG-radius-proxy configuration

Command History

Release	Modification
12.2(15)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use the **home-agent** command to configure a list of domain names for which dynamic Home Agent (HA) IP address assignment is applicable. You can configure each domain name with an HA address. You should also configure the IP address of a default local HA.

Use the **no home-agent address** command to remove any configured domain names. Use the **no home-agent domain** command to remove an entry for a specified domain.

Service Selection Gateway (SSG) determines that an Access-Request packet is for a new Mobile IP session when it receives a 3GPP2-Home-Agent-Attribute vendor-specific (VSA) with a value of 0.0.0.0. For authenticated users with a domain recognized by SSG that has a preconfigured HA address, the 3GPP2-Home-Agent-Attribute is changed to the per-domain HA address. For authenticated users with a domain recognized by SSG that does not have a preconfigured HA address, the 3GPP2-Home-Agent-Attribute is changed to the IP address of the default local HA.

For authenticated users with a domain that is not recognized by SSG, the 3GPP2-Home-Agent-Attribute is not changed.

Examples

The following example shows how to set the IP address of the default local HA to 172.16.0.0:

```
ssg radius-proxy
 home-agent address 172.16.0.0
```

The following example shows how to set the IP address of the HA to 172.16.0.0, for users in domain "home1.com":

```
ssg radius-proxy
 home-agent domain home1.com address 172.16.0.0
```

Related Commands

Command	Description
ssg radius-proxy	Enables SSG RADIUS Proxy and enters SSG-radius-proxy mode.

host overlap

Note Effective with Cisco IOS Release 15.0(1)M, the **host overlap** command is not available in Cisco IOS software.

To enable Service Selection Gateway (SSG) to support overlapping host IP addresses, use the **host overlap** command in SSG port-map configuration mode. To disable support for overlapping host IP addresses, use the **no** form of this command.

host overlap

no host overlap

Syntax Description

This command has no arguments or keywords.

Defaults

Overlapping host IP addresses are supported by default when SSG port-bundle host key functionality is configured.

Command Modes

SSG port-map configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

The SSG Port-Bundle Host Key feature enables subscribers to have overlapping IP addresses. To enable subscriber-side interface redundancy when SSG port-bundle host key functionality is configured, overlapping IP address support must be disabled so that interface binding is not needed. Use the **no host overlap** command to disable overlapping IP address support.

Examples

The following example shows how to disable support for overlapping hosts when the SSG Port-Bundle Host Key feature is configured:

```
Router(config)# ssg enable
Router(config)# ssg port-map
Router(ssg-port-map)# no host overlap
```

Related Commands

Command	Description
ssg port-map	Enables the SSG Port-Bundle Host Key feature and enters SSG port-map configuration mode.

idle (SSG-radius-proxy-timers)

Note Effective with Cisco IOS Release 15.0(1)M, the **idle** (SSG-radius-proxy-timers) command is not available in Cisco IOS software.

To configure a Service Selection Gateway (SSG) host object timeout value, use the **idle** command in SSG-radius-proxy-timers configuration mode. To disable the timeout value, use the **no** form of this command.

idle *timeout*

no idle *timeout*

Syntax Description

timeout	Timeout value, in seconds. Valid range is 30 to 65536 seconds. There is no default value.

Command Default

No idle timeout value is configured.

Command Modes

SSG-radius-proxy-timers

Command History

Release	Modification
12.2(15)B	This command was introduced to replace the **idle-timeout** command.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to configure an idle timeout value for a host object. Configuring this command prevents dangling host objects on SSG. If a RADIUS client reloads and does not indicate its fault condition to SSG, SSG retains host objects that are no longer valid. This command removes all host objects from a RADIUS client that has been idle for the time specified by the *timeout* argument. When configured, this timeout value is added to the host object.

Note Timeout values configured in the user profile that appears in the Access-Accept packet take precedence over any timeout value configured by the **timeouts** (SSG-radius-proxy) command.

Note This command replaces the **idle-timeout** command in SSG-radius-proxy configuration mode.

Examples

The following example shows how to configure an idle timeout value of 60 seconds:

```
ssg radius-proxy
 ssg timeouts
 idle 60
```

Related Commands

Command	Description
hand-off	Configures an SSG RADIUS proxy handoff timeout.
ip-address (SSG-radius-proxy-timers)	Configures an SSG RADIUS proxy IP address timeout.
key (SSG-radius-proxy-client)	Configures a shared secret between SSG and a RADIUS client.
ssg radius-proxy	Enables SSG RADIUS Proxy and enters SSG-radius-proxy mode.
timeouts (SSG-radius-proxy)	Enters SSG-radius-proxy-timers mode.

idle-timeout (SSG)

Note Effective with Cisco IOS Release 15.0(1)M, the **idle-timeout** (SSG) command is not available in Cisco IOS software.

Note Effective with Cisco IOS Releases 12.2(16)B and 12.3(4)T, this command was replaced by the **idle** (SSG radius-proxy-timers) command. The **idle-timeout** command is still supported for backward compatibility, but support for this command may be removed in a future Cisco IOS release.

To configure a host object timeout value, use the **idle-timeout** command in SSG-radius-proxy configuration mode. To disable the timeout value, use the **no** form of this command.

idle-timeout *timeout*

no idle-timeout *timeout*

Syntax Description

timeout	Timeout value, in seconds. Valid range is from 30 to 65536.

Command Default

No timeout value is configured.

Command Modes

SSG-radius-proxy configuration

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(16)B	This command was replaced by the **idle** (SSG radius-proxy-timers) command.
12.3(4)T	This command was replaced by the **idle** (SSG radius-proxy-timers) command.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to configure a timeout value for a host object. Configuring this command prevents dangling host objects on the Service Selection Gateway (SSG). If a RADIUS client reloads and does not indicate its fault condition to the SSG, the SSG retains the host objects that are no longer valid. This command removes all host objects from a RADIUS client that has been idle for the time specified by the *timeout* argument. When configured, this timeout value is added to the host object.

Note Timeout values configured in the user profile that appear in the Access-Accept take precedence over any timeout value configured by the **idle-timeout** command.

Examples

The following example shows how to configure a timeout value of 60 seconds:

```
ssg radius-proxy
 server-port auth 1645 acct 1646
 client-address 10.1.2.2 key secret1
 client-address 10.2.25.90 key secret2
 client-address 10.0.0.1 key secret3
 client-address 10.23.3.2 key secret4
 idle-timeout 60
 forward accounting-start-stop
 address-pool 10.1.1.1 10.1.40.250
 address-pool 10.1.5.1 10.1.5.30 domain ssg.com
```

Related Commands

Command	Description
address-pool	Defines local IP pools to be used by SSG to assign IP addresses to users for which SSG is acting as a RADIUS client.
clear ssg radius-proxy client-address	Clears all hosts connected to a specific RADIUS client.
clear ssg radius-proxy nas-address	Clears all hosts connected to a specific NAS.
forward accounting-start-stop	Proxies accounting start, stop, and update packets generated by any RADIUS clients to the AAA server.
server-port	Defines the ports for the SSG RADIUS proxy.
show ssg tcp-redirect group	Displays the pool of IP addresses configured for a router or for a specific domain.
ssg enable	Enables SSG.
ssg radius-proxy	Enables SSG RADIUS Proxy.

ip-address (SSG-radius-proxy-timers)

Note Effective with Cisco IOS Release 15.0(1)M, the **ip-address** (SSG-radius-proxy-timers) command is not available in Cisco IOS software.

To configure a Service Selection Gateway (SSG) RADIUS proxy IP address timeout, use the **ip-address** command in SSG-radius-proxy-timers configuration mode. To disable the IP address timeout, use the **no** form of this command.

ip-address *timeout*

no ip-address *timeout*

Syntax Description

timeout	Timeout value, in seconds. Valid range is 1 to 30 seconds. The default is 5 seconds.

Command Default

The default value of this timeout is 5 seconds.

Command Modes

SSG-radius-proxy-timers

Command History

Release	Modification
12.2(15)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to configure an SSG RADIUS proxy IP address timeout.

If SSG, acting as a RADIUS proxy for a client, does not allocate an IP address in the Access-Accept packet, a dormant host object is created. The dormant host object is not activated until SSG receives an Accounting-Start packet from the client device, containing a valid IP address.

When an IP address timeout is configured, SSG starts this timer on creation of the dormant host object. If a valid IP address is not received via an Accounting-Start packet from the client device, prior to the expiration of this timeout, the dormant host object is destroyed.

Examples

The following example shows how to configure an SSG RADIUS proxy IP address timeout of 10 seconds:

```
ssg radius-proxy
 ssg timeouts
 ip-address 10
```

Related Commands

Command	Description
address-pool	Defines local IP pools to be used by SSG to assign IP addresses to users for which SSG is acting as a RADIUS client.
hand-off	Configures an SSG RADIUS proxy handoff timeout.
idle (SSG-radius-proxy-timers)	Configures a host object timeout value.
key (SSG-radius-proxy-client)	Configures a shared secret between SSG and a RADIUS client.
ssg radius-proxy	Enables SSG RADIUS Proxy and enters SSG-radius-proxy mode.
timeouts (SSG-radius-proxy)	Enters SSG-radius-proxy-timers mode.

key (SSG-radius-proxy-client)

Note Effective with Cisco IOS Release 15.0(1)M, the **key** (SSG-radius-proxy-client) command is not available in Cisco IOS software.

To configure a shared secret between the Service Selection Gateway (SSG) and a RADIUS client, use the **key** command in SSG-radius-proxy-client mode. To unconfigure the shared secret, use the **no** form of this command.

key *secret*

no key *secret*

Syntax Description

secret	Description of the shared secret.

Command Default

No default behavior or values.

Command Modes

SSG-radius-proxy-client

Command History

Release	Modification
12.2(15)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to configure a shared secret between SSG and a RADIUS client. Use the *secret* attribute to configure each client IP with a unique shared secret. This shared secret should be the same one that is configured on the RADIUS client.

Note The **key** command in SSG-radius-proxy-client mode replaces the **client-address key** command in SSG-radius-proxy mode.

Examples

The following example shows how to configure the RADIUS client to proxy all requests from IP address 172.16.0.0 to the RADIUS server and assigns the shared secret “cisco” to the client:

```
client-address 172.16.0.0
 key cisco
```

Related Commands

Command	Description
client-address	Configures the RADIUS client to proxy requests from the specified IP address to the RADIUS server and enters SSG-radius-proxy-client mode.

length (SSG)

Note Effective with Cisco IOS Release 15.0(1)M, the **length** (SSG) command is not available in Cisco IOS software.

To modify the port-bundle length upon the next Service Selection Gateway (SSG) reload, use the **length** command in SSG portmap configuration mode. To return the port-bundle length to the default value, use the **no** form of this command.

length *bits*

no length *bits*

Syntax Description

bits	Port-bundle length, in bits. The range is from 0 to 10 bits. The default is 4 bits.

Command Default

4 bits.

Command Modes

SSG portmap configuration

Command History

Release	Modification
12.2(16)B	This command was introduced. This command replaces the **ssg port-map destination range** command.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

The port-bundle length is used to determine the number of bundles in one group and the number of ports in one bundle. By default, the port-bundle length is 4 bits. The maximum port-bundle length is 10 bits. See Table 8 for available port-bundle length values and the resulting port-per-bundle and bundle-per-group values. Increasing the port-bundle length can be useful when you see frequent error messages about running out of ports in a port bundle, but note that the new value does not take effect until SSG next reloads and Cisco Service Selection Dashboard (SSD) restarts.

Note For each Cisco SSD server, all connected SSGs must have the same port-bundle length.

Table 8 Port-Bundle Lengths and Resulting Port-per-Bundle and Bundle-per-Group Values

Port-Bundle Length (in Bits)	Number of Ports per Bundle	Number of Bundles per Group (and per-SSG Source IP Address)
0	1	64512
1	2	32256
2	4	16128
3	8	8064
4 (default)	16	4032
5	32	2016
6	64	1008
7	128	504
8	256	252
9	512	126
10	1024	63

Examples

The following example results in 64 ports per bundle and 1008 bundles per group:

```
ssg port-map
 length 6
```

Related Commands

Command	Description
source ip	Specifies SSG source IP addresses to which to map the destination IP addresses in subscriber traffic.
ssg port-map	Enables the SSG port-bundle host key and enters SSG portmap configuration mode.

local-profile

Note Effective with Cisco IOS Release 15.0(1)M, the **local-profile** command is not available in Cisco IOS software.

To configure a local service profile and enter profile configuration mode, use the **local-profile** command in global configuration mode. To delete the local service profile, use the **no** form of this command.

local-profile *profile-name*

no local-profile *profile-name*

Syntax Description

profile-name	Name of profile to be configured.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)DC	This command was introduced on the Cisco 6400 series node route processor.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to configure local service profiles.

Examples

The following example shows how to configure a RADIUS profile called “fictitiousname.com” and enter profile configuration mode:

```
Router(config)# local-profile fictitiousname.com
Router(config-prof)#
```

In the following example, two services called “og1” and “og2” are defined and added to the open garden:

```
!
ssg open-garden og1
ssg open-garden og2
!
local-profile og1
 attribute 26 9 251 "Oopengarden1.com"
 attribute 26 9 251 "D10.13.1.5"
```

```
 attribute 26 9 251 "R10.1.1.0;255.255.255.0"
local-profile og2
 attribute 26 9 251 "Oopengarden2.com"
 attribute 26 9 251 "D10.14.1.5"
 attribute 26 9 251 "R10.2.1.0;255.255.255.0"
 attribute 26 9 251 "R10.3.1.0;255.255.255.0"
!
ssg bind service og2 10.5.5.1
```

Related Commands

Command	Description
attribute	Configures attributes in local RADIUS profiles.
show ssg open-garden	Displays a list of all configured open garden services.
ssg open-garden	Designates a service, defined in a local service profile, as an open garden service.
ssg service-search-order	Specifies the order in which SSG searches for a service profile.

max-sessions host

Note Effective with Cisco IOS Release 15.0(1)M, the **max-sessions host** command is not available in Cisco IOS software.

To set the maximum number of TCP sessions that can be established by an unauthenticated host, use the **max-sessions host** command in SSG TCP-redirect server-group configuration mode. To remove this setting, use the **no** form of this command.

max-sessions host *number-of-sessions*

no max-sessions host *number-of-sessions*

Syntax Description

number-of-sessions	Maximum number of TCP sessions per unauthenticated host. The range is from 1 to 65535.

Command Default

No limit on the number of TCP sessions that can be established by an unauthenticated host.

Command Modes

SSG TCP-redirect server-group configuration

Command History

Release	Modification
12.2(16)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use the **max-sessions host** command to configure a per-host limit on the number of TCP sessions that can be established by unauthenticated hosts that are redirected to the server group.

The maximum number of TCP connections allowed per host, as configured by the **max-sessions host** command, should be greater than the average number of TCP connections required when a page is accessed.

Examples

The following example sets the maximum number of TCP sessions that can be established by an unauthenticated host at 20 sessions:

```
ssg tcp-redirect
 server-group test_group
  Server 10.10.10.1 90
  max-sessions host 20
```

Related Commands

Command	Description
server-group	Defines the group of one or more servers that make up a named captive portal group and enters SSG TCP-redirect server-group configuration mode.
ssg tcp-redirect	Enables SSG TCP redirect and enters SSG TCP-redirect configuration mode.

mode extended

Note Effective with Cisco IOS Release 15.0(1)M, the **mode extended** command is not available in Cisco IOS software.

To select extended Autodomain mode, use the **mode extended** command in SSG-auto-domain configuration mode. To reenable basic Autodomain mode, use the **no** form of this command.

mode extended

no mode extended

Syntax Description

This command has no arguments or keywords.

Command Default

Basic Autodomain mode is selected.

Command Modes

SSG-auto-domain configuration

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use the **mode extended** command to select the extended Autodomain mode. In basic Autodomain mode, the profile downloaded from the AAA server for the selected Autodomain name is a service profile, which may or may not contain attributes specific to Service Selection Gateway (SSG). In extended Autodomain mode, the profile is a “virtual user” profile, which may contain a list of services in addition to other account attributes. The “virtual user” profile contains one autoservice to an authenticated service such as a proxy, VPDN, or tunnel. Connection to the autoservice occurs in the same way as in basic Autodomain mode. The host object is not activated until the user is authenticated at the service. The presence of SSD allows the user to access any other service in the specified user profile. Extended mode also enables users with multiple service selection to log on.

Examples

The following example shows how to enable extended Autodomain mode:

```
ssg enable
ssg auto-domain
 mode extended
 select username
 exclude apn company
 exclude domain cisco
 download exclude-profile abc password1
 nat user-address
```

Related Commands

Command	Description
download exclude-profile	Adds to the Autodomain download exclusion list.
exclude	Configures the Autodomain exclusion list.
nat user-address	Enables NAT on Autodomain tunnel service.
select	Configures the Autodomain selection mode.
show ssg auto-domain exclude-profile	Displays the contents of an Autodomain exclude-profile downloaded from the AAA server.
ssg auto-domain	Enables SSG Autodomain mode.
ssg enable	Enables SSG functionality.

msid (SSG-radius-proxy-timers)

Note Effective with Cisco IOS Release 15.0(1)M, the **msid** (SSG-radius-proxy-timers) command is not available in Cisco IOS software.

To configure a Service Selection Gateway (SSG) RADIUS proxy mobile station ID (MSID) timeout, use the **msid** command in SSG-radius-proxy-timers configuration mode. To disable the MSID timeout, use the **no** form of this command.

msid *timeout* **retry** *retries*

no msid *timeout* **retry** *number-of-retries*

Syntax Description

timeout	Timeout value in seconds. Valid range is 1 to 5 seconds. The default is 1 second.
retry *number-of-retries*	Maximum number of retries. Valid range is 1 to 20 retries. The default is 10 retries.

Command Default

The default value of this timeout is 1 second, with a default retry count of 10.

Command Modes

SSG-radius-proxy-timers

Command History

Release	Modification
12.2(15)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to configure an MSID timeout.

Configure the MSID timer to associate an MSID to the host object for a Mobile IP connection. The MSID is associated with a host object only after SSG receives the Accounting-Start packets from the Packet Data Serving Node (PDSN)/Foreign Agent (FA) and the Home Agent (HA). The host object address is not assigned until SSG receives the Accounting-Start packet from the HA. If the Accounting-Start packet from the PDSN/FA arrives before the Accounting-Start packet from the HA, the host object cannot be located, and the MSID is not associated with the host object. When this occurs, the retry timer is started. When the retry timer expires, the MSID is associated with the host object.

If SSG does not receive the Account-Start packet with the correct MSID from the PDSN before the timeout expires, the host object is removed.

Examples

The following example shows how to configure an SSG RADIUS proxy MSID timeout of 3 seconds with 5 retries:

```
ssg radius-proxy
 timeouts
 msid 3 retry 5
```

Related Commands

Command	Description
hand-off	Configures an SSG RADIUS proxy hand off timeout.
idle (SSG-radius-proxy-timers)	Configures a host object timeout value.
ip-address (SSG-radius-proxy-timers)	Configures an SSG RADIUS proxy IP address timeout.
ssg radius-proxy	Enables SSG RADIUS Proxy and enters SSG-radius-proxy mode.
timeouts (SSG-radius-proxy)	Enters SSG-radius-proxy-timers mode.

nat user-address

Note Effective with Cisco IOS Release 15.0(1)M, the **nat user-address** command is not available in Cisco IOS software.

To enable Network Address Translation (NAT) toward Autodomain service, use the **nat user-address** command in SSG-auto-domain mode. To disable NAT on Autodomain service, use the **no** form of this command.

nat user-address

no nat user-address

Syntax Description

This command has no arguments or keywords.

Command Default

NAT is not applied toward Autodomain services and IP addresses assigned at the tunnel, VPDN, or proxy service will be assigned at the host and then sent back to the RADIUS client. NAT is always applied towards the Autodomain connection regardless of the configuration of the **nat user-address** command when the Access-Request from the RADIUS client contains an IP address.

Command Modes

SSG-auto-domain

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use the **nat user-address** command to enable NAT toward the Autodomain connection. When a host object has not been assigned an IP address using the Access-Request from the RADIUS client, Service Selection Gateway (SSG) by default passes an IP address assigned at the tunnel, VPDN, or proxy service back to the RADIUS client and NAT does not happen toward the Autodomain connection. The **nat user-address** command overrides the default behavior and specifies that NAT should be performed towards Autodomain services. If a host has been assigned an IP address via the Access-Request, NAT happens toward the Autodomain connection regardless of the status of this command.

Examples

The following example enables NAT toward the Autodomain connection:

```
ssg enable
ssg auto-domain
 mode extended
 select username
```

```
exclude apn motorola
exclude domain cisco
download exclude-profile abc password1
nat user-address
```

Related Commands

Command	Description
download exclude-profile	Adds to the Autodomain download exclusion list.
exclude	Configures the Autodomain exclusion list.
mode extended	Enables extended mode for SSG Autodomain.
select	Configures the Autodomain selection mode.
show ssg auto-domain exclude-profile	Displays the contents of an Autodomain exclude-profile downloaded from the AAA server.
ssg enable	Enables SSG functionality.

network (ssg-redirect)

Note Effective with Cisco IOS Release 15.0(1)M, the **network** (ssg-redirect) command is not available in Cisco IOS software.

To add an IP address to a named network list, use the **network** command in SSG-redirect-network configuration mode. To remove an IP address from a named network list, use the **no** form of this command.

network *ip-address mask*

no network *ip-address mask*

Syntax Description

ip-address	IP address that is to be added to a named network list.
mask	Mask for the associated IP subnet.

Command Default

No default behavior or values

Command Modes

SSG-redirect-network configuration

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to define an individual network that is found in a named network list. Use the **network-list** command to define and name the network list and the **network** command to add an individual IP address to the named network list.

Packets arriving from an authorized user who is attempting to access an unauthorized service from an IP address that is part of a named network list can be redirected to a captive portal group that presents the user with an appropriate response, such as a logon screen. Service Selection Gateway (SSG) TCP Redirect for Services uses a marked TCP port or TCP port list in addition to the destination IP address to determine if a packet is redirected to a captive portal group.

Define a named TCP port list using the **port-list** command, and add TCP ports to the named TCP port list using the **port (ssg-redirect)** command.

You must enable SSG using the **ssg enable** command and SSG TCP Redirect for Services using the **ssg tcp-redirect** command before you can define a named network list.

Examples

The following example creates a network list named “RedirectNw” and adds IP address 10.0.0.0 255.0.0.0 and address 10.2.2.0 255.255.255.0 to the “RedirectNw” network list:

```
ssg tcp-redirect
 network-list RedirectNw
  network 10.0.0.0 255.0.0.0
  network 10.2.2.0 255.255.255.0
```

Related Commands

Command	Description
network-list	Defines a list of one or more IP networks that make up a named network list.
ssg enable	Enables SSG.
ssg tcp-redirect	Enables SSG TCP redirect and enters SSG-redirect mode.

network-list

Note Effective with Cisco IOS Release 15.0(1)M, the **network-list** command is not available in Cisco IOS software.

To define a list of one or more IP networks that make up a named network list and to enter SSG-redirect-network configuration mode, use the **network-list** command in SSG-redirect configuration mode. To remove a named network list, use the **no** form of this command.

network-list *network-listname*

no network-list *network-listname*

Syntax Description

network-listname	Defines the name of the network list.

Command Default

No default behavior or values.

Command Modes

SSG-redirect configuration

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to define a list of one or more IP networks that make up a named network list. Use the *network-listname* attribute to name the IP network list.

Packets arriving from an authorized user who is attempting to access an unauthorized service from an IP address that is part of a named network list can be redirected to a captive portal group that presents the user with an appropriate response, such as a logon screen. Service Selection Gateway (SSG) TCP Redirect for Services uses a marked TCP port or TCP port list in addition to the destination IP address to determine if a packet is redirected to a captive portal group.

Define a named TCP port list using the **port-list** command, and add TCP ports to the named TCP port list using the **port (ssg-redirect)** command.

You must enable SSG using the **ssg enable** command and SSG TCP Redirect for Services using the **ssg tcp-redirect** command before you can define a named network list.

Examples

The following example defines an IP network list named “RedirectNw”:

```
network-list RedirectNw
```

Related Commands

Command	Description
network (ssg-redirect)	Adds an IP address to a named network list.
redirect unauthorized-service to	Sets a list of destination IP networks that can be redirected by a specified, named captive portal group.
show ssg tcp-redirect group	Displays information about the captive portal groups and the networks associated with the captive portal groups.
ssg enable	Enables SSG.
ssg tcp-redirect	Enables SSG TCP redirect and enters SSG-redirect mode.

port (ssg-redirect)

Note Effective with Cisco IOS Release 15.0(1)M, the **port** (ssg-redirect) command is not available in Cisco IOS software.

To add a TCP port to a named port list, use the **port** command in SSG-redirect-port configuration mode. To remove a TCP port from a named port list, use the **no** form of this command.

port *port-number*

no port *port-number*

Syntax Description

port-number	Incoming destination port number.

Command Default

No default behavior or values.

Command Modes

SSG-redirect-port configuration

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to add incoming destination ports to a named TCP port list. Incoming packets directed to a port in the named TCP port list can be redirected by the named captive portal group. Configure the named captive portal group using the **server-group** command, and add servers to the captive portal group using the **server** (SSG) command. Define and name the TCP port list using the **port-list** command.

You must enable Service Selection Gateway (SSG) using the **ssg enable** command and SSG TCP Redirect for Services using the **ssg tcp-redirect** command before you can define or add incoming destination ports to a named TCP port list.

Examples

The following example creates a named TCP port list named “WebPorts” and adds TCP ports 80 and 8080:

```
ssg enable
 ssg tcp-redirect
  port-list WebPorts
   port 80
   port 8080
```

Related Commands

Command	Description
port-list	Defines a list of one or more TCP ports that make up a named port list and enters SSG-redirect-port configuration mode.
server (SSG)	Adds a server to a captive portal group.
server-group	Defines the group of one or more servers that make up a named captive portal group and enters SSG-redirect-group configuration mode.
show ssg tcp-redirect group	Displays information about the captive portal groups and the networks associated with the captive portal groups.
show tcp-redirect mappings	Displays information about the TCP redirect mappings for hosts within your system.
ssg enable	Enables SSG.
ssg tcp-redirect	Enables SSG TCP redirect and enters SSG-redirect mode.

port-list

Note Effective with Cisco IOS Release 15.0(1)M, the **port-list** command is not available in Cisco IOS software.

To define a list of one or more TCP ports that make up a named port list and to enter SSG-redirect-port configuration mode, use the **port-list** command in SSG-redirect configuration mode. To disable a port list, use the **no** form of this command.

port-list *port-listname*

no port-list *port-listname*

Syntax Description

port-listname	Defines the name of the port list.

Command Default

No default behavior or values.

Command Modes

SSG-redirect configuration

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to define a named port list. Use this command to create a list of TCP ports that can be redirected by the captive portal group. Use the **port** (ssg-redirect) command in SSG-redirect-port configuration mode to add TCP ports to the named port list.

You must enable Service Selection Gateway (SSG) using the **ssg enable** command and SSG TCP Redirect for Services using the **ssg tcp-redirect** command before you can define a named port list.

Examples

The following example creates a port list named “WebPorts”:

```
ssg enable
 ssg tcp-redirect
  port-list WebPorts
```

Related Commands

Command	Description
port (ssg-redirect)	Adds a TCP port to a named port list.
redirect to	Marks a TCP port or named TCP port list for SSG TCP redirection.
server (SSG)	Adds a server to a captive portal group.
server-group	Defines the group of one or more servers that make up a named captive portal group and enters SSG-redirect-group configuration mode.
show ssg tcp-redirect group	Displays information about the captive portal groups and the networks associated with the captive portal groups.
show tcp-redirect mappings	Displays information about the TCP redirect mappings for hosts within your system.
ssg enable	Enables SSG.
ssg tcp-redirect	Enables SSG TCP redirect and enters SSG-redirect mode.

query ip dhcp

Note Effective with Cisco IOS Release 15.0(1)M, the **query ip dhcp** command is not available in Cisco IOS software.

To configure the Service Selection Gateway (SSG) to send a Dynamic Host Configuration Protocol (DHCP) lease query request for the subscriber session created under a RADIUS proxy client when no IP address appears in the accounting-start record, use the **query ip dhcp** command in the client-address submode of SSG-radius-proxy mode. To disable the sending of the lease query request, use the **no** form of this command.

query ip dhcp

no query ip dhcp

Syntax Description

This command has no arguments or keywords.

Command Default

SSG sends the subscriber's IP address as the username (RADIUS attribute 1).

Command Modes

Client-address submode of SSG-radius-proxy mode

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use the **query ip dhcp** command to send DHCP lease query requests for a subscriber session under a specified RADIUS proxy client when no IP address is received in the accounting start record.

Examples

The following example enables DHCP lease query requests for RADIUS proxy client 10.0.0.0:

```
ssg enable
 ssg radius-proxy
 client-address 10.0.0.0
 query ip dhcp
```

Related Commands

Command	Description
ssg query mac dhcp	Sends a DHCP lease query request to the DHCP server when a subscriber's MAC address is not known.
username mac	Sends a subscriber's MAC address as RADIUS attribute 1 in TAL requests.

redirect access-list

Note Effective with Cisco IOS Release 15.0(1)M, the **redirect access-list** command is not available in Cisco IOS software.

To associate an access control list with a Service Selection Gateway (SSG) TCP redirect server group, use the **redirect access-list** command in SSG-redirect mode. To remove the association, use the **no** form of this command.

redirect access-list {*number* | *name*} [**to** *groupname*]

no redirect access-list {*number* | *name*} [**to** *groupname*]

Syntax Description

number	Specifies the access control list number.
name	Specifies the access control list name.
to *groupname*	(Optional) Defines the group name of the server group to which the access control list is redirected. If no server group is specified, the access control list is used for redirection to any server group that does not have an access control list associated with it.

Command Default

An access control list is not associated with an SSG TCP redirect server group.

Command Modes

SSG-redirect

Command History

Release	Modification
12.3(1a)BW	This command was introduced.
12.3(3)B	This command was integrated into Cisco IOS Release 12.3(3)B.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to associate an access control list with a TCP redirect server group. By associating an access control list with a redirect group, you can limit the kind of traffic that is redirected on the basis of the source or destination IP address and TCP ports. It can also be used to redirect different sets of users to different dashboards for unauthenticated users and unauthorized service redirection.

If a port list and an access control list are both associated with a server group, the TCP packet must match the access control list and port list. Only one access control list can be associated with a server group. Either an access control list or a port or port list should be configured with server groups for unauthorized service redirection and captivation.

If a server group is not specified, the access control list is used for redirection to any server group that does not have an access control list associated with it.

The access control list can be a simple or extended access control list. It can also be a named or numbered access control list.

Examples

The following example redirects access control list 101 to server group "InitialCapt":

```
redirect access-list 101 to InitialCapt
```

The following example redirects access control list 50 to server group "SESM1":

```
redirect access-list 50 to SESM1
```

Related Commands

Command	Description
show ssg tcp-redirect group	Displays information about the captive portal groups and the networks associated with the captive portal groups.
ssg tcp-redirect	Enables SSG TCP redirect and enters SSG-redirect mode.

redirect captivate advertising default group

Note Effective with Cisco IOS Release 15.0(1)M, the **redirect captivate advertising default group** command is not available in Cisco IOS software.

To configure the default captive portal group, duration, and frequency for advertising captivation, use the **redirect captivate advertising default group** command in SSG-redirect configuration mode. To deselect a captive portal group as the default for advertising captivation, use the **no** form of this command.

redirect captivate advertising default group *group-name* **duration** *seconds* **frequency** *frequency*

no redirect captivate advertising default group *group-name* **duration** *seconds* **frequency** *frequency*

Syntax Description

group-name	Name of the captive portal group.
duration *seconds*	The duration in seconds of the advertising captivation. The valid range is from 1 to 65536 seconds.
frequency *frequency*	The frequency in seconds at which TCP packets are redirected to the captive portal group. The valid range is from 1 to 65536 seconds.

Command Default

No default behavior or values.

Command Modes

SSG-redirect configuration

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to select the default captive portal group for advertising captivation of users upon Account Logon. Use the *seconds* argument to configure the duration, in seconds, of the advertising captivation. Any packets arriving from the user and marked for one of the TCP ports configured in the captive portal group *group-name* are redirected to one of the captive portals defined in that captive portal group for the duration configured by the *seconds* argument.

Use the *frequency* argument to configure how often Service Selection Gateway (SSG) attempts to forward packets from the user to the captive portal.

The parameters set by this command can be overridden by the RADIUS attributes set for a user.

Examples

The following example shows how to configure the captive portal group named "CaptivateServer" to forward packets from a user for 30 seconds at intervals of 3600 seconds:

```
server-group SSD
 server 10.0.0.253 8080
!
 redirect port-list WebPorts to SSD
!
 redirect unauthenticated-user to RedirectServer
 redirect unauthorized-service to SSD
 redirect smtp group SMTPServer all
 redirect captivate initial default group CaptivateServer duration 10
 redirect captivate advertising default group CaptivateServer duration 30 frequency 3600
```

Related Commands

Command	Description
redirect captivate initial default group	Selects a default captive portal group and duration of the initial captivation of users on Account Logon.
redirect to	Marks a TCP port or named TCP port list for SSG TCP redirection.
redirect smtp group	Selects a captive portal group for redirection of SMTP traffic.
redirect unauthorized-service to	Sets a list of destination IP networks that can be redirected by a specified, named captive portal group.
redirect unauthenticated-user to	Redirects TCP traffic from unauthenticated users to a specified captive portal group.
show ssg tcp-redirect group	Displays information about the captive portal groups and the networks associated with the captive portal groups.
show tcp-redirect mappings	Displays information about the TCP redirect mappings for hosts within your system.
ssg enable	Enables SSG.
ssg tcp-redirect	Enables SSG TCP redirect and enters SSG-redirect mode.

redirect captivate initial default group

Note Effective with Cisco IOS Release 15.0(1)M, the **redirect captivate initial default group** command is not available in Cisco IOS software.

To select a default captive portal group and duration of the initial captivation of users on Account Logon, use the **redirect captivate initial default group** command in SSG-redirect configuration mode. To deselect a captive portal group as the default for initial captivation, use the **no** form of this command.

redirect captivate initial default group *group-name* **duration** *seconds*

no redirect captivate initial default group *group-name* **duration** *seconds*

Syntax Description

group-name	Name of the captive portal group.
duration *seconds*	Duration in seconds of the initial captivation. The valid range is from 1 to 65536 seconds.

Command Default

No default behavior or values.

Command Modes

SSG-redirect configuration

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to select the default captive portal group for initial captivation of users on Account Logon. Use the *seconds* argument to configure the duration, in seconds, of the initial captivation. Any packets arriving from the user and marked for one of the TCP ports configured in the captive portal group *group-name* are redirected to one of the captive portals defined in that captive portal group for the duration configured by the *seconds* argument.

The parameters set by this command can be overridden by the RADIUS attributes set for a user.

Examples

The following example shows that the captive portal group named “CaptivateServer” will be used to forward packets from a user for the first 10 seconds that the user is connected:

```
server-group SSD
 server 10.0.0.253 8080
!
 redirect port-list WebPorts to SSD
```

```
!
 redirect unauthenticated-user to RedirectServer
 redirect unauthorized-service to SSD
 redirect smtp group SMTPServer all
 redirect captivate initial default group CaptivateServer duration 10
 redirect captivate advertising default group CaptivateServer duration 30 frequency 3600
```

Related Commands

Command	Description
redirect captivate advertising default group	Configures the default captive portal group, duration, and frequency for advertising.
redirect to	Marks a TCP port or named TCP port list for SSG TCP redirection.
redirect smtp group	Selects a captive portal group for redirection of SMTP traffic.
redirect unauthorized-service to	Sets a list of destination IP networks that can be redirected by a specified, named captive portal group.
redirect unauthenticated-user to	Redirects TCP traffic from unauthenticated users to a specified captive portal group.
show ssg tcp-redirect group	Displays information about the captive portal groups and the networks associated with the captive portal groups.
show tcp-redirect mappings	Displays information about the TCP redirect mappings for hosts within your system.
ssg enable	Enables SSG.
ssg tcp-redirect	Enables SSG TCP redirect and enters SSG-redirect mode.

redirect permanent http to

Note Effective with Cisco IOS Release 15.0(1)M, the **redirect permanent http to** command is not available in Cisco IOS software.

To configure Service Selection Gateway (SSG) with permanent TCP redirection for HTTP proxy server support, use the **redirect permanent http to** command in SSG-redirect configuration mode. To disable permanent TCP redirection, use the **no** form of this command.

redirect permanent http {**authenticated** | **unauthenticated**} **to** *server-group*

no redirect permanent http {**authenticated** | **unauthenticated**} **to** *server-group*

Syntax Description

authenticated	Redirects HTTP traffic to the HTTP proxy server for authenticated users.
unauthenticated	Redirects HTTP traffic to the HTTP proxy server for unauthenticated users.
server-group	Server group name to which HTTP traffic will be sent.

Command Default

Permanent TCP redirection is not configured.

Command Modes

SSG-redirect configuration

Command History

Release	Modification
12.3(3)B	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Permanent TCP redirection enables SSG to support users whose web browsers are configured with HTTP proxy servers.

Examples

The following example shows how to configure SSG to support permanent TCP redirection for authenticated and unauthenticated HTTP proxy users:

```
ssg tcp-redirect
 server-group unauthen-group
  server 10.10.86.90 80
 !
 server-group auth_web_group
  server 10.10.36.253 80
!
 server-group unauth_web_group
  server 10.10.76.12 80
```

```
!
redirect unauthenticated-user to unauthen-group
!
redirect permanent http unauthenticated to unauth_web_group
!
redirect permanent http authenticated to auth_web_group
```

Related Commands

Command	Description
server	Adds a server to a captive portal group.
server-group	Defines the group of one or more servers that make up a named captive portal group.
show ssg host	Displays information about a subscriber and current connections of the subscriber.
show ssg tcp-redirect mapping	Displays information about the TCP redirect mappings for hosts within your system.

redirect prepaid-user to

Note Effective with Cisco IOS Release 15.0(1)M, the **redirect prepaid-user to** command is not available in Cisco IOS software.

To configure a captive portal group for redirection of prepaid user traffic, use the **redirect prepaid-user to** command in SSG-redirect configuration mode. To configure SSG not to redirect prepaid users to the specified captive portal group, use the **no** form of this command.

redirect prepaid-user to *group-name*

no redirect prepaid-user to *group-name*

Syntax Description

group-name	Name of the captive portal group

Command Default

If no redirect group is configured, prepaid traffic is dropped.

Command Modes

SSG-redirect

Command History

Release	Modification
12.2(15)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to configure and name a captive portal group to which prepaid user traffic is redirected. When a user that is logged on to a prepaid service runs out of quota on the billing server, the user is redirected to the configured captive portal group if the service is not configured with any specific redirect server group. Once redirected to the captive portal group, the user can refill the quota on the billing server without being disconnected from the original prepaid service.

The captive portal group is the default group for all services that are not configured with a redirect group.

Examples

The following example shows how to configure a captive portal group called “DefaultRedirectGroup”, add two servers to “DefaultRedirectGroup”, and redirect prepaid users to the newly created captive portal:

```
ssg enable
ssg tcp-redirect
 server-group DefaultRedirectGroup
  server 10.0.0.1 8080
```

```
 server 10.0.0.20 80
 end
redirect prepaid-user to DefaultRedirectGroup
```

Related Commands

Command	Description
server	Adds a server to a captive portal group.
server-group	Defines the group of one or more servers that make up a named captive portal group and enters SSG-redirect-group configuration mode.
ssg tcp-redirect	Enables SSG TCP redirect and enters SSG-redirect mode.

redirect smtp group

Note Effective with Cisco IOS Release 15.0(1)M, the **redirect smtp group** command is not available in Cisco IOS software.

To select a captive portal group for redirection of Simple Mail Transfer Protocol (SMTP) traffic, use the **redirect smtp group** command in SSG-redirect configuration mode. To stop redirecting SMTP traffic to a captive portal group, use the **no** form of this command.

redirect smtp group *group-name* [**all** | **user**]

no redirect smtp group *group-name* [**all** | **user**]

Syntax Description

group-name	Name of the captive portal group.
all	(Optional) Any SMTP packets are forwarded.
user	(Optional) SMTP packets from users that have SMTP forwarding permission are forwarded.

Command Default

SMTP traffic is not forwarded to a captive portal group.

Command Modes

SSG-redirect configuration

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to select a captive portal group for redirection of SMTP traffic. If you select the **all** keyword, all SMTP packets (TCP port 25) from authorized users are redirected to one of the servers in the captive portal group specified by the *group-name* argument. If you select the **user** keyword, only SMTP packets from authorized users that have SMTP forwarding permission set through a RADIUS attribute are redirected. If you do not select a keyword, the default is the **all** keyword.

Examples

The following example shows how to configure all SMTP packets from authorized users to be redirected to the captive portal group named “SMTPServer”:

```
server-group SSD
 server 10.0.0.253 8080
!
 redirect port-list WebPorts to SSD
```

```
!
 redirect unauthenticated-user to RedirectServer
 redirect unauthorized-service to SSD
 redirect smtp group SMTPServer all
 redirect captivate initial default group CaptivateServer duration 10
 redirect captivate advertising default group CaptivateServer duration 30 frequency 3600
```

The following example shows how to configure SMTP packets from any authorized user with the SMTP forwarding permission set through a RADIUS attribute to be redirected to the captive portal group named "SMTPServer":

```
redirect smtp group SMTPServer user
```

Related Commands

Command	Description
redirect captivate advertising default group	Configures the default captive portal group, duration, and frequency for advertising.
redirect captivate initial default group	Selects a default captive portal group and duration of the initial captivation of users on Account Logon.
redirect to	Marks a TCP port or named TCP port list for SSG TCP redirection.
redirect unauthorized-service to	Sets a list of destination IP networks that can be redirected by a specified, named captive portal group.
redirect unauthenticated-user to	Redirects TCP traffic from unauthenticated users to a specified captive portal group.
show ssg tcp-redirect group	Displays information about the captive portal groups and the networks associated with the captive portal groups.
show tcp-redirect mappings	Displays information about the TCP redirect mappings for hosts within your system.
ssg enable	Enables SSG.
ssg tcp-redirect	Enables SSG TCP redirect and enters SSG-redirect mode.

redirect to

Note Effective with Cisco IOS Release 15.0(1)M, the **redirect to** command is not available in Cisco IOS software.

To configure a TCP port or named TCP port list for Service Selection Gateway (SSG) TCP Redirect for Services, use the **redirect to** command in SSG-redirect configuration mode. To disable SSG TCP Redirect for Services on a TCP port or named TCP port list, use the **no** form of this command.

redirect {**port-list** *port-listname* | **port** *port-number*} **to** *group-name*

no redirect {**port-list** *port-listname* | **port** *port-number*} **to** *group-name*

Syntax Description

port-list	Specifies the named TCP port list to mark for SSG TCP redirection.
port-listname	Specifies the name of the named TCP port list.
port	Specifies a TCP port to mark for SSG TCP redirection.
port-number	Specifies the incoming destination port number of the TCP port to mark for SSG TCP redirection.
group-name	Defines the name of the captive portal group to redirect packets to that are marked for a destination port or named TCP port list.

Command Default

No default behavior or values.

Command Modes

SSG-redirect configuration

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to mark a TCP port or a named TCP port list for SSG TCP Redirect for Services. Define a named TCP port list using the **port-list** command and add TCP ports to the named TCP port list using the **port** (ssg-redirect) command. Packets arriving from an authorized user, or from an authorized user attempting to access an unauthorized service at a marked TCP port or named TCP port list can be redirected to a captive portal group that presents the user with an appropriate response, such as a logon screen.

Note You can associate only one port or port list with a portal group.

You must enable SSG using the **ssg enable** command and SSG TCP Redirect for Services using the **ssg tcp-redirect** command before you can define a TCP port or named TCP port list for SSG TCP redirection.

Note This command replaces the **ssg http-redirect port group** command.

Examples

The following example marks TCP port 8080 for SSG TCP redirection. Packets with a destination port of 8080 are redirected to the captive portal group named "RedirectServer":

```
server-group RedirectServer
 server 10.2.36.253 8080
!
 redirect port 8080 to RedirectServer
 redirect unauthorized-service destination network-list RedirectNw to RedirectServer
```

The following example marks the named TCP port "WebPorts" for SSG TCP redirection. Packets with a destination port that is one of the ports in the port list "WebPorts" are redirected to the captive portal group named "RedirectServer":

```
server-group SSD
 server 10.0.0.253 8080
!
 redirect port-list WebPorts to RedirectServer
!
```

Related Commands

Command	Description
port (ssg-redirect)	Adds a TCP port to a named port list.
port-list	Defines a list of one or more TCP ports that make up a named port list and enters SSG-redirect-port configuration mode.
redirect captivate advertising default group	Configures the default captive portal group, duration, and frequency for advertising.
redirect captivate initial default group	Selects a default captive portal group and duration of the initial captivation of users on Account Logon.
redirect unauthorized-service to	Sets a list of destination IP networks that can be redirected by a specified, named captive portal group.
server (SSG)	Adds a server to a captive portal group.
server-group	Defines the group of one or more servers that make up a named captive portal group and enters SSG-redirect-group configuration mode.
show ssg tcp-redirect group	Displays information about the captive portal groups and the networks associated with the captive portal groups.
show tcp-redirect mappings	Displays information about the TCP redirect mappings for hosts within your system.
ssg enable	Enables SSG.
ssg tcp-redirect	Enables SSG TCP redirect and enters SSG-redirect mode.

redirect unauthenticated-user to

Note Effective with Cisco IOS Release 15.0(1)M, the **redirect unauthenticated-user to** command is not available in Cisco IOS software.

To redirect TCP traffic from unauthenticated users to a specified captive portal group, use the **redirect unauthenticated-user to** command in Service Selection Gateway SSG-redirect configuration mode. To stop redirecting traffic from unauthenticated users to the specified captive portal group, use the **no** form of this command.

redirect unauthenticated-user to *group-name*

no redirect unauthenticated-user to *group-name*

Syntax Description

group-name	The name of the captive portal group.

Command Default

No default behavior or values.

Command Modes

SSG-redirect configuration

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to redirect traffic from unauthenticated users to a specified captive portal group.

Note This command replaces the **ssg http-redirect unauthorized-user group** command.

Examples

The following example sets redirection of traffic from unauthenticated users to the captive portal group named “RedirectServer”:

```
server-group SSD
 server 10.0.0.253 8080
!
 redirect port-list WebPorts to SSD
!
 redirect unauthenticated-user to RedirectServer
 redirect unauthorized-service to SSD
 redirect smtp group SMTPServer all
```

```
redirect captivate initial default group CaptivateServer duration 10
redirect captivate advertising default group CaptivateServer duration 30 frequency 3600
```

Related Commands

Command	Description
redirect captivate advertising default group	Configures the default captive portal group, duration, and frequency for advertising.
redirect captivate initial default group	Selects a default captive portal group and duration of the initial captivation of users on Account Logon.
redirect to	Marks a TCP port or named TCP port list for SSG TCP redirection.
redirect smtp group	Selects a captive portal group for redirection of SMTP traffic.
redirect unauthorized-service to	Sets a list of destination IP networks that can be redirected by a specified, named captive portal group.
show ssg tcp-redirect group	Displays information about the captive portal groups and the networks associated with the captive portal groups.
show tcp-redirect mappings	Displays information about the TCP redirect mappings for hosts within your system.
ssg enable	Enables SSG.
ssg tcp-redirect	Enables SSG TCP redirect and enters SSG-redirect mode.

redirect unauthorized-service service to

Note Effective with Cisco IOS Release 15.0(1)M, the **redirect unauthorized-service service to** command is not available in Cisco IOS software.

To redirect traffic that is destined for an unauthorized service to a specified server group, use the **redirect unauthorized-service service to** command in SSG TCP-redirect configuration mode. To remove this redirection, use the **no** form of this command.

redirect unauthorized-service service *service-name* **to** *server-group*

no redirect unauthorized-service service *service-name* **to** *server-group*

Syntax Description

service-name	Name of the unauthorized service.
server-group	Name of the server group to which traffic will be forwarded.

Command Default

Users trying to access a service that they are unauthorized to access will not be redirected.

Command Modes

SSG TCP-redirect configuration

Command History

Release	Modification
12.2(16)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

The **redirect unauthorized-service service to** command causes SSG to download the service profile from the authentication, authorization, and accounting (AAA) server and create mappings for the networks associated with the service. If traffic is received for the specified service while the service profile is being downloaded, the traffic either will be dropped or will be forwarded if Internet service is available to the user.

Examples

In the following example, users who are trying to access the service “test_service” but are unauthorized for that service will be forwarded to the server group “test_group”:

```
ssg tcp-redirect
 Server-group test_group
  Server 10.10.10.1 90
!
!
 Port-list test_ports
  Port 777
```

```
!
!
 redirect port-list test_ports to test_group
!
 redirect unauthorized-service service test_service to test_group
```

Related Commands

Command	Description
redirect unauthenticated-user to	Redirects TCP traffic from unauthenticated users to a specified captive portal group.
redirect unauthorized-service to	Sets a list of destination IP networks that can be redirected by a specified, named captive portal group.
ssg tcp-redirect	Enables SSG TCP redirect and enters SSG TCP-redirect configuration mode.

redirect unauthorized-service to

Note Effective with Cisco IOS Release 15.0(1)M, the **redirect unauthorized-service to** command is not available in Cisco IOS software.

To set a list of destination IP networks that can be redirected by a specified, named captive portal group, use the **redirect unauthorized-service to** command in SSG-redirect configuration mode. To remove the list of IP networks that can be redirected by a specified named captive portal group, use the **no** form of this command.

redirect unauthorized-service [**destination network-list** *network-listname*] **to** *group-name*

no redirect unauthorized-service [**destination network-list** *network-listname*] **to** *group-name*

Syntax Description

destination network list	(Optional) Checks incoming packets from authenticated hosts to networks that they are not authorized to access to determine if they need redirection.
network-listname	(Optional) Name of the list of destination IP networks.
group-name	Name of the captive portal group.

Command Default

No default behavior or values.

Command Modes

SSG-redirect configuration

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to set a list of destination IP networks that can be redirected by the named captive portal group specified by the *group-name* argument. Incoming packets from authenticated hosts to networks that they are not authorized to access are checked against the destination IP network list to determine if they need redirection. If you do not specify a destination IP network by configuring the optional **destination network-list** keywords, the captive portal group specified in the *group-name* argument is used as the default group for unauthorized service redirection when the IP address of the unauthorized packet does not fall into any network list associated with any captive portal group.

You can associate only one destination IP network list with a captive portal group. You can associate a destination IP network list with multiple captive portal groups.

When you associate a destination IP network list with a captive portal group, packets arriving marked with a destination IP network that matches an IP network list may be redirected via SSG TCP redirection. The incoming destination TCP port also determines whether a packet is a candidate for SSG TCP redirection.

You can associate different server groups with overlapping IP network addresses. You must configure the captive portal group associated with a more specific network group first. For example, you must configure

```
redirect 10.1.0.0/255.255.0.0 to IPTVGroup
```

before you can configure

```
redirect 10.0.0.0/255.0.0.0 to ISPGroup
```

Examples

The following example shows how to set the captive portal group called "RedirectServer" as a possible candidate for redirection when the destination of a packet matches one of the networks in the destination IP network list named "RedirectNW":

```
server-group RedirectServer
 server 10.2.36.253 8080
!
 redirect port 80 to RedirectServer
 redirect unauthorized-service destination network-list RedirectNw to RedirectServer
```

The following example shows how to set the captive portal group called "DefaultRedirectServer" as a possible candidate for redirection when the destination of a packet does not match any of the networks defined in any destination IP network list:

```
redirect unauthorized-service to DefaultRedirectServer
```

Related Commands

Command	Description
redirect captivate advertising default group	Configures the default captive portal group, duration, and frequency for advertising.
redirect captivate initial default group	Selects a default captive portal group and duration of the initial captivation of users on Account Logon.
redirect to	Marks a TCP port or named TCP port list for SSG TCP redirection.
redirect smtp group	Selects a captive portal group for redirection of SMTP traffic.
redirect unauthenticated-user to	Redirects TCP traffic from unauthenticated users to a specified captive portal group.
show ssg tcp-redirect group	Displays information about the captive portal groups and the networks associated with the captive portal groups.
show tcp-redirect mappings	Displays information about the TCP redirect mappings for hosts within your system.
ssg enable	Enables SSG.
ssg tcp-redirect	Enables SSG TCP redirect and enters SSG-redirect mode.

remove vsa

Note Effective with Cisco IOS Release 15.0(1)M, the **remove-vsa** command is not available in Cisco IOS software.

To allow all Third Generation Partnership Project 2 (3GPP2) vendor-specific attributes (VSAs) or all Cisco VSAs from Access-Accept packets proxied from a authentication, authorization, and accounting (AAA) server to a RADIUS client to be removed, use the **remove vsa** command in SSG-radius-proxy-client mode. To enable all 3GPP2 VSAs or Cisco VSAs to be passed transparently, use the **no** form of this command.

remove vsa {**3gpp2** | **cisco**}

no remove vsa {**3gpp2** | **cisco**}

Syntax Description

3gpp2	Removes all 3GPP2 VSAs.
cisco	Removes all Cisco VSAs.

Command Default

By default, Service Selection Gateway (SSG) removes all Cisco VSAs from Access-Accept packets proxied from the AAA server to the client device. All 3GPP2 VSAs are, by default, passed transparently.

Command Modes

SSG-radius-proxy-client

Command History

Release	Modification
12.2(15)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to remove all 3GPP2 VSAs or Cisco VSAs from a RADIUS client.

By default, SSG removes all Cisco VSAs from Access-Accept packets proxied from the AAA server to the client device. This is because the client device is unlikely to understand the VSAs, and their presence may cause interoperation difficulties. The **no remove vsa cisco** command may be used to allow these attributes to be passed transparently.

You can use this command to remove all 3GPP2 VSAs in addition to Cisco VSAs by using the **3gpp2** keyword. 3GPP2 VSAs are not filtered by default, whereas Cisco VSAs are filtered by default. SSG VSAs (a subset of Cisco VSAs) are always removed, irrespective of any configuration.

Examples

The following example shows how to remove all 3GPP2 VSAs from an Accept-Accept packet proxied from the AAA server to the client device:

```
remove vsa 3gpp2
```

The following example shows how to transparently pass all Cisco VSAs in an Accept-Accept packet proxied from the AAA server to the client device:

```
remove vsa cisco
```

Related Commands

Command	Description
client-address	Configures a RADIUS client to proxy requests from the specified IP address to a RADIUS server and enters SSG-radius-proxy-client mode.

select

Note Effective with Cisco IOS Release 15.0(1)M, the **select** command is not available in Cisco IOS software.

To override the default Autodomain selection algorithm, use the **select** command in SSG-auto-domain mode. To reenable the default algorithm for selecting the Autodomain, use the **no** form of this command.

select {**username** | **called-station-id**}

no select {**username** | **called-station-id**}

Syntax Description

username	Configures the algorithm to use only the username to select the Autodomain.
called-station-id	Configures the algorithm to use only the Access Point Name (APN) Called-Station-ID.

Command Default

The algorithm attempts to find a valid Autodomain based on the APN Called-Station-ID and then by username.

Command Modes

SSG-auto-domain

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use the **select** command to override the default algorithm for selecting the Autodomain. By default, the algorithm attempts to find a valid Autodomain based on APN Called-Station-ID and then by username. Using this command, you can configure the algorithm to use only the APN or only the username.

Note The Autodomain exclusion list is applied even if the mode is selected using the **select** command.

Examples

The following example shows how to configure the algorithm to search for a valid Autodomain based only on the username:

```
ssg enable
ssg auto-domain
 mode extended
 select username
```

```
exclude apn motorola
exclude domain cisco
download exclude-profile abc password1
nat user-address
```

The following example shows how to configure the algorithm to search for a valid Autodomain based only on the APN:

```
select called-station-id
```

Related Commands

Command	Description
download exclude-profile	Adds to the Autodomain download exclusion list.
exclude	Configures the Autodomain exclusion list.
mode extended	Enables extended mode for SSG Autodomain.
nat user-address	Enables NAT on Autodomain tunnel service.
show ssg auto-domain exclude-profile	Displays the contents of an Autodomain exclude-profile downloaded from the AAA server.
ssg auto-domain	Enables SSG Autodomain.
ssg enable	Enables SSG functionality.

server (SSG)

Note Effective with Cisco IOS Release 15.0(1)M, the **server** (SSG) command is not available in Cisco IOS software.

To add a server to a captive portal group, use the **server** command in SSG-redirect-group configuration mode. To remove a server from a captive portal group, use the **no** form of this command.

server *ip-address port*

no server *ip-address port*

Syntax Description

ip-address	IP address of the server to be added to the captive portal group.
port	TCP port of the server to be added to the captive portal group.

Command Default

No default behavior or values.

Command Modes

SSG-redirect-group configuration

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use the **server** command in SSG-redirect-group configuration mode to add a server, defined by its IP address and TCP port, to a captive portal group.

Service Selection Gateway (SSG) TCP Redirect for Services provides nonauthorized users access to controlled services within an SSG. Packets sent upstream from an unauthenticated user are forwarded to the captive portal that deals with the packets in a suitable manner, such as routing them to a logon page. You can also use captive portals to handle requests from authorized users who request access to services into which they are not logged.

You must enable SSG using the **ssg enable** command and SSG TCP Redirect for Services using the **ssg tcp-redirect** command before you can define a captive portal group. Use the **server-group** command in SSG-redirect configuration mode to create and name a captive portal group before using the **server** command to add servers to the captive portal group.

Examples

The following example adds a server at IP address 10.0.0.0 and TCP port 8080 and a server at IP address 10.1.2.3 and TCP port 8081 to a captive portal group named "RedirectServer":

```
ssg enable
 ssg tcp-redirect
  server-group RedirectServer
   server 10.0.0.0 8080
   server 10.1.2.3 8081
```

Related Commands

Command	Description
server-group	Defines the group of one or more servers that make up a named captive portal group and enters SSG-redirect-group configuration mode.
show ssg tcp-redirect group	Displays information about the captive portal groups and the networks associated with the captive portal groups.
show tcp-redirect mappings	Displays information about the TCP redirect mappings for hosts within your system.
ssg enable	Enables SSG.
ssg tcp-redirect	Enables SSG TCP redirect and enters SSG-redirect mode.

server-group

Note Effective with Cisco IOS Release 15.0(1)M, the **server-group** command is not available in Cisco IOS software.

To define a group of one or more servers that make up a named captive portal group and enter SSG-redirect-group configuration mode, use the **server-group** command in SSG-redirect configuration mode. To remove a captive portal group and any servers configured within that portal group, use the **no** form of this command.

server-group *group-name*

no server-group *group-name*

Syntax Description

group-name	The name of the captive portal group.

Command Default

No default behavior or values.

Command Modes

SSG-redirect configuration

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to define and name a captive portal group. Service Selection Gateway (SSG) TCP Redirect for Services provides nonauthorized users access to controlled services within an SSG. Packets sent upstream from an unauthenticated user are forwarded to the captive portal that deals with the packets in a suitable manner, such as routing them to a logon page. You can also use captive portals to handle requests from authorized users who request access to services into which they are not logged.

After defining a captive portal group with the **server-group** command, identify individual servers for inclusion in the captive portal group using the **server** *ip-address port* command in SSG-redirect-group configuration mode.

You must enable SSG using the **ssg enable** command and SSG TCP Redirect for Services using the **ssg tcp-redirect** command before you can define a captive portal group.

Note This command, along with the **server** command, replaces the **ssg http-redirect group** *group-name* **server** *ip-address port* command.

Examples

The following example defines a captive portal group named “RedirectServer”:

```
ssg enable
 ssg tcp-redirect
  server-group RedirectServer
```

Related Commands

Command	Description
server (SSG)	Adds a server to a captive portal group.
show ssg tcp-redirect group	Displays information about the captive portal groups and the networks associated with the captive portal groups.
show tcp-redirect mappings	Displays information about the TCP redirect mappings for hosts within your system.
ssg enable	Enables SSG.
ssg tcp-redirect	Enables SSG TCP redirect and enters SSG-redirect mode.

server-port

Note Effective with Cisco IOS Release 15.0(1)M, the **server-port** command is not available in Cisco IOS software.

To configure the ports on which Service Selection Gateway (SSG) listens for RADIUS-requests from configured RADIUS clients, use the **server-port** command in SSG-radius-proxy configuration mode. To stop SSG from listening for RADIUS requests from configured RADIUS clients on a port, use the **no** form of this command.

server-port [**auth** *auth-port*] [**acct** *acct-port*]

no server-port [**auth** *auth-port*] [**acct** *acct-port*]

Syntax Description

auth	(Optional) RADIUS authentication port.
auth-port	(Optional) Port number to be used for RADIUS authentication. The default is 1645.
acct	(Optional) RADIUS accounting port.
acct-port	(Optional) Port number to be used for RADIUS accounting. The default is 1646.

Command Default

Port 1645 is the default RADIUS authentication port.
Port 1646 is the default RADIUS accounting port.

Command Modes

SSG-radius-proxy configuration

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to configure the authentication and accounting ports for the SSG Autologon Using Proxy RADIUS feature. Ports configured with this command are global parameters that apply to all proxy clients in the SSG.

Examples

The following example shows how to configure port 23 as the RADIUS authentication port and port 45 as the RADIUS accounting port:

```
server-port auth 23 acct 45
```

Related Commands

Command	Description
address-pool	Defines local IP pools to be used by SSG to assign IP addresses to users for which SSG is acting as a RADIUS client.
clear ssg radius-proxy client-address	Clears all hosts connected to a specific RADIUS client.
clear ssg radius-proxy nas-address	Clears all hosts connected to a specific NAS.
forward accounting-start-stop	Proxies accounting start, stop, and update packets generated by any RADIUS clients to the AAA server.
idle-timeout (SSG)	Configures a host object timeout value.
show ssg tcp-redirect group	Displays the pool of IP addresses configured for a router or for a specific domain.
ssg enable	Enables SSG.
ssg radius-proxy	Enables SSG RADIUS Proxy.

session-identifier

Note Effective with Cisco IOS Release 15.0(1)M, the **session-identifier** command is not available in Cisco IOS software.

To override Service Selection Gateway (SSG) automatic RADIUS client session identification and to configure SSG to identify the specified client session by a specific type of ID attribute, use the **session-identifier** command in SSG-radius-proxy-client mode. To configure SSG to perform user identification only by the username without using a session identification, use the **no** form of this command.

session-identifier [**auto** | **msid** | **correlation-id** | **acct-sess-id**]

no session-identifier [**auto** | **msid** | **correlation-id** | **acct-sess-id**]

Syntax Description

auto	Automatically determines the session identifier.
msid	Uses the MSID as the client session identifier.
correlation-id	Uses the Correlation-ID as the client session identifier.
acct-sess-id	Uses the Accounting-Session-ID as a client session identifier.

Command Default

SSG selects the attribute used for session identification according to the type of client device.

Command Modes

SSG-radius-proxy-client

Command History

Release	Modification
12.2(15)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

By default, SSG automatically selects the attribute to use for session identification according to the type of RADIUS client device. This attribute is used in the SSG Proxy RADIUS logon table. SSG assigns the following vendor-specific attributes (VSAs) to identify client sessions:

- 3GPP2-Correlation-ID for Packet Data Serving Nodes (PDSNs)
- Accounting-Session-ID for Home Agents (HAs)
- Calling-Station-ID (MSID) for non-CDMA2000 devices such as a general packet radio system (GPRS)

Use the **session-identifier** command to override the automatic session identification. Use the **auto** keyword to return to automatic session identification.

Examples

The following example shows how to configure SSG to use the Correlation-ID to identify the specified client session:

```
session-identifier correlation-id
```

The following example shows how to configure the RADIUS client to proxy all requests from IP address 172.16.0.0 to the RADIUS server, to assign the shared secret "cisco" to the client, and to use the Accounting-Session-ID attribute to identify the specified client session:

```
client-address 172.16.0.0
 key cisco
 session-identifier acct-session-id
```

Related Commands

Command	Description
client-address	Configures the RADIUS client to proxy requests from the specified IP address to the RADIUS server and enters SSG-radius-proxy-client mode.
key (SSG-radius-proxy-client)	Configures a shared secret between SSG and a RADIUS client.

sessions auto cleanup

Note Effective with Cisco IOS Release 15.0(1)M, the **sessions auto-cleanup** command is not available in Cisco IOS software.

To configure an aggregation device to attempt to recover PPP over Ethernet (PPPoE) sessions that failed after reload by notifying customer premises equipment (CPE) devices about the PPPoE session failures, use the **sessions auto cleanup** command in BBA group configuration mode. To disable PPPoE session recovery after reload, use the **no** form of this command.

sessions auto cleanup

no sessions auto cleanup

Syntax Description

This command has no arguments or keywords.

Command Default

PPPoE session recovery after reload is not enabled.

Command Modes

BBA group configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.4	This command was integrated into Cisco IOS Release 12.4.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
15.0(1)M	This command was removed.

Usage Guidelines

If the PPP keepalive mechanism is disabled on a CPE device, the CPE device has no way to detect link or peer device failures over PPPoE connections. When an aggregation device that serves as the PPPoE session endpoint reloads, the CPE will assume that the link is up and will continue to send traffic to the aggregation device. The aggregation device will drop the traffic for the failed PPPoE session.

The **sessions auto cleanup** command enables an aggregation device to attempt to recover PPPoE sessions that existed before a reload. When the aggregation device detects a PPPoE packet for a “half-active” PPPoE session (a PPPoE session that is active on the CPE end only), the device notifies the CPE of the PPPoE session failure by sending a PPPoE active discovery terminate (PADT) packet. The CPE device is expected to respond to the PADT packet by taking failure recovery action.

The **sessions auto cleanup** command must be configured in a PPPoE profile. This command enables PPPoE session recovery after reload on all ingress ports that use the PPPoE profile.

Examples

In the following example, PPPoE session recovery after reload is configured in PPPoE profile “group1”.

```
bba-group pppoe group1
 virtual-template 1
 sessions auto cleanup
```

Related Commands

Command	Description
bba-group pppoe	Creates a PPPoE profile.

show ssg auto-domain exclude-profile

Note Effective with Cisco IOS Release 15.0(1)M, the **show ssg auto-domain exclude-profile** command is not available in Cisco IOS software.

To display the contents of an Autodomain exclude profile downloaded from the AAA server, use the **show ssg auto-domain exclude-profile** command in global configuration mode.

show ssg auto-domain exclude-profile

Syntax Description

This command has no arguments or keywords.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command in global configuration mode to display the contents of an Autodomain exclude-profile downloaded from the AAA server**.** If any exclude entries downloaded from the AAA server are removed by the **no exclude** {**apn** | **domain**} *name* command, these entries will not be displayed by the **show ssg auto-domain exclude-profile** command**.**

Examples

The following sample displays the contents of an Autodomain exclude profile downloaded from the AAA server. The report is self-explanatory.

```
Router# show ssg auto-domain exclude-profile

Exclude APN Entries Downloaded:

apn1.gprs   apr2.com

Exclude Domain Entries Downloaded:

cisco.com   abcd.com
```

Related Commands

Command	Description
exclude	Configures the Autodomain exclusion list.
mode extended	Enables extended mode for SSG Autodomain.
nat user-address	Enables NAT on Autodomain tunnel service.

Command	Description
select	Configures the Autodomain selection mode.
show ssg auto-domain exclude-profile	Adds to the Autodomain download exclusion list.
ssg enable	Enables SSG functionality.

show ssg binding

Note Effective with Cisco IOS Release 15.0(1)M, the **show ssg binding** command is not available in Cisco IOS software.

To display service names that have been bound to interfaces and the IP addresses to which they have been bound, use the **show ssg binding** command in privileged EXEC mode.

show ssg binding [**begin** *expression* | **exclude** *expression* | **include** *expression*]

Syntax Description

begin	(Optional) Begin with the line that contains *expression.*
expression	(Optional) Word or phrase used to determine what lines will be shown.
exclude	(Optional) Exclude lines that contain *expression.*
include	(Optional) Include lines that contain *expression.*

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(3)DC	This command was introduced on the Cisco 6400 node route processor.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to display services and the interfaces to which they have been bound.

Examples

The following example shows all service names that have been bound to interfaces:

```
Router# show ssg binding

WhipitNet            -> 192.168.1.1 (NHT)
Service1.com         -> 192.168.1.2 (NHT)
Service2.com         -> 192.168.1.3 (NHT)
Service3.com         -> 192.168.1.4 (NHT)
GoodNet              -> 192.168.2.1
Perftest             -> 192.168.1.6
```

Related Commands

Command	Description
clear ssg service	Removes a service.
show ssg service	Displays the information for a service.
ssg bind service	Specifies the interface for a service.

show ssg connection

Note Effective with Cisco IOS Release 15.0(1)M, the **show ssg connection** command is not available in Cisco IOS software.

To display the connections of a given Service Selection Gateway (SSG) host and a service name, use the **show ssg connection** command in privileged EXEC mode.

show ssg connection {*ip-address* | *network-id subnet-mask*} *service-name* [*interface*]

Syntax Description

ip-address	The IP address of an active SSG connection. This is always a subscribed host.
network-id	The IP network ID of an active SSG connection. This is always a subscribed host.
subnet-mask	The IP subnet mask of the subnet-based subscribed host.
service-name	Name of an active SSG connection.
interface	(Optional) IP address through which the host is connected.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(3)DC	This command was introduced on the Cisco 6400 node route processor.
12.2(2)B	The *interface* argument was added for the SSG Host Key feature.
12.2(4)B	This command was modified to display information about SSG prepaid billing.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(13)T	The modifications from Release 12.2(4)B were integrated into Cisco IOS Release 12.2(13)T.
12.3(1a)BW	This command was modified to display the MSISDN (Calling Station ID) used for service logon.
12.3(3)B	The modifications from Release 12.3(1a)BW were integrated into Cisco IOS Release 12.3(3)B.
12.3(7)T	The modifications from Release 12.3(1a)BW were integrated into Cisco IOS Release 12.3(7)T.
12.3(14)T	The *network-id* and *subnet-mask* arguments were added.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Examples

Prepaid Service Based on Volume: Example

The following example displays the SSG connection for a prepaid service that uses a volume-based quota:

```
Router# show ssg connection 10.10.1.1 InstMsg

------------------------ConnectionObject Content -----------------------

User Name:
Owner Host:10.10.1.1
Associated Service:InstMsg
Connection State:0 (UP)
Connection Started since:*00:25:58.000 UTC Tue Oct 23 2001
User last activity at:*00:25:59.000 UTC Tue Oct 23 2001
Connection Traffic Statistics:
          Input Bytes = 0, Input packets = 0
          Output Bytes = 0, Output packets = 0
          Quota Type = 'VOLUME', Quota Value = 100
Session policing disabled
```

Prepaid Service Based on Time: Example

The following example displays the SSG connection for a prepaid service that uses a time-based quota:

```
Router# show ssg connection 10.10.1.2 Prepaid-internet

------------------------ConnectionObject Content -----------------------
User Name:Host
Owner Host:10.10.1.2
Associated Service:Prepaid-internet
Connection State:0 (UP)
Connection Started since:*00:34:06.000 UTC Tue Oct 23 2001
User last activity at:*00:34:07.000 UTC Tue Oct 23 2001
Connection Traffic Statistics:
            Input Bytes = 0, Input packets = 0
            Output Bytes = 0, Output packets = 0
            Quota Type = 'TIME', Quota Value = 100
Session policing disabled
```

Autologin Service: Example

The following example shows the service connection for the autologon service to host 10.3.6.1:

```
Router# show ssg connection 10.3.6.1 autologin

------------------------ ConnectionObject Content -----------------------
User Name:autologin
Owner Host:10.3.6.1
Associated Service:autologin
Connection State:0 (UP)
Connection Started since:
*20:41:26.000 UTC Fri Jul 27 2001
User last activity at:*20:41:26.000 UTC Fri Jul 27 2001
Connection Traffic Statistics:
        Input Bytes = 0 (HI = 0), Input packets = 0
        Output Bytes = 0 (HI = 0), Output packets = 0
```

MSISDN: Example

The following sample output for the **show ssg connection** command shows the MSISDN that is used for service logon:

```
Router# show ssg connection 10.0.1.1 proxy2
```

```
------------------------ConnectionObject Content -----------------------
User Name: dev-user2
Owner Host: 10.0.1.1
Associated Service: proxy2
Calling station id: 12345
Connection State: 0 (UP)
Connection Started since: *17:44:59.000 GMT Sun Jul 6 2003
User last activity at: *17:44:59.000 GMT Sun Jul 6 2003
Connection Traffic Statistics:
        Input Bytes = 0, Input packets = 0
        Output Bytes = 0, Output packets = 0
Session policing disabled
```

Subnet-Based Subscriber: Example

The following sample output for the **show ssg connection** command shows the subnet mask of the subscribed host:

```
Router# show ssg connection 10.0.1.1 255.255.255.0 passthru

------------------------ConnectionObject Content -----------------------
User Name: dev-user2
Owner Host: 10.0.1.1 (Mask : 255.255.255.0)
Associated Service: passthru1
Calling station id: 00d0.792f.8054
Connection State: 0 (UP)
Connection Started since: *17:44:59.000 GMT Sun Jul 6 2004
User last activity at: *17:44:59.000 GMT Sun Jul 6 2004
Connection Traffic Statistics:
        Input Bytes = 0, Input packets = 0
        Output Bytes = 0, Output packets = 0
```

Table 9 describes the significant fields shown in the displays.

Table 9 show ssg connection Field Descriptions

Field	Description
User Name	Subscriber name supplied at authentication.
Owner Host	IP address and subnet mask of the subscribed host.
Associated Service	Service name of the connected service.
Calling station id	MSISDN used for service logon.
Connection State	State of activation (active or inactive).
Connection Started since	Time of host connection to the associated service.
User last activity at	Time of last data packet sent over this connection.
Input Bytes	Number of bytes received on this connection.
Input packets	Number of packets received on this connection.
Output Bytes	Number of bytes sent on this connection.
Output packets	Number of packets sent on this connection.
Quota Type	Form in which the quota value is expressed (time or volume).
Quota Value	Value of the quota (in bytes for volume or seconds for time).

Related Commands

Command	Description
clear ssg connection	Removes the connections of a given host and a service name.

show ssg dial-out exclude-list

Note Effective with Cisco IOS Release 15.0(1)M, the **show ssg dial-out exclude-list** command is not available in Cisco IOS software.

To display information about the Dialed Number Identification Service (DNIS) prefix profile and the DNIS exclusion list, use the **show ssg dial-out exclude-list** command in privileged EXEC mode.

show ssg dial-out exclude-list

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(15)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to display the DNIS profile name and all DNIS entries configured via CLI or downloaded from a authentication, authorization, and accounting (AAA) server.

Examples

The following example shows sample output for the **show ssg dial-out exclude-list** command:

```
Router# show ssg dial-out exclude-list

Exclude DNIS prefixes downloaded from profile exclude_dnis_aaa
```

Related Commands

Command	Description
dnis-prefix all service	Configures the dial-out global service.
download exclude-profile (ssg dial-out)	Downloads the DNIS exclusion list locally or from a AAA server.
exclude dnis-prefix	Configures the DNIS filter by adding a DNIS prefix to the DNIS exclusion list.
ssg dial-out	Enters SSG dial-out configuration mode.

show ssg direction

Note Effective with Cisco IOS Release 15.0(1)M, the **show ssg direction** command is not available in Cisco IOS software.

To display the direction of all interfaces for which a direction has been specified, use the **show ssg direction** command in privileged EXEC mode.

show ssg direction [**begin** *expression* | **exclude** *expression* | **include** *expression*]

Syntax Description

begin	(Optional) Begin with the line that contains *expression.*
expression	(Optional) Word or phrase used to determine what lines will be shown.
exclude	(Optional) Exclude lines that contain *expression.*
include	(Optional) Include lines that contain *expression.*

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(3)DC	This command was introduced on the Cisco 6400 node route processor.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to show all interfaces that have been specified as uplinks or downlinks.

Examples

The following example shows the direction of all interfaces that have been specified as uplinks or downlinks.

```
Router# show ssg direction

ATM0/0/0.10: Uplink
BVI1: Downlink
FastEthernet0/0/0: Uplink
```

Related Commands

Command	Description
ssg bind direction	Specifies an interface as a downlink or uplink interface.

show ssg host

Note Effective with Cisco IOS Release 15.0(1)M, the **show ssg host** command is not available in Cisco IOS software.

To display information about a Service Selection Gateway (SSG) subscriber and the current connections of the subscriber, use the **show ssg host** command in privileged EXEC mode. The command syntax of the **show ssg host** command depends on whether the SSG Port-Bundle Host Key feature is enabled.

When SSG Port-Bundle Host Key Is Not Enabled

show ssg host [*ip-address* | **count** | **username** [*subnet-mask*]]

When SSG Port-Bundle Host Key Is Enabled

show ssg host [*ip-address* | **count** | **username**] [*interface* [**username**] [*subnet-mask*]]

Syntax Description

ip-address	(Optional) Host IP address.
count	(Optional) Displays host object count, including inactive hosts.
username	(Optional) Displays all host usernames and IP addresses.
interface	(Optional) Downlink interface through which the host or subscriber is connected, such as ATM, Fast Ethernet, or Virtual-Access. For more information, use the question mark (?) online help function.
subnet-mask	(Optional) The IP subnet mask of the subnet-based subscribed host.

Command Default

If no argument is provided, all current connections are displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(3)DC	This command was introduced on the Cisco 6400 Node Route Processor (NRP).
12.2(2)B	The *interface* argument was added.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(15)B	This command was modified as follows: • Introduced syntax dependence on SSG host key. • Introduced **count** keyword. • Added fields to the output to display additional information about the status of hosts.
12.3(4)T	The modifications made in Cisco IOS Release 12.2(15)B were integrated into Cisco IOS Release 12.3(4)T.

Release	Modification
12.3(11)T	The output was enhanced to show information about the VPN routing/forwarding instance (VRF) that is associated with a host.
12.3(14)T	The *subnet-mask* argument was added.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

You can specify the Service Selection Gateway (SSG) downlink interface only when the SSG Port-Bundle Host Key feature is enabled. To enable the host key, enter the **ssg port-map** command in global configuration mode. To disable the host key, enter the **no ssg port-map** command.

Examples

Display All Active Hosts: Example

The following example shows all active hosts:

```
Router# show ssg host

1:10.3.1.1         [Host-Key 70.13.60.3:64]
2:10.3.6.1         [Host-Key 70.13.60.3:65]

### Active HostObject Count:2
```

Simple IP Host: Example

The following example shows information about a simple IP host with an IP address of 10.0.0.0:

```
Router# show ssg host 10.0.0.0

------------------------ HostObject Content -----------------------
Activated: TRUE
Interface:
User Name: user1
Owner Host: 10.0.0.0
Msg IP: 0.0.0.0 (0)
Host DNS IP: 0.0.0.0
Proxy logon from client IP: 10.0.48.3
    Device: PDSN (Simple IP)
    NASIP : 10.0.48.3
    SessID: 12345678
    APN   :
    MSID  : 5551000
    Timer : None
Maximum Session Timeout: 0 seconds
Host Idle Timeout: 60000 seconds
Class Attr: NONE
User policing disabled
User logged on since: *05:59:46.000 UTC Fri May 3 2002
User last activity at: *05:59:52.000 UTC Fri May 3 2002
SMTP Forwarding: NO
Initial TCP captivate: NO
TCP Advertisement captivate: NO
Default Service: NONE
DNS Default Service: NONE
Active Services: internet-blue;
AutoService: internet-blue;
Subscribed Services: internet-blue; iptv; games; distlearn; corporate; shop; banking;
vidconf;
```

```
Subscribed Service Groups: NONE
```

Mobile IP Host: Example

The following example shows information about a mobile IP host with an IP address of 10.0.0.0:

```
Router# show ssg host 10.0.0.0

----------------------- HostObject Content -----------------------
Activated: TRUE
Interface:
User Name: user1
Owner Host: 10.0.0.0
Msg IP: 0.0.0.0 (0)
Host DNS IP: 0.0.0.0
Proxy logon from client IP: 10.0.48.4
    Device: HA
    NASIP : 10.0.48.4
    SessID: 44444445
    APN   :
    MSID  : 5551001
    Timer : None
Maximum Session Timeout: 0 seconds
Host Idle Timeout: 60000 seconds
Class Attr: NONE
User policing disabled
User logged on since: *06:01:02.000 UTC Fri May 3 2002
User last activity at: *06:01:09.000 UTC Fri May 3 2002
SMTP Forwarding: NO
Initial TCP captivate: NO
TCP Advertisement captivate: NO
Default Service: NONE
DNS Default Service: NONE
Active Services: internet-blue;
AutoService: internet-blue;
Subscribed Services: internet-blue; iptv; games; distlearn; corporate; shop; banking;
vidconf;
Subscribed Service Groups: NONE
```

Two Hosts with the Same IP Address: Examples

The following example shows two host objects with the same IP address:

```
Router# show ssg host 10.3.1.1

SSG:Overlapping hosts for IP 10.3.1.1 at interfaces:FastEthernet0/0/0
Virtual-Access1
```

In this case, use the *interface* argument to uniquely identify the host:

```
Router# show ssg host 10.3.1.1 FastEthernet0/0/0
.
.
.
```

Note Note that the output produced by this command is the same as that produced by the command without the *interface* argument. The *interface* argument is used to uniquely identify a host only when there are overlapping host IP addresses.

The following example shows the usernames logged in to the active hosts:

```
Router# show ssg host username

   1:10.3.1.1        (active) Host name:pppoauser
```

```
   2:10.3.6.1        (active) Host name:ssguser2

### Total HostObject Count(including inactive hosts):2
```

Host Associated with a VRF: Example

The following sample output for the **show ssg host** command shows a VRF called "BLUE" associated with a host that has the IP address 10.0.0.2:

```
Router# show ssg host 10.0.0.2

------------------------ HostObject Content ----------------------
Activated: TRUE
Interface: Ethernet1/0   VRF Name: BLUE
User Name: prep-user1
Owner Host: 10.0.0.2
```

Subnet-Based Subscriber: Example

The following example shows information about a subnet-based subscriber with an IP address of 10.0.0.0 and a subnet mask of 255.255.255.0:

```
Router# show ssg host 10.0.0.0 255.255.255.0

------------------------ HostObject Content -----------------------
Activated: TRUE
Interface:
User Name: user1
Host IP : 10.0.0.0
Mask : 255.255.255.0
Msg IP: 0.0.0.0 (0)
Host DNS IP: 0.0.0.0
Maximum Session Timeout: 0 seconds
Host Idle Timeout: 60000 seconds
Class Attr: NONE
User policing disabled
User logged on since: *05:59:46.000 UTC Fri May 3 2004
User last activity at: *05:59:52.000 UTC Fri May 3 2004
SMTP Forwarding: NO
Initial TCP captivate: NO
TCP Advertisement captivate: NO
Default Service: NONE
DNS Default Service: NONE
Active Services: NONE
AutoService: NONE
Subscribed Services: passthru1; proxynat1; tunnel1; proxy1
Subscribed Service Groups: NONE
```

Table 10 describes the significant fields shown in the displays.

Table 10 show ssg host Field Descriptions

Field	Description
Activated:	State of host object. Can be activated or inactivated. Activated—IP address has been assigned to the host, and the host object was created successfully Inactivated—A host is inactivated in the following situations: • When SSG, acting as a RADIUS proxy, is waiting for the IP address of the host, the host object is created, but the state is inactive. • If a host that is using PPP logs off from SSG, but the virtual-access interface of that PPP host is still up, SSG moves the host object to the inactivated state.
Interface:	The interface on the SSG device from which the SSG host is routable.
User Name:	Username that is used to authenticate the host at the authentication, authorization, and accounting (AAA) server.
VRF Name:	VRF associated with the interface for the host.
Owner Host:	IP address and subnet mask assigned to host object.
Msg IP:	IP address of the messaging server. SSG notifies the messaging server of events such as the logging off of a host, an idle-timeout expiration, and a session-timeout expiration. The default messaging server is Subscriber Edge Services Manager (SESM).
Host DNS IP:	IP address of the Domain Name System (DNS) server of the host. This server will be used only if DNS queries cannot be forwarded to a DNS server for the services that are subscribed to by the host.
Device:	Type of device. Device types can be a home agent (HA), Packet Data Serving Node (PDSN), or Generic (for non-CDMA2000 devices).
SessID:	A numeric string derived from the attribute specified as the Session-Identifier.
Timer:	Timer type can be None, Wait for IP, Hand-off, or Wait for MSID.
Maximum Session Timeout:	Session timeout value (RADIUS attribute 27) defined in the user profile. The session timeout value is the amount of time for which the user will stay active after logging on. After this timer expires, the host object is deleted.
Host Idle Timeout:	Maximum amount of time that a host can stay idle (not forwarding any traffic) before the host is deleted from SSG.
Class Attr:	Class attribute (RADIUS attribute 25) defined in the user profile. The class attribute is sent in all host accounting records. This attribute is used by some accounting servers.

Table 10 show ssg host Field Descriptions (continued)

Field	Description
User logged on since:	Time at which the user logged on to SSG.
User last activity at:	Last time the user forwarded traffic via SSG.
Default Service:	This field is not currently supported.
DNS Default Service:	This field is not currently supported.
Active Services:	List of services to which the host has logged on.
AutoService:	List of services to which the host logged on at the time of SSG host logon. These services are defined in the user profile, and the user can access these services after logging on to SSG.
Subscribed Services:	List of services to which the host is able to log on.

Related Commands

Command	Description
clear ssg host	Removes a host object or a range of host objects.
ssg port-map	Enables the SSG port-bundle host key.

show ssg interface

Note Effective with Cisco IOS Release 15.0(1)M, the **show ssg interface** command is not available in Cisco IOS software.

To display information about Service Selection Gateway (SSG) interfaces, use the **show ssg interface** command in user EXEC or privileged EXEC mode.

show ssg interface [*interface* | **brief**]

Syntax Description

interface	(Optional) Specific interface for which to display information.
brief	(Optional) Gives brief information about each of the SSG interfaces and their usage.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(16)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command without any keywords or arguments to display information about all SSG interfaces.

Examples

The following example shows the **show ssg interface brief** command:

```
Router# show ssg interface brief

Interface   Direction          bindingtype    Status
ATM3/0.1    Uplink             Dynamic        Up
ATM3/0.2    Downlink           Static         Down
```

Related Commands

Command	Description
show ssg binding	Displays service names that have been bound to interfaces and the IP addresses to which they have been bound.
show ssg direction	Displays the direction of all interfaces for which a direction has been specified.
show ssg summary	Displays a summary of the SSG configuration.

show ssg multidomain ppp exclude-list

Note Effective with Cisco IOS Release 15.0(1)M, the **show ssg multidomain ppp exclude-list** command is not available in Cisco IOS software.

To display the contents of a PPP Termination Aggregation-Multidomain (PTA-MD) exclusion list, use the **show ssg multidomain ppp exclude-list** command in privileged EXEC mode.

show ssg multidomain ppp exclude-list

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(15)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

This command is used to verify the contents of a PTA-MD exclusion list.

Examples

Adding Domains to an Existing PTA-MD Exclusion List

In the following example, a PTA-MD exclusion list that already includes “cisco”, “motorola”, “nokia”, and “voice-stream” is downloaded from the authentication, authorization, and accounting (AAA) server. After the exclusion list is downloaded, “microsoft” and “sun” are added to the exclusion list.

The exclusion list currently on the AAA server includes “cisco”, “motorola”, “nokia”, and “voice-stream”:

```
user = pta_md{
profile_id = 119
profile_cycle = 2
member = SSG-DEV
radius=6510-SSG-v1.1 {
check_items= {
2=cisco
}
reply_attributes= {
9,253="XPcisco"
9,253="XPmotorola"
9,253="XPnokia"
9,253="XPvoice-stream"
```

In the following example, the PTA-MD exclusion list is downloaded to the router from the AAA server. The password to download the exclusion list is “cisco”. After the PTA-MD exclusion list is downloaded, “microsoft” and “sun” are added to the list using the router command-line interface (CLI).

```
ssg multidomain ppp
 download exclude-profile pta_md cisco
 exclude domain microsoft
 exclude domain sun
```

The enhancements to the exclusion list are then verified:

```
Router# show ssg multidomain ppp exclude-list

Profile name :pta_md
1   cisco
2   motorola
3   nokia
4   voice-stream

Domains added via CLI :
1   microsoft
2   sun
```

Related Commands

Command	Description
download exclude-profile (SSG PTA-MD)	Downloads the PTA-MD exclusion list from the AAA server to the router.
exclude (SSG PTA-MD)	Adds a domain name to the existing PTA-MD exclusion list.
ssg multidomain ppp	Enters PTA-MD configuration mode.

show ssg next-hop

Note Effective with Cisco IOS Release 15.0(1)M, the **show ssg next-hop** command is not available in Cisco IOS software.

To display the next-hop table, use the **show ssg next-hop** command in privileged EXEC mode.

show ssg next-hop [**begin** *expression* | **exclude** *expression* | **include** *expression*]

Syntax Description

begin	(Optional) Displays lines beginning with the line that contains *expression.*
expression	(Optional) Word or phrase used to determine what lines will be shown.
exclude	(Optional) Excludes lines that contain *expression.*
include	(Optional) Includes lines that contain *expression.*

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(3)DC	This command was introduced on the Cisco 6400 node route processor.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to display all next-hop IP addresses.

Examples

The following example shows the next-hop table:

```
Router# show ssg next-hop

Next hop table loaded from profile prof-nhg:
        WhipitNet            -> 192.168.1.6
        Service1.com         -> 192.168.1.3
        Service2.com         -> 192.168.1.2
        Service3.com         -> 192.168.1.1
        GoodNet              -> 192.168.1.2
        Perftest             -> 192.168.1.5
End of next hop table.
```

Related Commands

Command	Description
clear ssg next-hop	Removes the next-hop table.
ssg next-hop download	Downloads the next-hop table from a RADIUS server.

show ssg open-garden

Note Effective with Cisco IOS Release 15.0(1)M, the **show ssg open-garden** command is not available in Cisco IOS software.

To display a list of all configured open garden services, use the **show ssg open-garden** command in privileged EXEC mode.

show ssg open-garden

Syntax Description

This command has no keywords or arguments.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(5)DC	This command was introduced on the Cisco 6400 series node route processor.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Examples

In the following example, all configured open garden services are displayed:

```
Router# show ssg open-garden

nrp1-nrp2_og1
nrp1-nrp2_og2
nrp1-nrp2_og3
nrp1-nrp2_og4
```

Related Commands

Command	Description
local-profile	Configures a local service profile.
ssg open-garden	Designates a service, defined in a local service profile, as an open garden service.
ssg service-search-order	Specifies the order in which SSG searches for a service profile.

show ssg pass-through-filter

Note Effective with Cisco IOS Release 15.0(1)M, the **show ssg pass-through-filter** command is not available in Cisco IOS software.

To display the downloaded filter for transparent pass-through, use the **show ssg pass-through-filter** command in privileged EXEC mode.

show ssg pass-through-filter [**begin** *expression* | **exclude** *expression* | **include** *expression*]

Syntax Description

begin	(Optional) Begin with the line that contains *expression.*
expression	(Optional) Word or phrase used to determine what lines will be shown.
exclude	(Optional) Exclude lines that contain *expression.*
include	(Optional) Include lines that contain *expression.*

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(3)DC	This command was introduced on the Cisco 6400 node route processor.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to display the downloaded transparent pass-through filter. The filter prevents pass-through traffic from accessing the specified IP address and subnet mask combinations. The filter is set using the **ssg pass-through** command.

To display a filter defined on the command line, use the **show running-config** command.

Examples

The following example shows the pass-through filter:

```
Router# show ssg pass-through-filter

        Service name:  filter01
        Password:      cisco

        Direction:     Uplink

Extended IP access list (SSG ACL)
    permit tcp 172.16.6.0 0.0.0.255 any eq telnet
    permit tcp 172.16.6.0 0.0.0.255 192.168.250.0 0.0.0.255 eq ftp
```

Related Commands

Command	Description
clear ssg pass-through-filter	Removes the downloaded filter for transparent pass-through.
ssg pass-through	Enables transparent pass-through.

show ssg pending-command

Note Effective with Cisco IOS Release 15.0(1)M, the **show ssg pending-command** command is not available in Cisco IOS software.

To display current pending commands, such as next-hop or filters, use the **show ssg pending-command** command in privileged EXEC mode.

show ssg pending-command

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(3)DC	This command was introduced on the Cisco 6400 node route processor.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to display the current pending commands.

Examples

The following example shows the pending commands:

```
Router# show ssg pending-command

SSG pending command list:
    ssg bind service Service1.com 192.168.103.1
    ssg bind service Perftest206 192.168.104.5
```

Related Commands

Command	Description
clear ssg pending-command	Removes all pending commands.

show ssg port-map ip

Note Effective with Cisco IOS Release 15.0(1)M, the **show ssg port-map ip** command is not available in Cisco IOS software.

To display information about a particular port bundle, use the **show ssg port-map ip** command in privileged EXEC mode.

show ssg port-map ip *ip-address* **port** *port-number*

Syntax Description

ip-address	IP address used to identify the port bundle.
port *port-number*	TCP port number used to identify the port bundle.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)B	This command was introduced on the Cisco 6400 series.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3(11)T	This command was modified to display the downlink VRF associated with the port bundle.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

This command displays the following information about a port bundle:

- Port maps in the port bundle
- IP address of the subscriber
- Interface through which the subscriber is connected
- Downlink VRF

Examples

The following is sample output for the **show ssg port-map ip** command:

```
Router# show ssg port-map ip 192.168.0.1 port 64

State = RESERVED
Subscriber Address = 10.1.1.1
Downlink Interface = Ethernet1/0
Downlink VRF = BLUE

Port-mappings:-

Subscriber Port:   1           Mapped Port:   1039
```

Table 11 describes the significant fields shown in the display.

Table 11 show ssg port-map ip Field Descriptions

Field	Description
State	Port bundle status.
Subscriber Address	Subscriber IP address.
Downlink Interface	Interface through which the subscriber is connected.
Downlink VRF	VRF associated with the port bundle.
Port-mappings	Port maps in the port bundle.
Subscriber Port	Subscriber port number.
Mapped Port	Port assigned by SSG.

Related Commands

Command	Description
show ssg port-map status	Displays information on port bundles.

show ssg port-map status

Note Effective with Cisco IOS Release 15.0(1)M, the **show ssg port-map status** command is not available in Cisco IOS software.

To display information on port bundles, use the **show ssg port-map status** command in privileged EXEC mode.

show ssg port-map status [**free** | **reserved** | **inuse**]

Syntax Description

free	(Optional) Lists the port bundles that are in the "free" state for each bundle group.
reserved	(Optional) Lists the port bundles that are in the "reserved" state for each bundle group. Also displays the associated subscriber IP address and interface for each port bundle.
inuse	(Optional) Lists the port bundles that are in the "inuse" state for each bundle group. Also displays the associated subscriber IP address and interface for each port bundle.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)B	This command was introduced on the Cisco 6400 series.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Entered without any keywords, the command displays a summary of all port-bundle groups, including the following information:

- A list of port-bundle groups
- Port-bundle length
- Number of free, reserved, and in-use port bundles in each group

Examples

Display All Bundles Example

The following example shows output for the **show ssg port-map status** command with no keywords:

```
Router# show ssg port-map status

Bundle-length = 4

Bundle-groups:-
```

```
IP Address              Free Bundles            Reserved Bundles         In-use Bundles
10.13.60.2                      4032                    0                       0
```

Table 12 describes the significant fields shown in the display.

Table 12 show ssg port-map status Field Descriptions

Field	Description
Bundle-length	The bundle-length value indicates the number of ports per bundle and the number of bundles per bundle group.
Bundle-groups	List of bundle groups.
IP Address	IP address of a bundle group.
Free Bundles	Number of free bundles in the specified bundle group.
Reserved Bundles	Number of reserved bundles in the specified bundle group.
In-use Bundles	Number of in-use bundles in the specified bundle group.

Display In-Use Bundles Example

The following example shows output for the **show ssg port-map status** command with the **inuse** keyword:

```
Router# show ssg port-map status inuse

Bundle-group 10.13.60.2 has the following in-use port-bundles:-

Port-bundle             Subscriber Address              Interface

64                      10.10.3.1                       Virtual-Access2
```

Table 13 describes the significant fields shown in the display.

Table 13 show ssg port-map status inuse Field Descriptions

Field	Description
Port-bundle	Port-bundle number.
Subscriber Address	Subscriber IP address of the subscriber.
Interface	Interface through which the subscriber is connected.

Related Commands

Command	Description
show ssg port-map ip	Displays information on a particular port bundle.

show ssg prepaid default-quota

Note Effective with Cisco IOS Release 15.0(1)M, the **show ssg prepaid default-quota** command is not available in Cisco IOS software.

To display the values of the Service Selection Gateway (SSG) prepaid default quota counters, use the **show ssg prepaid default-quota** command in privileged EXEC mode.

show ssg prepaid default-quota

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(11)T	This command was introduced.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

SSG maintains two counters to keep track of the number of times the SSG prepaid default quota has been allotted. One counter is for the total number of default quotas allotted by SSG (irrespective of how many times the prepaid server has become available and unavailable). The other counter keeps track of the number of default quotas allotted by SSG during the latest instance of prepaid server unavailability.

Note that the value of the counter for currently allocated default quotas will be zero when the prepaid billing server is available. The counter for currently allocated default quotas restarts at 1 each time the prepaid billing server becomes unavailable.

The **clear ssg prepaid default-quota** command clears the SSG default quota counters.

Examples

The following example shows sample output for the **show ssg prepaid default-quota** command:

```
Router# show ssg prepaid default-quota

### Total default quotas allocated since this counter was last cleared:10

    Default Quota Threshold:100
    Currently allocated Default Quotas:4
```

Table 14 describes the significant fields shown in the display.

Table 14 show ssg prepaid default-quota Field Descriptions

Field	Description
Total default quotas allocated since this counter was last cleared	Total number of default quotas allocated by SSG since the last time the **clear ssg prepaid default-quota** command was entered.
Default Quota Threshold	The maximum number of default quotas that SSG will allocate each time the prepaid billing server is unavailable. This value can be configured by using the **ssg prepaid threshold** command.
Currently allocated Default Quotas	Number of default quotas allocated by SSG during the current instance of prepaid billing server unavailability.

Related Commands

Command	Description
clear ssg prepaid default-quota	Clears the SSG prepaid default quota counters.
ssg prepaid threshold	Configures an SSG prepaid threshold value.

show ssg radius-proxy

Note Effective with Cisco IOS Release 15.0(1)M, the **show ssg radius-proxy** command is not available in Cisco IOS software.

To display a list of all RADIUS proxy clients, details of a particular RADIUS proxy client, or the pool of IP addresses configured for a router or for a specific domain, use the **show ssg radius-proxy** command in privileged EXEC mode.

show ssg radius-proxy [*ip-address* [**vrf** *vrf-name*]] | [**address-pool** [**domain** *domain-name*] [**free** | **inuse**]]

Syntax Description

ip-address	(Optional) Details for the RADIUS proxy client at this IP address.
vrf *vrf-name*	(Optional) Details for the RADIUS proxy client associated with the specified VPN routing/forwarding (VRF) instance.
address-pool	(Optional) IP addresses configured in an IP pool.
domain	(Optional) IP addresses configured for a specific domain.
domain-name	(Optional) Name of the domain to display.
free	(Optional) IP addresses currently available in the free pool.
inuse	(Optional) IP addresses currently in use.

Command Default

Displays a list of RADIUS proxy clients.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(15)B	This command was enhanced to allow display of a list of RADIUS proxy clients.
12.3(4)T	The enhancements from Cisco IOS Release 12.2(15)B were integrated into Cisco IOS Release 12.3(4)T.
12.3(11)T	This command was enhanced to display information about VRFs associated with RADIUS proxy clients.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use the **show ssg radius-proxy** command without any keywords or arguments to display a list of RADIUS proxy clients. This command also displays the IP addresses, device types, timers, and the number of proxy users for each proxy client. Use the *ip-address* argument to display the full list of proxy users for the specified RADIUS proxy client.

Use the **address-pool** keyword to display the IP address pools configured for a router or for a specific domain. You can also display which IP addresses are available or are in use.

Examples

The following example shows how to display a list of RADIUS proxy clients:

```
Router# show ssg radius-proxy

::::: SSG RADIUS CLIENT TABLE :::::

Client IP       VRF             Device type     Users
10.0.0.2       Global          PDSN            2
10.1.1.1        BLUE            HA              1
```

The following example shows how to display details about the RADIUS proxy client at IP address 172.16.0.0:

```
Router# show ssg radius-proxy 172.16.0.0

::::: SSG RADIUS PROXY LOGON TABLE :::::
User                    SessionID       Host IP           Timer           IP Tech
user1                    12345678        50.0.0.100      None            Simple
user1                    12345679        (no host)         None            Mobile
```

The following example shows how to display information for IP addresses in the IP address pool:

```
Router# show ssg radius-proxy address-pool

Global Pool:  Free Addresses= 10234   Inuse Addresses= 0
```

The following example shows how to display information about the IP addresses in the IP address pool in the domain called “ssg.com”:

```
Router# show ssg radius-proxy address-pool domain ssg.com

Domain Pool(ssg.com):  Free Addresses= 20   Inuse Addresses= 10
```

The following example shows how to display information about the IP addresses in the IP address pool for the domain called “ssg.com” that are currently in use:

```
Router# show ssg radius-proxy address-pool domain ssg.com inuse

Inuse Addresses in Domain Pool(ssg.com):10
10.1.5.1
10.1.5.2
10.1.5.3
10.1.5.4
10.1.5.5
10.1.5.6
10.1.5.7
10.1.5.8
10.1.5.9
10.1.5.10
```

The following example shows how to display information about the IP addresses in the IP address pool for the domain called “ssg.com” that are currently available:

```
Router# show ssg radius-proxy address-pool domain ssg.com free

Free Addresses in Domain Pool(ssg.com):20
10.1.5.11
10.1.5.12
10.1.5.13
10.1.5.14
10.1.5.15
10.1.5.16
10.1.5.17
10.1.5.18
10.1.5.19
10.1.5.20
10.1.5.21
10.1.5.22
10.1.5.23
10.1.5.24
10.1.5.25
10.1.5.26
10.1.5.27
10.1.5.28
10.1.5.29
10.1.5.30
```

Table 15 describes significant fields shown in the displays.

Table 15 show ssg radius-proxy Field Descriptions

Field	Description
Client IP	IP address of the client device.
VRF	Name of the VRF associated with a RADIUS proxy client. The value “Global” indicates that the client is not associated with a VRF.
Device type	Type of client device. Device types can be PDSN, HA, or Generic (for non-CDMA2000 devices).
Users	Number of users connected to client device.
User	The user name for the end user.
SessionID	A numeric string derived from the attribute specified as the “Session-Identifier”.
Host IP	IP address of the user.
Timer	Timer type can be “None”, “Wait for IP”, “Hand-off” or “Wait for MSID”.
IP Tech	IP technology: simple or mobile.

Related Commands

Command	Description
debug radius	Displays information associated with RADIUS.
debug ssg ctrl-errors	Displays all error messages for control modules.
debug ssg ctrl-event	Displays all event messages for control modules.
debug ssg ctrl-packet	Displays packet contents handled by control modules.
debug ssg data	Displays all data-path packets.

Command	Description
show ssg binding	Displays service names that have been bound to interfaces and the interfaces to which they have been bound.
show ssg connection	Displays the connections of a given host and a service name.
show ssg service	Displays the information for a service.

show ssg service

Note Effective with Cisco IOS Release 15.0(1)M, the **show ssg service** command is not available in Cisco IOS software.

To display the information for a Service Selection Gateway (SSG) service, use the **show ssg service** command in privileged EXEC mode.

show ssg service [*service-name* [**begin** *expression* | **exclude** *expression* | **include** *expression*]]

Syntax Description

service-name	(Optional) Name of an active Service Selection Gateway (SSG) service.
begin	(Optional) Begin with the line that contains *expression.*
expression	(Optional) Word or phrase used to determine what lines will be shown.
exclude	(Optional) Exclude lines that contain *expression*.
include	(Optional) Include lines that contain *expression*.

Command Default

If no service name is provided, the command displays information for all services.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(3) DC	This command was introduced on the Cisco 6400 node route processor.
12.1(1) DC1	The output of this command was modified on the Cisco 6400 node route processor to display the following Service-Info Attributes when they are present in the proxy RADIUS service profile: • Service-Defined Cookie • Full Username Attribute
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.3(1a)BW	This command was modified to display the attribute filter that is set in the service profile.
12.3(3)B	The modifications in Release 12.3(1a)BW were integrated into Cisco IOS Release 12.3(3)B. The output for this command was modified to display information about default DNS redirection.
12.3(7)T	The modifications in Release 12.3(3)B were integrated into Cisco IOS Release 12.3(7)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to display connection information for a service.

Examples

L2TP Tunnel Service: Example

The following example shows the information for the L2TP tunnel service called "tunnel1". The attribute filter that is set in the service profile can be seen in the output.

```
Router# show ssg service tunnel1

------------------------ ServiceInfo Content -----------------------
Uplink IDB:  gw: 0.0.0.0
Name: tunnel1
Type: TUNNEL
Mode: CONCURRENT
Service Session Timeout: 0 seconds
Service Idle Timeout: 0 seconds
Service refresh timeleft: 99 minutes
No Authorization Required
Authentication Type: CHAP
Attribute Filter: 31
Session policing disabled
Reference Count: 1

DNS Server(s):
No Radius server group created. No remote Radius servers.

TunnelId: ssg1
TunnelPassword: cisco
HomeGateway Addresses: 172.0.0.1
ConnectionCount 1
Full User Name not used


Domain List: Included Network Segments:
        0.0.0.0/0.0.0.0

Active Connections:
        1   : RealIP=172.0.1.1, Subscriber=10.0.1.1

------------------------ End of ServiceInfo Content ----------------
```

Proxy Service: Example

The following example shows information for the proxy service called "serv1-proxy":

```
Router# show ssg service serv1-proxy

------------------------ ServiceInfo Content -----------------------
Uplink IDB:
Name:serv1-proxy
Type:PROXY
Mode:CONCURRENT
Service Session Timeout:0 seconds
Service Idle Timeout:0 seconds
Class Attr:NONE
Authentication Type:CHAP
Reference Count:1

Next Hop Gateway Key:my-key

DNS Server(s):Primary:10.13.1.5
```

```
Radius Server:IP=10.13.1.2, authPort=1645, acctPort=1646, secret=my-secret

Included Network Segments:
         10.13.0.0/255.255.0.0
Excluded Network Segments:
Full User Name Used
Service Defined Cookie exist


Domain List:service1.com;

Active Connections:
         1   :Virtual=255.255.255.255, Subscriber=10.20.10.2



------------------------ End of ServiceInfo Content ----------------
```

Table 16 describes the significant fields shown in the display.

Table 16 show ssg service Field Descriptions

Field	Description
Uplink IDB	Interface through which the service is reachable.
Name	Service name.
Type	Type of service.
Mode	One of the following values: Concurrent—user can log into this service and other services simultaneously. Sequential—user cannot log into this service simultaneously with other services.
Service Session Timeout	Period of time after which the session (SSG connection) will be terminated.
Service Idle Timeout	If the session (SSG connection) is idle for this many seconds, the session will be terminated.
Service refresh timeleft	Amount of time after which SSG will refresh the service profile.
Authentication Type	Type of authentication that will be used for proxy or tunnel services. Values are PAP and CHAP.
Attribute Filter	RADIUS attribute that is being filtered out from user authentication.
Next Hop Gateway Key	Defines the next-hop binding. Services can be bound to the next hop using next-hop gateways. The key to next-hop-gateway mapping is present in the next-hop profile.
DNS Server(s)	DNS server used for this service.
TunnelId	ID for tunneling services.
TunnelPassword	Password for tunneling services.
HomeGateway Addresses	IP address of the LNS.

Table 16 show ssg service Field Descriptions (continued)

Field	Description
Radius Server: IP authPort acctPort secret	Information about the RADIUS server where proxy users are authenticated for service connectivity.
Included Network Segments	IP address subnets that form the service network.
Excluded Network Segments	IP address subnets that are excluded from the service network.
Full User Name Used	Indicates that the RADIUS authentication and accounting requests use the full username (user@service).
Service Defined Cookie exist	Indicates that user-defined information is included in RADIUS authentication and accounting requests.
Domain List	List of domain names that belong to the service and can be resolved by the DNS server specified for this service.
Active Connections Virtual Subscriber	Lists the host IP address for active connections. The subscriber IP address is the IP address of the host. In cases where there is a service-defined NAT, the virtual IP address is not zero and is the IP address given by the service.

Related Commands

Command	Description
clear ssg service	Removes a service.
show ssg binding	Displays service names that have been bound to interfaces and the interfaces to which they have been bound.
ssg bind service	Specifies the interface for a service.

show ssg summary

Note Effective with Cisco IOS Release 15.0(1)M, the **show ssg summary** command is not available in Cisco IOS software.

To display a summary of the Service Selection Gateway (SSG) configuration, use the **show ssg summary** command in user EXEC or privileged EXEC mode.

show ssg summary

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(16)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to display information such as which SSG features are enabled, how many users are active, how many services are active, and what filters are active.

Examples

The following example shows the **show ssg summary** command:

```
Router# show ssg summary

SSG Features Enabled:
TCP Redirect: Unauthenticated, Service, Captive portal.
QOS: User policing, Session Policing.
Host Key: Enabled
```

Related Commands

Command	Description
show ssg binding	Displays service names that have been bound to interfaces and the IP addresses to which they have been bound.
show ssg direction	Displays the direction of all interfaces for which a direction has been specified.
show ssg interface	Displays information about SSG interfaces.

show ssg tcp-redirect group

Note Effective with Cisco IOS Release 15.0(1)M, the **show ssg tcp-redirect group** command is not available in Cisco IOS software.

To display information about the captive portal groups and the networks associated with those portal groups, use the **show ssg tcp-redirect group** command in privileged EXEC mode.

show ssg tcp-redirect group [*group-name*]

Syntax Description

group-name	(Optional) The previously defined name for the captive portal group.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(4)B	This command was introduced. This command replaced the **show ssg http-redirect group** command.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3(1a)BW	This command was modified to display the access lists that are associated with TCP redirection.
12.3(3)B	The modifications in Release 12.3(1a)BW were integrated into Cisco IOS Release 12.3(3)B.
12.3(7)T	The modifications in Release 12.3(3)B were integrated into Cisco IOS Release 12.3(7)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to display information about the captive portal groups and their associated networks as defined in your system.

If you omit the optional *group-name* argument, this command displays a list of all defined captive portal groups. If you specify the *group-name* argument, this command displays information about that group and its associated networks.

Examples

The following example shows how to display a list of all of the defined captive portal groups:

```
Router# show ssg tcp-redirect group

Current TCP redirect groups:
  SESM1
  SESM2
Default access-list: 101
Default unauthenticated user redirect group: None Set
Default service redirect group: None Set
```

```
Prepaid user default redirect group: None Set
SMTP forwarding group: None Set
Default initial captivation group: None Set
Default advertising  captivation group: None Set
```

Table 17 describes the significant fields shown in the display.

Table 17 show ssg tcp-redirect group Field Descriptions

Field	Description
Current TCP redirect groups	List of all TCP-redirect groups.
Default access-list	Name of the default access-list.
Default unauthenticated user redirect group	Name of the captivation group to which unauthenticated users are redirected.
Default service redirect group	Default service redirect group.
Prepaid user default redirect group	Name of the captivation group to which prepaid users are redirected.
SMTP forwarding group	SMTP redirection settings.
Default initial captivation group	Name of the default initial captivation group and duration of captivation.
Default advertising captivation group	Name of the default advertising captivation group and duration and frequency of advertising captivation.

The following example shows how to display a detailed description of the captive portal group called "RedirectServer":

```
Router# show ssg tcp-redirect group RedirectServer

TCP redirect group RedirectServer:
Showing all TCP servers (Address, Port):
  10.2.36.253, 8080, FastEthernet0/0
Networks to redirect to (network-list RedirectNw):
  172.16.10.0 /24
  172.20.0.0 /16
TCP port to redirect:
  80
```

Table 18 describes the significant fields shown in the display.

Table 18 show ssg tcp-redirect group group-name Field Descriptions

Field	Description
Showing all TCP servers (Address, Port)	List of all servers.
10.2.36.253	Server IP address.
8080	Server port number.
FastEthernet0/0	Interface on which this server is reachable.
Networks to redirect to	List of networks.
(network-list RedirectNw)	Network list name.
TCP port to redirect	Name of port list (if port list is used).

Related Commands

Command	Description
debug ssg tcp-redirect	Turns on debug information for the SSG TCP Redirect for Services feature.
network (ssg-redirect)	Adds an IP address to a named network list.
network-list	Defines a list of one or more IP networks that make up a named network list.
port (ssg-redirect)	Adds a TCP port to a named port list.
port-list	Defines a list of one or more TCP ports that make up a named port list and enters SSG-redirect-port configuration mode.
redirect captivate advertising default group	Configures the default captive portal group and duration and frequency for advertising.
redirect captivate initial default group duration	Selects a default captive portal group and duration of the initial captivation of users on account logon.
redirect port to	Marks a TCP port or named TCP port list for SSG TCP redirection.
redirect smtp group	Selects a captive portal group for redirection of SMTP traffic.
redirect unauthenticated-user to	Redirects the traffic from authenticated users to a specified captive portal group.
redirect unauthorized-service to	Sets a list of destination IP networks that can be redirected by a specified named captive portal group.
server (SSG)	Adds a server to a captive portal group.
server-group	Defines the group of one or more servers that make up a named captive portal group and enters SSG-redirect-group configuration mode.
show tcp-redirect mappings	Displays information about the TCP redirect mappings for hosts within your system.
ssg tcp-redirect	Enables SSG TCP redirect and enters SSG-redirect mode.

show ssg user transparent

Note Effective with Cisco IOS Release 15.0(1)M, the **show ssg user transparent** command is not available in Cisco IOS software.

To display a list of all the Service Selection Gateway (SSG) transparent autologon users, use the **show ssg user transparent** command in privileged EXEC mode.

show ssg user transparent

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(1a)BW	This command was introduced.
12.3(3)B	This command was integrated into Cisco IOS Release 12.3(3)B.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to display the IP addresses and the states of all transparent autologon users that are active on SSG. The transparent autologon user states are passthrough (TP), suspect (SP), unidentified (NR), and waiting for authorization (WA).

Examples

The following is sample output from the **show ssg user transparent** command:

```
Router# show ssg user transparent

10.10.10.10      Passthrough
10.11.11.11      Suspect
10.120.120.120  Authorizing

### Total number of transparent users: 3
```

Related Commands

Command	Description
ssg login transparent	Enables the SSG Transparent Autologon feature.

show ssg user transparent authorizing

Note Effective with Cisco IOS Release 15.0(1)M, the **show ssg user transparent authorizing** command is not available in Cisco IOS software.

To display a list of all Service Selection Gateway (SSG) transparent autologon users for whom authorization is in progress and who are waiting for authentication, authorization, and accounting (AAA) server response, use the **show ssg user transparent authorizing** command in privileged EXEC mode.

show ssg user transparent authorizing [**count**]

Syntax Description

count	(Optional) Displays the number of authorizing users.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(1a)BW	This command was introduced.
12.3(3)B	This command was integrated into Cisco IOS Release 12.3(3)B.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to display all SSG transparent autologon users that are waiting for authorization (WA).

Examples

The following is sample output from the **show ssg user transparent authorizing** command with the **count** keyword:

```
Router# show ssg user transparent authorizing count

### Total number of WA users : 1
```

Related Commands

Command	Description
ssg login transparent	Enables the SSG Transparent Autologon feature.

show ssg user transparent passthrough

Note Effective with Cisco IOS Release 15.0(1)M, the **show ssg user transparent passthrough** command is not available in Cisco IOS software.

To display information about Service Selection Gateway (SSG) transparent autologon pass-through users, use the **show ssg user transparent passthrough** command in privileged EXEC mode.

show ssg user transparent passthrough [*ip-address* | **count**]

Syntax Description

ip-address	(Optional) Display details for specified user IP address.
count	(Optional) Displays the number of pass-through users.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(1a)BW	This command was introduced.
12.3(3)B	This command was integrated into Cisco IOS Release 12.3(3)B.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to display all SSG transparent autologon pass-through (TP) users that are active on SSG.

Examples

The following is sample output from the **show ssg user transparent passthrough** command for the user having IP address 10.10.10.10:

```
Router# show ssg user transparent passthrough 10.10.10.10

User IP Address :       10.10.10.10
Session Timeout :       200 (seconds)
Idle Timeout :          100 (seconds)

User logged on since : *16:33:57.000 GMT Mon May 19 2003
User last activity at : *16:33:57.000 GMT Mon May 19 2003

Current Time : *16:35:17.000 GMT Mon May 19 2003
```

Related Commands

Command	Description
ssg login transparent	Enables the SSG Transparent Autologon feature.

show ssg user transparent suspect

Note Effective with Cisco IOS Release 15.0(1)M, the **show ssg user transparent suspect** command is not available in Cisco IOS software.

To display a list of all Service Selection Gateway (SSG) transparent autologon suspect (SP) user IP addresses, use the **show ssg user transparent suspect** command in privileged EXEC mode.

show ssg user transparent suspect [**count**]

Syntax Description

count	(Optional) Displays the number of suspect users.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(1a)BW	This command was introduced.
12.3(3)B	This command was integrated into Cisco IOS Release 12.3(3)B.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

An SSG transparent autologon suspect user is a user whose authentication, authorization, and accounting (AAA) authorization resulted in an Access Reject.

Examples

The following is sample output from the **show ssg user transparent suspect** command with and without the **count** keyword:

```
Router# show ssg user transparent suspect count

### Total number of SP users : 1

Router# show ssg user transparent suspect

        10.0.0.1


### Total number of SP users : 1

Router#
```

Related Commands

Command	Description
ssg login transparent	Enables the SSG Transparent Autologon feature.

show ssg user transparent unidentified

Note Effective with Cisco IOS Release 15.0(1)M, the **show ssg user transparent unidentified** command is not available in Cisco IOS software.

display a list of Service Selection Gateway (SSG) transparent autologon users for whom there is no response from the authentication, authorization, and accounting (AAA) server to an authorization request (unidentified users), use the **show ssg user transparent unidentified** command in privileged EXEC mode.

show ssg user transparent unidentified [**count**]

Syntax Description

count	(Optional) Displays the number of unidentified (NR) users.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(1a)BW	This command was introduced.
12.3(3)B	This command was integrated into Cisco IOS Release 12.3(3)B.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to display all SSG transparent autologon unidentified (NR) users that are active on the SSG.

Examples

The following is sample output from the **show ssg user transparent unidentified** command with and without the **count** keyword:

```
Router# show ssg user transparent unidentified count

### Total number of NR (Unidentified) users : 1

Router# show ssg user transparent unidentified

        10.0.0.2


### Total number of NR (Unidentified) users : 1

Router#
```

Related Commands

Command	Description
ssg login transparent	Enables the SSG Transparent Autologon feature.

show ssg vc-service-map

Note Effective with Cisco IOS Release 15.0(1)M, the **show ssg vc-service-map** command is not available in Cisco IOS software.

To display virtual circuit (VC)-to-service-name mappings, use the **show ssg vc-service-map** command in privileged EXEC mode.

show ssg vc-service-map [*vpi*/*vci* | **service** *service-name*]

Syntax Description

vpi/*vci*	(Optional) Virtual path identifier (VPI)/virtual channel identifier (VCI) value, including the slash; for example, 3/33.
service	(Optional) Displays the VCs mapped to a service name.
service-name	(Optional) Service name.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(5)DC	This command was introduced on the Cisco 6400 node route processor.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to display VC-to-service-name mappings.

Examples

The following example shows the VCs mapped to the service name “Worldwide”:

```
Router# show ssg vc-service-map service Worldwide

Interface  From       To         Service Name                Type
All        3  /33     None       Worldwide                   non-exclusive
```

Related Commands

Command	Description
ssg vc-service-map	Maps VCs to service names.

source ip

Note Effective with Cisco IOS Release 15.0(1)M, the **source ip** command is not available in Cisco IOS software.

To specify Service Selection Gateway (SSG) source IP addresses to which to map the destination IP addresses in subscriber traffic, use the **source ip** command in SSG portmap configuration mode. To remove this specification, use the **no** form of this command.

source ip {*ip-address* | *interface*}

no source ip {*ip-address* | *interface*}

Syntax Description

ip-address	SSG source IP address.
interface	Interface whose main IP address is used as the SSG source IP address.

Command Default

No default behavior or values.

Command Modes

SSG portmap configuration

Command History

Release	Modification
12.2(16)B	This command was introduced. This command replaces the **ssg port-map source ip** command.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

With the SSG Port-Bundle Host Key feature, SSG maps the destination IP addresses in subscriber traffic to specified SSG source IP addresses.

All SSG source IP addresses configured with the **source ip** command must be routable in the management network where the Cisco Service Selection Dashboard (SSD) or Subscriber Edge Services Manager (SESM) resides.

If the interface for the source IP address is deleted, the port-map translations will not work correctly.

Because a subscriber can have several simultaneous TCP sessions when accessing a web page, SSG assigns a bundle of ports to each subscriber. Because the number of available port bundles is limited, you can assign multiple SSG source IP addresses (one for each group of port bundles). By default, each group has 4032 bundles, and each bundle has 16 ports. To modify the number of bundles per group and the number of ports per bundle, use the **length** command.

Examples

The following example shows the SSG source IP address specified with an IP address and with specific interfaces:

```
ssg port-map
 source ip 10.0.50.1
 source ip Ethernet 0/0/0
 ssg port-map source ip Loopback 1
```

Related Commands

Command	Description
length (SSG)	Modifies the port-bundle length upon the next SSG reload.
ssg port-map	Enables the SSG port-bundle host key and enters SSG portmap configuration mode.

ssg aaa group prepaid

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg aa group prepaid** command is not available in Cisco IOS software.

To specify the server group to be used for Service Selection Gateway (SSG) prepaid authorization, use the **ssg aaa group prepaid** command in global configuration mode. To remove this specification, use the **no** form of this command.

ssg aaa group prepaid *server-group*

no ssg aaa group prepaid *server-group*

Syntax Description

server-group	Name of the server group to be used for SSG prepaid authorization.

Command Default

If a server group is not specified by using the **ssg aaa group prepaid** command, the default RADIUS server configured on the router will be used for SSG prepaid authorization.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(16)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

The **ssg aaa group prepaid** command allows you to configure a global server for SSG prepaid authorization. Configure the global server group by using the **aaa group server radius** command. Use the **ssg aaa group prepaid** command to attach the server group to SSG for SSG prepaid authorization.

Examples

The following example shows how to configure a global SSG prepaid authorization server:

```
aaa group server radius ssg_prepaid
 server 10.2.3.4 auth-port 1645 acct-port 1646
.
.
.
ssg aaa group prepaid ssg_prepaid
```

Related Commands

Command	Description
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.

ssg accounting

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg accounting** command is not available in Cisco IOS software.

To enable Service Selection Gateway (SSG) accounting, use the **ssg accounting** command in global configuration mode. To disable SSG accounting, use the **no** form of this command.

ssg accounting [**per-host**] [**per-service**] [**interval** *seconds*] [{**stop rate-limit** *records*}]

no ssg accounting [**per-host**] [**per-service**] [**interval** *seconds*] [{**stop rate-limit** *records*}]

Syntax Description

per-host	(Optional) Enables the sending of per-host accounting records only.
per-service	(Optional) Enables the sending of per-service accounting records only.
interval	(Optional) Specifies the interval at which accounting updates are sent to the accounting server.
seconds	(Optional) Number of seconds after which an accounting update will be sent to the accounting server. The range is from 60 to 2,147,483,647 seconds, in increments of 60 seconds. The value entered will be rounded up to the next multiple of 60. Default is 600.
stop	(Optional) Enables rate-limiting of SSG accounting records.
rate-limit	(Optional) Specifies the number of accounting records sent per second.
records	(Optional) Number of accounting stop records sent per second. The range is from 10 to 5000.

Command Default

Accounting is enabled.
The interval is set at 600 seconds.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)DC	This command was introduced on the Cisco 6400 node route processor.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(16)B	The **per-host** and **per-service** keywords were added.
12.3(4)T	The **per-host** and **per-service** keywords were integrated into Cisco IOS Release 12.3(4)T.
12.3(14)T	The stop and rate-limit keywords and the records argument were integrated into Cisco IOS Release 12.3(14)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

The **ssg accounting** command enables the sending of start, stop, and interim accounting records for hosts and connections.

Examples

The following example shows how to enable the sending of per-host SSG accounting records at intervals of 60 seconds:

```
ssg accounting per-host interval 60
```

ssg attribute 44 suffix host ip

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg attribute 44 suffix host ip** command is not available in Cisco IOS software.

To enable the appending of a client IP address to an accounting session ID to create a unique SSG accounting session ID, use the **ssg attribute 44 suffix host ip** command in global configuration mode. To disable the appending of the IP address, use the **no** form of this command.

ssg attribute 44 suffix host ip

no ssg attribute 44 suffix host ip

Syntax Description

This command has no arguments or keywords.

Command Default

SSG does not append the client IP address to the accounting session ID.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(16)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use the **ssg attribute 44 suffix host ip** command to create a unique session ID by appending the client's IP address to the RADIUS accounting session number (acct-session-id). This functionality applies to accounting packets generated by SSG for host accounting or connection accounting records.

Examples

The following example enables the SSG unique session ID:

```
ssg attribute 44 suffix host ip
```

Related Commands

Command	Description
ssg accounting	Enables SSG accounting.

ssg auto-domain

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg auto-domain** command is not available in Cisco IOS software.

To enable Service Selection Gateway (SSG) Autodomain, use the **ssg auto-domain** command in global configuration mode. To remove all Autodomain configuration from the running configuration and to prevent further activation of autodomains, use the **no** form of this command.

ssg auto-domain

no ssg auto-domain

Syntax Description

This command has no arguments or keywords.

Command Default

Autodomain is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

To enable SSG Autodomain, use this command in global configuration mode. SSG must be enabled before the **ssg auto-domain** command can be entered.

Note The **ssg auto-domain** command enables basic Autodomain. In basic Autodomain, the profile downloaded from the AAA server for the Autodomain name is a service profile (either with or without SSG-specific attributes). By default, an attempt is made to find a valid service profile first based on Access Point Name (APN), then based on username. Use the **mode extended** command to configure Autodomain extended mode.

Use the **no ssg auto-domain** command to prevent further activations of autodomains and to remove all Autodomain configuration from the running-configuration. Subsequent reissuing of the **ssg auto-domain** command restores Autodomain to its former state.

Examples

The following example enables basic SSG Autodomain:

```
ssg enable
ssg auto-domain
```

Related Commands

Command	Description
download exclude-profile	Adds to the Autodomain download exclusion list.
exclude	Configures the Autodomain exclusion list.
mode extended	Enables extended mode for SSG Autodomain.
nat user-address	Enables NAT on Autodomain tunnel service.
select	Configures the Autodomain selection mode.
show ssg auto-domain exclude-profile	Displays the contents of an Autodomain exclude-profile downloaded from the AAA server.
ssg enable	Enables SSG functionality.

ssg auto-logoff arp

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg auto-logoff arp** command is not available in Cisco IOS software.

To configure Service Selection Gateway (SSG) to automatically log off hosts that have lost connectivity with SSG and to use the Address Resolution Protocol (ARP) ping mechanism to detect connectivity, use the **ssg auto-logoff arp** command in global configuration mode. To disable SSG Autologoff, use the **no** form of this command.

ssg auto-logoff arp [**match-mac-address**] [**interval** *seconds*]

no ssg auto-logoff arp

Syntax Description

match-mac-address	(Optional) Configures SSG to check the MAC address of a host each time that host performs an ARP ping.
interval *seconds*	(Optional) ARP ping interval, in seconds. The interval specified is rounded to the nearest multiple of 30. An interval of less than 30 is rounded up to 30 seconds. The default interval is 30 seconds.

Command Default

SSG autologoff is not enabled by default.
The default ARP ping interval is 30 seconds.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(15)B	The **match-mac-address** keyword was added.
12.3(4)T	The **match-mac-address** keyword was integrated into Cisco IOS Release 12.3(4)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use the **ssg auto-logoff arp** command to configure SSG to use the ARP ping mechanism to detect connectivity to hosts. Use the optional **match-mac-address** keyword to configure SSG to check the MAC address of a host each time that host performs an ARP ping. If the SSG finds that the MAC address of the host has changed, SSG automatically initiates the logoff of that host.

Note ARP ping should be used only in deployments in which all hosts are directly connected to SSG through a broadcast interface (such as an Ethernet interface) or a bridged interface (such as a routed bridge encapsulation (RBE) or an integrated routing and bridging (IRB) interface).

ARP request packets are smaller than Internet Control Message Protocol (ICMP) ping packets, so it is recommended that you configure SSG autologoff to use ARP ping in cases in which hosts are directly connected.

ICMP ping can be used in all types of deployments. Refer to the **ssg auto-logoff icmp** command reference page for more information about SSG autologoff using ICMP ping.

ARP ping will work only on hosts that have a MAC address. ARP ping will not work for PPP users because they do not have a MAC table entry.

ARP ping does not support overlapping IP addresses.

SSG autologoff that uses the ARP ping mechanism will not work for hosts with static ARP entries.

You can use only one method of SSG autologoff at a time: ARP ping or ICMP ping. If you configure SSG to use ARP ping after ICMP ping has been configured, the ICMP ping function will become disabled.

Examples

The following example shows how to enable SSG autologoff and to configure SSG to use ARP ping to detect connectivity to hosts:

```
ssg auto-logoff arp interval 60
```

The following example shows how to enable SSG MAC address checking for autologoff:

```
ssg auto-logoff arp match-mac-address
```

The following example shows how to enable SSG MAC address checking for autologoff and to specify an ARP ping interval of 60 seconds:

```
ssg auto-logoff arp match-mac-address interval 60
```

Related Commands

Command	Description
ssg auto-logoff icmp	Configures the SSG to automatically log off hosts that have lost connectivity with SSG and to use the ICMP ping mechanism to detect connectivity.

ssg auto-logoff icmp

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg auto-logoff icmp** command is not available in Cisco IOS software.

To configure Service Selection Gateway (SSG) to automatically log off hosts that have lost connectivity with SSG and to use the Internet Control Message Protocol (ICMP) ping mechanism to detect connectivity, use the **ssg auto-logoff icmp** command in global configuration mode. To disable SSG autologoff, use the **no** form of this command.

ssg auto-logoff icmp [**timeout** *milliseconds*] [**packets** *number*] [**interval** *seconds*]

no auto-logoff icmp

Syntax Description

timeout *milliseconds*	(Optional) ICMP ping response timeout. The default is 500 milliseconds.
packets *number*	(Optional) Number of ICMP ping packets that will be sent after a ping packet indicates that a host is unreachable. The default is 2 packets.
interval *seconds*	(Optional) ICMP ping interval, in seconds. The interval specified will be rounded to the nearest multiple of 30. An interval less than 30 will be rounded up to 30 seconds. The default interval is 30 seconds.

Command Default

SSG autologoff is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

When the **ssg auto-logoff icmp** command is specified, SSG will use the ICMP ping mechanism to detect connectivity to hosts.

Note ICMP ping may be used in all types of deployment situations.

ICMP ping supports overlapping IP addresses.

If a user is not reachable, a configured number of packets (p) will be sent, and each packet will be timed out (t). The user will be logged off in $p * t$ milliseconds after the first pinging attempt. If $p * t$ milliseconds is greater than the configured pinging interval, then the time taken to log off the host after

connectivity is lost will be greater than the configured autologoff interval. If parameters are configured this way, the following warning will be issued: "Hosts will be auto-logged off (*p* * *t*) msecs after connectivity is lost." When the pinging interval is less than *p* * *t*, the timeout process for a host that has become unreachable will be invoked when the pinging to that host is still occurring. However, because the timeout process will check the status of the host object and find that it is in a pinging state, the host will not be pinged again.

You can use only one method of SSG autologoff at a time: Address Resolution Protocol (ARP) ping or ICMP ping. If you configure SSG to use ARP ping after ICMP ping has been configured, the ICMP ping function will become disabled.

Default values will be applied if a value of zero is configured for any parameters.

The **ssg auto-logoff arp** command will configure SSG to use the ARP ping mechanism to detect connectivity to hosts. ARP ping should be used only in deployment situations in which all hosts are directly connected to the SSG through a broadcast interface such as an Ethernet interface or a bridged interface such as a routed bridge encapsulation or an integrated routing and bridging interface.

ARP request packets are smaller than ICMP ping packets, so it is recommended that you configure SSG autologoff to use ARP ping in situations in which hosts are directly connected. For more information about SSG autologoff that uses ARP ping, see the **ssg auto-logoff arp** command reference page.

Examples

The following example shows how to enable SSG autologoff. SSG will use ICMP ping to detect connectivity to hosts.

```
Router(config)# ssg auto-logoff icmp interval 60 timeout 300 packets 3
```

Related Commands

Command	Description
ssg auto-logoff arp	Configures the SSG to automatically log off hosts that have lost connectivity with SSG and to use the ARP ping mechanism to detect connectivity.

ssg bind direction

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg bind direction** command is not available in Cisco IOS software.

Note Effective with Cisco IOS Release 12.2(16)B, this command was replaced by the **ssg direction** command. The **ssg bind direction** command is still supported for backward compatibility, but support for this command may be removed in a future Cisco IOS release.

To specify an interface as a downlink or uplink interface, use the **ssg bind direction** command in global configuration mode. To disable the directional specification for the interface, use the **no** form of this command.

ssg bind direction {**downlink** | **uplink**} {**ATM** *atm-interface* | **Async** *async-interface* | **BVI** *bvi-interface* | **Dialer** *dialer-interface* | **Ethernet** *ethernet-interface* | **FastEthernet** *fastethernet-interface* | **Group-Async** *group-async-interface* | **Lex** *lex-interface* | **Loopback** *loopback-interface* | **Multilink** *multilink-interface* | **Null** *null-interface* | **Port-channel** *port-channel-interface* | **Tunnel** *tunnel-interface* | **Virtual-Access** *virtual-access-interface* | **Virtual-Template** *virtual-template-interface* | **Virtual-TokenRing** *virtual-tokenring-interface*}

no ssg bind direction {**downlink** | **uplink**} {**ATM** *atm-interface* | **Async** *async-interface* | **BVI** *bvi-interface* | **Dialer** *dialer-interface* | **Ethernet** *ethernet-interface* | **FastEthernet** *fastethernet-interface* | **Group-Async** *group-async-interface* | **Lex** *lex-interface* | **Loopback** *loopback-interface* | **Multilink** *multilink-interface* | **Null** *null-interface* | **Port-channel** *port-channel-interface* | **Tunnel** *tunnel-interface* | **Virtual-Access** *virtual-access-interface* | **Virtual-Template** *virtual-template-interface* | **Virtual-TokenRing** *virtual-tokenring-interface*}

Syntax Description

downlink	Specifies interface direction as downlink.
uplink	Specifies interface direction as uplink.
ATM	Indicates that the interface is ATM.
atm-interface	ATM interface.
Async	Indicates that the interface is asynchronous.
async-interface	Async interface.
BVI	Indicates that the interface is BVI.
bvi-interface	Bridge-Group Virtual Interface.
Dialer	Indicates that the interface is dialer.
dialer-interface	Dialer interface.
Ethernet	Indicates that the interface is IEEE 802.3 Ethernet.
ethernet-interface	Ethernet interface.
FastEthernet	Indicates that the interface is IEEE 802.3 Fast Ethernet.
fastethernet-interface	Fast Ethernet interface.
Group-Async	Indicates that the interface is group async.

group-async-interface	Group async interface.
Lex	Indicates that the interface is lex.
lex-interface	Lex interface.
Loopback	Indicates that the interface is loopback.
loopback-interface	Loopback interface.
Multilink	Indicates that the interface is multilink.
multilink-interface	Multilink interface.
Null	Indicates that the interface is null.
null-interface	Null interface.
Port-channel	Indicates that the interface is port channel.
port-channel-interface	Port channel interface.
Tunnel	Indicates that the interface is tunnel.
tunnel-interface	Tunnel interface.
Virtual-Access	Indicates that the interface is virtual access.
virtual-access-interface	Virtual access interface.
Virtual-Template	Indicates that the interface is virtual template.
virtual-template-interface	Virtual template interface.
Virtual-TokenRing	Indicates that the interface is virtual token ring.
virtual-tokenring-interface	Virtual token ring interface.

Command Default

All interfaces are configured as uplink interfaces by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(3)DC	This command was introduced on the Cisco 6400 node route processor.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(16)B	This command was replaced by the **ssg direction** command.
12.3(4)T	This command was replaced by the **ssg direction** command.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to specify an interface as downlink or uplink. An uplink interface is an interface to services; a downlink interface is an interface to subscribers.

Examples

The following example shows how to specify an ATM interface as a downlink interface:

```
configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
 ssg bind direction downlink ATM 0/0/0.10
```

Related Commands

Command	Description
show ssg binding	Displays service names that have been bound to interfaces and the interfaces to which they have been bound.

ssg bind service

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg bind service** command is not available in Cisco IOS software.

To specify the interface for a service, use the **ssg bind service** command in global configuration mode. To unbind the service and the interface, use the **no** form of this command.

ssg bind service *service-name* {*ip-address* | *interface-type interface-number*} [*distance-metric*]

no ssg bind service *service-name* {*ip-address* | *interface-type interface-number*} [*distance-metric*]

Syntax Description

service-name	Service name.
ip-address	IP address of the next-hop router.
interface-type	Type of interface.
interface-number	Number of the interface.
distance-metric	(Optional) Metric to be used to determine the path for upstream traffic. The range is from 1 to 255. Default is 0.

Command Default

A service is not bound to an interface.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(3)DC	This command was introduced on the Cisco 6400 node route processor.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.3(8)T	This command was modified to enable the configuration of interface redundancy for a service, and the *distance-metric* argument was added.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to bind a service to an interface. You can enter this command more than once in order to bind a service to more than one interface for interface redundancy.

Use the *distance-metric* argument to control the routing of upstream traffic. If more than one entry of the **ssg bind service** command for a service have the same metric, the upstream traffic will be load-balanced.

If a service is configured for multiple uplink interfaces, downstream traffic will be allowed on all the interfaces for any service bound to even one of those interfaces.

Examples

The following example shows the interface for the service defined as “MyService”:

```
ssg bind service MyService ATM 0/0/0.10
```

The following example shows uplink interface redundancy configured for the service “sample-service”. ATM interface 1/0.1 is configured as the primary interface and ATM interface 1/0.2 as the secondary interface.

```
ssg bind service sample-service atm 1/0.1
ssg bind service sample-service atm 1/0.2 100
```

Related Commands

Command	Description
clear ssg service	Removes a service.
show ssg binding	Displays service names that have been bound to interfaces and the interfaces to which they have been bound.
show ssg service	Displays the information for a service.

ssg default-network

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg default-network** command is not available in Cisco IOS software.

To specify the default network IP address or subnet and mask, use the **ssg default-network** command in global configuration mode. To disable the default network IP address and mask, use the **no** form of this command.

ssg default-network *ip-address mask*

no ssg default-network *ip-address mask*

Syntax Description

ip-address	Service Selection Gateway (SSG) default IP address or subnet.
mask	SSG default network destination mask.

Command Default

No default behavior or values.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(3)DC	This command was introduced on the Cisco 6400 node route processor.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to specify the first IP address or subnet that users will be able to access without authentication. This is the address where the Cisco Service Selection Dashboard (SSD) resides. After users enter the URL for the Cisco SSD, they will be prompted for a username and password. A mask provided with the IP address specifies the range of IP addresses that users will be able to access without authentication.

Examples

The following example shows a default network IP address, 192.168.1.2, and mask 255.255.255.255:

```
configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
 ssg default-network 192.168.1.2 255.255.255.255
```

ssg dfp ip

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg dfp ip** command is not available in Cisco IOS software.

To specify the interface between Service Selection Gateway (SSG) and a load-balancing device, use the **ssg dfp ip** command in global configuration mode. To remove this specification, use the **no** form of this command.

ssg dfp ip {*interface* | *ip-address*}

no ssg dfp ip {*interface* | *ip-address*}

Syntax Description

interface	Type and number of the interface between SSG and the load balancer.
ip-address	IP address of the SSG interface to the load balancer.

Command Default

An interface between SSG and the load balancer is not specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(11)T	This command was introduced.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

The interface between the load balancer and SSG must be configured on SSG, or SSG will not be able to hand load-balancing weights to the DFP agent.

The interface or the IP address configured with this command must be the same as the interface or IP address configured on the load balancer under the server configuration. The interface or IP address is sent in the DFP packet along with the weight to the load balancer. The load balancer uses this information to identify the server from which the weight was received. If the interface or IP address is not the same as that configured on the load balancer, the weight information will not be associated with the correct SSG.

The interface specified by the **ssg dfp ip** command should be a downlink interface.

Examples

The following examples show the configuration of the interface between SSG and load balancer and the corresponding configuration on the load-balancing device:

Configuration on SSG Device: Example

```
ssg enable
```

```
ssg dfp weight 25
ssg dfp ip Ethernet1/0
!
!
interface Ethernet1/0
 ip address 10.0.0.20 255.0.0.0
 duplex half
 pppoe enable
 ssg direction downlink
!
```

Configuration on Cisco IOS Server Load Balancing Device: Example

```
!
ip slb serverfarm SSGFARM
 real 10.0.0.20
  inservice
!
ip slb vserver VSSG
 virtual 10.8.8.8 tcp 0
 serverfarm SSGFARM
 inservice
!
ip slb dfp
 agent 10.0.0.20 655
!
```

Related Commands

Command	Description
ssg dfp weight	Specifies the DFP weight, which will be used to calculate load balancing among SSGs, for an SSG device.

ssg dfp weight

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg dfp weight** command is not available in Cisco IOS software.

To specify the Dynamic Feedback Protocol (DFP) weight used to calculate load balancing for a Service Selection Gateway (SSG) device, use the **ssg dfp weight** command in global configuration mode. To reset the weight to the default value of 100, use the **no** form of this command.

ssg dfp weight *weight*

no ssg dfp weight

Syntax Description

weight	Weight to be used in the DFP load-balancing algorithm for load balancing among SSGs. Range is from 0 to 100. 100 is the default. A higher weight indicates higher availability. A weight of zero indicates that a server has no availability.

Command Default

The default DFP weight is 100.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(11)T	This command was introduced.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

The DFP weight is used to calculate load balancing among SSGs.

You can use the **ssg dfp weight** command to prioritize SSGs that are being load-balanced. A higher weight indicates that the device can accept a heavier load.

Every time the DFP weight is changed by using the **ssg dfp weight** command, SSG sends the new weight to the DFP agent.

SSG calculates the weight that it hands over to the DFP agent on the basis of three factors:

- The DFP weight configured for the SSG
- CPU load
- Memory utilization

The DFP agent forwards the calculated weight to the load balancer.

Examples

The following example shows how to configure SSG with a DFP weight of 25:

```
ssg dfp weight 25
```

Related Commands

Command	Description
ssg dfp ip	Specifies the interface between SSG and the load-balancing device.

ssg dial-out

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg dial-out** command is not available in Cisco IOS software.

To enable the SSG L2TP Dial-Out feature and enter SSG dial-out configuration mode, use the **ssg dial-out** command in global configuration mode. To remove all SSG dial-out configurations, use the **no** form of this command.

ssg dial-out

no ssg dial-out

Syntax Description

This command has no arguments or keywords.

Command Default

The SSG L2TP Dial-Out feature is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to enter SSG dial-out configuration mode to configure the SSG L2TP Dial-Out feature. Use the **no** form of this command to remove all Service Selection Gateway (SSG) L2TP dial-out configurations.

Examples

The following example shows how to enable the SSG L2TP Dial-Out feature and enter SSG dial-out configuration mode:

```
Router(config)# ssg dial-out
Router(config-dial-out)#
```

Related Commands

Command	Description
dnis-prefix all service	Configures the dial-out global service.
download exclude-profile (ssg dial-out)	Downloads the DNIS exclusion list locally or from a AAA server.

Command	Description
exclude dnis-prefix	Configures the DNIS filter by adding a DNIS prefix to the DNIS exclusion list.
show ssg dial-out exclude-list	Displays information about the DNIS prefix profile and the DNIS exclusion list.

ssg direction

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg direction** command is not available in Cisco IOS software.

To configure an interface or range of subinterfaces as downlink or uplink, use the **ssg direction** command in interface configuration mode or subinterface configuration mode. To clear the directional specification, use the **no** form of this command.

ssg direction {**downlink** | **uplink** [**member** *group-name*]}

no ssg direction

Syntax Description

downlink	Specifies the interface direction as downlink. A downlink interface is an interface to subscribers.
uplink	Specifies the interface direction as uplink. An uplink interface is an interface to services.
member	(Optional) Specifies that the uplink interface is a member of a group of uplink interfaces that reach the same services.
group-name	(Optional) Name of the group of uplink services.

Command Default

An interface is neither uplink nor downlink.

Command Modes

Interface configuration (config-if)
Subinterface configuration (config-subif)

Command History

Release	Modification
12.2(16)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.3(8)T	The **member** keyword and *group-name* argument were added.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Service Selection Gateway (SSG) applies the concept of an interface direction, either uplink or downlink. It uses this direction when determining the forwarding path of an incoming packet. The **ssg direction** command allows you to specify a direction for an interface or a range of subinterfaces.

The **ssg direction** command allows you to configure the direction for a range of permanent virtual circuits (PVCs). All members of a range must have the same direction.

Before you can change a direction from uplink to downlink or vice versa, you must use the **no ssg direction** command to clear the direction.

The **ssg direction** command replaces the **ssg bind direction** command. If you reboot a router that uses an old configuration, the **ssg bind direction** commands will be converted to **ssg direction** commands until the **ssg bind direction** command is made obsolete. In a later release, the **ssg bind direction** command may no longer be supported.

Note An interface that does not exist will not be created as a result of the **ssg direction** command.

In cases where a service has a single next-hop IP address, the **ssg direction** uplink command can be used with the **member** keyword and *group-name* argument to group together uplink interfaces that share a common service and enable the interfaces to be treated similarly.

The group setting for an uplink interface cannot be changed when there are active services bound to that interface.

The **no** form of the **ssg direction** command can be used only when there are no active services bound to the uplink interface.

The command operates on a variety of interfaces, including async, group async, ATM, extended tag ATM (XTagATM), bridge group virtual (BVI), CTunnel, tunnel, dialer, IEEE 802.3 Ethernet, IEEE 802.3 Fast Ethernet, IEEE 802.3z GigabitEthernet, loopback, multilink Frame Relay (MFR) bundle, multilink group, Pragmatic General Multicast (PGM) Host (Vif), virtual access, virtual template, and virtual Token Ring.

Examples

The following example sets the direction of a Fast Ethernet interface to downlink while in interface configuration mode:

```
ssg enable
interface FastEthernet 1/0
 ssg direction downlink
```

The next example creates a range called “MyRange” and sets the direction of all subinterfaces in the range to downlink while in subinterface configuration mode:

```
ssg enable
interface ATM 1/0.1 point-to-point
 range MyRange pvc 1/32 1/42
 ssg direction downlink
```

Related Commands

Command	Description
range pvc	Defines a range of ATM PVCs.
show ssg direction	Displays the direction of all interfaces for which a direction has been specified.
show ssg interface	Displays SSG information about one or more interfaces.

ssg enable

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg enable** command is not available in Cisco IOS software.

To enable SSG, use the **ssg enable** command in global configuration mode. To disable SSG, use the **no** form of this command.

ssg enable

no ssg enable [**force-cleanup**]

Syntax Description

force-cleanup	(Optional) Unconfigures SSG and releases all resources that were acquired by SSG.

Command Default

SSG is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)DC	This command was introduced on the Cisco 6400 node route processor (NRP).
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(15)B	The **force-cleanup** keyword was added.
12.3(4)T	The **force-cleanup** keyword was integrated into Cisco IOS Release 12.3(4)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to enable SSG. If you enter the **ssg enable** command while the system is in the process of unconfiguring SSG, you will see a warning message, and the command will have no effect.

Use the **no ssg enable force-cleanup** command to unconfigure SSG and release all system resources for SSG.

Examples

The following example shows how to enable SSG:

```
Router(config)# ssg enable
```

The following example shows how to stop SSG packet processing and control events:

```
Router(config)# no ssg enable
```

The following example shows how to stop SSG packet processing and control events, unconfigure SSG, and release all SSG resources:

```
Router(config)# no ssg enable force-cleanup
```

ssg intercept dhcp

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg intercept dhcp** command is not available in Cisco IOS software.

To configure the Service Selection Gateway (SSG) to force subscribers to get IP addresses from their ISPs using Dynamic Host Configuration Protocol (DHCP), use the **ssg intercept dhcp** command in global configuration mode. To disable IP address assignment from the ISP via DHCP, use the **no** form of this command.

ssg intercept dhcp

no ssg intercept dhcp

Syntax Description

This command has no arguments or keywords.

Command Default

SSG performs Network Address Translation (NAT) between the IP address assigned by the ISP with the original IP address of the subscriber.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use the **ssg intercept dhcp** command to force subscribers to request IP addresses from their ISPs using DHCP.

When a subscriber's router acts either as an IOS DHCP server or an IOS DHCP relay agent and the subscriber is a DHCP client, then configuring SSG/DHCP Awareness will remove the SSG host object. When an active host object receives a DHCPRELEASE or when the DHCP lease for an active host object expires, the SSG host object is removed.

For more information on the **ssg intercept dhcp** command, see the *Cisco IOS Intelligent Service Gateway Configuration Guide.*

Examples

The following example shows how to enable the IP address assignment from the ISP via DHCP:

```
ssg intercept dhcp
```

Related Commands

Command	Description
debug ssg dhcp	Enables the display of control errors and events related to SSG-DHCP IP address allocation.

ssg local-forwarding

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg local-forwarding** command is not available in Cisco IOS software.

To enable Service Selection Gateway (SSG) to forward packets locally, use the **ssg local-forwarding** command in global configuration mode. To disable local forwarding, use the **no** form of this command.

ssg local-forwarding

no ssg local-forwarding

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(1) DC1	This command was introduced on the Cisco 6400 node route processor.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Examples

The following example enables local forwarding:

```
ssg local-forwarding
```

ssg login transparent

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg login transparent** command is not available in Cisco IOS software.

To enable the Service Selection Gateway (SSG) Transparent Autologon feature and enable transparent auto-logon configuration mode, use the **ssg login transparent** command in global configuration mode. To disable the Transparent Autologon feature, remove all the commands that were configured under transparent auto-logon mode, log off all the transparent autologon users, and refuse new logons, use the **no** form of this command.

ssg login transparent

no ssg login transparent

Syntax Description

This command has no arguments or keywords.

Command Default

The SSG Transparent Autologon feature is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(1a)BW	This command was introduced.
12.3(3)B	This command was integrated into Cisco IOS Release 12.3(3)B.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Examples

The following example enables the SSG Transparent Autologon feature:

```
ssg login transparent
```

Related Commands

Command	Description
show ssg user transparent	Displays a list of all the SSG transparent autologon users.

ssg maximum host

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg maximum host** command is not available in Cisco IOS software.

To limit the number of user connections (hosts) allowed on a Service Selection Gateway (SSG) device, use the **ssg maximum host** command in global configuration mode. To remove the limitation on the number of hosts, use the **no** form of this command.

ssg maximum host *number-of-hosts*

no ssg maximum host *number-of-hosts*

Syntax Description

number-of-hosts	Limits the number of host objects allowed on an SSG device. Range: 1 to 2147483647.

Command Default

Unlimited hosts are allowed on an SSG device.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(2)T	This command was introduced.
15.0(1)M	This command was removed.

Usage Guidelines

This command prevents resource exhaustion on a router by limiting the number of host connections. When the router reaches the maximum number of connections, it refuses any new connections. As users log out, new users are allowed to connect.

This command limits only the number of host connections; it does not limit the number of services available to users.

Examples

The following example limits the number of host connections to 1,000:

```
Router(config)# ssg maximum host 1000
```

Related Commands

Command	Description
ssg maximum service	Limits the number of services available to SSG users.
user passthrough maximum	Limits the number of SSG transparent autologon users on an SSG device.

ssg maximum service

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg maximum service** command is not available in Cisco IOS software.

To limit the number of services available to a user on a Service Selection Gateway (SSG) device, use the **ssg maximum service** command in global configuration mode. To remove the limitation on the number of services, use the **no** form of this command.

ssg maximum service *number-of-services*

no ssg maximum service *number-of-services*

Syntax Description

number-of-services	Limits the number of services available to a user on an SSG device. The valid range of services is 1 to 20.

Command Default

Users have up to 20 services available.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(2)T	This command was introduced. This command replaces the **ssg maxservice** command.
15.0(1)M	This command was removed.

Usage Guidelines

This command enables you to limit the number of services available to a user. This command replaces the **ssg maxservice** command. If you issue the **ssg maxservice** command and save your configuration, the saved configuration shows the **ssg maximum service** command.

Examples

The following example limits the number of user services to 10:

```
Router(config)# ssg maximum service 10
```

Related Commands

Command	Description
ssg maximum host	Limits the number of host connections on an SSG device.

ssg maxservice

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg maxservice** command is not available in Cisco IOS software.

Note Effective with Cisco IOS Release 12.4(2)T, the **ssg maxservice** command is replaced by the **ssg maximum service** command. See the **ssg maximum service** command for more information.

To set the maximum number of services per user, use the **ssg maxservice** command in global configuration mode. To reset the maximum number of services per user to the default, use the **no** form of this command.

ssg maxservice *number*

no ssg maxservice

Syntax Description

number	Maximum number of services per user. The minimum value is 0; the maximum is 20.

Command Default

The default maximum number of services per user is 20.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(3)DC	This command was introduced on the Cisco 6400 node route processor.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
12.4(2)T	This command was replaced by the **ssg maximum service** command.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to limit the number of services to which a user can be logged on simultaneously.

Examples

The following example shows how to set the maximum number of services per user to 10:

```
ssg maxservice 10
```

ssg multidomain ppp

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg multidomain ppp** command is not available in Cisco IOS software.

To enter PPP Termination Aggregation-Multidomain (PTA-MD) configuration mode, use the **ssg multidomain ppp** command in global configuration mode. To disable all PTA-MD configurations, use the **no** form of this command.

ssg multidomain ppp

no ssg multidomain ppp

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

It is important to note that the **no** form of this command disables everything configured for PTA-MD. If you want to exit PTA-MD configuration mode, enter the **exit** command.

Examples

Adding Domains to an Existing PTA-MD Exclusion List

In the following example, a PTA-MD exclusion list that already includes “cisco”, “motorola”, “nokia”, and “voice-stream” is downloaded from the AAA server. After the exclusion list is downloaded, “microsoft” and “sun” are added to the exclusion list.

The exclusion list currently on the AAA server includes “cisco”, “motorola”, “nokia”, and “voice-stream”:

```
user = pta_md{
profile_id = 119
profile_cycle = 2
member = SSG-DEV
radius=6510-SSG-v1.1 {
check_items= {
2=cisco
```

```
}
reply_attributes= {
9,253="XPcisco"
9,253="XPmotorola"
9,253="XPnokia"
9,253="XPvoice-stream"
```

In the following example, the PTA-MD exclusion list is downloaded to the router from the AAA server. The password to download the exclusion list is “cisco”. After the PTA-MD exclusion list is downloaded, “microsoft” and “sun” are added to the list using the router CLI:

```
ssg multidomain ppp
 download exclude-profile pta_md cisco
 exclude domain microsoft
 exclude domain sun
```

The enhancements to the exclusion list are then verified:

```
Router# show ssg multidomain ppp exclude-list

Profile name :pta_md
1   cisco
2   motorola
3   nokia
4   voice-stream

Domains added via CLI :
1   microsoft
2   sun
```

Related Commands

Command	Description
download exclude-profile (SSG PTA-MD)	Downloads the PTA-MD exclusion list on the AAA server to the router.
exclude (SSG PTA-MD)	Adds a domain name to the existing PTA-MD exclusion list.
show ssg multidomain ppp exclude-list	Displays the contents of the PTA-MD exclusion list.

ssg next-hop download

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg next-hop download** command is not available in Cisco IOS software.

To download the next-hop table from a RADIUS server, use the **ssg next-hop download** command in global configuration mode. To remove the command from the configuration, use the **no** form of this command.

ssg next-hop download [*profile-name*] [*profile-password*]

no ssg next-hop download [*profile-name*] [*profile-password*]

Syntax Description

profile-name	(Optional) Profile name.
profile-password	(Optional) Profile password.

Command Default

If no profile name and password are provided, the previous profile specified with this command is downloaded. If no previous profile was specified, an error message is generated.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(3)DC	This command was introduced on the Cisco 6400 node route processor.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

When this command is used, an entry is made in the running configuration. When the configuration is reloaded, the next-hop table is automatically downloaded. If the **no** form of this command is used to remove the command from the running configuration, a next-hop table will not be automatically downloaded when the configuration is reloaded.

Examples

The following example shows how to download the next-hop table called “MyProfile” from a RADIUS server:

```
ssg next-hop download MyProfile MyProfilePassword
```

Related Commands

Command	Description
clear ssg next-hop	Removes the next-hop table.
show ssg next-hop	Displays the next-hop table.

ssg open-garden

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg open-garden** command is not available in Cisco IOS software.

To designate a service as an open garden service, use the **ssg open-garden** command in global configuration mode. To remove a service from the open garden, use the **no** form of this command.

ssg open-garden *profile-name*

no ssg open-garden *profile-name*

Syntax Description

profile-name	Local service profile name.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(5)DC	This command was introduced on the Cisco 6400 series node route processor.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.4	This command was integrated into Cisco IOS Release 12.4.

Usage Guidelines

Use this command to designate a service, defined in a local service profile, as an open garden service.

Examples

In the following example, the service called “fictitiousname.com” is defined in a local service profile and added to the open garden:

```
local-profile cisco.com
 attribute 26 9 251 "Oopengarden1.com"
 attribute 26 9 251 "D10.13.1.5"
 attribute 26 9 251 "R10.1.1.0;255.255.255.0"
 exit
ssg open-garden fictitiousname.com
```

Related Commands

Command	Description
clear ssg open-garden	Removes open garden configurations and all open garden service objects.
clear ssg service	Removes an SSG service.
local-profile	Configures a local service profile.

Command	Description
show ssg open-garden	Displays all open garden services.
ssg service-search-order	Specifies the order in which SSG searches for a service profile.

ssg pass-through

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg pass-through** command is not available in Cisco IOS software.

To enable transparent pass-through, use the **ssg pass-through** command in global configuration mode. To disable transparent pass-through, use the **no** form of this command

ssg pass-through [**filter** {*ip-access-list* | *ip-extended-access-list* | *access-list-name* | **download** [*profile-name* | *profile-name profile-password*]} [**downlink** | **uplink**]}]

no ssg pass-through [**filter** {*ip-access-list* | *ip-extended-access-list* | *access-list-name* | **download** [*profile-name* | *profile-name profile-password*]} [**downlink** | **uplink**]}]

Syntax Description

filter	(Optional) Specify access control for packets.
ip-access-list	(Optional) IP access list (standard or extended).
ip-extended-access-list	(Optional) IP extended access list (standard or extended).
access-list-name	(Optional) Access list name.
download	(Optional) Load a service profile and use its filters as default filters.
profile-name	(Optional) Service profile name.
profile-password	(Optional) Service profile password.
downlink	(Optional) Apply filter to downlink packets.
uplink	(Optional) Apply filter to uplink packets.

Command Default

Transparent pass-through is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(3)DC	This command was introduced on the Cisco 6400 node route processor.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to enable transparent pass-through if you want to allow unauthenticated traffic to pass through the Service Selection Gateway (SSG) in either direction without modification. If you want all traffic to be authenticated by the SSG, use this command to disable transparent pass-through. You can use the filter option to prevent pass through traffic from accessing the specified IP address and subnet mask combinations.

Use the **no** form of this command to remove a transparent pass-through filter that was configured at the command line. This will also remove it from the running configuration.

Examples

The following example shows how to enable SSG transparent pass-through and download a pass-through filter from the AAA server called "filter01":

```
ssg pass-through
ssg pass-through filter download filter01 cisco

Radius reply received:
        Created Upstream acl from it.
Loading default pass-through filter succeeded.
```

Related Commands

Command	Description
clear ssg pass-through-filter	Removes the downloaded filter for transparent pass-through.
show ssg pass-through-filter	Displays the downloaded filter for transparent pass-through.

ssg port-map

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg port-map** command is not available in Cisco IOS software.

To enable the Service Selection Gateway (SSG) Port-Bundle Host Key feature and enter SSG portmap configuration mode, use the **ssg port-map** command in global configuration mode. To disable the port-bundle host key feature, use the **no** form of this command.

ssg port-map

no ssg port-map

Syntax Description

This command has no arguments or keywords.

Command Default

The Port-Bundle Host Key feature is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(16)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

This command will not take effect until the router has reloaded.

The SSG Port-Bundle Host Key feature requires Cisco Service Selection Dashboard (SSD) Release 3.0(1) or Cisco Subscriber Edge Services Manager (SESM) Release 3.1(1).

Examples

The following example shows how to enable the SSG port-bundle host key and enter SSG portmap configuration mode:

```
Router(config)# ssg port-map
Router(ssg-port-map)#
```

Related Commands

Command	Description
destination access-list	Specifies packets for port-mapping by specifying an access list to compare against the subscriber traffic.
destination range	Identifies packets for port-mapping by specifying the TCP port range to compare against the subscriber traffic.
length (SSG)	Modifies the port-bundle length upon the next SSG reload.
source ip	Specifies SSG source IP addresses to which to map the destination IP addresses in subscriber traffic.

ssg port-map destination access-list

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg port-map destination access-list** command is not available in Cisco IOS software.

Note Effective with Cisco IOS Releases 12.2(16)B and 12.3(4)T, this command is replaced by the **destination access-list** command. See the **destination access-list** command page for more information.

To identify packets for port-mapping by specifying an access list to compare against subscriber traffic, use the **ssg port-map destination access-list** command in global configuration mode. To remove this specification, use the **no** form of this command.

ssg port-map destination access list *access-list-number*

no ssg port-map destination access list *access-list-number*

Syntax Description

access-list-number	Integer from 100 to 199 that is the number or name of an extended access list.

Command Default

No default behavior or values.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(2)B	This command was introduced on the Cisco 6400 series.
12.2(4)B	Support for this command was added to other platforms.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(16)B	This command was replaced by the **destination access-list** command in Cisco IOS Release 12.2(16)B.
12.3(4)T	This command was replaced by the **destination access-list** command in Cisco IOS Release 12.3(4)T.
15.0(1)M	This command was removed.

Usage Guidelines

When the **ssg port-map destination access list** command is configured, any traffic going to the default network and matching the access list will be port-mapped.

Note A default network must be configured and routable from SSG in order for this command to be effective.

You can use multiple entries of the **ssg port-map destination access-list** command. The access lists are checked against the subscriber traffic in the order in which they are defined.

Examples

In the following example, packets permitted by access list 100 will be port-mapped:

```
ssg port-map enable
ssg port-map destination access-list 100
ssg port-map source ip Ethernet0/0/0
!
....
!
access-list 100 permit ip 10.0.0.0 0.255.255.255 host 70.13.6.100
access-list 100 deny   ip any any
```

Related Commands

Command	Description
ssg port-map destination range	Identifies packets for port-mapping by specifying the TCP port range to compare against the subscriber traffic.

ssg port-map destination range

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg port-map destination range** command is not available in Cisco IOS software.

Note Effective with Cisco IOS Releases 12.2(16)B and 12.3(4)T, this command is replaced by the **destination range** command. See the **destination range** command page for more information.

To identify packets for port-mapping by specifying the TCP port range to compare against the subscriber traffic, use the **ssg port-map destination range** command in global configuration mode. To remove this specification, use the **no** form of this command.

ssg port-map destination range from *port-number-1* **to** *port-number-2* [**ip** *ip-address*]

no ssg port-map destination range from *port-number-1* **to** *port-number-2* [**ip** *ip-address*]

Syntax Description

from	Specifies lower end of TCP port range.
port-number-1	Port number at lower end of TCP port range.
to	Specifies higher end of TCP port range.
port-number-2	Port number at higher end of TCP port range.
ip *ip-address*	(Optional) Destination IP address in the packets.

Command Default

If an IP address is not specified, Service Selection Gateway (SSG) will allow any destination IP address in the subscriber traffic to be port-mapped, as long as the packets match the specified port ranges.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(2)B	This command was introduced on the Cisco 6400 series.
12.2(4)B	Support for this command was added to other platforms.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(16)B	This command was replaced by the **destination range** command in Cisco IOS Release 12.2(16)B.
12.3(4)T	This command was replaced by the **destination range** command in Cisco IOS Release 12.3(4)T.
15.0(1)M	This command was removed.

Usage Guidelines

If the destination IP address is not configured, a default network must be configured and routable from SSG in order for this command to be effective.

If the destination IP address is not configured, any traffic going to the default network with the destination port will fall into the destination port range and will be port mapped.

You can use multiple entries of the **ssg port-map destination range** command. The port ranges are checked against the subscriber traffic in the order in which they were defined.

Examples

In the following example, packets that are going to the default network and have a destination port within the range from 8080 to 8081 will be port-mapped:

```
ssg port-map destination range from 8080 to 8081
```

Related Commands

Command	Description
ssg port-map destination access-list	Identifies packets for port-mapping by specifying an access list to compare against the subscriber traffic.

ssg port-map enable

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg port-map enable** command is not available in Cisco IOS software.

Note Effective with Cisco IOS Releases 12.2(16)B and 12.3(4)T, this command is replaced by the **ssg port-map** command. See the **ssg port-map** command page for more information.

To enable the Service Selection Gateway (SSG) port-bundle host key, use the **ssg port-map enable** command in global configuration mode. To disable the SSG port-bundle host key, use the **no** form of this command.

ssg port-map enable

no ssg port-map enable

Syntax Description

This command has no arguments or keywords.

Command Default

SSG port-bundle host key is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(2)B	This command was introduced on the Cisco 6400 series.
12.2(4)B	Support for this command was added to other platforms.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(16)B	This command was replaced by the **ssg port-map** command in Cisco IOS Release 12.2(16)B.
12.3(4)T	This command was replaced by the **ssg port-map** command in Cisco IOS Release 12.3(4)T.
15.0(1)M	This command was removed.

Usage Guidelines

This command will not take effect until the router has been reloaded.

The SSG Port-Bundle Host Key feature requires Cisco Service Selection Dashboard (SSD) Release 3.0(1) or CiscoSubscriber Edge Services Manager (SESM) Release 3.1(1). If you are using an earlier release of SSD, use the **no ssg port-map enable command to** disable the SSG Port-Bundle Host Key feature.

Examples

The following example shows how to enable the SSG port-bundle host key:

```
ssg port-map enable
```

Related Commands

Command	Description
ssg port-map destination access-list	Identifies packets for port-mapping by specifying an access list to compare against the subscriber traffic.
ssg port-map destination range	Identifies packets for port-mapping by specifying the TCP port range to compare against the subscriber traffic.
ssg port-map source ip	Specifies SSG source IP addresses to which to map the destination IP addresses in subscriber traffic.

ssg port-map length

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg port-map length** command is not available in Cisco IOS software.

Note Effective with Cisco IOS Releases 12.2(16)B and 12.3(4)T, this command is replaced by the length command. See the **length (SSG)** command page for more information.

To modify the port-bundle length upon the next Service Selection Gateway (SSG) reload, use the **ssg port-map length** command in global configuration mode. To return the port-bundle length to the default value, use the **no** form of this command.

ssg port-map length *bits*

no ssg port-map length *bits*

Syntax Description

bits	Port-bundle length, in bits. The maximum port-bundle length is 10 bits.

Command Default

4 bits.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(2)B	This command was introduced on the Cisco 6400 series.
12.2(4)B	Support for this command was added to other platforms.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(16)B	This command was replaced by the **length** command in Cisco IOS Release 12.2(16)B.
12.3(4)T	This command was replaced by the **length** command in Cisco IOS Release 12.3(4)T.
15.0(1)M	This command was removed.

Usage Guidelines

The port-bundle length is used to determine the number of bundles in one group and the number of ports in one bundle. By default, the port-bundle length is 4 bits. The maximum port-bundle length is 10 bits. See Table 19 for available port-bundle length values and the resulting port-per-bundle and bundle-per-group values. Increasing the port-bundle length can be useful when you see frequent error messages about running out of ports in a port bundle, but note that the new value does not take effect until SSG next reloads and Cisco Service Selection Dashboard (SSD) restarts.

Note For each Cisco SSD server, all connected SSGs must have the same port-bundle length.

Table 19 Port-Bundle Lengths and Resulting Port-per-Bundle and Bundle-per-Group Values

Port-Bundle Length (in Bits)	Number of Ports per Bundle	Number of Bundles per Group (and per SSG Source IP Address)
0	1	64512
1	2	32256
2	4	16128
3	8	8064
4 (default)	16	4032
5	32	2016
6	64	1008
7	128	504
8	256	252
9	512	126
10	1024	63

Examples

The following example results in 64 ports per bundle and 1008 bundles per group:

```
Router(config)# ssg port-map length 6
```

Related Commands

Command	Description
show ssg port-map status	Displays information on port bundles, including the port-bundle length.

ssg port-map source ip

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg port-map source ip** command is not available in Cisco IOS software.

Note Effective with Cisco IOS Releases 12.2(16)B and 12.3(4)T, this command is replaced by the **source ip** command. See the **source ip** command page for more information.

To specify Service Selection Gateway (SSG) source IP addresses to which to map the destination IP addresses in subscriber traffic, use the **ssg port-map source ip** command in global configuration mode. To remove this specification, use the **no** form of this command.

ssg port-map source ip {*ip-address* | *interface*}

no ssg port-map source ip {*ip-address* | *interface*}

Syntax Description

ip-address	SSG source IP address.
interface	Interface whose main IP address is used as the SSG source IP address.

Command Default

No default behavior or values.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(2)B	This command was introduced on the Cisco 6400 series.
12.2(4)B	Support for this command was added to other platforms.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(16)B	This command was replaced by the **source ip** command in Cisco IOS Release 12.2(16)B.
12.3(4)T	This command was replaced by the **source ip** command in Cisco IOS Release 12.3(4)T.
15.0(1)M	This command was removed.

Usage Guidelines

With the SSG Port-Bundle Host Key feature, SSG maps the destination IP addresses in subscriber traffic to specified SSG source IP addresses.

All SSG source IP addresses configured with the **ssg port-map source ip** command must be routable in the management network where the Cisco SSD resides.

If the interface for the source IP address is deleted, the port-map translations will not work correctly.

Because a subscriber can have several simultaneous TCP sessions when accessing a web page, SSG assigns a bundle of ports to each subscriber. Because the number of available port bundles are limited, you can assign multiple SSG source IP addresses (one for each group of port bundles). By default, each group has 4032 bundles, and each bundle has 16 ports. To modify the number of bundles per group and the number of ports per bundle, use the **ssg port-map length** command in global configuration mode.

Examples

The following example shows the SSG source IP address specified with an IP address and with specific interfaces:

```
Router(config)# ssg port-map source ip 10.0.50.1
Router(config)# ssg port-map source ip Ethernet0/0/0
Router(config)# ssg port-map source ip Loopback 1
```

Related Commands

Command	Description
ssg port-map length	Modifies the port-bundle length upon the next SSG reload.

ssg prepaid reauthorization drop-packet

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg prepaid reauthorization drop-packet** command is not available in Cisco IOS software.

To configure Service Selection Gateway (SSG) to drop prepaid traffic during reauthorization if threshold values are not configured, use the **ssg prepaid reauthorization drop-packet** command in global configuration mode. To configure SSG to forward traffic during reauthorization and not to drop traffic during reauthorization, use the **no** form of this command.

ssg prepaid reauthorization drop-packet

no ssg prepaid reauthorization drop-packet

Syntax Description

This command has no arguments or keywords.

Command Default

SSG forwards traffic during reauthorization by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

SSG sends a service reauthorization request to the billing server when a prepaid user's quota is consumed or after the configured idle timeout expires. If the billing sever returns a zero quota in the reauthorization response, the connection is terminated, but the data that was in progress during the reauthorization is not counted in the reauthorization.

Use this command to configure how traffic is handled during reauthorization. This command configures SSG to drop all prepaid user traffic during reauthorization when threshold values are not configured. If you configure SSG to drop traffic during reauthorization and a threshold value is configured, traffic is not dropped during reauthorization until the user exhausts the allotted quota. If a user exhausts the allotted quota, traffic gets dropped until SSG receives the reauthorization response. By default, traffic continues during reauthorization.

Use the **no ssg prepaid reauthorization drop-packet** command to configure SSG not to drop any traffic during reauthorization.

Examples

The following example shows how to configure SSG to drop traffic during reauthorization:

```
ssg prepaid reauthorization drop-packet
```

Related Commands

Command	Description
ssg prepaid threshold	Configures SSG to reauthorize a prepaid user's connection when the user's remaining quota reaches the configured threshold value.

ssg prepaid threshold

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg prepaid threshold** command is not available in Cisco IOS software.

To configure a Service Selection Gateway (SSG) prepaid threshold value, use the **ssg prepaid threshold** command in global configuration mode. To disable the SSG prepaid threshold value, use the **no** form of this command.

ssg prepaid threshold {**volume** *bytes* | **time** *seconds* | **default-quota** *number-of-times*}

no ssg prepaid threshold {**volume** *bytes* | **time** *seconds* | **default-quota** *number-of-times*}

Syntax Description

volume	Prepaid threshold volume configuration.
bytes	Threshold volume, in bytes. Range: 0 to 65535566.
time	Prepaid threshold time configuration.
seconds	Threshold time, in seconds. Range: 0 to 6565656.
default-quota	Default quota for prepaid server failure.
number-of-times	Maximum number of times SSG will allocate the default quota.

Command Default

No SSG prepaid threshold values are configured, and reauthorization happens only after a user has completely exhausted the allotted quota.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.3(11)T	The **default-quota** keyword was added.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to configure an SSG prepaid threshold value. By default, SSG reauthorizes a prepaid user's connection only after the user's allotted quota has been consumed. When a prepaid threshold value is configured, SSG reauthorizes a prepaid user's connection before the user has completely consumed the allotted quota for a service.

For a prepaid threshold time configuration, the threshold time is in seconds and should be configured to be at least equal to the connection reauthorization time.

For a prepaid threshold volume configuration, the threshold volume is in bytes and should be at least equal to the user's bandwidth multiplied by the reauthorization time. Calculate the prepaid threshold volume value using the following formula:

(*threshold value*) >= *B* * *T*

where

B (Bps) = user's bandwidth

T (seconds) = reauthorization time

SSG can be configured to allocate a default quota when the prepaid server fails to respond to an authorization or reauthorization request. Use the **default-quota** keyword to specify the maximum number of times that SSG will allocate the default quota per instance of prepaid billing server unavailability.

Examples

The following example shows how to configure a threshold time value of 10 seconds:

```
ssg prepaid threshold time 10
```

The following example shows how to configure a threshold volume value of 2000 bytes:

```
ssg prepaid threshold volume 2000
```

The following example shows how to configure a prepaid default quota threshold of 65:

```
ssg prepaid threshold default-quota 65
```

Related Commands

Command	Description
ssg prepaid reauthorization drop-packet	Configures SSG to drop prepaid traffic during reauthorization.

ssg profile-cache

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg profile-cache** command is not available in Cisco IOS software.

To enable caching of user profiles for non-PPP users, use the **ssg profile-cache** command in global configuration mode. To disable caching of user profiles, use the **no** form of this command.

ssg profile-cache

no ssg profile-cache

Syntax Description

This command has no arguments or keywords.

Command Default

User-profile caching is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(2)B	This command was introduced.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

The **ssg profile-cache** command allows Service Selection Gateway (SSG) to cache the user profiles of non-PPP users. User profiles of PPP and RADIUS proxy users are always cached by SSG by default. In situations in which the user profile is not available from other sources, SSG user-profile caching makes the user profile available for RADIUS status queries, providing support for single-sign-on functionality and for failover from one Subscriber Edge Services Manager (SESM) to another.

In order for a user profile to be cached, the **ssg profile-cache** command must be configured before account login occurs. Once the user authentication has been done (as part of the account login), the host object is created, and the user profile is cached.

Note If you are using SSG with the SESM in Lightweight Directory Access Protocol (LDAP) mode, you may want to disable SSG user-profile caching in order to save memory and improve scalability. SSG user-profile caching is required only when SSG is used with the SESM in RADIUS mode.

Examples

The following example shows how to enable user-profile caching:

```
ssg profile-cache
```

ssg qos police

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg qos police** command is not available in Cisco IOS software.

To enable the limiting transmission rates for an Service Selection Gateway (SSG) subscriber or for a service being used by an SSG subscriber, use the **ssg qos police** command in global configuration mode. To disable the limiting of transmission rates, use the **no** form of this command.

ssg qos police [**user** | **session**]

no ssg qos police [**user** | **session**]

Syntax Description

user	(Optional) Specifies per-user policing. Per-user policing is used to police bandwidth allocations for separate subscribers of an SSG service.
session	(Optional) Specifies per-session policing. Per-session policing is used to police the bandwidth used by one subscriber for multiple services.

Command Default

Traffic is forwarded with no SSG policing restrictions if the **ssg qos police** command is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

This command enables the SSG Hierarchical Policing feature, which is used to limit the output transmission rate for a subscriber or for a specific SSG service used by a subscriber. The parameters used to police traffic (committed rate, normal burst, and excess burst) are configured in a RADIUS user profile (per-user policing) or a RADIUS service profile (per-session policing) by using the Q option.

Examples

The following is an example of a user profile with the SSG Hierarchical Policing enabled for downstream traffic. In this example, an excess burst size is set at 0 so all dropped packets are tail-dropped. In this particular profile, only downstream traffic is policed (although it is important to note that an upstream token bucket algorithm would operate identically to the downstream policing algorithm).

```
user = johndoe
radius = 7200-SSG-v1.1
check_items= {
2 = cisco
```

```
}
reply_attributes={
9,250="Nproxy_ser"
9,250="Ntunnel_ser"
9,250="QD8000;2000;0"
```

Per-user policing must be enabled on the router before the traffic directed to the subscriber is policed. Per-user policing is enabled on the router by entering the following global configuration command:

```
Router(config)# ssg qos police user
```

Note The following steps provide an example of how traffic going to the subscriber is treated in the example configuration. Because packet sizes are variable, the packet sizes used in this example are created for the sake of the example.

The token bucket starts at 1000 tokens. Although the committed rate is specified in bits per seconds, the token bucket operates based on bytes. 8000 bits is equal to 1000 bytes, so a full token bucket has 1000 tokens. The normal burst parameter is set at 2000. For the sake of the example, no actual debt has been accrued before the arrival of the first packet.

- The first packet is 500 bytes and arrives 3/4 second after the last packet.
  - The packet size is 500 bytes.
  - The time difference (td) is 3/4 of a second.
  - actual_debt = previous_actual_debt + packet_size = 0 + 500 = 500
  - tokens = committed_rate * td = 1000 * 3/4 = 750
  - 750 > 500. Therefore, the tokens are greater than the actual debt.

    Because tokens are greater than the actual debt, the user has been idle for a sufficient amount of time and the packet is transmitted.
- The second packet is 1500 bytes and arrives 1/2 second after the previous packet.
  - The packet size is 1500 bytes.
  - The td is 1/2 of a second.
  - actual_debt = 0 + 1500 = 1500
  - tokens = 1000 * 1/2 = 500
  - 500 < 1500. Therefore, the tokens are less than the actual debt. Because the tokens are less than the actual debt, an updated actual debt must be calculated and compared to the normal burst size.
  - New actual_debt = previous_actual_debt – tokens = 1500 – 500 = 1000
  - Normal burst is configured at 2000.
  - 1000 < 2000. Because the actual debt is less than the normal burst size, the packet is forwarded.
- The next packet is 4000 bytes and it arrives 1/2 second later.
  - The packet size is 4000 bytes.
  - The td is 1/2 second.
  - actual_debt = previous_actual_debt + packet_size = 1000 + 4000 = 5000
  - tokens = 1000 * 1/2 = 500
  - 500 < 5000. The tokens are less than the actual debt, so the new actual debt must be computed.
  - actual_debt = previous_actual_debt – tokens = 5000 – 500 = 4500

– 4500 > 2000. Because the actual debt is greater than the normal burst size, the packet is dropped.

Future packets will be policed similarly on the basis of this algorithm.

Related Commands

Command	Description
attribute	Specifies the attributes of a service profile for SSG. The parameters that are used by the token bucket to police traffic are specified using the **attribute** command.
show ssg host	Displays information about an SSG host, including whether policing is enabled or disabled and the policing configurations of a particular host.
show ssg connection	Displays information about a particular SSG connection, including the policing parameters.

ssg query mac dhcp

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg query mac dhcp** command is not available in Cisco IOS software.

To configure the Service Selection Gateway (SSG) to send a Dynamic Host Control Protocol (DHCP) lease query request to the configured DHCP server when a subscriber's Media Access Control (MAC) address is not already known, use the **ssg query mac dhcp** command in global configuration mode. To disable the sending of DHCP lease query requests, use the **no** form of this command.

ssg query mac dhcp

no ssg query mac dhcp

Syntax Description

This command has no arguments or keywords.

Command Default

SSG does not send DHCP lease query requests.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

SSG can be configured to authenticate a subscriber on the basis of the subscriber's MAC address. Use the **ssg query mac dhcp** command to configure SSG to request a subscriber's MAC address when the MAC address is not already present in a subscriber's user profile.

Examples

The following example enables SSG to send a DHCP lease query request to determine the MAC address of a subscriber:

```
ssg query mac dhcp
```

Related Commands

Command	Description
query ip dhcp	Sends DHCP lease query requests for the subscriber session when no IP address is received in the accounting start record.
username mac	Sends a subscriber's MAC address as RADIUS attribute 1 in TAL requests.

ssg radius-helper

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg radius-helper** command is not available in Cisco IOS software.

To enable communications with the Cisco Service Selection Dashboard (SSD) and specify port numbers and secret keys for receiving packets, use the **ssg radius-helper** command in global configuration mode. To disable communications with the Cisco SSD, use the **no** form of this command.

ssg radius-helper [**acct-port** *port-number* | **auth-port** *port-number* | **key** *key* | **access-list** *acl-id* | **validate**]

no ssg radius-helper [**acct-port** *port-number* | **auth-port** *port-number* | **key** *key* | **access-list** *acl-id* | **validate**]

Syntax Description

acct-port *port-number*	(Optional) UDP[1] destination port for RADIUS accounting requests; the host is not used for accounting if set to 0. The default is 1646.
auth-port *port-number*	(Optional) UDP destination port for RADIUS authentication requests; the host is not used for authentication if set to 0. The default is 1645.
key *key*	(Optional) Key shared with the RADIUS clients.
access-list *acl-id*	(Optional) Specifies the access list to be applied to traffic from the Subscriber Edge Services Manager (SESM). • *acl-id* specifies the IP access list number (or list name) for packets from radius clients. The number range is 1 to 99 (or 1300 to 2699 for an expanded range of RADIUS clients). **Note** The *acl-id* argument also allows you to enter the IP access list name for packets from RADIUS clients.
validate	(Optional) Enables the validation of SESM IP addresses. **Note** The Service Selection Gateway (SSG) accepts commands only from validated IP addresses.

1. UDP = User Datagram Protocol

Command Default

Communications with the Cisco SSD is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(3)DC	This command was introduced on the Cisco 6400 node route processor.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.

Release	Modification
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.3(3)T	The **validate** keyword was added.
12.3(4)T	The **access-list** *acl-id* keyword and argument were added.
15.0(1)M	This command was removed.

Usage Guidelines

You must use this command to specify a key so that SSG can communicate with the Cisco SSD.

Examples

The following example shows how to enable communications with the Cisco SSD:

```
router(config)# ssg radius-helper acct-port 1646 auth-port 1645
router(config)# ssg radius-helper key MyKey
router(config)# ssg radius-helper access-list 98
router(config)# ssg radius-helper validate
```

ssg radius-proxy

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg radius-proxy** command is not available in Cisco IOS software.

To enable SSG RADIUS Proxy, use the **ssg radius-proxy** command in global configuration mode. To prevent further connection of proxy users, use the **no** form of this command

ssg radius-proxy

no ssg radius-proxy

Syntax Description

This command has no arguments or keywords.

Command Default

SSG RADIUS Proxy is not enabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to enable SSG RADIUS Proxy.

This command also enables SSG-radius-proxy configuration mode. You must enable SSG with the **ssg enable** command before you can enter the **ssg radius-proxy** command. If you do not enter the **ssg radius-proxy** command, SSG continues to proxy RADIUS packets containing SSG vendor-specific attributes (VSAs) received from the Service Selection Dashboard (SSD), but does not act as a generic RADIUS proxy.

The **no ssg radius-proxy** command does not log off RADIUS client hosts that are already logged in.

If you configure the **no ssg radius-proxy** command, no further connections of proxy users are allowed, but hosts from already configured RADIUS clients remain connected. If you subsequently configure the **ssg radius-proxy** command, the previous RADIUS proxy configuration is restored.

Examples

The following example enables SSG RADIUS Proxy:

```
ssg enable
ssg radius-proxy
```

Related Commands

Command	Description
address-pool	Defines local IP pools to be used by SSG to assign IP addresses to users for which SSG is acting as a RADIUS client.
clear ssg radius-proxy client-address	Clears all hosts connected to a specific RADIUS client.
clear ssg radius-proxy nas-address	Clears all hosts connected to a specific NAS.
forward accounting-start-stop	Proxies accounting start, stop, and update packets generated by any RADIUS clients to the AAA server.
idle-timeout (SSG)	Configures a host object timeout value.
server-port	Defines the ports for the SSG RADIUS proxy.
show ssg tcp-redirect group	Displays the pool of IP addresses configured for a router or for a specific domain.
ssg enable	Enables SSG.

ssg service-cache

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg service-cache** command is not available in Cisco IOS software.

To enable the Service Selection Gateway (SSG) Service Profile Caching feature, or to change the refresh interval for services in the service profile cache, use the **ssg service-cache** command in global configuration mode. To disable Service Selection Gateway (SSG) service profile caching, use the **no** form of this command.

ssg service-cache [**refresh-interval** *minutes*]

no ssg service-cache [**refresh-interval** *minutes*]

Syntax Description

refresh-interval	(Optional) Changes the refresh rate for the SSG service profile cache. An SSG service profile refreshes by getting the service profile from the authentication, authorization, and accounting (AAA) server. If the **refresh-interval** argument is not entered, the default refresh rate of every 120 minutes is used.
minutes	(Optional) Specifies how often, in minutes, the service profiles in the SSG service profile cache will be refreshed.The refresh interval can be configured in one-minute increments between 10 minutes and 34,560 minutes (24 days). The default is every 120 minutes.

Command Default

SSG service profile caching is enabled by default.
The default refresh interval for the SSG service profile cache is every 120 minutes.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
15.0(1)M	This command was removed.

Usage Guidelines

The **ssg service-cache** command is used to enable SSG service profile caching. A refresh interval does not have to be specified (the default of 120 minutes will be used if no refresh interval is configured).

If the refresh interval is set at 180, the SSG service profile cache will check the AAA server for the service profiles in the cache every 180 minutes.

This command enhances the authentication process for SSG service logon by allowing users to authorize to a service using a service profile cached in SSG instead of downloading the service profile from the AAA server.

When this command is entered, all of the service profiles currently in use in SSG are immediately cached.

Examples

In the following example, SSG service profile caching is enabled:

```
ssg service-cache enable
```

In the following example, the service profiles in the SSG service profile cache will be updated from the AAA server every 240 minutes:

```
ssg service-cache refresh-interval 240
```

Related Commands

Command	Description
show ssg service	Displays various information about an SSG service, including the time remaining for the specified service to refresh.
ssg service-cache refresh	Manually updates the SSG service profile cache with the service profiles available on the AAA server.

ssg service-cache refresh

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg service-cache refresh** command is not available in Cisco IOS software.

To trigger an update to the Service Selection Gateway (SSG) service profile cache with the service profiles available on the authentication, authorization, and accounting (AAA) server, use the **ssg service-cache refresh** command in privileged EXEC mode.

ssg service-cache refresh [*service-name* | **all**]

no ssg service-cache refresh [*service-name* | **all**]

Syntax Description

service-name	Specifies a specific service should be refreshed. Required to refresh one SSG service profile in the SSG service profile cache.
all	Specifies that all of the service profiles in the SSG service profile cache should be refreshed. Required to refresh all SSG profiles in the SSG profile cache.

Command Default

The SSG service profile cache, if enabled, is refreshed at intervals based on the **ssg service-cache refresh-interval** configuration. If an **ssg service-cache refresh-interval** is not specified, the default refresh rate is every 120 minutes.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(15)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

This command is used to refresh the profiles in the SSG service profile cache manually from the AAA server. The service profiles in the SSG service profile cache are automatically refreshed with the profiles from the AAA server at user-configurable intervals using the **ssg service-cache refresh-interval** command. The user can trigger a refresh at any time by issuing this command.

If an SSG service cache refresh fails for any reason (for instance, the AAA server is unreachable or down), the service profile caching for that service is disabled. Once a user is able to download the service successfully, caching for the service begins again.

Examples

In the following example, all of the service profiles in the SSG service profile cache will be retrieved from the AAA server and will replace the service profiles in the SSG service profile cache:

```
ssg service-cache refresh all
```

In the following example, service profile "service1" will be retrieved from the AAA server and will replace the current "service1" profile in the SSG service profile cache:

```
ssg service-cache refresh service1
```

Related Commands

Command	Description
ssg service-cache	Enables SSG service profile caching.

ssg service-password

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg service-password** command is not available in Cisco IOS software.

To specify the password for downloading a service profile, use the **ssg service-password** command in global configuration mode. To disable the password, use the **no** form of this command.

ssg service-password *password*

no ssg service-password *password*

Syntax Description

password	Service profile password.

Command Default

No default behavior or values.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(3)DC	This command was introduced on the Cisco 6400 node route processor.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

This command sets the password required to authenticate with the authentication, authorization, and accounting (AAA) server and download a service profile.

Examples

The following example shows how to set the password for downloading a service profile:

```
ssg service-password MyPassword
```

ssg service-search-order

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg service-search-order** command is not available in Cisco IOS software.

To specify the order in which Service Selection Gateway (SSG) searches for a service profile, use the **ssg service-search-order** command in global configuration mode. To disable the search order, use the **no** form of this command.

ssg service-search-order {**local** | **remote** | **local remote** | **remote local**}

no ssg service-search-order {**local** | **remote** | **local remote** | **remote local**}

Syntax Description

local	Search for service profiles in local Flash memory.
remote	Search for service profiles on a RADIUS server.
local remote	Search for service profiles in local Flash memory, then on a RADIUS server.
remote local	Search for service profiles on a RADIUS server, then in local Flash memory.

Command Default

The default search order is **remote**; that is, SSG searches for service profiles on the RADIUS server.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(3)DC	This command was introduced on the Cisco 6400 node route processor.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

SSG can search for service profiles in local Flash memory, on a remote RADIUS server, or both. The possible search orders are:

- Local—search only in Flash memory
- Remote—search only on the RADIUS server
- Local remote—search in Flash memory first, then on the RADIUS server
- Remote local—search on the RADIUS server, then in Flash memory

Examples

The following example shows how to set the search order to local remote, so that SSG will always look for service in Flash memory first, then on the RADIUS server:

```
ssg service-search-order local remote
```

Related Commands

Command	Description
show ssg binding	Configures a local RADIUS service profile.

ssg tcp-redirect

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg tcp-redirect** command is not available in Cisco IOS software.

To enable SSG TCP redirection and SSG-redirect mode, use the **ssg tcp-redirect** command in global configuration mode. To disable SSG TCP redirection, use the **no** form of this command.

ssg tcp-redirect

no ssg tcp-redirect

Syntax Description

SSG TCP redirect is not enabled.

Command Default

This command has no default behavior.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(4)B	This command was introduced. This command replaces the **ssg http-redirect group** command.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to enable SSG TCP redirection. This command also enables SSG-redirect mode. The **no ssg tcp-redirect** command disables SSG TCP Redirect and removes all configurations created in the SSG-redirect mode. You must enable SSG by issuing the **ssg enable** command before you can configure SSG TCP redirect.

Examples

The following example shows how to select a captive portal group for redirection of traffic from unauthorized users. In the following example, traffic from unauthorized users is redirected to the captive portal group named “RedirectServer”:

```
ssg enable
ssg tcp-redirect
 redirect unauthenticated-user to RedirectServer
```

The following example shows how to define a port list named "WebPorts" and adds TCP ports 80 and 8080 to the port list. Port 8080 is configured to be redirected by the captive portal group named "Redirect Server":

```
ssg enable
ssg tcp-redirect
 port-list WebPorts
  port 80
  port 8080
  exit
 redirect port 8080 to RedirectServer
```

Related Commands

Command	Description
debug ssg tcp-redirect	Turns on debug information for the SSG TCP Redirect for Services feature.
network (ssg-redirect)	Adds an IP address to a named network list.
network-list	Defines a list of one or more IP networks that make up a named network list.
port (ssg-redirect)	Adds a TCP port to a named port list.
port-list	Defines a list of one or more TCP ports that make up a named port list and enters SSG-redirect-port configuration mode.
redirect captivate advertising default group	Configures the default captive portal group, duration, and frequency for advertising.
redirect captivate initial default group duration	Selects a default captive portal group and duration of the initial captivation of users on Account Logon.
redirect port to	Marks a TCP port or named TCP port list for SSG TCP redirection.
redirect smtp group	Selects a captive portal group for redirection of SMTP traffic.
redirect unauthorized-service to	Sets a list of destination IP networks that can be redirected by a specified, named captive portal group.
redirect unauthenticated-user to	Redirects traffic from authenticated users to a specified captive portal group.
server (SSG)	Adds a server to a captive portal group.
server-group	Defines the group of one or more servers that make up a named captive portal group and enters SSG-redirect-group configuration mode.
show ssg tcp-redirect group	Displays information about the captive portal groups and the networks associated with the captive portal groups.
show tcp-redirect mappings	Displays information about the TCP redirect mappings for hosts within your system.
ssg enable	Enables SSG.
ssg tcp-redirect	Enables SSG TCP redirect and enters SSG-redirect mode.

ssg vc-service-map

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg vc-service-map** command is not available in Cisco IOS software.

To map virtual circuits (VCs) to service names, use the **ssg vc-service-map** command in global configuration mode. To disable VC-to-service-name mapping, use the **no** form of this command.

ssg vc-service-map *service-name* [**interface** *interface-number*] *start-vpi* | *start-vpi*/*vci* [*end-vpi* | *end-vpi*/*vci*] **exclusive** | **non-exclusive**

no ssg vc-service-map *service-name* [**interface** *slot-module-port*] *start-vpi* | *start-vpi*/*vci* [*end-vpi* | *end-vpi*/*vci*] **exclusive** | **non-exclusive**

Syntax Description

service-name	Service name.
interface	(Optional) Specifies a service name mapping for an interface.
interface-number	(Optional) Number of the interface (such as 1/0) through which SSG will access the mapped service.
start-vpi	Virtual path identifier (VPI) or start of a range of VPIs that will be mapped to the service. The range is from 0 to 255.
start-vpi/*vci*	VPI/virtual channel identifier (VCI) or start of a range of VPI/VCIs that will be mapped to the service. The range is from 0 to 255.
end-vpi	(Optional) End of a range of VPIs that will be mapped to the service. The range is from 0 to 255.
end-vpi/*vci*	(Optional) End of a range of VPI/VCIs that will be mapped to the service. The range is from 0 to 255.
exclusive	Users will be able to access only the mapped service.
non-exclusive	Users will be able to access the mapped service and any other services to which they are subscribed. Users can log in to the Service Selection Gateway (SSG) with a username and password, establishing a non-PPP Termination Aggregation (PTA) session, and a PTA session to the mapped service will be established by default. If **non-exclusive** is specified for the service mapping, users can also establish a PTA session to another service to which they are subscribed.

Command Default

The service mapping is non-exclusive by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)DC	This command was introduced on the Cisco 6400 node route processor.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.

Release	Modification
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to map VCs to service names. If you specify a VC-to-service-name mapping as exclusive, specifying a username will log you in to the mapped service. However, specifying username@service will not log you in. If you specify a mapping as nonexclusive, specifying a username will log you in to the mapped service. However, username@service1 will log you in to service1.

Examples

The following example shows how to map all users coming into SSG on VPI/VCI 3/33 to the service "Worldwide" exclusively:

```
ssg vc-service-map Worldwide 3/33 exclusive
```

Related Commands

Command	Description
ssg vc-service-map	Displays VC-to-service-name mappings.

ssg wlan reconnect

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg wlan reconnect** command is not available in Cisco IOS software.

To enable Extensible Authentication Protocol (EAP) users to reconnect after logging off or after idle timeout has occurred, use the **ssg wlan reconnect** command in global configuration mode. To disable the ability of EAP users to reconnect, use the **no** form of this command.

ssg wlan reconnect

no ssg wlan reconnect

Syntax Description

This command has no arguments or keywords.

Command Default

EAP users cannot reconnect.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(16)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

EAP users do not have a username and password. If they access Subscriber Edge Services Manager (SESM), log off, and try to reconnect to the service later, SESM presents them with a logon page, which they cannot use. To allow users to reconnect without being asked to log on again, enable the user reconnect feature with the **ssg wlan reconnect** command.

If a user logs off through SESM, when the Service Selection Gateway (SSG) EAP transparency user reconnect functionality has been enabled, SSG inactivates the host. If the user tries to access the service again, SESM queries SSG, and SSG activates the host and enables autologon services.

The SSG host, whether active or inactive, is deleted when the Access Zone Router (AZR) sends an Accounting Stop packet to SSG (when the user walks out of the private wireless LAN (PWLAN) or the Dynamic Host Configuration Protocol (DHCP) address is released).

Note If user reconnect is enabled and a user refreshes or reloads the SESM page after an account logoff, SESM sends a query to SSG, which causes SSG to activate the host. It is recommended that users be made aware of this behavior so they do not accidentally activate the host.

Examples

The following example enables EAP users to reconnect after logging off:

```
ssg wlan reconnect
```

timeouts (SSG-radius-proxy)

Note Effective with Cisco IOS Release 15.0(1)M, the **timeouts** (SSG-radius-proxy) command is not available in Cisco IOS software.

To enter SSG-radius-proxy-timers configuration mode, use the **timeouts** command in SSG-radius-proxy configuration mode. To restore all timeouts, use the **no** form of this command.

timeouts

no timeouts

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

SSG-radius-proxy configuration

Command History

Release	Modification
12.2(15)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to enter SSG-radius-proxy-timeouts configuration mode to configure SSG RADIUS proxy handoff, idle, IP address, and Mobile Station ID (MSID) timeouts.

Examples

The following example shows how to enter SSG-radius-proxy-timeouts mode:

```
ssg radius-proxy
 timeouts
```

user passthrough maximum

Note Effective with Cisco IOS Release 15.0(1)M, the **user passthrough maximum** command is not available in Cisco IOS software.

To limit the number of Service Selection Gateway (SSG) transparent autologon (TAL) users on an SSG device, use the **user passthrough maximum** command in SSG login transparent submode. To remove the limitation on the number of SSG TAL users, use the **no** form of this command.

user passthrough maximum *number-of-users*

no user passthrough maximum *number-of-users*

Syntax Description

number-of-users	Limits the number of SSG TAL users on an SSG device. Range: 1 to 2147483647.

Command Default

Unlimited TAL users can access an SSG device.

Command Modes

SSG login transparent submode

Command History

Release	Modification
12.4(2)T	This command was introduced.
15.0(1)M	This command was removed.

Usage Guidelines

This command prevents resource exhaustion on a router by limiting the number of SSG TAL users on a device. When the router reaches the maximum number of users, it refuses any new connections.

Examples

The following example limits the number of SSG TAL users to 400:

```
Router(config)# ssg logon transparent
Router(config-login-transparent)# user passthrough maximum 400
```

Related Commands

Command	Description
ssg maximum host	Limits the number of host connections on an SSG device.
ssg maximum service	Limits the number of services available to a user on an SSG device.

user suspect maximum

Note Effective with Cisco IOS Release 15.0(1)M, the **user suspect maximum** command is not available in Cisco IOS software.

To specify the maximum number of Service Selection Gateway (SSG) transparent autologon suspect (SP) users that can be added to the suspect user list, use the **user suspect maximum** command in transparent auto-logon configuration mode. To remove the specification, use the **no** form of this command.

user suspect maximum *value*

no user suspect maximum *value*

Syntax Description

value	Maximum number of suspect users that can be added to the SP list. Valid range is from 10 to 5000.

Command Default

5000 suspect users.

Command Modes

Transparent auto-logon configuration

Command History

Release	Modification
12.3(1a)BW	This command was introduced.
12.3(3)B	This command was integrated into Cisco IOS Release 12.3(3)B.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
15.0(1)M	This command was removed.

Usage Guidelines

An SSG transparent autologon user becomes suspect when the user's authentication, authorization, and accounting (AAA) attempt is rejected.

If the number of suspect users exceeds the maximum value configured, SSG sends a system logging message and does not add any further users to the SP list.

Examples

The following example specifies that the maximum number of suspect users that can be added to the SP list is 200:

```
Router(config-login-transparent)# user suspect maximum 200
```

Related Commands

Command	Description
ssg login transparent	Enables the SSG Transparent Autologon feature.

user suspect timeout

Note Effective with Cisco IOS Release 15.0(1)M, the **user suspect timeout** command is not available in Cisco IOS software.

To specify the maximum length of time for which a Service Selection Gateway (SSG) transparent autologon suspect (SP) user remains in the suspect user list, use the **user suspect timeout** command in transparent auto-logon configuration mode. To return to the default length of time, use the **no** form of this command.

user suspect timeout *timeout*

no user suspect timeout *timeout*

Syntax Description

timeout	Maximum length of time (in minutes) that a suspect user remains in the suspect user list. Range is from 1 to 34560.

Command Default

60 minutes.

Command Modes

Transparent auto-logon configuration

Command History

Release	Modification
12.3(1a)BW	This command was introduced.
12.3(3)B	This command was integrated into Cisco IOS Release 12.3(3)B.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
15.0(1)M	This command was removed.

Usage Guidelines

If a packet is received for a user who is marked as an SP user, packets to or from this user are dropped or TCP-redirected until the *timeout* value is reached. When the *timeout* value is reached, any new traffic received by SSG from the user triggers the transparent autologon procedure.

Examples

The following example specifies that a suspect user will remain in the suspect user list for 30 minutes:

```
Router(config-login-transparent)# user suspect timeout 30
```

Related Commands

Command	Description
ssg login transparent	Enables the SSG Transparent Auto-Logon feature.

user unidentified timeout

Note Effective with Cisco IOS Release 15.0(1)M, the **user unidentified timeout** command is not available in Cisco IOS software.

To specify the maximum length of time for which a Service Selection Gateway (SSG) transparent autologon unidentified user remains marked as no response (NR), use the **user unidentified timeout** command in transparent auto-logon configuration mode. To return to the default timeout value, use the **no** form of this command.

user unidentified timeout *timeout*

no user unidentified timeout *timeout*

Syntax Description

timeout	Length of time (in minutes) that a user remains marked as NR. Range is from 1 to 34560.

Command Default

10 minutes.

Command Modes

Transparent auto-logon

Command History

Release	Modification
12.3(1a)BW	This command was introduced.
12.3(3)B	This command was integrated into Cisco IOS Release 12.3(3)B.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
15.0(1)M	This command was removed.

Usage Guidelines

An unidentified user is marked NR if there is no response from the authentication, authorization, and accounting (AAA) server to an authorization request and the authorization request times out.

If a packet is received for a user who is marked as an NR user, packets to or from this user are dropped or TCP-redirected until the *timeout* value is reached. When the *timeout* value is reached, any new traffic received by SSG from the user triggers the transparent logon procedure.

Examples

The following example sets the user-unidentified timeout to 5 minutes:

```
Router(config-login-transparent)# user unidentified timeout 5
```

Related Commands

Command	Description
ssg login transparent	Enables the SSG Transparent Auto-Logon feature.

user unidentified traffic permit

Note Effective with Cisco IOS Release 15.0(1)M, the **user unidentified traffic permit** command is not available in Cisco IOS software.

To specify that packets received from a Service Selection Gateway (SSG) transparent autologon user whose authorization request has timed out will be forwarded or received, use the **user unidentified traffic permit** command in transparent auto-logon configuration mode. To return to the default, use the **no** form of this command.

user unidentified traffic permit

no user unidentified traffic permit

Syntax Description

This command has no arguments or keywords.

Command Default

Packets received from a user whose authorization request has timed out are dropped.

Command Modes

Transparent auto-logon configuration

Command History

Release	Modification
12.3(1a)BW	This command was introduced.
12.3(3)B	This command was integrated into Cisco IOS Release 12.3(3)B.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
15.0(1)M	This command was removed.

Usage Guidelines

Configuring this command allows traffic flow for NR users toward the service network.

Examples

The following example specifies that packets received from a user whose authorization request has timed out will be forwarded or received:

```
Router(config-login-transparent)# user unidentified traffic permit
```

Related Commands

Command	Description
ssg login transparent	Enables the SSG Transparent Auto-Logon feature.

username mac

Note Effective with Cisco IOS Release 15.0(1)M, the **username mac** command is not available in Cisco IOS software.

To configure the Service Selection Gateway (SSG) to send a subscriber's MAC address as the username (RADIUS attribute 1) in transparent autologon (TAL) authorization requests, use the **username mac** command in SSG login transparent submode. To disable the sending of the subscriber's MAC address and send the subscriber's IP address instead, use the **no** form of this command.

username mac

no username mac

Syntax Description

This command has no arguments or keywords.

Command Default

SSG sends the subscriber's IP address as the username (RADIUS attribute 1).

Command Modes

SSG login transparent submode

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use the **username mac** command to configure SSG to send a subscriber's MAC address as the username in TAL authorization requests.

Examples

The following example enables SSG to send a subscriber's MAC address as the username in TAL authorization requests:

```
username mac
```

Related Commands

Command	Description
query ip dhcp	Sends DHCP lease query requests for the subscriber session when no IP address is received in the accounting start record.
ssg query mac dhcp	Sends a DHCP lease query request to the DHCP server when a subscriber's MAC address is not known.