

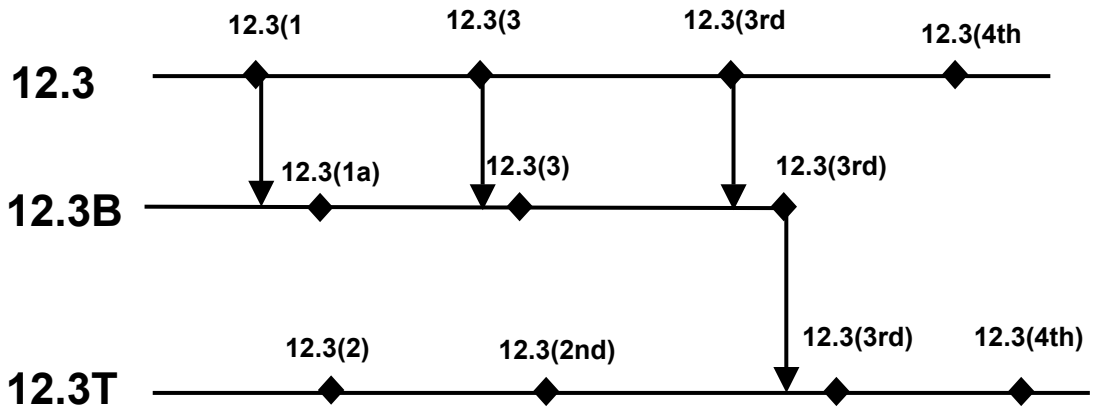
# Cisco IOS Software Early Deployment Release 12.3B

## Introduction

The purpose of this product bulletin is to announce the Cisco IOS® Software Early Deployment Release 12.3B. This product bulletin describes the content and delivery information about Cisco IOS® Software Release 12.3B. This release focuses on the Cisco 7200 Series, 7301, 7400 Series, and Multiprocessor WAN Application Module (MWAM) platforms. The features delivered with this release train will be incorporated into the Cisco IOS Software Release 12.3 (3rd)T release, but Cisco IOS Software Release 12.3B represents a release vehicle that provides these features sooner. There are no other features planned for 12.3B other than those listed in the Software feature section of this product bulletin (Table 1). Rebuilds of the maintenance release will be provided as instructed by Product Security Incident Response Team (PSIRT) when the maintenance release is vulnerable to security defect. For more information about the Cisco IOS Software release process, see Cisco Product Bulletin 537.

Figure 1 displays Cisco IOS Software Release 12.3B capability relative to the 12.3 and 12.3T releases. There are three maintenance releases planned for 12.3B. This diagram also identifies the recommended migration path.

Figure 1. 12.3B Migration Guide



## New Features in Cisco IOS Release 12.3B

The following features will be delivered in the initial release of 12.3B  
 Table 1. Cisco IOS Release Features in 12.3B



	Platform 1	Platform 2	Platform 3
	7200	7301	7401
SSG EAP SIM Enhancements	X	X	X
IP Pool Backup	X	X	X
MQC Hierarchical Shaping in PXF	X	X	X
Multilink PPP minimum links Mandatory	X	X	X
PPPoE Session Limit per NAS Port	X	X	X
RFC 2867 Radius Tunnel Accounting	X	X	X
Service Selection Gateway	X	X	X
SSG Auto log off Enhancement			
SSG ARP Ping	X	X	X
SSG Complete ID	X	X	X
SSG EAP Transparency			
SSG Open Garden Configuration Enhancements	X	X	X
SSG L2TP Dial-out	X	X	X
SSG Prepaid Enhancements	X	X	X
SSG Prepaid Idle Time Out	X	X	X
SSG Proxy for CDMA 2000	X	X	X
SSG Proxy for CDMA 2000 for Mobile IP	X	X	X
Dynamic Home Agent Assignment	X	X	X
Multiple Radius Server Support	X	X	X
SSG PTA-MD Exclusion Lists	X	X	X
SSG Range Command Bind Statements	X	X	X
SSG Service Profile Caching	X	X	X
SSG Support of NAS port ID	X	X	X
SSG Suppression of Unused Accounting Records	X	X	X
SSG Unique Session ID	X	X	X
VRF in PXF			X
MQC Hierarchical Shaping in PXF			X



The next section lists documents that address details on these new features. Any early deployment release of software should be used first in a test network before being deployed in a production network.

## Hardware Feature

### *Cisco 7301 Router Platform*

Platforms: Cisco 7301 routers

The Cisco 7301 Router provides application-specific features for broadband subscriber aggregation and network application services with high-processing performance.

Each Cisco 7301 router consists of the following features:

- Small form factor—One-rack-unit (1RU) high with stacking capability:  
1.72 x 17.3 x 13.87 in. (4.27 x 43.9 x 30 cm); the weight is approximately 10.5 lb (4.76 kg)
- Three native Gigabit Ethernet interfaces—six ports:
  - Three optical fiber Gigabit Ethernet (1000-Mbps) ports that use Small Form-Factor Pluggable (SFP) gigabit interface converters (GBICs) with LC connectors
  - Three Gigabit Ethernet (10-/100-/1000-Mbps) ports with RJ-45 connectors (any three ports are available at any one time)
- Both 25- and 50-MHz port adapter operation
- A 64- or 128-MB compact Flash disk
- Two SFP GBIC modules: SX and LH options
- Power supplies:
  - Single or dual AC power supplies
  - Single 24-VDC power supply
  - Dual 48-VDC power supply
- BCM 1250 microprocessor that operates at an internal clock speed of 700 MHz
- 512-KB boot ROM
- 32-MB boot Flash
- Three synchronous dynamic RAM (SDRAM) memory options: 256 MB, 512 MB, and 1 GB
- Auxiliary port
- Console port
- Online insertion and removal (OIR)—Allows you to add, replace, or remove port adapters with minimal interruption of the system
- Environmental monitoring and reporting functions—Allow you to maintain normal system operation by resolving adverse environmental conditions prior to loss of operation
- Downloadable software—Allows you to load new images into Flash memory remotely, without having to physically access the router, for fast, reliable upgrades
- Front-to-back airflow—Allows you to mount the router from either front or back into 19-inch two-post racks and 21- to 23-inch four-post racks



## Software Features

Platforms: Cisco 7200 Series routers, Cisco 7301 routers, and Cisco 7401 Application Specific Router

### IP Pool Backup

Platforms: Cisco 7200 Series routers, Cisco 7301 routers, and Cisco 7401 ASR routers

The IP Pool Backup feature introduces two new interface configuration commands, **peer pool backup** and **peer pool static**, which allow you to define alternate sources for IP address pools if the original address pool is not present or is exhausted.

The **peer pool backup** command is useful in large-scale dial-out environments with large numbers of independently controlled authentication, authorization, and accounting (AAA) servers that can make it difficult for the network access server to provide proper IP address pool resolution in the following cases:

- A new pool name is introduced by one of the AAA servers before that pool is set up on the network access server.
- An existing local pool becomes exhausted, but the owner of that AAA server has other pools that would be acceptable as an IP address source.

The **peer pool backup** command uses the local pool names configured with the **peer default ip address pool** interface configuration command to supplement the pool names supplied by AAA. The problems of pool name resolution and specific local pool exhaustion can be solved by configuring backup pool names on a per-interface basis using the **peer default ip address pool** and **peer pool backup** interface configuration commands.

The **peer pool static** command controls attempts by the pool software to load dynamic pools in response to a pool request from a specific interface. These dynamic pools are loaded at system startup and refreshed whenever a pool name not configured on the network access server is specified for IP address allocation. Because the behavior of the network access server in response to a missing pool name can be changed using the **peer pool backup** interface configuration command, you can use the **peer pool static** command to control attempts to load all dynamic pools when the AAA-supplied pool name is not an existing local pool name.

### MQC Hierarchical Shaping in PXF

Platforms: Cisco 7401 ASR routers

MQC hierarchical shaping in PXF implements MQC hierarchical shaping in the hardware accelerated PXF path.

### PXF

The PXF processor enables parallel IP multi-packet processing functions, working with the Route Processor to provide accelerated packet switching, as well as accelerated IP Layer 3 feature processing.

For more information about PXF, including troubleshooting information, refer to the [Cisco 7401 ASR Installation and Configuration Guide](#).

### MQC



MQC is designed to simplify the configuration of quality of service (QoS) on Cisco routers and switches by defining common command syntax and resulting set of QoS behaviors across platforms. This model replaces the previous model of defining unique syntaxes for each QoS feature and for each platform.

The MQC contains the following three steps:

1. Define a traffic class by issuing the **class-map** command.
2. Create a traffic policy by associating the traffic class with one or more QoS features by issuing the **policy-map** command.
3. Attach the traffic policy to the interface, subinterface, or virtual circuit by issuing the **service-policy** command.

For more information about MQC, refer to the [Modular Quality of Service Command-Line Interface](#) document.

### Hierarchical Shaping

Using hierarchical shaping, it is possible to configure a group of classes to which Class-Based Weighted Fair Queuing (CBWFQ) is applied. These separate classes can then be treated as an aggregate class for the purpose of shaping among other classes.

For more information about other QoS features supported by PXF, refer to the “[Quality of Service Features for Parallel Express Forwarding](#)” section of the *Release Notes for Cisco 7000 Family for Cisco IOS Software Release 12.2 B* for Cisco IOS Software Release 12.2(4)B.

## VRF in PXF

Platforms: Cisco 7200 Series routers, Cisco 7301 routers, and Cisco 7401 ASR routers

Virtual Route Forwarding (VRF) in PXF implements VRF+ in the PXF path.

### PFX

The PXF processor enables parallel IP multipacket processing functions, working with the Route Processor to provide accelerated packet switching, as well as accelerated IP Layer 3 feature processing.

For more information about PXF, including troubleshooting information, refer to the [Cisco 7401 ASR Installation and Configuration Guide](#).

### MQC

MQC is designed to simplify the configuration of QoS on Cisco routers and switches by defining a common command syntax and resulting set of QoS behaviors across platforms. This model replaces the previous model of defining unique syntaxes for each QoS feature and for each platform.

The MQC contains the following three steps:

1. Define a traffic class by issuing the **class-map** command.
2. Create a traffic policy by associating the traffic class with one or more QoS features by issuing the **policy-map** command.
3. Attach the traffic policy to the interface, subinterface, or virtual circuit by issuing the **service-policy** command.

For more information about MQC, refer to the [Modular Quality of Service Command-Line Interface](#) document.

### Hierarchical Shaping

Using hierarchical shaping, it is possible to configure a group of classes to which CBWFQ is applied within that group of classes. These separate classes can then be treated as an aggregate class for the purpose of shaping among other classes.



For more information about other QoS features supported by PXF, refer to the “[Quality of Service Features for Parallel Express Forwarding](#)” section of the *Release Notes for Cisco 7000 Family for Cisco IOS Software Release 12.2 B* for Cisco IOS Software Release 12.2(4)B.

## VRF

A VRF consists of an IP routing table, a derived Cisco Express Forwarding CANNOT USE C FOR CISCO IN ACRONYMS FOR LEGAL REASONS] table (including Forwarding Information Base [FIB] and Adjacency tables), and a set of interfaces that use this forwarding table. A VRF consists of the following:

- IP routing table
- Cisco Express Forwarding table
- Set of interfaces that use the Cisco Express Forwarding table
- Set of rules and routing protocol parameters to control the information in the routing tables

VRF PXF offloads any VRF-related routing from the Route Processor to the PXF.

## Multilink PPP Minimum Links Mandatory

Platforms: Cisco 7200 Series routers, Cisco 7301 routers, and Cisco 7401 ASR routers

MLPPP allows multiple PPP links to be established in parallel to the same destination. MLPPP is often used with dialup lines or ISDN connections to easily increase the amount of bandwidth between points.

With the introduction of the MLPPP Minimum Links Mandatory feature, you can configure the minimum number of links in a MLPPP bundle required to keep that bundle active by entering the **ppp multilink min-links links mandatory** command. When you configure this command, all Network Control Programs (NCPs) for an MLPPP bundle are disabled until the MLPPP bundle has the required minimum number of links. When a new link is added to the MLPPP bundle that brings the number of links up to the required minimum number of links, the NCPs are activated for the MLPPP bundle. When a link is removed from an MLPPP bundle and the number of links falls below the required minimum number of links for that MLPPP bundle, the NCPs are disabled for that MLPPP bundle.

## PPPoE Session Limit per Network-Access-Server Port

Platforms: Cisco 7200 Series routers, Cisco 7301 routers, and Cisco 7401 ASR routers

Using the PPPoE Session Limit per Network-Access-Server Port feature, you can limit the number of sessions on a specific virtual circuit or VLAN configured on a L2TP access concentrator (LAC). The network-access-server port is either an ATM virtual circuit or a configured VLAN ID.

The PPPoE session limit per network-access-server port is maintained in a RADIUS server customer-profile database. This customer-profile database is connected to a LAC and is separate from the RADIUS server that the LAC and L2TP network server (LNS) use for the authentication and authorization of incoming users. When the customer profile database receives a preauthorization request from the LAC, it sends the PPPoE per network-access-server port session limit to the LAC.

The LAC sends a preauthorization request to the customer-profile database when the LAC is configured for subscriber-service-switch (SSS) preauthorization. Configure the LAC for SSS preauthorization using the **sss-subscriber access pppoe pre-authorize** command. When the LAC receives the PPPoE per network-access-server port session limit from the customer-profile database, the LAC compares the PPPoE per network-access-server port session limit to the number of sessions currently on the network-access-server port. The LAC then decides whether to accept or reject the current call based upon the configured PPOE per network-access-server port session limit and the number of calls currently on the network-access-server port.



You can configure other types of session limits on the LAC, including session limit per virtual circuit, per VLAN, per MAC, or a global session limit for the LAC. When PPPoE Session Limit per Network-Access-Server Port is enabled (that is, when you have enabled SSS preauthorization on the LAC), local configurations for session limit per virtual circuit and per VLAN are overwritten by the PPPoE per network-access-server port session limit downloaded from the customer-profile database. Configured session limits per virtual circuit and per VLAN serve as backups in case of a PPPoE per network-access-server port session limit download failure.

The customer-profile database consists of user profiles for each user connected to the LAC. Each user profile contains the NAS-IP-Address (Attribute #4) and the NAS-Port-ID (Attribute #5.) When the LAC is configured for SSS preauthorization, it queries the customer-profile database using the username. When a match is found in the customer-profile database, the customer-profile database sends the PPPoE per network-access-server port session limit in the user profile. The PPPoE per network-access-server port session limit is defined in the username as a Cisco attribute-value pair.

## RFC 2867 RADIUS Tunnel Accounting

Platforms: Cisco 7200 Series routers, Cisco 7301 routers, and Cisco 7401 ASR routers

The RFC 2867 RADIUS Tunnel Accounting feature introduces six new RADIUS accounting types that are used with the RADIUS accounting attribute Acct-Status-Type (attribute 40), which indicates whether an accounting request marks the beginning of user service (start) or the end (stop). These new accounting types are designed to support the provision of compulsory tunneling in dialup networks; that is, these attribute types allow you to better track tunnel status changes.

This feature also introduces two new commands—**vpdn session accounting network** (tunnel-link-type records) and **vpdn tunnel accounting network** (tunnel-type records)—that help identify the following events:

- A virtual-private-dialup-network (VPDN) tunnel is brought up or destroyed.
- A request to create a VPDN tunnel is rejected.
- A user session within a VPDN tunnel is brought up or brought down.
- A user session create request is rejected.
  - The first two events are tunnel-type accounting records: AAA sends Tunnel-Start, Tunnel-Stop, or Tunnel-Reject accounting records to the RADIUS server. The next two events are tunnel-link-type accounting records: AAA sends Tunnel-Link-Start, Tunnel-Link-Stop, or Tunnel-Link-Reject accounting records to the RADIUS server.
  - The accounting types are divided into two separate tunnel types so users can decide if they want tunnel type, tunnel-link type, or both types of accounting.

## Service Selection Gateway

Platforms: Cisco 7200 Series routers, Cisco 7301 routers, and Cisco 7401 ASR routers

### SSG

**Cisco Service Selection** is an extensible solution that supports value added, billable services over most access methods. Service Selection solution is a combination hardware/software that allows subscribers to select various network-based services and applications independently or simultaneously. Service Selection has many unique features that allows subscribers to select services, dynamically change bandwidth and many other features like "captive portal". Service Selection requires a [Cisco IOS](#) based router that supports Service Selection Gateway , SSG, feature set, [Subscriber Edge Services Manager, SESM](#), software, which takes care of the User Interface



aspects: selection, notification and has hooks into SSG and an [Authentication system](#) that can be RADIUS or Directory based.

SSG is a solution for service providers that offer intranet, extranet, and Internet connections to subscribers using broadband access technology such as xDSL, cable modems, or wireless to allow simultaneous access to network services.

For more information about SSG, refer to the [Service Selection Gateway](#) document.

### **EAP SIM Enhancements**

Cisco offers two EAP-SIM enhancements:

- AZR issue—This SSG cleans up the active hosts (EAP-SIM and Cisco Subscriber Edge Services Manager [SESM]) users on receiving an Accounting On/Off from AZR due to a reboot. It is needed to close a security hole through which an illegal user can seize the session of a valid user by using the IP address of the valid user after the AZR reboot.
- Cisco SESM reconnect for EAP-SIM users—this requires that EAP-SIM users access the Cisco SESM and perform an account logoff. Subsequent to the logoff they can access the Cisco SESM and do accounts logon again.

## **SSG Auto-logoff Enhancement**

Platforms: Cisco 7200 Series routers, Cisco 7301 routers, and Cisco 7401 ASR routers

The SSG Auto-logoff Enhancement feature configures SSG to check the MAC address of a host each time that SSG performs an ARP ping. If SSG finds that the MAC address of the host has changed, SSG automatically initiates the logoff of that host. This prevents unauthorized reuse of IP addresses (spoofing). SSG MAC address checking also detects the assignment of a host IP address to a different host before the original host initiates a logoff and clears its host object. This prevents session reuse by a second host.

### **ARP Ping**

The ARP is an Internet protocol used to map IP addresses to MAC addresses in directly connected devices. A router that uses ARP broadcasts ARP requests for IP address information. When an IP address is successfully associated with a MAC address, the router stores the information in the ARP cache.

When SSG Auto-logoff is configured to use ARP ping, SSG periodically checks the ARP cache tables. If a table entry for a host is found, SSG forces ARP to refresh the entry and checks the entry again after a configured interval. If a table entry is not found, SSG initiates Auto-logoff for the host. However, if any data traffic to or from the host occurred during the interval, SSG does not ping the host because the reach ability of the host during that interval was established by the data traffic.

When SSG MAC address checking is configured, SSG checks the MAC address of a host when an ARP ping is performed. If SSG detects a different host MAC address, it initiates an automatic logoff of that host.

ARP ping should be used only in deployment scenarios 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 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 Auto-logoff to use ARP ping in scenarios where hosts are directly connected.



## SSG Complete ID

Platforms: Cisco 7200 Series routers, Cisco 7301 routers, and Cisco 7401 ASR routers

**Cisco Service Selection** is an extensible solution that supports value added, billable services over most access methods. Service Selection solution is a combination hardware/software that allows subscribers to select various network-based services and applications independently or simultaneously. Service Selection has many unique features that allows subscribers to select services, dynamically change bandwidth and many other features like "captive portal". Service Selection requires a [Cisco IOS](#) based router that supports Service Selection Gateway , SSG, feature set, [Subscriber Edge Services Manager, SESM](#), software, which takes care of the User Interface aspects: selection, notification and has hooks into SSG and an [Authentication system](#) that can be RADIUS or Directory based.

SSG is a solution for service providers that offer intranet, extranet, and Internet connections to subscribers using broadband access technology such as xDSL, cable modems, or wireless to allow simultaneous access to network services.

For more information about SSG, refer to the [Service Selection Gateway](#) document.

### SSG Complete ID

SSG Complete ID provides enhancements to the current interaction mechanism that is used between SSG and Cisco SESM, allowing SSG to pass along the following additional information:

- Client IP address
- Client MAC address
- Subinterface
- Virtual path identifier (VPI) and virtual channel identifier (VCI)

### MSISDN

[IF ACRONYM, DEFINE] MSISDN allows the Cisco SESM to offer greater customization of Web portals, specifically by locations. Each hotspot can now have its own branded portal.

## SSG EAP Transparency

Platforms: Cisco 7200 Series routers, Cisco 7301 routers, and Cisco 7401 ASR routers

### SSG

**Cisco Service Selection** is an extensible solution that supports value added, billable services over most access methods. Service Selection solution is a combination hardware/software that allows subscribers to select various network-based services and applications independently or simultaneously. Service Selection has many unique features that allows subscribers to select services, dynamically change bandwidth and many other features like "captive portal". Service Selection requires a [Cisco IOS](#) based router that supports Service Selection Gateway , SSG, feature set, [Subscriber Edge Services Manager, SESM](#), software, which takes care of the User Interface aspects: selection, notification and has hooks into SSG and an [Authentication system](#) that can be RADIUS or Directory based.



SSG is a solution for service providers that offer intranet, extranet, and Internet connections to subscribers using broadband access technology such as xDSL, cable modems, or wireless to allow simultaneous access to network services.

For more information about SSG, refer to the [Service Selection Gateway](#) document.

### **SSG EAP Transparency**

The SSG EAP Transparency feature allows SSG to transparently pass EAP-SIM, EAP-Transport Layer Security (TLS) and Cisco EAP (LEAP) authentication.

## **SSG Open-Garden-Configuration Enhancements**

Platforms: Cisco 7200 Series routers, Cisco 7301 routers, and Cisco 7401 ASR routers

### **SSG**

**Cisco Service Selection** is an extensible solution that supports value added, billable services over most access methods. Service Selection solution is a combination hardware/software that allows subscribers to select various network-based services and applications independently or simultaneously. Service Selection has many unique features that allows subscribers to select services, dynamically change bandwidth and many other features like "captive portal". Service Selection requires a [Cisco IOS](#) based router that supports Service Selection Gateway, SSG, feature set, [Subscriber Edge Services Manager, SESM](#), software, which takes care of the User Interface aspects: selection, notification and has hooks into SSG and an [Authentication system](#) that can be RADIUS or Directory based.

SSG is a solution for service providers that offer intranet, extranet, and Internet connections to subscribers using broadband access technology such as xDSL, cable modems, or wireless to allow simultaneous access to network services.

For more information about SSG, refer to the [Service Selection Gateway](#) document.

### **SSG Open-Garden-Configuration Enhancements**

The SSG is a Cisco IOS feature that implements Layer 3 service selection through selective routing of IP packets to destination networks on a per-subscriber basis. Of its many features, SSG Open Garden is one that is very useful for service providers to provide trial-based services to customers.

An open garden is a collection of Websites that a user can access as long as the user has physical access to the network. The user does not need to provide any authentication information before accessing the Websites in the open garden.

Currently, SSG open-garden services can be configured and managed on the router itself, even though they are similar to normal SSG (subscribed) services. The modifications being proposed will allow open-garden services to be defined and managed on the RADIUS server as well.

## **SSG L2TP Dialout**

Platforms: Cisco 7200 Series routers, Cisco 7301 routers, and Cisco 7401 ASR routers

### **SSG**

**Cisco Service Selection** is an extensible solution that supports value added, billable services over most access methods. Service Selection solution is a combination hardware/software that allows subscribers to select various



network-based services and applications independently or simultaneously. Service Selection has many unique features that allows subscribers to select services, dynamically change bandwidth and many other features like "captive portal". Service Selection requires a [Cisco IOS](#) based router that supports Service Selection Gateway , SSG, feature set, [Subscriber Edge Services Manager, SESM](#), software, which takes care of the User Interface aspects: selection, notification and has hooks into SSG and an [Authentication system](#) that can be RADIUS or Directory based.

SSG is a solution for service providers that offer intranet, extranet, and Internet connections to subscribers using broadband access technology such as xDSL, cable modems, or wireless to allow simultaneous access to network services.

For more information about SSG, refer to the [Service Selection Gateway](#) document.

### **SSG L2TP Dialout**

The SSG L2TP Dial out feature enhances SSG tunnel services and provides a dial out facility to users. Many small offices/home offices (SOHOs) use the public switched telephone network (PSTN) to access their intranet. SSG L2TP provides mobile users with a way to securely connect to their SOHO through the PSTN.

To provide SSG L2TP Dial out, SSG requires a Digital Number Identification Service (DNIS) number for the SOHO to which the user wants to connect, the address of the LAC closest to the SOHO, and configured tunnel parameters to establish a tunnel to the LAC.

Users can access SSG L2TP Dial out by selecting the dial out service using Cisco SESM from the list of subscribed services or by using a structured username. The user must provide the DNIS number when using either method of connecting to the dial out service.

## **SSG Prepaid Enhancements**

Platforms: Cisco 7200 Series routers, Cisco 7301 routers, and Cisco 7401 ASR routers

### **SSG**

**Cisco Service Selection** is an extensible solution' that supports value added, billable services over most access methods. Service Selection solution is a combination hardware/software that allows subscribers to select various network-based services and applications independently or simultaneously. Service Selection has many unique features that allows subscribers to select services, dynamically change bandwidth and many other features like "captive portal". Service Selection requires a [Cisco IOS](#) based router that supports Service Selection Gateway , SSG, feature set, [Subscriber Edge Services Manager, SESM](#), software, which takes care of the User Interface aspects: selection, notification and has hooks into SSG and an [Authentication system](#) that can be RADIUS or Directory based.

SSG is a solution for service providers that offer intranet, extranet, and Internet connections to subscribers using broadband access technology such as xDSL, cable modems, or wireless to allow simultaneous access to network services.

For more information about SSG, refer to the [Service Selection Gateway](#) document.

### **SSG Prepaid**

The SSG Prepaid feature allows SSG to check a subscriber's available credit to determine whether to connect the subscriber to a service and how long the connection can last. The subscriber's credit is administered by the billing server as a series of quotas representing either duration of use (in seconds) or an allowable data volume (in bytes). A quota is an allotment of available credit.

To obtain the first quota for a connection, SSG submits an authorization request to the AAA server. The AAA server contacts the prepaid billing server, which forwards the quota values to SSG. SSG then monitors the connection to



track the quota usage. When the quota runs out, SSG performs reauthorization. During reauthorization, the billing server may provide SSG with an additional quota if there is available credit. If no further quota is provided, SSG logs off the user.

For more information, refer to the [SSG Prepaid](#) document.

### **SSG Prepaid Enhancements**

SSG Prepaid Enhancements introduces prepaid tariff switching, simultaneous volume- and time-based prepaid billing, and postpaid tariff switching.

## **SSG Prepaid Idle Timeout**

Platforms: Cisco 7200 Series routers, Cisco 7301 routers, and Cisco 7401 ASR routers

### **SSG**

**Cisco Service Selection** is an extensible solution that supports value added, billable services over most access methods. Service Selection solution is a combination hardware/software that allows subscribers to select various network-based services and applications independently or simultaneously. Service Selection has many unique features that allows subscribers to select services, dynamically change bandwidth and many other features like "captive portal". Service Selection requires a [Cisco IOS](#) based router that supports Service Selection Gateway , SSG, feature set, [Subscriber Edge Services Manager, SESM](#), software, which takes care of the User Interface aspects: selection, notification and has hooks into SSG and an [Authentication system](#) that can be RADIUS or Directory based.

SSG is a solution for service providers that offer intranet, extranet, and Internet connections to subscribers using broadband access technology such as xDSL, cable modems, or wireless to allow simultaneous access to network services.

For more information about SSG, refer to the [Service Selection Gateway](#) document.

### **SSG Prepaid**

The SSG Prepaid feature allows SSG to check a subscriber's available credit to determine whether to connect the subscriber to a service and how long the connection can last. The subscriber's credit is administered by the billing server as a series of quotas representing either duration of use (in seconds) or an allowable data volume (in bytes). A quota is an allotment of available credit.

To obtain the first quota for a connection, SSG submits an authorization request to the AAA server. The AAA server contacts the prepaid billing server, which forwards the quota values to SSG. SSG then monitors the connection to track the quota usage. When the quota runs out, SSG performs reauthorization. During reauthorization, the billing server may provide SSG with an additional quota if there is available credit. If no further quota is provided, SSG logs off the user.

For more information, refer to the [SSG Prepaid](#) document.

### **SSG Prepaid Idle Timeout**

The SSG Prepaid Idle Timeout feature enhances the SSG Prepaid feature by enabling SSG to return residual quota to the billing server from services that a user is logged into but not actively using. The quota that is returned to the billing center can be applied to the quota for the services the user is actively using.

When SSG is configured for SSG Prepaid Idle Timeout, a user's connection to services can be open even when the billing server returns a zero quota, but the status of the connection depends on the combination of the quota and the



idle timeout value returned. Depending on the connection service, SSG requests the quota for a connection from the billing server after the user starts using a particular service, when the user runs out of quota, or after the configured idle timeout value has expired.

The SSG Prepaid Idle Timeout feature enhances handling of a returned zero quota from the billing server. If a billing server returns a zero quota and nonzero idle timeout, this indicates that a user has run out of credit for a service. When a user runs out of credit for a service, the user is redirected to the billing server to replenish the quota. When the user is redirected to the billing server, the user's connection to the original service or services is retained. Although the connection remains up, any traffic passing through the connection is dropped. This enables a user to replenish quota on the billing server without losing connections to services or having to perform additional service logons.

Using the SSG Prepaid Idle Timeout feature, you can configure SSG to reauthorize a user before the user completely consumes the allocated quota. You can also configure SSG to not pass traffic during reauthorization. This setup prevents revenue leaks if the billing server returns a zero quota for the user. Without the SSG Prepaid Idle Timeout feature, traffic passed during reauthorization represents a revenue leak if the billing server returns a zero quota for the user. You can prevent this type of revenue leak by configuring a threshold value, causing SSG to reauthorize a user's connection before the user completely consumes the allocated quota for a service.

SSG Prepaid Idle Timeout enhances SSG to inform the billing server upon any connection failure. This enables the billing server to free quota that was reserved for the connection that failed and to apply this quota immediately to some other active connection.

## **SSG Proxy for CDMA 2000**

Platforms: Cisco 7200 Series routers, Cisco 7301 routers, and Cisco 7401 ASR routers

The SSG Proxy for CDMA 2000 extends the functionality of the existing SSG RADIUS proxy so that it may be used in CDMA 2000 networks.

When used in a CDMA 2000 network, SSG provides RADIUS proxy services to the packet data serving node (PDSN) and the home agent for both simple IP and mobile IP authentication. SSG also provides service selection management and policy-based traffic direction for subscribers.

SSG Proxy for CDMA 2000, used with Cisco SESM, provides users with on-demand services and service providers with service management and subscriber management.

SSG Proxy for CDMA 2000 supports time- and volume-based usage accounting for simple IP and mobile IP sessions. Prepaid and postpaid services are supported. Host accounting records can be sent to multiple network elements, including content services gateways (CSGs), content optimization engines (COEs), and Wireless Application Protocol (WAP) gateways.

### **CDMA**

CDMA is a digital spread-spectrum modulation technique used mainly with personal communications devices such as mobile phones. CDMA digitizes the conversation and tags it with a special frequency code. The data is then scattered across the frequency band in a pseudorandom pattern. The receiving device is instructed to decipher only the data corresponding to a particular code to reconstruct the signal.

For more information about CDMA, refer to the "CDMA Overview" knowledge byte on the [Mobile Wireless Knowledge Bytes](#) Web page.

### **CDMA 2000**

CDMA 2000 RADIUS Transmission Technology (RTT) is a wideband, spread-spectrum radio interface that uses CDMA technology to satisfy the needs of third-generation (3G) wireless communication systems. CDMA 2000 is backward-compatible with CDMA.

For more information about CDMA 2000, refer to the "CDMA 2000 Overview" knowledge byte on the [Mobile Wireless Knowledge Bytes](#) Web page.

### **SSG**



**Cisco Service Selection** is an extensible solution that supports value added, billable services over most access methods. Service Selection solution is a combination hardware/software that allows subscribers to select various network-based services and applications independently or simultaneously. Service Selection has many unique features that allows subscribers to select services, dynamically change bandwidth and many other features like "captive portal". Service Selection requires a [Cisco IOS](#) based router that supports Service Selection Gateway, SSG, feature set, [Subscriber Edge Services Manager, SESM](#), software, which takes care of the User Interface aspects: selection, notification and has hooks into SSG and an [Authentication system](#) that can be RADIUS or Directory based.

SSG is a solution for service providers that offer intranet, extranet, and Internet connections to subscribers using broadband access technology such as xDSL, cable modems, or wireless to allow simultaneous access to network services.

For more information about SSG, refer to the [Service Selection Gateway](#) document.

### **SSG Proxy for CDMA 2000 for Simple IP**

When used in a CDMA 2000 environment, SSG acts as a RADIUS proxy to the PDSN and to the home agent for simple IP authentication. SSG sets up a host object for the following three access modes:

- Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP) authentication—In this mode, PAP and CHAP are performed during PPP setup and the network access identifier (NAI) is received from a mobile node.
- Mobile station identifier (MSID)-based access—In this mode, the mobile node does not negotiate CHAP or PAP and no NAI is received by the PDSN. The PDSN does not perform additional authentication; it constructs an NAI based on the MSID and generates accounting records. Because a user password is not available from the mobile node, a globally configured password is used as the service password.
- MSID-based access - Cisco variant—In this mode, a Cisco PDSN supports MSID-based access by using a realm retrieved from the RADIUS server. This realm is retrieved during an extra authentication phase with the RADIUS server.

SSG operating in a CDMA 2000 network correlates Accounting-Start and Accounting-Stop requests. A PDSN may send out many Accounting-Start and Accounting-Stop requests during a session. These Accounting-Start and Accounting-Stop requests can be generated by PDSN hand-off, packet-control-function (PCF) hand-off, interim accounting, and time-of-date accounting. SSG terminates a session only when it receives an Accounting-Stop request with the 3GPP2-Session-Continue vendor-specific attribute (VSA) set to "FALSE" or if a subsequent Accounting-Start request is not received within a configured timeout. PPP renegotiation during a PDSN hand-off is treated as a new session.

In SSG Proxy for CDMA 2000 for simple IP, the end-user IP address may be assigned statically by the PDSN, RADIUS server, or SSG. The end-user IP address also can be assigned directly from the automain service.

Network Address Translation (NAT) is automatically performed when necessary. NAT is generally necessary when IP address assignment is performed by any mechanism other than directly from the automain service (which may be a VPN). You can also configure SSG to always use NAT.

If the user profile contains Cisco attribute-value pairs of VPDN attributes, SSG initiates L2TP VPN.

### **SSG Proxy for CDMA 2000 for Mobile IP**

For mobile IP, SSG functions as the RADIUS proxy for both PDSN and the home agent. SSG proxies PPP, PAP or CHAP and mobile-node and foreign-agent CHAP authentication. SSG Proxy for CDMA 2000 for Mobile IP can assign IP addresses statically by the PDSN, RADIUS server, or SSG. The end-user IP address can also be assigned directly from the automain service.



Home agent-mobile node (HA-MN) authentication and reverse tunneling must be enabled so that SSG can create host objects for mobile IP sessions based on proxied RADIUS packets received from the home agent.

The home agent must generate RADIUS accounting packets so that SSG can discover the user IP address and detect the termination of the session. Multiple mobile IP sessions with the same NAI are supported. RADIUS packets must contain the Accounting-Session-ID attribute to be associated with the correct user session. SSG correlates RADIUS packets from the PDSN in order to obtain MSID information for a host object of a mobile IP session. SSG can set up a host object either with or without PAP or CHAP performed during the original PPP session.

SSG initiates L2TP VPN according to the SSG tunnel service VSAs in the user's profile. If the user profile contains Cisco attribute-value pairs of VPDN, SSG sets up the L2TP tunnel per these VPDN attributes. SSG removes these attribute-value pairs when sending the Access-Accept packet back to the PDSN.

Either the home agent or the RADIUS server can assign the user's IP address.

### **Dynamic Home-Agent Assignment**

Dynamic home-agent assignment based on a mobile user's location is supported.

SSG proxy for CDMA 2000 provides three options for dynamic home-agent assignment:

- The RADIUS server selects the local home agent or any home agent that is configured for session requests. For foreign-user call requests, the AAA server assigns the home agent.
- SSG modifies the fixed home-agent address received from the RADIUS server to a local home-agent address. This method can be implemented without making any changes to the RADIUS server configuration. SSG does not modify the home-agent address for a foreign user. The foreign-user call request is registered with the home-agent address assigned by the AAA server.
- The PDSN implements dynamic home-agent assignment based on detection of the PDSN hand-off.

### **Multiple RADIUS Server Support**

SSG proxy for CDMA 2000 provides geographical redundancy by copying host object accounting packets and sending them to multiple RADIUS servers.

## **SSG PTA-MD Exclusion Lists**

Platforms: Cisco 7200 Series routers, Cisco 7301 routers, and Cisco 7401 ASR routers

Beginning in Cisco IOS Software Release 12.2(8)B, the option of passing the entire structured username in the form "user@service" to PPP for authenticating an SSG request became available. The entire structured username can be passed to PPP through the use of a PTA-MD exclusion list; if an entire structured username is passed to PPP, the domain (the "@service" portion of the structured username) should be added to a PTA-MD exclusion list. The PTA-MD exclusion list can be configured on the AAA server directly or via the router command-line interface (CLI). Structured usernames are parsed for authentication unless a PTA-MD exclusion list is configured for the particular domain requesting a service.

For additional information about SSG PTA-MD exclusion lists, refer to the SSG feature module.

## **SSG Range Command for BIND Statements**

Platforms: Cisco 7200 Series routers, Cisco 7301 routers, and Cisco 7401 ASR routers

### **SSG**

**Cisco Service Selection** is an extensible solution that supports value added, billable services over most access methods. Service Selection solution is a combination hardware/software that allows subscribers to select various



network-based services and applications independently or simultaneously. Service Selection has many unique features that allows subscribers to select services, dynamically change bandwidth and many other features like "captive portal". Service Selection requires a [Cisco IOS](#) based router that supports Service Selection Gateway , SSG, feature set, [Subscriber Edge Services Manager, SESM](#), software, which takes care of the User Interface aspects: selection, notification and has hooks into SSG and an [Authentication system](#) that can be RADIUS or Directory based.

SSG is a solution for service providers that offer intranet, extranet, and Internet connections to subscribers using broadband access technology such as xDSL, cable modems, or wireless to allow simultaneous access to network services.

For more information about SSG, refer to the [Service Selection Gateway](#) document.

### **SSG Range Command for BIND Statements**

SSG Range Command for BIND Statements creates a "range" command for SSG BIND statements. This is useful when provisioning RBE subscribers as a whole, because it allows for streamlined provisioning and configuration with a decreased CPU load.

## **SSG Service Profile Caching**

Platforms: Cisco 7200 Series routers, Cisco 7301 routers, and Cisco 7401 ASR routers

The SSG Service Profile Caching feature enhances the authentication process for SSG services by allowing users to authenticate a service using the service profile cached in SSG.

When SSG Service Profile Caching is not enabled, an AAA transaction is required to download a service profile each time an SSG subscriber logs on to the service. The other SSG subscribers already logged on to the service also have their service parameters automatically refreshed as a result of this AAA transaction. In many cases, this automatic refresh causes unnecessary traffic in SSG and on the AAA server.

The SSG Service Profile Caching feature creates a cache of service profiles in SSG. A service profile is downloaded from the AAA server and then stored in the SSG service-profile cache as a service-info object. Subsequent SSG subscribers hoping to use that service are authorized by the SSG service-profile cache provided that service profile remains in the cache. To ensure that the service profiles in the SSG service-profile cache remain updated, the SSG service-profile cache automatically refreshes the service profiles by downloading the service profiles from the AAA server at user-configured intervals (the default is every 120 minutes). SSG service-profile caches also can be refreshed manually at any time. Service profiles that are not being used by any SSG subscriber are removed from the SSG service-profile cache.

## **SSG Support of Network-Access-Server Port ID**

Platforms: Cisco 7200 Series routers, Cisco 7301 routers, and Cisco 7401 ASR routers

### **SSG**

**Cisco Service Selection** is an extensible solution that supports value added, billable services over most access methods. Service Selection solution is a combination hardware/software that allows subscribers to select various network-based services and applications independently or simultaneously. Service Selection has many unique features that allows subscribers to select services, dynamically change bandwidth and many other features like "captive portal". Service Selection requires a [Cisco IOS](#) based router that supports Service Selection Gateway , SSG, feature set, [Subscriber Edge Services Manager, SESM](#), software, which takes care of the User Interface aspects: selection, notification and has hooks into SSG and an [Authentication system](#) that can be RADIUS or Directory based.



SSG is a solution for service providers that offer intranet, extranet, and Internet connections to subscribers using broadband access technology such as xDSL, cable modems, or wireless to allow simultaneous access to network services.

For more information about SSG, refer to the [Service Selection Gateway](#) document.

### **SSG Support of Network-Access-Server Port ID**

This feature carries the NAS-Port attribute in the authentication packet, thereby allowing the authentication server to use consistent policies while authenticating PPPoX users and RFC 1483 users. Currently, the NAS-Port attribute is sent only for PPPoX users.

With this feature, SSG sends nas-port information for certain IP users in the authentication-request and accounting-request packets.

## **SSG Suppression of Unused Accounting Records**

Platforms: Cisco 7200 Series routers, Cisco 7301 routers, and Cisco 7401 ASR routers

### **SSG**

**Cisco Service Selection** is an extensible solution that supports value added, billable services over most access methods. Service Selection solution is a combination hardware/software that allows subscribers to select various network-based services and applications independently or simultaneously. Service Selection has many unique features that allows subscribers to select services, dynamically change bandwidth and many other features like "captive portal". Service Selection requires a [Cisco IOS](#) based router that supports Service Selection Gateway , SSG, feature set, [Subscriber Edge Services Manager, SESM](#), software, which takes care of the User Interface aspects: selection, notification and has hooks into SSG and an [Authentication system](#) that can be RADIUS or Directory based.

SSG is a solution for service providers that offer intranet, extranet, and Internet connections to subscribers using broadband access technology such as xDSL, cable modems, or wireless to allow simultaneous access to network services.

For more information about SSG, refer to the [Service Selection Gateway](#) document.

### **SSG Suppression of Unused Accounting Records**

The SSG Suppression of Unused Accounting Records feature provides the ability to turn off those accounting records that are not needed on the router.

## **SSG Unconfig**

Platforms: Cisco 7200 Series routers, Cisco 7301 routers, and Cisco 7401 ASR routers

### **SSG**

SSG is a switching solution for service providers that offer intranet, extranet, and Internet connections to subscribers using broadband access technology such as xDSL, cable modems, or wireless to allow simultaneous access to network services.

For more information about SSG, refer to the [Service Selection Gateway](#) document.

### **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.

The SSG Unconfig feature enhances several Cisco IOS commands to delete all host objects, or delete a range of host objects. You can also delete all service objects or connection objects. The **show ssg host** command has been enhanced to display information about an interface and its IP address when host-key mode is enabled on that interface.

### **System Resource Cleanup When SSG Is Unconfigured**

When you enable SSG, the SSG subsystem in 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 by entering the **no ssg enable force-cleanup** command.

## **SSG Unique Session ID**

Platforms: Cisco 7200 Series routers, Cisco 7301 routers, and Cisco 7401 ASR routers

### **SSG**

**Cisco Service Selection** is an extensible solution that supports value added, billable services over most access methods. Service Selection solution is a combination hardware/software that allows subscribers to select various network-based services and applications independently or simultaneously. Service Selection has many unique features that allow subscribers to select services, dynamically change bandwidth and many other features like "captive portal". Service Selection requires a [Cisco IOS](#) based router that supports Service Selection Gateway, SSG, feature set, [Subscriber Edge Services Manager, SESM](#), software, which takes care of the User Interface aspects: selection, notification and has hooks into SSG and an [Authentication system](#) that can be RADIUS or Directory based.

SSG is a solution for service providers that offer intranet, extranet, and Internet connections to subscribers using broadband access technology such as xDSL, cable modems, or wireless to allow simultaneous access to network services.

For more information about SSG, refer to the [Service Selection Gateway](#) document.

### **SSG Unique Session ID**

SSG does not currently support a totally unique accounting session ID in the RADIUS accounting records. The SSG Unique Session ID feature provides a unique format in the RADIUS accounting records in order to be compatible with a customer's existing backend billing systems.

### **Support**

Cisco IOS Software Release 12.3B follows the standard Cisco support policy as indicated at:  
<http://www.cisco.com/warp/public/437/27.html>.

### **Release Notes**

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123relnt/7000/rn7000b.htm>



## Product Numbers

Table 2 Cisco IOS Release 12.3B Feature Sets, Images, and Memory Recommendations



	Software Feature Set	Product Code	Image	Flash	DRAM
Cisco 7200 VXR Universal Broadband Router	Cisco 7200 Series IOS ENTERPRISE SSG	S72AS-12301B	C7200-g4js-mz	48 MB	128 MB
Cisco 7200 VXR	Cisco 7200 Series IOS IP	S72C-12301B	C7200-is-mz	48 MB	128 MB
Cisco 7200 VXR	Cisco 7200 Series IOS ENTERPRISE/FW/IDS IPSEC 56	S72AHK8-12301B	C7200-jk803s- mz	48 MB	128 MB
Cisco 7200 VXR	Cisco 7200 Series IOS ENTERPRISE/FW/IDS IPSEC 3DES	S72AHK9-12301B	C7200-jk9o3s- mz	48 MB	128 MB
Cisco 7200 VXR	Cisco 7200 Series IOS ENTERPRISE/FW/IDS	S72AH-12301B	C7200-jo3s-mz	48 MB	128 MB
Cisco 7200 VXR	Cisco 7200 Series IOS ENTERPRISE	S72A-12301B	c7200-js-mz	48 MB	128 MB
Cisco 7301	Cisco 7301 Series IOS ENTERPRISE SSG	S73AS-12301B	c7301-g4js-mz	64 MB	128 MB
Cisco 7301	Cisco 7301 Series IOS IP	S73C-12301B	c7301-is-mz	64 MB	128 MB
Cisco 7301	Cisco 7301 Series IOS ENTERPRISE/FW/IDS IPSEC 56	S73AHK8-12301B	c7301-jk8o3s- mz	64 MB	128 MB
Cisco 7301	Cisco 7301 Series IOS ENTERPRISE/FW/IDS IPSEC 3DES	S73AHK9-12301B	c7301-jk9o3s- mz	64 MB	128 MB
Cisco 7301	Cisco 7301 Series IOS ENTERPRISE/FW/IDS	S73AH-12301B	c7301-jo3s-mz	64 MB	128 MB
Cisco 7301	Cisco 7301 Series IOS ENTERPRISE	S73A-12301B	c7301-js-mz	64 MB	128 MB
Cisco 7400	Cisco 7400 Series IOS ENTERPRISE SSG	S74AS-12301B	c7400-g4js-mz	64 MB	128 MB
Cisco 7400	Cisco 7400 Series IOS IP	S74C-12301B	c7400-is-mz	64 MB	128 MB
Cisco 7400	Cisco 7400 Series IOS ENTERPRISE/FW/IDS IPSEC 56	S74AHK8-12301B	c7400-jk8o3s- mz	64 MB	128 MB
Cisco 7400	Cisco 7400 Series IOS ENTERPRISE/FW/IDS IPSEC 3DES	S74AHK9-12301B	c7400-jk9o3s- mz	64 MB	128 MB
Cisco 7400	Cisco 7400 Series IOS ENTERPRISE/FW/IDS	S74AH-12301B	c7400-jo3s-mz	64 MB	128 MB
Cisco 7400	Cisco 7400 Series IOS ENTERPRISE	S74A-12301B	c7400-js-mz	64 MB	128 MB

**Download Information**

Customers can download *Cisco IOS Software Release 12.3B* from Cisco.com in the Software Image Library:  
<http://www.cisco.com/public/sw-center/sw-ios.shtml>.

***Special note to customer: The end-of-life announcement of Cisco IOS Software Release 12.2B will be published in Q4 CY03.***

Copyright © 2003 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, the Cisco Systems logo, and Cisco IOS are registered trademarks or 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)

## CISCO SYSTEMS



### 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](http://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. CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO 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)