



## PWLAN Access Routers

---

Cisco IOS release 12.3(7)T adds support for the combined Access Zone Router (AZR) and Service Selection Gateway (SSG) features, providing both centralized and distributed public wireless LAN (PWLAN) solutions.

### Feature History for PWLAN Access Router Features

Release	Modification
12.0(3)DC	SSG features were introduced on the Cisco 6400 series routers.
12.2(4)B	SSG features were integrated into Cisco IOS Release 12.2(4)B and support was added for the Cisco 7200 series routers.
12.2(8)T	New SSG features were integrated into Cisco IOS Release 12.2(8)T.
12.3(2)T	SSG feature support was added for Cisco 2650XM and the Cisco 3700 series routers.
12.3(4)XD	SSG plug and play features were added on all platforms that support SSG. Explicit SSG and AZR features in a centralized deployment model were added.
12.3(7)T	Support for combined AZR and SSG features was added.

### Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Information About PWLAN Access Router Features](#)
- [Deployment Models](#)
- [Additional References](#)



---

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

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

# Information About PWLAN Access Router Features

This section provides an overview of the PWLAN features.

- [Definition of Terms, page 2](#)
- [AZR Features, page 2](#)
- [SSG Features, page 4](#)

## Definition of Terms

The following are terms related to PWLAN features.

- **AZR**—A standard Cisco router with PWLAN enhancements. An AZR router performs functions such as edge routing and WAN connectivity, 802.1q VLAN support for traffic segmentation, and Dynamic Host Configuration Protocol (DHCP) services. PWLAN-specific functions include Address Resolution Protocol (ARP), secure ARP (rogue IP spoofing protection), and client session accounting.
- **SSG**—The SSG is the central component in a PWLAN, providing services related to access and service selection. The SSG maintains the state of all users in the hotspot, providing access to open garden services and controlling access to walled garden services. In order to maintain the necessary information, the SSG provides a RADIUS proxy function for access points (APs) and AZRs in the hotspots. Other PWLAN functions (such as Domain Name System (DNS) redirections and permanent TCP reduction) are used to support statically configured clients.
- **Integrated AZR and SSG router**—A single router providing simultaneous support for AZR and SSG.
- **Centralized PWLAN deployment**—A network where an AZR is deployed at the hotspot site with the APs, and the SSG is deployed at a central point of presence. Centralized PWLAN architectures are usually deployed with a dedicated connection (such as T1/E1) between the AZR and the SSG routers.
- **Distributed PWLAN deployment**—A network where an integrated AZR and SSG router is deployed at the hotspot site. Also called a *local SSG*, *decentralized SSG*, or *distributed SSG*, this architecture is typically used at hotspot sites served by multiple service providers (such as an airport), or for sites that are directly connected to the Internet (using DSL, cable, or satellite service) instead of the service provider's point of presence.

## AZR Features

PWLAN access routers support AZR features in a range of Cisco routers and offers flexible solutions for the PWLAN.

### Secure ARP

Secure Address Resolution Protocol (ARP), or IP spoofing prevention, synchronizes the database of the Dynamic Host Configuration Protocol (DHCP) server with the ARP table to avoid address hijacking. Secure ARP adds an entry to the ARP table for a client when an address is allocated that can be deleted by the Cisco IOS DHCP server only when a binding expires.

For more information on this feature, go to one of the following locations:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftdsiaa.htm>

[http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products\\_feature\\_guide09186a00801543c8.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a00801543c8.html)

## DHCP Session Accounting

DHCP session accounting, or session termination, indicates whether a user should be deleted (logged off) or maintained in an environment such as a PWLAN where a user may not explicitly log off. Therefore, when the DHCP lease expires, the DHCP server sends a message to the SSG. The SSG, on receipt of this message, resets the host object or host state.

For more information on this feature, go to one of the following locations:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftdhcpac.htm>

[http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products\\_feature\\_guide09186a00801543c7.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a00801543c7.html)

## Authorized ARP

When a router is used in a secured environment, it is sometimes desirable to allow only specific components to install ARP entries for certain network interfaces. Authorized ARP learning addresses this requirement. When authorized ARP learning is configured on an interface, dynamic ARP learning is automatically disabled on that interface. The IP/Mac mapping for that interface can be installed only by an authorized component such as DHCPD.

For more information on this feature, go to one of the following locations:

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t\\_4/gtautarp.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gtautarp.htm)

[http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products\\_feature\\_guide09186a00801d2df4.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801d2df4.html)

## Location Identification (DHCP Option 82)

In some instances of DHCP address allocation, the DHCP server cannot differentiate between two IP address ranges. To solve this problem, a relay agent residing at the switch must insert relay information to the port.

For more information on this feature, go to one of the following locations:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftdbeo82.htm>

[http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products\\_feature\\_guide09186a0080087ad8.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a0080087ad8.html)

## Static IP

Static IP allows hosts with static IP addresses to interact with the PWLAN provider.



**Note**

---

Static IP is not supported in an integrated AZR and SSG router (distributed PWLAN architecture).

---

## SSG Features

The SSG feature is a switching solution for service providers who 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 links to additional SSG feature documentation indexes, refer to the [“Additional References” section on page 16](#).

### Accounting Update Interval per Service

The SSG Accounting Update Interval per Service feature enhances SSG accounting by allowing users to configure an interim accounting interval for a particular service. Without the SSG Accounting Update Interval per Service feature, all accounting information is sent simultaneously, and accounting information for a particular SSG service cannot be sent at a separate, independent interval.

SSG accounting sends information such as billing, auditing, and reporting. The SSG Accounting Update Interval Per Service feature allows for more granular interim accounting interval options for all these functions.

For more information on this feature, go to the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ssg/ftaccu.htm>

### AutoDomain

When you configure the SSG AutoDomain feature, users can automatically connect to a service based on either Access Point Name (APN) or the domain part of the structured username specified in an access request. When SSG AutoDomain is configured, user authentication is not performed at the network access server (NAS), but instead at the service (for example, at an authentication, authorization, and accounting (AAA) server within a corporate network).

For more information on this feature, go to the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ssg/ftauto.htm>

### Autologoff

When SSG automatic logoff (autologoff) is configured, the 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.

For more information on this feature, go to the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ssg/ftssgalt.htm>

### Autologon Using Proxy RADIUS

The SSG AutoLogon Using Proxy RADIUS feature enables SSG to act as a Remote Authentication Dial-In User Service (RADIUS) proxy for clients other than signed service description (SSD) clients whose access requests do not contain vendor-specific attributes (VSAs). Non-SSD access requests must originate from configured, trusted, downstream network access server (NAS) IP addresses that share a RADIUS secret key with the SSG. This shared secret key is different from the one shared between SSG and the SSD. You must configure the IP addresses for each router for which SSG is acting as a RADIUS proxy. Packets received from unrecognized sources are discarded.

For more information on this feature, go to the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ssg/ftprxy.htm>

## Hierarchical Policing

Traffic policing is the concept of limiting the transmission rate of traffic entering or leaving a node. In SSG, traffic policing can be used to allocate bandwidth between subscribers per-user policing and between services to a particular subscriber per-user policing to ensure all types of services are allocated a proper amount of bandwidth. 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), this complete feature is called SSG Hierarchical Policing.

For more information on this feature, go to the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ssg/fthier.htm>

## MAC Address in Accounting Records

This feature adds the MAC address of the host to accounting records to determine when multiple users authenticate with the same username and password.

For more information on this feature, go to the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122reInt/7000/rn7000b.htm#233799>

## Open Garden

An *open garden* is a collection of Web sites or networks 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 Web sites in an open garden. In contrast, a *walled garden* refers to a collection of websites or networks that subscribers can access after providing minimal authentication information.

For more information on this feature, go to the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ssg/ftssgogt.htm>

## Port-Bundle Host Key

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. When a subscriber sends an HTTP packet to the SESM server, SSG creates a port map that changes the source IP address to a configured SSG source IP address and changes the source TCP port to a port allocated by SSG. SSG assigns a bundle of ports to each subscriber, because one subscriber can have several simultaneous TCP sessions when accessing a web page. The assigned host key, or combination of port bundle and SSG source IP address, uniquely identifies each subscriber. The host key is carried in RADIUS packets sent between the SESM server and SSG in the Subscriber IP vendor-specific attribute (VSA).

For more information on this feature, go to the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ssg/ftssgket.htm>

## 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 a duration of use (in seconds) or an allowable data volume (in bytes). A quota is an allotment of available credit.

For more information on this feature, go to the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ssg/ftssgpb.htm>

## TCP Redirect for Services

The SSG TCP Redirect for Services feature redirects certain packets, which would otherwise be dropped, to captive portals that can handle the packets in a suitable manner. For example, packets sent upstream by unauthorized users are forwarded to a captive portal that can redirect the users to a logon page. Similarly, if users try to access a service to which they have not logged on, the packets are redirected to a captive portal that can provide a service logon screen.

For more information on this feature, go to the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ssg/fthttp.htm>

## 3-Key Authentication

Uses the “phone number” (OF WHAT? EXPOUND) in addition to the existing 2-key authentication (which consists of a userID and password) to perform end-user identification.

For more information on this feature, go to the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122reInt/7000/rn7000b.htm#73871>

## AAA Nonblocking API

SSG uses authentication, authorization, and accounting (AAA) client APIs to send and receive AAA information to AAA server. The AAA nonblocking API maintains the SSG process when performing calls to an AAA module to increase the number of requests that SSG can maintain.

For more information on this feature, go to the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122reInt/7000/rn7000b.htm#185019>

## Cached Service Profiles

Cached service profiles store logon information that the system previously downloaded at each instance of a logon.

For more information on this feature, go to the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122reInt/7000/rn7000b.htm#185110>

## L2TP Dial Out

The SSG L2TP Dial Out feature enhances SSG tunnel services and provides a dial-out facility to users. Many small office 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 the SSG L2TP Dial Out feature, SSG requires a digital number identification service (DNIS) number for the SOHO to which the user wants to connect, the address of the L2TP access concentrator (LAC) closest to the SOHO, and configured tunnel parameters to establish a tunnel to the LAC.

Users can access the SSG L2TP Dial Out feature by selecting the dial out service using Cisco Subscriber Edge Services Manager (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.

For more information on this feature, go to the following URL:

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122b/122b\\_15/12b\\_dia.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122b/122b_15/12b_dia.htm)

## MAC Address Check in Auto Logoff

SSG checks the MAC address of the host each time that it performs an ARP ping and if it finds that the MAC address has changed, it performs an automatic logoff of the host to prevent IP address spoofing and DHCP IP address reassignment.

For more information on this feature, go to the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122reInt/7000/rn7000b.htm#185022>

## PDSN Interworking

The packet data serving node (PDSN) Internetworking feature enables Service Selection in CDMA2000 networks through enhancements to the SSG Proxy functionality

For more information on this feature, go to the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122reInt/7000/rn7000b.htm#184988>

## Prepaid Idle Timeout

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 a 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 authentication, authorization, and accounting (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 on this feature, go to the following URL:

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122b/122b\\_15/12b\\_pre.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122b/122b_15/12b_pre.htm)

For additional information, go to the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122reInt/7000/rn7000b.htm#185046>

## PTA-MD Exclusion List

SSG parses the structured user names (in the format “user@domain”) for PPP users and tries to search domains for SSG services. The PTA-MD Exclusion List feature inhibits certain (or all) domains to default behavior.

For more information on this feature, go to the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122reInt/7000/rn7000b.htm#185105>

## RADIUS Proxy Enhancements for CHAP

The RADIUS proxy enhancements for CHAP feature provides CHAP authentication support for SSG VPDN service in autodomains mode.

For more information on this feature, go to the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122reInt/7000/rn7000b.htm#185063>

## SESM Web Proxy (Plug-and-Play)

The SSG Web proxy feature provides transparent support for Web clients configured for Web proxy in PWLAN scenarios. Cisco SSG directs unresolved DNS requests to the SESM DNS proxy, which inserts a local Web proxy address so that HTTP requests can be properly handled.

For more information on this feature, go to the following URL:

[http://www.cisco.com/univercd/cc/td/doc/solution/sesm/sesm\\_320/pluginplay/intro.htm](http://www.cisco.com/univercd/cc/td/doc/solution/sesm/sesm_320/pluginplay/intro.htm)

## SSG EAP Transparency

The SSG EAP Transparency feature allows the SSG on a Cisco router to act as a RADIUS proxy during Extensible Authentication Protocol (EAP) authentication and to create the host. This feature also prevents the use of previously valid IP addresses after an AZR reboot and allows EAP users who have logged out to reconnect through Subscriber Edge Services Manager (SESM).

For more information on this feature, go to the following URL:

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122b/122b\\_16/shortcap.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122b/122b_16/shortcap.htm)

## 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.

For more information on this feature, go to the following URL:

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122b/122b\\_15/12b\\_unc.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122b/122b_15/12b_unc.htm)

# Deployment Models

PWLAN access routers support the following deployment models:

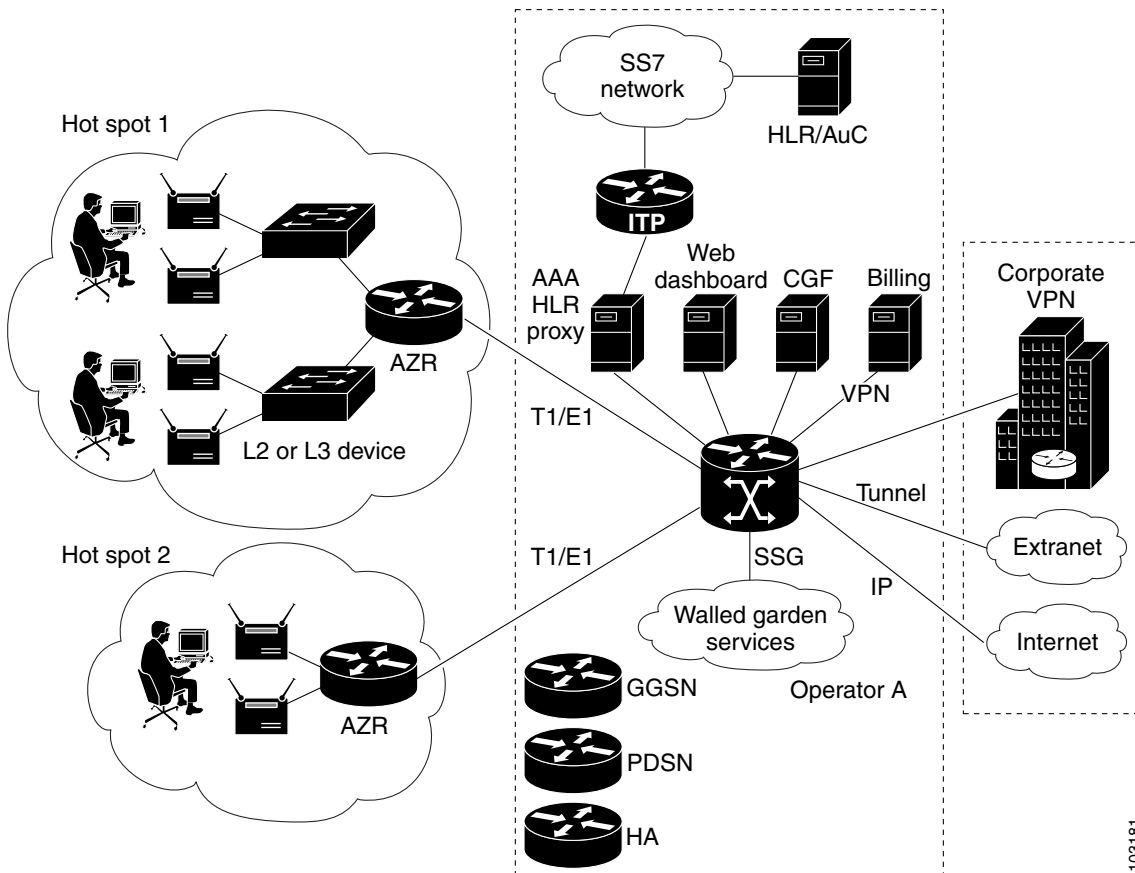
- [Centralized PWLAN Deployment](#)
- [Distributed PWLAN Deployment](#)

## Centralized PWLAN Deployment

In a centralized PWLAN deployment, there is a centralized SSG in the service provider's data center that is used to authenticate, authorize, bill, and provide other services. The AAA servers and subscriber management data are often collocated with the SSG router. PWLAN access routers, with AZR functionality, provide the link between hotspots and the central SSG router.

[Figure 1](#) shows an example of a centralized PWLAN deployment.

Figure 1 Centralized PWLAN Deployment



103181

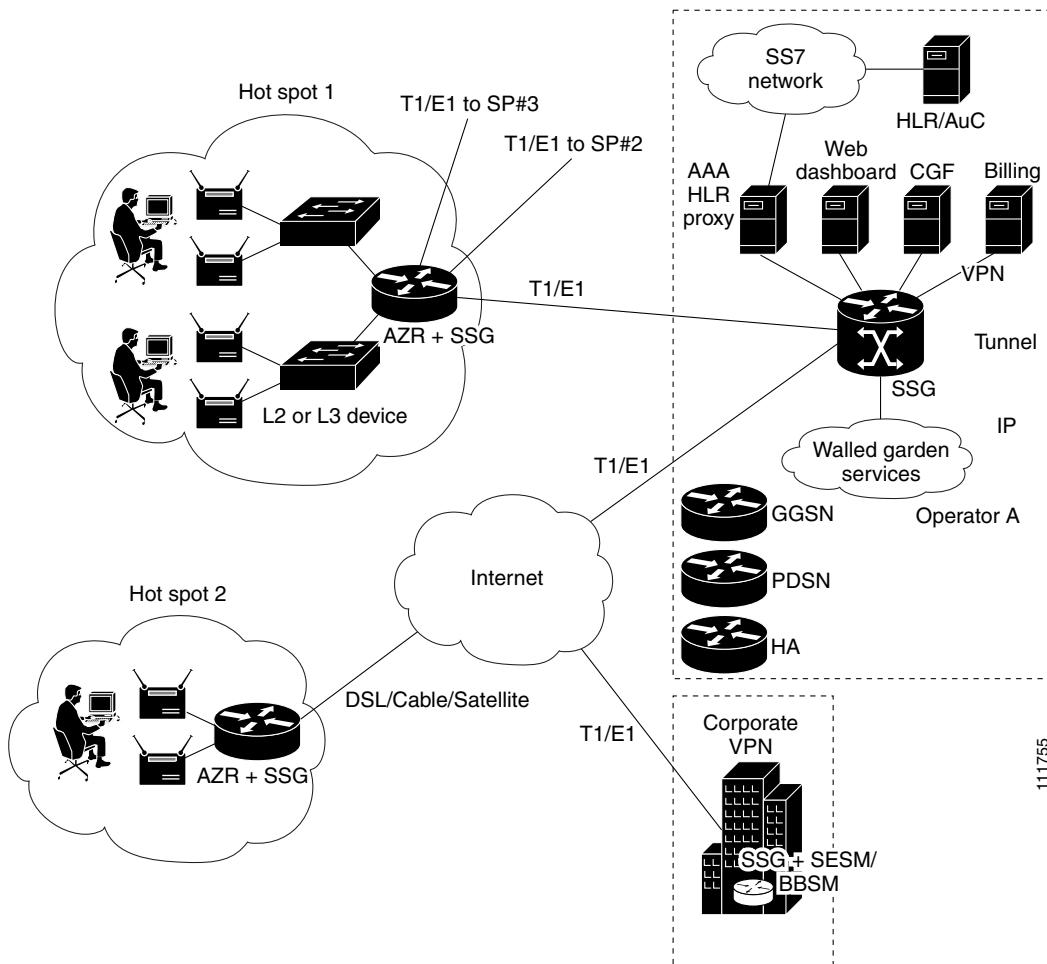
<b>L2, L3</b>	Layer 2, Layer 3	<b>VPN</b>	Virtual private network
<b>SS7</b>	Signaling System 7	<b>GGSN</b>	Gateway GPRS support node
<b>HLR</b>	Home location register	<b>GPRS</b>	General packet radio service
<b>AuC</b>	Authentication center	<b>PDSN</b>	Packet data serving node
<b>AAA</b>	Authentication, authorization, and accounting	<b>HA</b>	Home agent
<b>CGF</b>	Charging gateway function		

# Distributed PWLAN Deployment

Distributed PWLAN deployment does not require a central SSG router. This model enables the use of Cisco 2600XM and 3700 series routers as AZRs with built-in subscriber access control capabilities (the SSG) integrated into a single system, without dedicated connections to the service provider's point of presence (POP). [Figure 2](#) shows a distributed PWLAN deployment model.

The minimum Cisco IOS image for the distributed PWLAN model is the IPBASE image. The distributed PWLAN model is supported with the Advanced Enterprise Services feature set.

**Figure 2** Distributed PWLAN Deployment Model



<b>L2, L3</b>	Layer 2, Layer 3	<b>VPN</b>	Virtual private network
<b>SS7</b>	Signaling System 7	<b>GGSN</b>	Gateway GPRS support node
<b>HLR</b>	Home location register	<b>GPRS</b>	General packet radio service
<b>AuC</b>	Authentication center	<b>PDSN</b>	Packet data serving node
<b>AAA</b>	Authentication, authorization, and accounting	<b>HA</b>	Home agent
<b>CGF</b>	Charging gateway function	<b>SP #2, SP #3</b>	Service providers

## Configuration Example for the Distributed PWLAN Deployment Model

This section shows an example of the configuration for the distributed deployment model. Explanations of some of the configuration tasks are included.

```
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname swiss-soln-3725
!
clock timezone PST -8
!
aaa new-model
!
aaa group server radius rad-car
 server 1.4.11.10 auth-port 1812 acct-port 1813
!
```

The following lines show the configuration for SSG RADIUS proxy/DHCP session accounting.

```
aaa group server radius rad-proxy
 server 20.2.1.1 auth-port 1812 acct-port 1813
!
```

The following lines show the prepaid RADIUS configuration.

```
aaa group server radius SSG-PREPAID
 server 1.3.27.60 auth-port 1812 acct-port 1813
!
```

The following line shows the system accounting configuration.

```
aaa authorization network default group radius
```

The following lines show the configuration of the SSG RADIUS proxy.

```
aaa accounting network acc-ssg start-stop group rad-proxy
aaa accounting system default start-stop group rad-car
aaa session-id common
ip subnet-zero
ip cef
!
!
ip tcp synwait-time 13
```

The following lines show the definition of addresses that should not be assigned to DHCP clients. These are the addresses that will be used by provider owned devices such as the AZR and SSG.

```
ip dhcp excluded-address 20.1.1.1
ip dhcp excluded-address 20.1.1.2
ip dhcp excluded-address 20.2.1.1
ip dhcp excluded-address 20.2.1.2
!
```

The following lines show the configuration of the AZR local DHCP pool with the open (no WEP) authentication option.

```
ip dhcp pool swiss-open
 network 20.1.1.0 255.255.255.0
 default-router 20.1.1.1
```

```
dns-server 1.3.27.1
```

The following line shows the enabling of Secure ARP for each DHCP pool.

```
update arp
!
```

The following lines show the configuration of the AZR local DHCP pool for LEAP authentication.

```
ip dhcp pool swiss-leap
network 20.2.1.0 255.255.255.0
default-router 20.2.1.1
dns-server 1.3.27.1
lease 0 0 1
```

The following line shows the configuration of Secure ARP for each DHCP pool.

```
update arp
```

The following line shows the enabling of session termination for each DHCP pool for which this is required by referencing the AAA accounting list (SSG as RADIUS proxy).

```
accounting acc-ssg
!
ip name-server 1.3.27.1
ip audit notify log
ip audit po max-events 100
no ftp-server write-enable
!
ssg enable
```

The following line shows the access to the default SESM server.

```
ssg default-network 1.3.27.1 255.255.255.255
```

The following line defines the password used to download the service from AAA server.

```
ssg service-password servicecisco
```

The following line defines SESM as a RADIUS helper and specifies the port numbers to be used.

```
ssg radius-helper auth-port 1812 acct-port 1813
```

The following line defines the key to use for SESM to secure communication.

```
ssg radius-helper key Cisco
```

```
ssg auto-logoff arp interval 240
ssg prepaid reauthorization drop-packet
ssg prepaid threshold volume 2000
ssg prepaid threshold time 10
ssg aaa group prepaid SSG-PREPAID
```

The following lines configure bind service to the uplink interface.

```
ssg bind service og1 FastEthernet0/0
ssg bind service service2 FastEthernet0/0
ssg bind service service3 FastEthernet0/0
ssg bind service service1 FastEthernet0/0
ssg bind service prepaid1 FastEthernet0/0
ssg open-garden og1
!
```

The following lines configure the SSG port bundle host key.

```
ssg port-map
```

```

destination access-list 101
source ip FastEthernet0/0
length 2
!
ssg radius-proxy
server-port auth 1812 acct 1813
client-address 20.2.0.0 255.255.0.0
key cisco
no remove vsa cisco
!

```

The following lines show the configuration of the SSG TCP-redirect/captive portal.

```

ssg tcp-redirect
port-list web
port 80
port 8080
!
server-group sesm-cp
server 1.3.27.1 8090
!
redirect port-list web to sesm-cp
redirect unauthenticated-user to sesm-cp
!
server-group PrepaidRedirectGroup
server 1.3.27.1 8096
!
!
redirect prepaid-user to PrepaidRedirectGroup
ssg service-search-order remote local
!

```

The following lines define the service profile for the profile "service1."

```

local-profile service1
attribute 26 9 251 "R1.0.0.0;255.0.0.0"
attribute 26 9 251 "D1.3.27.1"
attribute 26 9 251 "O*"
!
!
local-profile og1
attribute 26 9 251 "O*"
attribute 26 9 251 "R1.0.0.0;255.0.0.0"
attribute 26 9 251 "D1.3.27.1"
!
!
local-profile prepaid1
attribute 26 9 251 "D1.3.27.1"
attribute 26 9 251 "O*"
attribute 26 9 251 "R1.0.0.0;255.0.0.0"
attribute 26 9 253 "QX100;1;5"
!
!

```

The following lines configure the upstream connectivity between the SSG and the core Network.

```

interface FastEthernet0/0
ip address 1.3.27.51 255.255.0.0
duplex auto
speed auto
ssg direction uplink
!
interface FastEthernet0/1
no ip address

```

```
duplex auto
speed auto
!
```

The following lines show the AZR 802.1Q baseline configuration.

```
interface FastEthernet0/1.1
 encapsulation dot1Q 1 native
 ip address 20.1.1.1 255.255.0.0
```

The following lines show the configuration of the downstream connectivity between the SSG and the hotspot.

```
ssg direction downlink
no cdp enable
```

The following lines enable authorized ARP on each interface and define the ARP timeout, indicating how long the ARP entry should remain valid in the ARP table.

```
arp authorized
arp timeout 120
```

The following lines show the AZR 802.1Q baseline configuration.

```
interface FastEthernet0/1.2
 encapsulation dot1Q 2
 ip address 20.2.1.1 255.255.0.0
 ssg direction downlink
 arp authorized
 arp timeout 120
!
interface FastEthernet0/1.3
 encapsulation dot1Q 3
 ip address 20.3.1.1 255.255.0.0
 arp timeout 120
!
ip classless
ip route 0.0.0.0 0.0.0.0 1.3.0.1
ip route 50.50.50.0 255.255.255.0 1.3.27.56
ip route 223.255.254.254 255.255.255.255 1.3.0.1
!
no ip http server
no ip http secure-server
!
!
SSG Port-Bundle HostKey
access-list 101 permit ip 20.0.0.0 0.255.255.255 1.0.0.0 0.255.255.255
```

The following lines define a static ARP entry for each device that does not have its address assigned using DHCP and which exists on the downlink interface configured with the **arp authorized** command (for example, any access point).

```
arp 20.2.1.2 000d.bce4.6573 ARPA
arp 20.1.1.2 000d.bce4.6573 ARPA
!
!
```

The following lines show the SSG prepaid service configuration.

```
radius-server attribute 44 include-in-access-req
radius-server attribute 55 include-in-acct-req
```

The following lines define RADIUS settings for each SSG within the server group.

```
radius-server host 1.4.11.10 auth-port 1812 acct-port 1813 key cisco
radius-server host 20.2.1.1 auth-port 1812 acct-port 1813 key cisco
radius-server host 1.3.27.60 auth-port 1812 acct-port 1813 timeout 5 retransmit 3 key
cisco
radius-server retransmit 0
radius-server vsa send accounting
radius-server vsa send authentication
!
control-plane
!
!
!
no mgcp timer receive-rtcp
!
!
!
dial-peer cor custom
!
!
!
!
line con 0
  exec-timeout 0 0
  speed 115200
line aux 0
line vty 0 4
!
!
end
```

## Additional References

The following sections provide references related to PWLAN access routers.

## Related Documents

Related Topic	Document Title
SSG features	Service Selection Gateway (SSG) Features in Release 12.3(4)T, available at: <a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/ssg/">http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/ssg/</a>

## MIBs

MIBs	MIBs Link
<b>MIBs</b> <ul style="list-style-type: none"> <li>No new MIBs are supported by this feature.</li> </ul>	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:  <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	<a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a>

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0711R)

Copyright © 2004 Cisco Systems, Inc. All rights reserved.

