



Configuring SSG to Authenticate PPP Subscribers

First Published: May 2, 2005
Last Updated: October 2, 2009



Effective with Cisco IOS Release 15.0(1)M, this feature is not available in Cisco IOS software.

Service Selection Gateway (SSG) supports PPP as a subscriber access protocol. PPP provides router-to-router and host-to-network connections over both synchronous and asynchronous circuits. This document provides information about how to configure SSG to support PPP subscribers, including information about PPP Termination Aggregation-multidomain (PTA-MD), virtual-circuit (VC)-to-service-name mapping, and single sign-on for PPP users.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for Configuring SSG to Authenticate PPP Subscribers”](#) section on page 14.

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.

Contents

- [Prerequisites, page 2](#)
- [Restrictions, page 2](#)
- [Information About SSG Authentication of PPP Subscribers, page 2](#)



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

- [How to Configure SSG to Authenticate PPP Subscribers, page 4](#)
- [Configuration Examples for SSG Authentication of PPP Subscribers, page 9](#)
- [Where to Go Next, page 12](#)
- [Additional References, page 13](#)
- [Feature Information for Configuring SSG to Authenticate PPP Subscribers, page 14](#)

Prerequisites

Before you can perform the tasks in this module, SSG must be enabled. See the “Enabling SSG” section in the *Implementing SSG: Initial Tasks* module for more information.

If Cisco Subscriber Edge Services Manager (SESM) is part of your SSG network, SESM and the RADIUS server must be configured to support the subscriber logon method. See the *Cisco Subscriber Edge Services Manager* documentation for information about how to configure SESM.

If SSG is configured to work with SESM in RADIUS mode, service profiles, subscriber profiles, and control profiles must be configured on the authentication, authorization, and accounting (AAA) server before SSG will work. See the *RADIUS Profiles and Attributes for SSG* document for information about RADIUS profiles and vendor-specific attributes (VSAs) for SSG.

Restrictions

- Virtual path identifier (VPI)/virtual channel identifier (VCI) indexing to service profile works only for PPP over ATM (PPPoA) and PPP over Ethernet over ATM (PPPoEoA).
- In the event of a server failure, SSG ignores configured **server group** *group-name* commands and, instead, will failover to the server that is specified by the next **radius-server host** command in the configuration no matter how these servers are partitioned into groups by **server group** *group-name* command(s).

For more information about the **radius-server host** command, see the *Cisco IOS Security Configuration Guide*, Release 12.4. Refer to “[Configuring Authorization](#)” section in the Part 1: Authentication, Authorization, and Accounting (AAA).

Information About SSG Authentication of PPP Subscribers

Before you configure SSG to authenticate PPP subscribers, you should understand the following concepts:

- [PPP Subscriber Access, page 3](#)
- [PPP Termination Aggregation \(PTA\), page 3](#)
- [PTA-Multidomain, page 4](#)
- [PTA-MD Exclusion Lists, page 4](#)
- [Single Sign-on for PPP Subscribers, page 4](#)
- [VPI/VCI Indexing to Service Profiles, page 4](#)

PPP Subscriber Access

SSG implements Layer 3 service selection through selective routing of IP packets to destination networks on a per-subscriber basis. SSG uses the concept of interface direction (uplink or downlink) to help determine the forwarding path of an incoming packet. An uplink interface is an interface to services; a downlink interface is an interface to subscribers.

There are two types of access-side interfaces in SSG, SSG-enabled interfaces and interfaces on which SSG is not enabled. For PPP users, virtual-access interfaces are created and destroyed dynamically, so for SSG functionality to be applied to traffic on a virtual access interface, SSG must be enabled on the interface dynamically. The following methods allow SSG to be enabled on an interface dynamically:

- Beginning with Cisco IOS Release 12.2(16)B, the virtual template that is used to create PPP sessions may be configured as a downlink interface using **ssg direction** command. All virtual access created using the virtual template will be configured as SSG-enabled interfaces
- If the user profile downloaded during PPP authentication has SSG attributes, SSG will automatically consider that user to be an SSG user and the virtual access interface for that user will be configured as an SSG-enabled interface
- If the user has a structured username (such as user@domain) and the domain name is a valid SSG service profile, SSG will create a user to log on to the service domain as the primary service (check PTA, PTA-MD)

Note that user authentication can be based on a simple username (such as “user”) or structured username (such as “user@domain.com”). The structured username may be used in the following situations:

- To allow access providers to terminate user PPP sessions and logically associate each session with a particular service
- To allow SSG to bind a user session and its service to the appropriate network side interface

PPP Termination Aggregation (PTA)

PPP Termination Aggregation (PTA) is a PPP method of aggregating IP traffic by terminating PPP sessions and aggregating the IP traffic into a single routing domain. PTA service selection is based on a structured name (for example, username@service.com). Users can access only one service.

The following is a high-level description of the process for user authentication in a PTA scenario:

1. A subscriber logs in to a service by using a PPP dialer application with a username of the form user@service.
2. SSG recognizes service as a service profile and loads the service profile from the local configuration or a AAA server.
3. SSG forwards the AAA request to the remote RADIUS server as specified by the RADIUS-Server attribute of the service profile.
4. An address is assigned to the subscriber through RADIUS attribute 8 or Cisco Attribute-Value (AV) pair “ip:addr-pool.”
5. Network Address Translation (NAT) is not performed, and all user traffic is aggregated to the remote network.

PTA-Multidomain

Whereas PTA terminates the PPP session into a single routing domain, PTA-MD terminates the PPP sessions into multiple IP routing domains, thus supporting a wholesale virtual private network (VPN) model in which each domain is isolated from the others and has the capability to support overlapping IP addresses.

PTA-MD Exclusion Lists

The PTA-MD exclusion list allows you to create a set of domains that you want to exclude from normal SSG structured username processing. When a PPP user attempts to establish a PPP session using a domain that is part of the exclusion list, the traffic is treated as a simple username and hence the domain or service part in the structured username is ignored by SSG. SSG will treat the user as an SSG user if the user profile has SSG attributes or the corresponding virtual template is configured with SSG.

The PTA-MD exclusion list can be configured on the AAA server or directly on the router by using the command-line interface (CLI).

Single Sign-on for PPP Subscribers

SSG creates a host after a successful PPP authentication, but SESM has no knowledge of this host. SSG user profile caching makes the user profile available to SESM through status queries, providing support for single sign-on functionality and for failover from one SESM to another. User profile caching allows SSG to cache the user profiles for users. The feature is enabled by default.

In order to use single sign-on for PPP subscribers, you must also enable the single sign-on feature in SESM.

VPI/VCI Indexing to Service Profiles

**Note**

VPI/VCI indexing to services works only for PPPoA and PPPoEoA.

SSG supports VPI/VCI closed user groups by allowing VPI/VCIs to be bound to a given service. All users accessing SSG through the VPI/VCI or a range of VPI/VCIs will be able to access the configured service. You can specify whether users are allowed to access only the bound service or other additional services to which they subscribe. A closed user group service can be selected only through the VPI/VCI and not by entering the domain name in the username of a PPP session.

How to Configure SSG to Authenticate PPP Subscribers

To configure SSG to authenticate PPPoA, PPP over Ethernet (PPPoE) and PPP over Layer 2 Tunneling Protocol (PPPoL2TP) subscribers, perform the following tasks:

- [Configuring SSG Support for PPP Subscribers, page 5](#) (required)
- [Configuring a PTA-MD Exclusion List, page 6](#) (optional)
- [Configuring VPI/VCI Indexing to Services, page 7](#) (optional)

- [Configuring Single Sign-on for PPP Subscribers, page 8](#) (optional)

Configuring SSG Support for PPP Subscribers

Perform this task to configure SSG support for PPP subscribers. Configuring SSG to authenticate PPP users will create hosts when one of the conditions outlined in the “[PPP Subscriber Access](#)” section on [page 3](#), are met.

For PPP subscribers, the virtual template must be configured as the downlink interface. Configuring the virtual template as a downlink interface is particularly important when SSG users are coming through CPE and the CPE establishes a PPP session with SSG. In order for the users coming through the CPE to be treated as SSG users, the PPP interface must be marked as downlink, by configuring the virtual template as downlink.

All configuration commands that apply to serial interfaces can also be applied to virtual template interfaces, except shutdown and dialer commands. For further information on virtual templates and how to configure them, refer to the following URL:

http://www.cisco.com/en/US/docs/ios/dial/configuration/guide/dia_virtual_temp_ifs.html

SUMMARY STEPS

1. **interface virtual-template** *number*
2. **ssg direction downlink**
3. **ip unnumbered** [loopback 1 | ethernet 0]
4. **encapsulation ppp**
5. **virtual-profile**

DETAILED STEPS

Step 1	interface virtual-template <i>number</i> Example: Router(config)# interface virtual-template 60	Creates a virtual template interface and enters interface configuration mode.
Step 2	ssg direction downlink Example: ssg direction downlink	Sets the direction of the interface. <ul style="list-style-type: none"> • A downlink interface is an interface to subscribers.
Step 3	ip unnumbered [loopback 1 ethernet 0] Example: Router(config-if)# ip unnumbered loopback 1	Enables IP without assigning a specific IP address on the LAN.

Step 4	<code>encapsulation ppp</code> Example: Router(config-if)# encapsulation ppp	Enables PPP encapsulation on the virtual template interface.
Step 5	<code>virtual-profile</code> Example: Router(config-if)# virtual-profile	(Optional) Creates a virtual-access interface only if the inbound connection requires one.

Configuring a PTA-MD Exclusion List

A PTA-MD exclusion list is used to eliminate parsing of PPP structured usernames during authentication. A PTA-MD exclusion list can be configured directly on the AAA server or through the use of the router CLI. Perform this task to configure a PTA-MD exclusion list locally on the router.

SUMMARY STEPS

1. `ssg multidomain ppp`
2. `exclude {domain name | all-domains}`
3. `download exclude-profile profile-name [password]`
4. `end`
5. `show ssg multidomain ppp exclude-list`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>ssg multidomain ppp</code> Example: Router(config)# ssg multidomain ppp	Enters SSG PTA-MD configuration mode.
Step 2	<code>exclude {domain name all-domains}</code> Example: Router(config-ssg-ppp-md)# exclude domain xyz	Adds names to the PTA-MD exclusion list. <ul style="list-style-type: none"> • domain—Adds a domain to the exclusion list. • <i>name</i>—Name of the domain to be added to the exclusion list. • all-domains—Excludes all domains; in other words, disables parsing of PPP structured usernames.

	Command or Action	Purpose
Step 3	<p>download exclude-profile <i>profile-name</i> [<i>password</i>]</p> <p>Example: Router(config-ssg-ppp-md)# download exclude-profile abc cisco</p>	<p>Downloads the specified exclusion list from the AAA server.</p> <ul style="list-style-type: none"> • <i>profile-name</i>—Specifies the name for a list of excluded names that may be downloaded from the AAA server. • <i>password</i>—Specifies the 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.
Step 4	<p>end</p> <p>Example: Router(config-ssg-ppp-md)# end</p>	(Optional) Returns to privileged EXEC mode.
Step 5	<p>show ssg multidomain ppp exclude-list</p> <p>Example: Router# show ssg multidomain ppp exclude-list</p>	(Optional) Displays the contents of a PTA-MD exclusion list.

Configuring VPI/VCI Indexing to Services

To configure VPI/VCI closed user groups, you must map VPI/VCI to a given service. Perform this task to map VCs to service names.

SUMMARY STEPS

1. **ssg vc-service-map** *service-name* [**interface** *interface-number*] *start-vpi* | *start-vpi/vci* [*end-vpi* | *end-vpi/vci*] **exclusive** | **non-exclusive**
2. **exit**
3. **show ssg vc-service-map**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre>ssg vc-service-map service-name [interface interface-number] start-vpi start-vpi/vci [end-vpi end-vpi/vci] exclusive non-exclusive</pre> <p>Example: Router(config)# ssg vc-service-map Worldwide 3/33 exclusive</p>	<p>Maps VCs to service names.</p> <ul style="list-style-type: none"> The exclusive keyword means that the user has to use the service specified. The non-exclusive keyword means that the user may optionally choose to override the configuration by using a structured username with a different domain.
Step 2	<pre>exit</pre> <p>Example: Router(config-auto-domain)# exit</p>	(Optional) Returns to global configuration mode.
Step 3	<pre>show ssg vc-service-map</pre> <p>Example: Router# show ssg vc-service-map</p>	(Optional) Displays VC-to-service-name mappings.

Configuring Single Sign-on for PPP Subscribers

SSG user-profile caching allows SESM to recover the user profiles of PPP users from SSG, which enables functionality such as single sign-on. This feature is enabled by default.

**Note**

In order to use single sign-on for PPP subscribers, you must first enable the single sign-on feature in SESM.

Perform this task to enable SSG user-profile caching.

SUMMARY STEPS

1. ssg profile-cache

DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre>ssg profile-cache</pre> <p>Example: Router(config)# ssg profile-cache</p>	Enables the caching of user profiles for non-PPP users.

Configuration Examples for SSG Authentication of PPP Subscribers

This section contains the following configuration examples:

- [Adding Domains to an Existing PTA-MD Exclusion List: Examples, page 9](#)
- [Disabling Parsing of PPP Structured Usernames: Example, page 10](#)
- [Service-Name-to-VC Mapping: Example, page 10](#)
- [Configuring the Virtual Template to Support PPP Subscribers: Example, page 10](#)
- [Basic PPPoA and PPPoE Configuration: Examples, page 10](#)

Adding Domains to an Existing PTA-MD Exclusion List: Examples

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

The exclusion list currently on the AAA server includes cisco, motorola, nokia, and voice-stream. This exclusion list is in the ACS format.

```
user = pta_md{
profile_id = 119
profile_cycle = 2
member = SSG-DEV
radius=6510-SSG-v1.1 {
check_items= {
2=password
}
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 downloading the PTA-MD exclusion list, 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: Example

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

```
exclude all-domains
```

Service-Name-to-VC Mapping: Example

The following example shows the service name “public” mapped to a VC:

```
ssg vc-service-map public interface atm3/0 1/37 non-exclusive
```

The following example shows the service name “public” mapped to a range of VCs:

```
ssg vc-service-map public interface atm3/0 1/37 1/82 non-exclusive
```

Configuring the Virtual Template to Support PPP Subscribers: Example

The following example shows a virtual template configured as a downlink interface. Any PPP connection to SSG that uses this template will be marked as a downlink interface.

```
interface Virtual-Template1
  description PPPoE v-interface
  mtu 1492
  ip unnumbered Loopback0
  ip nat inside
  ssg direction downlink
  ppp authentication pap chap
!
```

Basic PPPoA and PPPoE Configuration: Examples

The following configuration examples show how to establish basic PPPoA and PPPoE user connections:

- [PPPoA Users: Example, page 10](#)
- [PPPoEoA Users: Example, page 11](#)
- [PPPoEoE Users: Example, page 12](#)

PPPoA Users: Example

Configure AAA authentication through the RADIUS mechanism.

```
aaa authentication ppp default group radius
aaa authorization network default group radius

radius-server host 10.76.86.90 auth-port 1812 acct-port 1813 key cisco
radius-server vsa send accounting
radius-server vsa send authentication
```

Configure the PPP IP address on the aggregation side.

```
interface Loopback1
  ip address 21.6.6.1 255.255.255.0
```

Configure the IP address pool if SSG is going to assign IP addresses.

```
ip local pool ppp-pool 21.9.9.2 21.9.9.10
```

Configure the virtual template.

```
interface Virtual-Template1
  description "PPP virtual-template for PPP host"
  ip unnumbered Loopback1
  peer default ip address pool ppp-pool
  ppp authentication pap chap
```

Configure the ATM interface on which PPPoA user comes in.

```
interface ATM4/0.21 point-to-point
  description "Connected to 36/7 for PPP user"
  pvc 21/40
    encapsulation aal5mux ppp Virtual-Template1
  !
```

PPPoEoA Users: Example

Configure AAA authentication through the RADIUS mechanism.

```
aaa authentication ppp default group radius
aaa authorization network default group radius

radius-server host 10.76.86.90 auth-port 1812 acct-port 1813 key cisco
radius-server vsa send accounting
radius-server vsa send authentication
```

Configure the PPP IP address on the aggregation side.

```
interface Loopback1
  ip address 21.6.6.1 255.255.255.0
```

Configure the IP address pool if SSG is going to assign IP addresses.

```
ip local pool ppp-pool 21.9.9.2 21.9.9.10
```

Configure the PPPoE server using a VPDN group.

```
vpdn enable
vpdn-group 3
  accept-dialin
  protocol pppoe
  virtual-template 1
```

Configure the virtual template.

```
interface Virtual-Template1
  description "PPP virtual-template for PPP host"
  ip unnumbered Loopback1
  peer default ip address pool ppp-pool
  ppp authentication pap chap
```

Configure the ATM interface on which the PPPoEoA user comes in.

```
interface ATM4/0.23 point-to-point
  description "Connected to 36/7 for PPPoE user"
  ip address 23.6.6.1 255.255.255.0
  pvc 23/40
    encapsulation aal5snap
    protocol pppoe
```

PPPoE Users: Example

Configure AAA authentication through the RADIUS mechanism.

```
aaa authentication ppp default group radius
aaa authorization network default group radius

radius-server host 10.76.86.90 auth-port 1812 acct-port 1813 key cisco
radius-server vsa send accounting
radius-server vsa send authentication
```

Configure the PPP IP address on the aggregation side.

```
interface Loopback1
 ip address 21.6.6.1 255.255.255.0
```

Configure the IP address pool if SSG is going to assign IP addresses.

```
ip local pool ppp-pool 21.9.9.2 21.9.9.10
```

Configure the PPPoE server using a VPDN group.

```
vpdn enable
vpdn-group 3
 accept-dialin
protocol pppoe
virtual-template 1
```

Configure the virtual template.

```
interface Virtual-Template1
 description "PPP virtual-template for PPP host"
 ip unnumbered Loopback1
 peer default ip address pool ppp-pool
 ppp authentication pap chap
```

Configure the Ethernet interface on which the PPPoE user comes in.

```
interface fastethernet 1/0
 description "Interface for PPPoE user"
 ip address 23.8.8.1 255.255.255.0
 pppoe enable
```

Where to Go Next

To configure other methods of subscriber authentication, refer to the following modules:

- [Configuring SSG to Authenticate Web Logon Subscribers](#)
- [Configuring SSG to Authenticate Subscribers with Transparent Autologon](#)
- [Configuring SSG to Authenticate Subscribers Automatically in the Service Domain](#)
- [Configuring SSG Support for Subnet-Based Authentication](#)
- [Configuring SSG for MAC-Address-Based Authentication](#)

Additional References

The following sections provide references related to configuring SSG to authenticate PPP subscribers.

Related Documents

Related Topic	Document Title
SESM	<i>Cisco Subscriber Edge Services Manager</i> documentation
RADIUS commands	<i>Cisco IOS Security Command Reference</i>
RADIUS configuration tasks	“Configuring RADIUS” chapter in the <i>Cisco IOS Security Configuration Guide</i>
Configuring L2TP	<ul style="list-style-type: none"> <i>Cisco IOS Dial Technologies Configuration Guide</i> <i>Cisco IOS Dial Technologies Command Reference</i>

Technical Assistance

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

Feature Information for Configuring SSG to Authenticate PPP Subscribers

[Table 3](#) lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.2(1) or a later release appear in the table.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

For information on a feature in this technology that is not documented here, see the [Service Selection Gateway Features Roadmap](#).

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

**Note**

[Table 3](#) lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 3 Feature Information for Configuring SSG to Authenticate PPP Subscribers

Feature Name	Releases	Feature Configuration Information
PPP Subscriber Access	12.2(16)B 12.3(4)T 12.4	<p>The PPP subscriber access feature supports PPP as a subscriber access protocol.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • PPP Subscriber Access, page 3 • PPP Termination Aggregation (PTA), page 3 • Configuring SSG Support for PPP Subscribers, page 5 • Configuring Single Sign-on for PPP Subscribers, page 8 • Configuring the Virtual Template to Support PPP Subscribers: Example, page 10 • Basic PPPoA and PPPoE Configuration: Examples, page 10 <p>The following command was introduced by this feature: ssg direction downlink.</p>
PTA-MD Exclusion List	12.2(15)B 12.3(4)T 12.4	<p>The PTA-MD Exclusion List feature allows you to create a set of domains that are excluded from normal SSG structured username processing.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • PTA-Multidomain, page 4 • PTA-MD Exclusion Lists, page 4 • Configuring a PTA-MD Exclusion List, page 6 • Adding Domains to an Existing PTA-MD Exclusion List: Examples, page 9 <p>The following commands were introduced by this feature: download exclude-profile (PTA-MD), exclude (PTA-MD), show ssg multidomain, ppp exclude-list, ssg multidomain ppp.</p>
Configuring SSG to Authenticate PPP Subscribers	15.0(1)M	This feature was removed in Cisco IOS Release 15.0(1)M.

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.

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