

Cisco IOS Software Release 12.2(16)BX for Cisco 10000 Series Router

This product bulletin provides information about Cisco IOS[®] Software Release 12.2(16)BX, which provides Cisco[®] Service Selection Gateway features for the Cisco 10000 Series Router.

These product bulletins are updated as needed to describe new features, memory requirements, hardware support, software platform deferrals, and changes to the microcode and related documents.

Cisco IOS Software Release 12.2(16)BX is based on the previous release, Cisco IOS Software Release 12.2(15)BX. Release 12.2(16)BX will run only on Cisco 10000 Series Performance Routing Engine PRE-2. There will be no support for PRE or PRE-1 routing engines.

New Features in Cisco IOS Software Release 12.2(16)BX

The following features and enhancements are newly supported on the Cisco 10000 Series Router in Cisco IOS Release 12.2(16)BX:

- Service Selection Gateway
- Field Diagnostics
- 8-Port DS3/E3 ATM Line Card

Service Selection Gateway

The Cisco 10000 Series Router supports the following Service Selection Gateway (SSG) features in Cisco IOS Software Release 12.2(16)BX:

Access Protocols

- *Subscriber side*—PPPoE, PPPoA, RBE, RFC 2684 IP
- *Network side*—ATM PVCs and subinterfaces, Ethernet interfaces and subinterfaces, packet-over-SONET (POS) interfaces, serial and channelized interfaces

SSG Logon and Logoff

- Single Host Logon
- SSG Autologoff
- SSG Prepaid and SSG Prepaid Idle Timeout
- SSG Session and Idle Timeout

Authentication and Accounting

- SSG Full Username RADIUS Attribute
- Account Login and Logout
- Service Connection and Termination

Service Selection Methods

- PPP Terminated Aggregation
- PTA-Multidomain
- Web Service Selection



Service Connection

- SSG AutoDomain
- SSG Open Garden
- SSG Port-Bundle Host Key
- Exclude Networks
- Mutually Exclusive Service Selection

Service Profiles

- Service Profiles and Cached Service Profiles

Interface Configuration

- Transparent Passthrough
- Multicast Protocols on SSG Interfaces

Policing

- SSG Hierarchical Policing

Redirection

- SSG TCP Redirect

Miscellaneous Features

- VPI/VCI Static Binding to a Service Profile
- RADIUS Virtual Circuit Logging
- AAA Server Group Support for Proxy Services
- Packet Filtering
- SSG Unconfig
- Per-Service Statistics

The following sections describe the Service Selection Gateway features. For more information about configuring these features, refer to the *Cisco 10000 Series Router Service Selection Gateway Configuration Guide*.

Single Host Logon

The Single Host Logon feature enables Cisco Subscriber Edge Services Manager (SESM) software to authenticate subscribers by using the PPP authenticated information from the SSG; a subscriber does not need to log on to the SESM. To log on to a service through the SESM Web application, a subscriber enters authentication information once for the PPP session and once for the service.

For non-PPP users, when a subscriber authenticates using the SESM application, the subscriber does not have to log on again for the remainder of the non-PPP session. However, the subscriber still has to log on to services.



SSG Autologoff

The SSG Autologoff feature enables SSG to verify connectivity with each host. SSG checks the status of the connection with each host at configured intervals. If SSG finds that a host is not reachable, SSG automatically initiates the logoff of that host. SSG has two methods of checking the connectivity of hosts: ARP ping and ICMP ping.

SSG Prepaid and SSG Prepaid Idle Timeout

The SSG Prepaid feature allows a user to connect to a service if the user has prepaid for the service. The SSG Prepaid feature is time-based only.

When SSG Prepaid is configured, SSG checks a subscriber's available credit to determine whether to connect the subscriber to the service and how long the connection can last. The billing server administers the subscriber's credit as a series of quotas. These quotas are allotments of available credit and represent the duration of use.

The SSG Prepaid Idle Timeout feature enables SSG to return residual quotas (allotments of prepaid credit) to the billing server from services that a user is logged into but not actively using. The SSG can reauthorize a user before the user completely consumes the allocated quota. The SSG Prepaid Idle Timeout feature also enhances the handling of a returned zero quota from the billing server. A user's connection to services can be open even when the billing server returns a zero quota. The SSG can notify the billing server when a connection fails, enabling the billing server to free quota reserved for the failed connection.

SSG Session and Idle Timeout

The Session-Timeout RADIUS attribute and the Idle-Timeout RADIUS attribute are two mechanisms used to prevent the SSG from continuing to allow traffic to pass from the IP address of a user who has disconnected from the network access server without logging out from the SSG. These attributes specify the following:

- *Session-Timeout RADIUS attribute*—Specifies the maximum length of time for which a host or connection object can remain continuously active.
- *Idle-Timeout RADIUS attribute*—Specifies the maximum length of time for which a session or connection can remain idle before it is disconnected.

SSG Full Username RADIUS Attribute

The Full Username RADIUS attribute allows SSG to include the user's full username and domain (user@service) in the RADIUS authentication and accounting requests.

Account Login and Logout

SSG sends a RADIUS accounting-request record to the local RADIUS server when a user logs in to or out of the SSG. The Acct-Status-Type attribute included in the accounting-request record indicates if the accounting-request marks the start of the user service or the end of the service.

When a user logs in, SSG sends an accounting-start record to RADIUS. When a user logs out, SSG sends an accounting-stop record.

Service Connection and Termination

SSG also sends a RADIUS accounting-request record to the local RADIUS server when a user accesses or terminates a service. The Acct-Status-Type attribute included in the accounting-request record indicates whether the accounting-request marks the start of the user service or the end of the service.



When a user accesses a service, SSG sends an accounting-start record to RADIUS. When a user terminates a service, SSG sends an accounting-stop record.

PPP Terminated Aggregation

PPP Terminated Aggregation (PTA) is a PPP selection method in which service selection is based on a structured domain name (for example, username@service.com). PTA terminates the PPP session into a single routing domain. Users can only access one service and users do not have access to the default network or SESM.

The PTA-MD exclusion list allows you to create a set of domains that you want to exclude from SSG processing.

PTA-Multidomain

PTA-Multidomain (PTA-MD) is a PPP selection method in which service selection is based on a structured domain name (for example, username@service.com). PTA-MD terminates the PPP sessions into multiple IP routing domains. SSG features and processing are applied to the user traffic and users can access one or more services at a time. PTA-MD service selection supports a wholesale VPN model where each domain is isolated from the other and has the capability to support overlapping IP addresses.

Web Service Selection

Web service selection enables users to concurrently access multiple on-demand services from a list of personalized services. The Cisco 10000 Series Router supports the Cisco SESM application for Web service selection.

The SESM application provides subscriber authentication, service selection, and service connection capabilities to subscribers of Internet services. Subscribers interact with the SESM Web application using a standard Internet browser. They do not need to download any software or plug-ins to use the SESM Web pages. After a subscriber successfully authenticates, the SESM Web application presents a list of services that the subscriber is currently authorized to use. The subscriber can gain access to one or more of those services by selecting them from a Web page. Alternatively, an automatic connection feature might provide automatic connection to services.

SSG AutoDomain

The SSG AutoDomain feature allows users to automatically connect to a service based on the domain part of the structured username specified in an Access-Request. When SSG AutoDomain is configured, user authentication is performed at the service (for example, at the AAA server within a corporate network), instead of at the network access server (NAS).

SSG Open Garden

An Open Garden is a collection of networks or Web sites that subscribers can access as long as they have physical access to the network. Subscribers do not have to provide authentication information before accessing the networks in an Open Garden. The network is not restricted by service selection, subscription, or policing.

SSG Port-Bundle Host Key

The SSG Port-Bundle Host Key feature enhances communication and functions between Cisco SSG and Cisco SESM by introducing a mechanism that uses the host source IP address and source port to identify and monitor subscribers. With the SSG Port-Bundle Host Key feature, SSG performs Port Address Translation (PAT) and Network Address Translation (NAT) on the HTTP traffic between the subscriber and the SESM server.



Exclude Networks

The Exclude Networks feature allows you to specify networks that you do not want users to automatically log on to.

Mutually Exclusive Service Selection

The Mutually Exclusive Service Selection feature restricts a subscriber to accessing only one service at a time in a specified group of services.

Service Profiles and Cached Service Profiles

Service profiles define the services that subscribers can select. Each service that is accessible has a profile that defines the attributes of the service. Service profiles are configured on the RADIUS server or directly on the Cisco 10000 Series Router. The RADIUS server or SESM downloads the service profiles to the router as needed.

The Cached Service Profiles feature enables SSG to use a cached copy of a service profile instead of downloading the profile from RADIUS every time a user logs on to the service.

SSG Hierarchical Policing

The Traffic Policing feature limits the transmission rate of traffic entering or leaving a node. In SSG, traffic policing can be used to allocate bandwidth between subscribers and between services to a particular subscriber to ensure all types of services are allocated a proper amount of bandwidth. SSG uses per-user and per-service policing to ensure bandwidth is distributed properly between subscribers (per-user policing) and between services to a particular subscriber (per-session policing). Because these policing techniques are hierarchical in nature (bandwidth can be first policed between users and then policed again between services to a particular user), the feature is called SSG Hierarchical Policing.

Transparent Passthrough

The Transparent Passthrough feature allows unauthenticated traffic to pass through an interface. Interfaces configured as transparent passthrough are treated as Cisco IOS Software interfaces and not SSG interfaces. The Cisco 10000 Series Router can receive transparent passthrough traffic on both the access side and the network side. When an interface is configured as transparent passthrough, SSG does not process the traffic to and from the interface or apply SSG features. Instead, Cisco IOS Software processes the traffic and applies Cisco IOS features.

Multicast Protocols on SSG Interfaces

SSG supports multicast traffic, which includes normal multicast packets and Internet Group Management Protocol (IGMP) packets. The multicast traffic is separate from the SSG traffic and is routed through normal Cisco IOS Software processing and features; it is not routed through SSG authentication or features such as per-service statistics or hierarchical policing.

SSG TCP Redirect

The SSG TCP Redirect feature redirects certain user packets to an alternative location that can handle the packets in a suitable manner. This feature works in conjunction with the SESM Web interface. SSG TCP Redirect forces subscribers to authenticate before accessing the network or specific services and ensures that subscribers are only allowed to access the services that the service provider wants them to.



The SSG TCP Redirect feature supports the following:

- Redirection for unauthenticated users
- Redirection for unauthorized services
- Initial captivation

For more information, refer to the “Service Selection Gateway” chapter in the *Cisco 10000 Series Router Service Selection Gateway Configuration Guide*.

VPI/VCI Static Binding to a Service Profile

The VPI/VCI Static Binding to a Service Profile feature allows users accessing SSG through a VPI/VCI or a range of VPIs/VCI to access the server. When a user session arrives on a VPI/VCI or a VPI/VCI range and the session specifies the username but does not specify the domain name, SSG maps the user session to the service to which the VPI/VCI or VPI/VCI range is bound.

RADIUS Virtual Circuit Logging

RADIUS Virtual Circuit (VC) Logging extends and modifies the RADIUS network access server (NAS) port field to carry VPI/VCI information. With RADIUS VC Logging enabled, the Cisco 10000 Internet router (the SSG node) can send NAS port information to the RADIUS server, accurately recording the virtual path interface (VPI) and virtual circuit interface (VCI) of an incoming user or subscriber session. The VPI/VCI of the incoming permanent virtual circuit (PVC) is recorded at the point of entry on SSG, which offers the RADIUS client a unique VPI/VCI for each incoming PVC. This information is logged in the RADIUS accounting record that was created at session startup.

AAA Server Group Support for Proxy Services

The AAA Server Group Support for Proxy Services feature allows you to configure multiple AAA servers for redundancy. The RADIUS Server attribute enables AAA server group support for proxy services. Each group is associated with a service that requires proxy RADIUS AAA. You can configure each remote RADIUS server with timeout and retransmission parameters. When necessary, the SSG performs failover among the servers in the predefined group.

Packet Filtering

The Cisco 10000 Series Router supports per-user ACLs to prevent users from accessing specific IP addresses and ports. When an ACL attribute is added to a user profile, the attribute applies globally to all the user’s traffic.

SSG accepts Cisco IOS ACLs and SSG ACLs. SSG ACLs take precedence over Cisco IOS ACLs when both Cisco IOS and SSG ACLs are configured on the same SSG interface.

An SSG ACL can have a maximum of eight access-list entries (ACEs). If you use the TCP Redirect feature, TCP Redirect uses one of the eight ACEs; therefore, you can configure only seven ACEs.

SSG Unconfig

The SSG Unconfig feature enhances your ability to disable SSG at any time and releases the data structures and system resources created by SSG when SSG is unconfigured.

SSG Unconfig removes SSG allocated resources when you globally disable SSG after it was enabled. When you enable SSG, the SSG subsystem in the Cisco IOS Software acquires system resources that are never released, even after you disable SSG. The SSG Unconfig feature enables you to release and clean up system resources when SSG is not in use.



Per-Service Statistics

The Cisco 10000 Series Router collects statistics about router interfaces and the connections to them in both the input and output directions. Cisco CLI commands, such as show interface, are used to display information about the interfaces. SSG commands, such as show ssg connection, are used to display information about the connection to the router.

Field Diagnostics

Field Diagnostics provides customers with a method of testing and verifying line card hardware problems.

If you would like to perform a hardware diagnostic test on any line card in your Cisco 10000 Series Router, a Field Diagnostic image can be downloaded free of charge from Cisco Systems® and used to test whether the line card problems are indeed due to faulty hardware. The test results will verify whether or not the hardware is faulty.

For additional information about Field Diagnostic tests, refer to the *Field Diagnostics for the Cisco 10000 Series Router* at:

<http://www.cisco.com/univercd/cc/td/doc/product/aggr/10000/tblshoot/fdiags/index.htm>

8-Port DS3/E3 ATM Line Card

The 8-port DS3/E3 ATM line card is a full-height card that provides eight DS3 or E3 connections to ATM networks. The line card function focuses on Layer 2 ATM services and relies on the performance routing engine (PRE, Part Number ESR-PRE2) to provide Layer 3 services. The DS3/E3 ATM line card receives and transmits ATM cells on the physical interfaces while transmitting and receiving packets from the backplane.

The 8-port DS3/E3 ATM line card provides the following hardware features:

- Eight DS3/E3 ports on a full-height, single-slot line card
- Rear chassis cabling with BNC connectors
- DS3 features:
 - Per-interface M23 or C-bit parity framing mode
 - Per-line-card DSX3 modes: T3 ADM, T3 PLCP
 - DS3 line or payload loopback
 - Internal or loop timing
 - Per-interface line build out: 450 ft. of 75-ohm coaxial cable
- E3 features:
 - Per-interface G.751 or G.832 framing mode
 - Per-line-card DSX3 modes: E3 ADM, E3 PLCP
 - E3 line or payload loopback
 - Internal or loop timing
- ATM features:
 - Supports up to 32,000 VCs per line card, maximum of 4000 VCs per port, all 16 VCI and 8 VPI bits are available
 - Supports AAL5 data transport, F4 and F5 OAM cells
 - Per-VC and per-VP traffic shaping
- 64-MB packet memory in each direction



Mixing DSX3 modes on a per-port basis is not supported. When you configure the 8-port E3/DS3 ATM line card for a DSX3 mode, all eight ports of the line card operate in the mode you have selected.

The DS3/E3 ATM line card supports the throughput rates and ATM framing for the specified DSX3 modes as shown in Table 1.

Table 1 Throughput Rates and ATM Framing Information

DSX3 Mode	Throughput Rate	ATM Framing
T3 ADM	44200 kbps	CBIT or M23
T3 PLCP	40700 kbps	CBIT or M23
E3 ADM	34000 kbps	G.751 or G.832
E3 PLCP	30600 kbps	G.751 only

For more information, refer to the “Configuring the 8-Port E3/DS3 ATM Line Card” in the *Cisco 10000 Series Router Software Configuration Guide*.

Cisco 10000 Series Router MIB Enhancements

Cisco IOS Software Release 12.2(16)BX adds support for the CISCO-SSG-MIB. For more information about the MIB capabilities on the router, refer to the *Cisco 10000 Series Broadband MIB Specifications Guide*. (Chapter 3, “MIB Specifications,” lists MIBs constraints.). Or refer to:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

Product Numbers

Table 2 provides the product part numbers associated with this product bulletin.

Note: PRE-2s ship with 1 GB of SDRAM, 64 MB of Boot Flash, and a 64-MB PCMCIA Flash disk (with an option to upgrade to 128 MB).

Table 2 Cisco IOS Software Release 12.2(16)BX Feature Sets, Images, and Memory Recommendations

Standard Licenses					
Platform	Product Description	Product Code	Image	Flash	DRAM
Cisco 10000	Cisco 10000 Series IOS BROADBAND ROUTER 8K subscribers	S10KZ11A-12216BX	c10k2-p11-mz	64 MB	1 GB
Cisco 10000	Cisco 10000 Series IOS BROADBAND ROUTER 16K	S10KZ11B-12216BX	c10k2-p11-mz	64 MB	1 GB
Cisco 10000	Cisco 10000 Series IOS BROADBAND ROUTER 32K	S10KZ11C-12216BX	c10k2-p11-mz	64 MB	1 GB
Cisco 10000	Cisco 10000 Series IOS BROADBAND ROUTER 48K	S10KZ11D-12216BX	c10k2-p11-mz	64 MB	1 GB



Table 2 Cisco IOS Software Release 12.2(16)BX Feature Sets, Images, and Memory Recommendations

Standard Licenses					
Platform	Product Description	Product Code	Image	Flash	DRAM
Cisco 10000	Cisco 10000 Series IOS BROADBAND ROUTER 61.5K	S10KZ11E-12216BX	c10k2-p11-mz	64 MB	1 GB
Cisco 10000	Cisco 10000 Series IOS SERVICE PROVIDER/SECURED SHELL 3DES	S10KK5Z-12216BX	C10k2-k9p11-mz	64 MB	1 GB
License Upgrades					
Cisco 10000	Cisco 10000 Series IOS BROADBAND ROUTER UPGRADE 8K-16K	S10KZ11AB-12216BX	c10k2-p11-mz	64 MB	1 GB
Cisco 10000	Cisco 10000 Series IOS BROADBAND ROUTER UPGRADE 8K-32K	S10KZ11AC-12216BX	c10k2-p11-mz	64 MB	1 GB
Cisco 10000	Cisco 10000 Series IOS BROADBAND ROUTER UPGRADE 8K-48K	S10KZ11AD-12216BX	c10k2-p11-mz	64 MB	1 GB
Cisco 10000	Cisco 10000 Series IOS BROADBAND ROUTER UPGRADE 8K-61.5K	S10KZ11AE-12216BX	c10k2-p11-mz	64 MB	1 GB
Cisco 10000	Cisco 10000 Series IOS BROADBAND ROUTER UPGRADE 16K-32K	S10KZ11BC-12216BX	c10k2-p11-mz	64 MB	1 GB
Cisco 10000	Cisco 10000 Series IOS BROADBAND ROUTER UPGRADE 16K-48K	S10KZ11BD-12216BX	c10k2-p11-mz	64 MB	1 GB
Cisco 10000	Cisco 10000 Series IOS BROADBAND ROUTER UPGRADE 16K-61.5K	S10KZ11BE-12216BX	c10k2-p11-mz	64 MB	1 GB
Cisco 10000	Cisco 10000 Series IOS BROADBAND ROUTER UPGRADE 32K-48K	S10KZ11CD-12216BX	c10k2-p11-mz	64 MB	1 GB
Cisco 10000	Cisco 10000 Series IOS BROADBAND ROUTER UPGRADE 32K-61.5K	S10KZ11CE-12216BX	c10k2-p11-mz	64 MB	1 GB
Cisco 10000	Cisco 10000 Series IOS BROADBAND ROUTER UPGRADE 48K-61.5K	S10KZ11DE-12216BX	c10k2-p11-mz	64 MB	1 GB

Download Information

Registered Cisco.com customers with Cisco software support contracts can download Cisco IOS Software Release 12.2(16)BX software at the following URL:

<http://www.cisco.com/kobayashi/sw-center/sw-ios.shtml>

Additional Sources

For more information about Cisco IOS Software Release 12.2(16)BX, please refer to the following sources:

Release Notes for Cisco IOS Release 12.2(16)BX:

http://www.cisco.com/en/US/products/hw/routers/ps133/prod_release_note09186a008019ef2e.html

Cisco 10000 Series MIB Specifications Guide:

http://www.cisco.com/en/US/products/hw/routers/ps133/products_mib_quick_reference_chapter09186a00804d37f1.html



Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the
Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992-2003 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, the Cisco Systems logo, and Cisco IOS are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site 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.
(0304R) CCGSP_VT_LW4911_08/03