Cisco ISG Design and Deployment Guide: Gigabit Ethernet Aggregation

First Published: March 22, 2006
Last Updated: January 21, 2008

This document uses a model network tested in a Cisco lab to describe how to deploy a service provider broadband-based network using Cisco 7200 and 7300 series routers as a Cisco Intelligent Service Gateway (ISG) and Gigabit Ethernet (GE) as the aggregation technology. The Cisco ISG software provides a feature set that assists the service provider with provisioning and maintaining broadband networks that have many types of edge devices and many subscribers and services. The Cisco ISG software combines real-time session and flow control with programmable, dynamic policy control to deliver flexible and scalable subscriber session management capabilities. The role of the Cisco ISG software is to execute policies that identify and authenticate subscribers, and to provide access to the services that the subscriber is entitled to access. The role of the Cisco ISG router is deployment at network access control points so subscribers can access services through the software.

ISG Software Feature Sets

Cisco IOS software is packaged in feature sets that are supported on specific platforms. The Cisco ISG software is supported on Cisco 7200 and 7300 series routers. To get updated information regarding platform support and ISG feature sets, access Cisco Feature Navigator at http://www.cisco.com/go/fn. To access Cisco Feature Navigator, you must have an account on Cisco.com. Qualified users can establish an account on Cisco.com by following the directions at http://www.cisco.com/register. If you have an account but have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you.

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

Contents

Information About ISG and GE Aggregation

This section provides the following information about ISG and GE aggregation:

GE Aggregation

Higher performance LAN segment capacity and faster response times are needed to ease the demands placed on networks brought about by increases in the numbers of users buying faster computers and using bit-intensive applications such as video and gaming. Centralized, high-performance servers also contribute to traffic congestion. GE provides both the infrastructure and bandwidth needed to ease these demands. GE provides 1000 Mbps of raw bandwidth and is built upon the existing Institute of Electrical and Electronics Engineers (IEEE) 802.3 Ethernet standard. The installed base of over 70 million Ethernet nodes, and GE's adherence to the Ethernet standard, makes it a logical choice for deployment in high-speed broadband networks. Ethernet supports a variety of physical media with different maximum link distances, including copper-based links, fiber optic, and Category 5 Unshielded Twisted Pair (UTP) wiring.

The shift towards Ethernet-based solutions offers the following benefits:

- Ability to use simpler and lower-cost provisioning options for broadband subscribers over an Ethernet-based backhaul network rather than on an ATM-based network.
- Ability to use higher bandwidth connectivity options available from Ethernet not possible on ATM.
- Ability to upgrade to next-generation Digital Subscriber Line Access Multiplexers (DSLAMs) with support for higher bandwidth, asymmetric dual-latency modems such as the ADSL2.
- Ability to inject high-bandwidth content such as video into an Ethernet network.

The result of deploying GE in a broadband-based network such as digital subscriber line (DSL) is delivery of higher-bandwidth services at lower cost than other broadband aggregation methods while preserving quality of service.

The result of configuring an ISG is a collection of powerful and dynamic policies that can be applied to the subscriber session. The new policies are a superset of the Service Selection Gateway (SSG) concept of a *service*. With the ISG software, new subscriber rules allow you to build policies based on conditional events and by triggering service actions. Services can be implemented within virtual routing contexts.

The dynamic policy enforcement inherent in the ISG software allows consistent, tailored, and secure user services to be deployed in the network, triggered by a service or by a user—concepts referred to in the ISG software as *push* and *pull*.

The ISG has the ability to initiate and manage sessions consistently, regardless of the access protocol type, network service, or session traffic policies configured. The ISG software provides seamless integration with existing Cisco IOS IP services such as Domain Name System (DNS), access control lists (also access lists or ACLs), Dynamic Host Configuration Protocol (DHCP), virtual private network (VPN) routing and forwarding (VRF) instance, and Multiprotocol Label Switching (MPLS).

The ISG software also provides enhanced accounting of services for both use and application, and for advanced accounting for services such as prepaid. You will also find enhanced distributed conditional debugging that provides the ability to monitor and debug sessions and services based on identity.

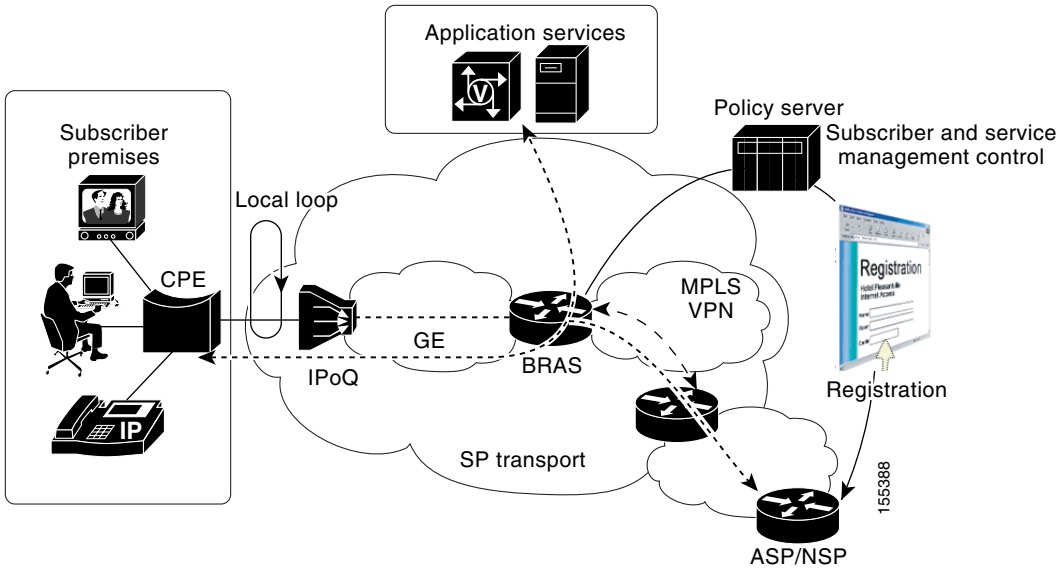
ISG with GE Aggregation Platform Support

Cisco's broadband aggregation portfolio offers comprehensive solutions for broadband service deployment that provides innovative technologies for simplified operations, revenue-generating network services, comprehensive management, and proven high availability. The aggregation of traffic received from a GE-based DSL network element is supported in the ISG software by the Cisco 7200 series router and the stackable, operationally efficient Cisco 7301 series router. Both routers are compact and mid-ranged, designed for incremental expansion of the service provider network, and targeted for deployment at the network edge. Both routers have a long list of features especially suited for GE and broadband aggregation and the network service provider and are capable of supporting 16,000 sessions with extended memory configurations.

ISG with GE Aggregation High-Level Network Topology

Figure 1 shows basic network elements in a GE-based network topology.

Figure 1 GE Aggregation Network Elements



The following elements play key roles in the network topology shown in Figure 1:

- CPE—The customer premises equipment (CPE) router is a small router such as the Cisco 800 series router that is used either as a bridge or to initiate IP connections from the customer PC to the ISG.
- Local loop—DSL services provide dedicated, point-to-point, public network access over twisted-pair copper wire on the local loop that occurs in the last mile between the service provider's central office and a customer site such as a house or office building. DSL technology uses existing twisted-pair telephone lines to transport high-bandwidth data to service subscribers. DSL delivers high-bandwidth data rates to dispersed locations with relatively small changes to the existing telco infrastructure.
- DSLAM—The Digital Subscriber Line Access Multiplexer (DSLAM) aggregates multiple incoming DSL connections into a single GE link. It is maintained at a point of presence (POP) separate from the Internet service provider's (ISP's) central network.

Note The configuration of the DSLAM will not be discussed in this document.

- ISG—A Cisco router such as the Cisco 7200 and 7300 series is configured as an ISG to control subscriber access at the edge of an IP/MPLS network.
- ISG as BRAS—A Broadband Remote Access Server (BRAS) is a high-density ISG router that supports thousands of simultaneous active sessions for the widest variety of broadband architectures. BRAS platform enhancements are enabling service providers to generate additional per-subscriber revenue while lowering operating and capital expenditures.
- PE—The provider edge (PE) router maintains VRF information. It is the final endpoint on the ISP's network that terminates the user session. The ISP uses VRF to segment customers easily without having to specify different subnets for different classes of customers.
- DHCP server—A DHCP server can be used to dynamically assign reusable IP addresses to devices in the network. Using a DHCP server can simplify device configuration and network management by centralizing network addressing. In the deployments described in this document, a Cisco CNS Network Registrar (CNR) server is used as the DHCP server.

- Policy server—A policy server is the network element that provides the service control that allows for the management and modification of services in real time. The Cisco Subscriber Edge Services Manager (SESM) is a policy server that provides service selection and connection management in broadband and mobile wireless networks. The Cisco SESM provides a web portal to enable users to access services. ISPs can customize the web portal to their needs. A detailed *Installation and Configuration Guide for the Cisco SESM* is at the following URL: http://www.cisco.com/en/US/docs/net_mgmt/subscriber_edge_services_manager/3.2/administration/guide/captive_portal/cportal.html
- Billing server—The billing server maintains user account information, including the amount of credit remaining for prepaid services. When users initiate services, the ISG contacts the billing server to determine if the user has credit available.
- AAA server—In IP deployments, the network utilizes a single authentication, authorization, and accounting (AAA) server. The AAA server maintains user authentication information and information about services available to users. When the ISG receives a username and password, it forwards them to the AAA server for authentication. When a user activates a service, the ISG contacts the AAA server, which replies to the ISG with information on the service.

Routing Protocols and Traffic Delivery

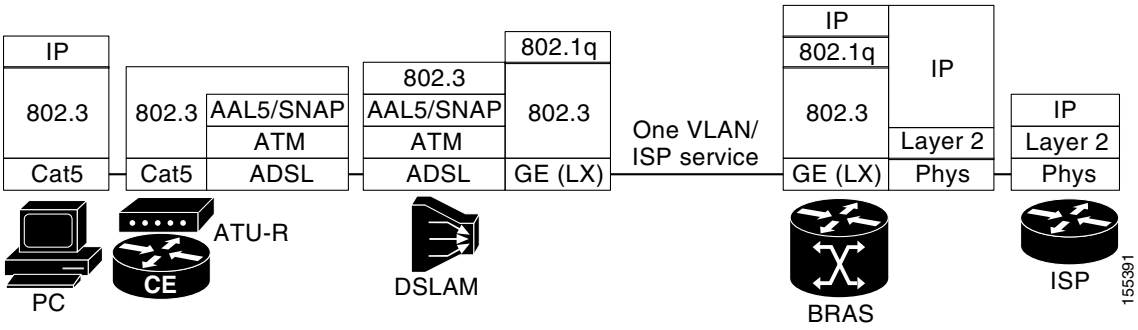
The following sections summarize the routing protocols used in the ISG GE network:

- Routing Protocols, page 5
- DHCP, page 6
- IP Sessions, page 6

Routing Protocols

Figure 2 provides a high-level view of the protocol stacks that are used in GE-based network topologies.

Figure 2 Protocol Stacks



IP over Ethernet is routed to the ISP via the BRAS. The identity of the customer is maintained at Layer 2 by a unique customer source Media Access Control (MAC) address all the way to the BRAS. It is possible to insert IP routed application services at the BRAS. IP address allocation mechanisms must be tightly coordinated between the ISP and the BRAS operators, especially if run by different companies.

The CPE is typically an ADSL modem or ADSL terminating unit router (ATU-R). The CPE communicates to the rest of the network through a customer edge (CE) router.

DHCP

As described in RFC 2131, *Dynamic Host Configuration Protocol*, DHCP provides configuration parameters to Internet hosts. DHCP consists of two components: a protocol for delivering host-specific configuration parameters from a DHCP server to a host and a mechanism for allocating network addresses to hosts. DHCP is built on a client/server model, where designated DHCP server hosts allocate network addresses and deliver configuration parameters to dynamically configured hosts. By default, Cisco routers running Cisco IOS software include DHCP server and relay agent software.

DHCP supports three mechanisms for IP address allocation:

- Automatic allocation—DHCP assigns a permanent IP address to a client.
- Dynamic allocation—DHCP assigns an IP address to a client for a limited period of time (or until the client explicitly relinquishes the address).
- Manual allocation—The network administrator assigns an IP address to a client, and DHCP is used simply to convey the assigned address to the client.

Automatic DHCP address allocation is typically based on an IP address, whether it be the gateway IP or the incoming interface IP address. In some networks, it is necessary to use additional information to further determine which IP addresses to allocate. Using the relay agent information option (option 82) permits the Cisco IOS relay agent to include additional information about itself when forwarding client-originated DHCP packets to a DHCP server.

IP Sessions

An IP session includes all the traffic that is associated with a single subscriber IP address. If the IP address is not unique to the system, other distinguishing characteristics such as VRF or a MAC address form part of the identity of the session. An ISG can be configured to create IP sessions upon receipt of DHCP messages (packets) and unknown IP source addresses. IP sessions may be hosted for a connected subscriber device (one routing hop from the ISG) or one that is many hops from the gateway.

The following events may be used to signal the start of an IP session:

- DHCPDISCOVER message.

  If the following conditions are met, receipt of a DHCPDISCOVER message will trigger the creation of an IP session:

  - The ISG serves as a DHCP relay or server for new IP address assignments.
  - Subscribers are configured for DHCP.
  - The DHCPDISCOVER message is the first DHCP request received from the subscriber.
- Unrecognized source IP address.

  In the absence of a DHCPDISCOVER message, a new IP session is triggered by the appearance of an IP packet with an unrecognized source IP address.

Because there is no inherent control protocol for IP sessions, the following events can be used to terminate a session:

- DHCPRELEASE message from the host or subscriber, or a lease expiry packet.
- Idle timeout.
- Session timeout.
- Account logoff.

ISG Service Bundles for GE Deployment Models

Because of the large number of ISG software services available, we have developed a list of services that are representative of what the general market is using. We have grouped the features into *service bundles*. This part of the document describes the following service bundles and features that were deployed in the network models used in this document:

- Basic Internet Access Service Bundle, page 7
- Double Play Service Bundle, page 7

Basic Internet Access Service Bundle

The Basic Internet Access service bundle consists of traditional Layer 3 VPN access. Subscribers establish Layer 2 access connections over a Layer 3 VPN technology—in this case, an MPLS VPN. The bandwidth for all users is capped at a static 128 kbps upstream and 256 kbps downstream.

Note The specific bandwidths described in this document are used only as examples. ISPs are free to configure any bandwidth levels that their service requires.

Double Play Service Bundle

The term *double play* refers to delivery of two foundation services for broadband networks, as follows:

- Basic broadband (Internet) connectivity
- Advance services, such as Voice over IP (VoIP)

When subscribers initiate a session, they are granted basic broadband connectivity. If subscribers wish to activate one of the advanced services such as VoIP, they go the web portal maintained by Cisco SESM and select the service.

Note In the deployments described in this document, the advanced services are deployed only for IP sessions; however, the ISG software supports these services on both IP and PPP over Ethernet (PPPoE).

The Best Effort Access Network Deployment Model

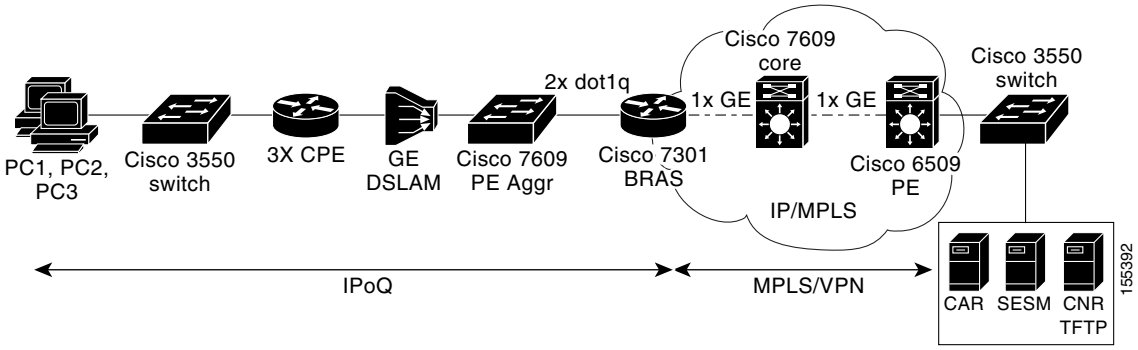
The deployment model described in the following sections was tested on a Cisco 7301 router acting as BRAS. In this scenario, a best effort access network and core network are overprovisioned to service different application services.

- Best Effort Access Network Topology, page 8
- Best Effort Access Network Device List, page 8
- Best Effort Access Network Data Flow, page 8
- Best Effort Access Network Call Flow, page 9

Best Effort Access Network Topology

Figure 3 shows the network topology for GE best effort access network deployment model with IP sessions.

Figure 3 Best Effort Network Topology



Best Effort Access Network Device List

Table 1 lists devices used in the ISG test network.

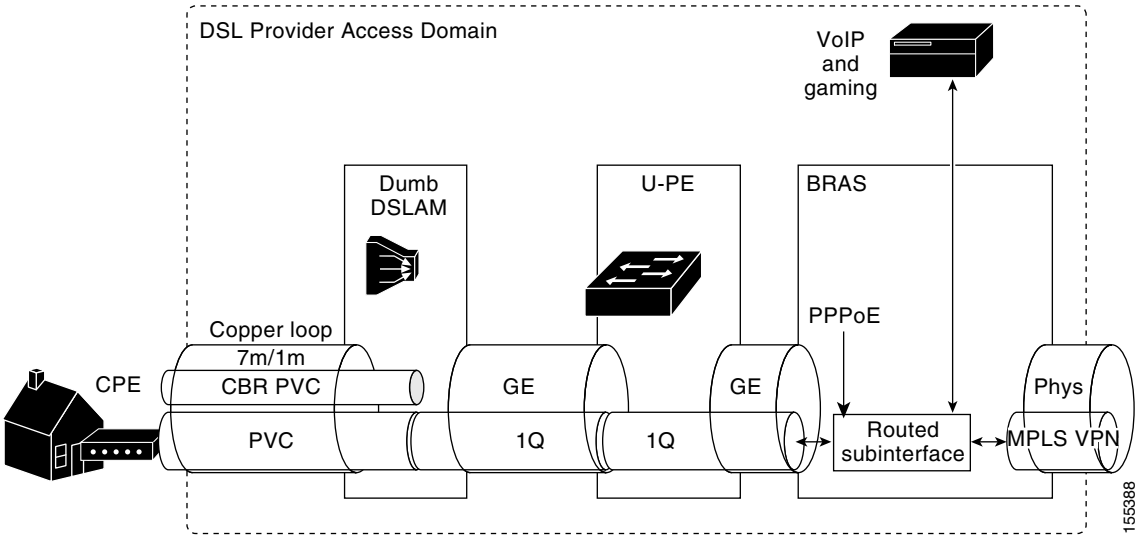
Table 1 Best Effort Network Network Device List

Device	Platform
BRAS	Cisco 7301
Core	Cisco 7609
CPE	Cisco 837
PE	Cisco 6509
PE-Agg	Cisco7609
Switches	Cisco 3550

Best Effort Access Network Data Flow

Figure 4 provides a high-level view of data flow across the network. The service provider is implementing a GE DSLAM network without Class-Based Queueing (CBQ).

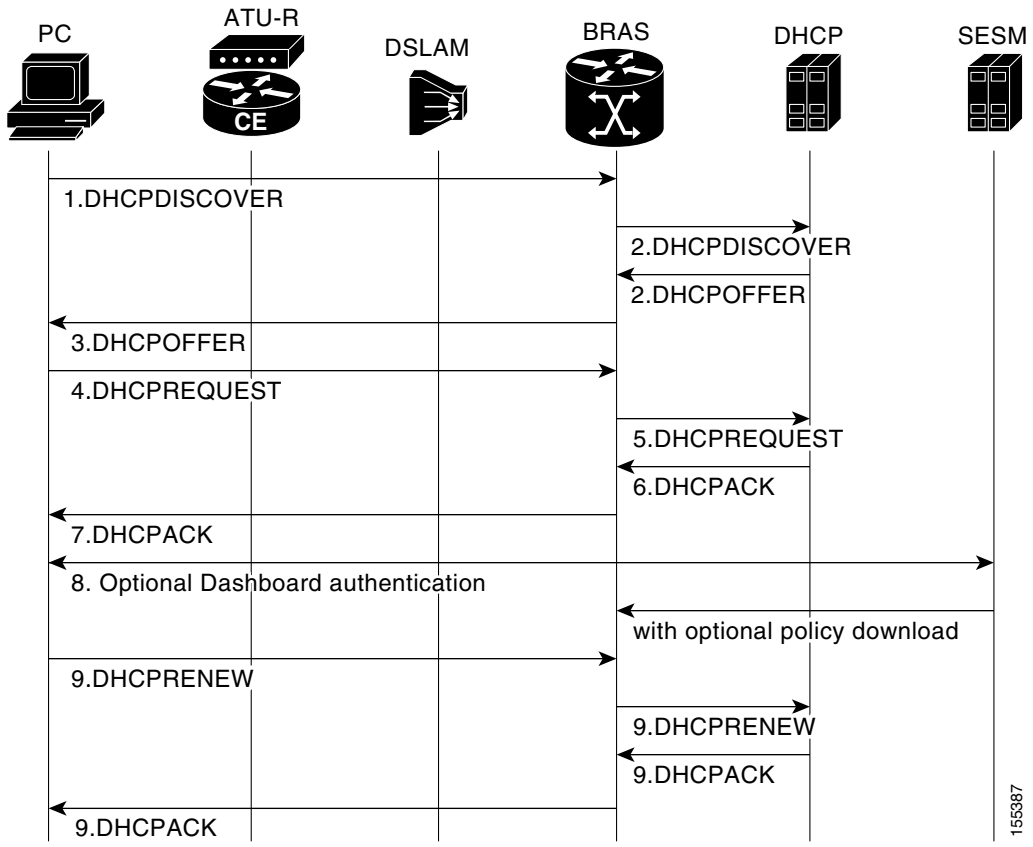
Figure 4 Best Effort Network Data Flow



Best Effort Access Network Call Flow

Figure 5 shows the DHCP call flow for the GE deployment model.

Figure 5 Best Effort Network DHCP Relay Call Flow



The following describes the sequence of events in Figure 5:

1. To begin, a DHCPDISCOVER message is sent from the client.
2. The BRAS allows the message to go to the DHCP server. The DHCP server replies with an DHCPOFFER message, and provides an IP address.
3. The BRAS forwards the DHCPOFFER message; however, the BRAS changes the IP address to its own, in order to maintain control of the session.
4. The client sends a DHCPREQUEST message to the IP address of the BRAS's unicast MAC because the client believes the BRAS is the offering DHCP server.
5. The BRAS creates a session and identifies the class name from a default service assigned to the session. This session will be be used to associate the client's logical port to the IP address returned from the DHCP server. The BRAS then places its IP address in memory (giaddr), and Option 82 is used to identify the subscriber DSL port. It is possible that VPN information could also be encoded in the subnet-selection suboption. The updated DHCPREQUEST message is then sent to the DHCP server.
6. The DHCP server allocates an IP address, which could potentially be used to initiate a VPN. The Layer 2 identity of the client is copied into the response and unicast to giaddr on the PE. The response to the PE is a DHCPOFFER message.
7. The PE removes any VPN-specific information from the DHCPOFFER message. Using the VPN ID suboption, the response is sent to the DHCP client on the correct VPN. The DHCPOFFER message is unicast to the client.
8. Optionally, web-based and user and service authentication occurs, and the BRAS port is fully enabled.
9. As timers start to expire, the RENEWING message is sent from the client, and the DHCP server acknowledges the request to extend service with a DHCPACK message.

Automatic DHCP address allocation is based on an IP address, whether it be the gateway or the incoming interface IP address. In some networks, it is necessary to use additional information to further determine which IP addresses to allocate. By using the relay agent information option (option 82), the Cisco IOS relay agent can include additional information about itself when forwarding client-originated DHCP packets to a DHCP server.

Best Effort Access Network Configuration

The following tasks describe how to configure a best effort access network using GE aggregation:

Prerequisites

This section provides prerequisites for configuration in the following sections:

Basic Configuration Requirements

Before beginning the configuration tasks, make sure that the following conditions are met:

- Basic IP connectivity is established across the entire network.
- MPLS is configured between the BRAS and PE routers; see Figure 1.
- Layer 3 VPN is configured between the BRAS and PE router.
- VRF and various other VRF services are configured.
- CPE is configured to bridge multiple IP clients.

Network administrators should also be familiar with the topics listed in the "Additional References" section on page 35.

Configuration Passwords

As you read through the configurations in this document, you will come across several types of passwords that will be required, such as for the Cisco IOS, for the Cisco Access Registrar (CAR) and AAA RADIUS server, for the billing server, and so on. The configurations in this document use the word "cisco" frequently as a password. You will need to provide unique passwords for each of these areas in your network, and determine some secure method for identifying which passwords are associated with a particular service.

Vendor-Specific Attributes

The configurations in this document use RADIUS vendor-specific attributes. These attributes are described in the following Cisco documentation:

- *RADIUS Attribute-Value Pairs and Dictionary Management* at http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/cs_unx/csu212ug/app_e.htm
- *RADIUS Vendor-Proprietary Attributes* at http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/secur_c/scprt6/scradatb.htm#wp8767
- "RADIUS Service and User Profile Attributes " in the *Cisco SSG-to-ISG DSL Broadband Migration Guide* at http://lbj.cisco.com/targets/ucdit/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/isa/migv1.htm#wp1114661

Table 2 summarizes the numeric definitions for some more commonly used RADIUS subattributes.

Note The Command-Code string must be converted to hexadecimal in ISGs running Cisco IOS Software Release 12.2(28)SB or earlier software. Also note that the attribute identifier is always 26, and the Cisco vendor identifier is always 9.

Table 2 Commonly Used RADIUS Vendor-Specific Subattributes

Subattribute Name	Attribute ID	Vendor ID	Subattribute ID	Subattribute Data Type
Cisco-AVPair	26	9	1	String
Account-Info	26	9	250	String
Service-Info	26	9	251	String
Command-Code	26	9	252	String
Control-Info	26	9	253	String

Configuring the ISG

The following tasks are performed to configure the ISG as BRAS in the best effort access network:

- Configuring AAA and Connection to the RADIUS Server, page 12
- Configuring Inbound and Outbound Access Lists, page 13
- Configuring Baseline ISG Subscriber Services, page 13
- Configuring IP Sessions, page 14
- Configuring Routing on the ISG Side, page 14

Figure 3 on page 8 shows the devices that are configured.

Configuring AAA and Connection to the RADIUS Server

The following example shows a basic AAA configuration that includes connection to the RADIUS server, and SESM installed and configured with the AAA information:

```
!
aaa new-model
!
!
aaa group server radius AAA-SERVERS
 server 10.12.12.57 auth-port 1812 acct-port 1813
!
aaa authentication login default none
aaa authentication login WEB_LOGON group AAA-SERVERS
aaa authorization network default group AAA-SERVERS
aaa authorization subscriber-service default local group AAA-SERVERS
aaa accounting network default start-stop group AAA-SERVERS
aaa accounting network AAA-MLIST start-stop group AAA-SERVERS
!
aaa server radius sesm
 client 10.12.12.55
 key cisco
 message-authenticator ignore
!
!
```

```
aaa session-id common
ip subnet-zero
!
!
```

The following example shows how to configure the RADIUS server and enable a unique session ID for accounting by configuring the **radius-server attribute 44 include-in-access-req** global configuration command on the ISG:

```
!
radius-server attribute 44 include-in-access-req
radius-server attribute 8 include-in-access-req
radius-server attribute 55 access-request include
radius-server attribute 25 access-request include
radius-server host 10.12.12.57 auth-port 1812 acct-port 1813 key cisco
radius-server vsa send accounting
radius-server vsa send authentication
!
```

Configuring Inbound and Outbound Access Lists

Basic access lists are configured to govern subscribers' Internet access. In the following example, the access lists are referenced in the AAA subscriber profile and govern incoming and outgoing Internet traffic. The Internet access lists should prevent subscribers from accessing the Cisco SESM and other management devices, to help prevent denial-of-service attacks.

```
ip access-list extended GAMING_ACL_IN
 permit ip 192.168.0.0 0.0.255.255 10.100.199.0 0.0.0.255
ip access-list extended GAMING_ACL_OUT
 permit ip 10.100.199.0 0.0.0.255 192.168.0.0 0.0.255.255
ip access-list extended INTERNET_ACL_IN
 deny   ip 10.0.0.0 0.255.255.255 any
 permit ip any any
ip access-list extended INTERNET_ACL_OUT
 deny   ip 10.0.0.0 0.255.255.255 any
 permit ip any any
ip access-list extended VOIP_ACL_IN
 permit ip 172.16.0.0 0.0.255.255 10.100.199.0 0.0.0.255
ip access-list extended VOIP_ACL_OUT
 permit ip 10.100.199.0 0.0.0.255 172.16.0.0 0.0.255.255
ip radius source-interface Loopback0
logging source-interface Loopback0
logging 10.12.12.55
access-list 101 permit ip any host 10.12.12.55
access-list 101 deny   ip any any
access-list 199 deny   tcp any host 10.12.12.55 eq www
access-list 199 deny   tcp any host 10.12.12.55 eq 8080
access-list 199 permit tcp any any eq www
access-list 199 deny   tcp host 10.12.12.55 any
```

Configuring Baseline ISG Subscriber Services

When the Port-Bundle Host Key (PBHK) feature is enabled, TCP packets from subscribers are mapped to a local IP address for the ISG gateway and a range of ports. The following mapping allows the portal to identify the ISG gateway from which the session originated.

```
! Configures the connection to the Cisco SESM for Layer 4 Redirect functionality.
redirect server-group DASHBOARD
 server ip 10.12.12.55 port 8090
```

```
! Enables port bundle host key (PBHK) access to the Cisco SESM. Each loopback interface
! can support up to 4031 bundles. If additional capacity is required, configure additional
! loopback interfaces.

ip portbundle
 match access-list 101
! The Loopback 0 interface is used to communicate with the Cisco SESM.
 source Loopback0
!

interface GigabitEthernet0/2
 mtu 1508
 ip address 10.50.1.2 255.255.255.0
 ip portbundle outside
 duplex auto
 speed auto
 media-type gbic
 negotiation auto
 mpls label protocol ldp
 mpls ip
!
```

Configuring IP Sessions

The following example configures an interface IP session using a DHCP initiator with class-aware capability:

```
interface GigabitEthernet0/0.1
 encapsulation dot1Q 101
 ip address 10.100.1.1 255.255.255.0 secondary vrf VPN73-1
 ip address 10.100.2.1 255.255.255.0 secondary vrf VPN73-2
 ip address 10.1.1.1 255.255.255.0
 ip subscriber
  initiator dhcp class-aware
 ip vrf autoclassify source
 no snmp trap link-status
 service-policy type control IP_RULE1
```

Configuring Routing on the ISG Side

The following example shows a typical configuration to enable routing in the network:

```
ip vrf VPN73-1
 rd 10:1
 route-target export 10:1
 route-target import 10:1
!
ip vrf VPN73-2
 rd 10:2
 route-target export 10:2
 route-target import 10:2

router ospf 100
 router-id 10.11.11.2
 log-adjacency-changes
 redistribute connected
 network 10.11.11.2 0.0.0.0 area 73
 network 10.50.0.0 0.0.255.255 area 73
!
```

```
router bgp 100
 no synchronization
 bgp router-id 10.11.11.2
 bgp log-neighbor-changes
 neighbor 10.11.11.9 remote-as 100
 neighbor 10.11.11.9 update-source Loopback0
 no auto-summary
 !
 address-family vpnv4
 neighbor 10.11.11.9 activate
 neighbor 10.11.11.9 send-community both
 exit-address-family
 !
 address-family ipv4 vrf VPN73-1
 redistribute connected
 redistribute static
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family ipv4 vrf VPN73-2
 redistribute connected
 redistribute static
 no auto-summary
 no synchronization
 exit-address-family
!
```

Configuring ISG Control Policies

Control policies define the actions that the system will take in response to specified events and conditions. For example, a control policy can be configured to authenticate specific subscribers and then provide them with access to specific services.

A control policy is made of one or more control policy rules. A control policy rule is an association of a control class and one or more actions. The control class defines the conditions that must be met before the actions will be executed. There are three steps involved in defining a control policy:

- Create one or more control class maps.

  A control class map specifies the conditions that must be met for a policy to be activated, and, optionally, the event that causes the class to be evaluated. A control class map may contain many conditions, each of which will be evaluated as either true or false. Match directives can be used to specify whether all, any, or none of the individual conditions must evaluate true in order for the class to evaluate true.

- Create a control policy map.

  A control policy map contains one or more control policy rules. A control policy rule associates a control class map with one or more actions. Actions are numbered and executed sequentially.

- Apply the control policy map.

The following example shows how to configure subscriber rule IP_RULE1 for IP Transparent Autologin (TAL) sessions using MAC address authentication, and then apply common services that are configured remotely on the AAA server, such as PBHK_SERVICE, INTERNET, and so on. The L4 REDIRECT service is applied for unauthenticated users in the subscriber rule.

```
! This command is enabled by default. It sets the number of rules that are displayed
! in the show subscriber session detail command.
subscriber policy recording rules limit 64
subscriber authorization enable
!

!
class-map type control match-all IP-UNAUTH-COND
 match timer IP-UNAUTH-TIMER
 match authen-status unauthenticated
!
!
policy-map type control IP_RULE1
 class type control IP-UNAUTH-COND event timed-policy-expiry
  1 service disconnect
!
 class type control always event session-start
  1 service-policy type service name PBHK_SERVICE
  2 authorize aaa password lab identifier mac-address
  3 service-policy type service name L4_REDIRECT_SERVICE
  4 set-timer IP-UNAUTH-TIMER 5
!
 class type control always event account-logon
  1 authenticate aaa list WEB_LOGON
  2 service-policy type service unapply name L4_REDIRECT_SERVICE
!
```

Configuring Profiles

AAA is configured with various service and user profiles.

In this section, the following service profile examples are provided:

- INTERNET Service Profile, page 16
- PBHK_SERVICE Service Profile, page 17
- L4_REDIRECT_SERVICE Profile, page 17

User and RADIUS profiles include:

- GAMING Attributes, page 18
- INTERNET Attributes, page 18
- PBHK_SERVICE Attributes, page 19
- VOIP Attributes, page 19

INTERNET Service Profile

This profile specifies one traffic class.

```
Name = INTERNET
     Description =
     Password = <encrypted>
     Enabled = TRUE
     Group~ =
     BaseProfile~ =
     AuthenticationScript~ =
     AuthorizationScript~ =
     UserDefined1 =
```

```
AllowNullPassword = FALSE
Attributes/
    Cisco-AVPair = "ip:traffic-class=in access-group name INTERNET_ACL_IN"
    Cisco-AVPair = "ip:traffic-class=in default drop"
    Cisco-AVPair = "ip:traffic-class=out access-group name INTERNET_ACL_OUT"
    Cisco-AVPair = "ip:traffic-class=out default drop"
    Cisco-AVPair = subscriber:accounting-list=AAA_ACCNT_LIST
    Cisco-SSG-Service-Info = R10.10.10.0;255.255.255.0
    Cisco-SSG-Service-Info = IINTERNET
CheckItems/
```

As a variation, the following profile shows the strings that configure no traffic class:

```
Name = INTERNET
Description =
Password = <encrypted>
Enabled = TRUE
Group~ =
BaseProfile~ =
AuthenticationScript~ =
AuthorizationScript~ =
UserDefined1 =
AllowNullPassword = FALSE
Attributes/
    Cisco-AVPair = ip:outacl=INTERNET_ACL_OUT
    Cisco-AVPair = ip:inacl=INTERNET_ACL_IN
CheckItems/
```

PBHK_SERVICE Service Profile

The following script creates the PBHK_SERVICE service profile:

```
Name = PBHK_SERVICE
Description =
Password = <encrypted>
Enabled = TRUE
Group~ =
BaseProfile~ =
AuthenticationScript~ =
AuthorizationScript~ =
UserDefined1 =
AllowNullPassword = FALSE
Attributes/
    Cisco-AVpair = ip:portbundle=enable
CheckItems/
```

L4_REDIRECT_SERVICE Profile

The following script creates the L4_REDIRECT_SERVICE profile:

```
[ //localhost/Radius/UserLists/Common-Services/L4_REDIRECT_SERVICE/Attributes ]
    Cisco-AVPair = "ip:l4redirect=redirect list 199 to group DASHBOARD"
```

User Profiles

The following scripts create user profiles:

```
[ //localhost/Radius/UserLists/7301-users/00e0.8121.799a/Attributes ]
    cisco-Avpair = subscriber:classname=c73-1
    cisco-Avpair = accounting-list=AAA-MLIST
    Cisco-SSG-Account-Info = AINTERNET
    Cisco-SSG-Account-Info = NGAMING
    Cisco-SSG-Account-Info = NVOIP

--> cd /Radius/UserLists/7301-users/00e0.8121.7dde/att

[ //localhost/Radius/UserLists/7301-users/00e0.8121.7dde/Attributes ]
    cisco-Avpair = subscriber:classname=C73-2
    cisco-Avpair = accounting-list=AAA-MLIST
    Cisco-SSG-Account-Info = AINTERNET
    Cisco-SSG-Account-Info = AGAMING
    Cisco-SSG-Account-Info = AVOIP
    User-Name = User1

--> cd /Radius/UserLists/7301-users/00e0.8122.25b6/att

[ //localhost/Radius/UserLists/7301-users/00e0.8122.25b6/Attributes ]
    Cisco-Avpair = subscriber:classname=73-1
    Cisco-Avpair = accounting-list=AAA-MLIST
    Cisco-SSG-Account-Info = AINTERNET
    Cisco-SSG-Account-Info = AGAMING
    Cisco-SSG-Account-Info = AVOIP
    User-Name = User2
```

RADIUS Profiles

The following script begins creation of RADIUS profiles for the common services:

```
    Name = Common-Services
    Description =
    GAMING/
    INTERNET/
    L4_REDIRECT_SERVICE/
    PBHK_SERVICE/
    VOIP/
```

The following RADIUS service profiles define attributes for gaming, Internet access, and VoIP, and for the L4 redirect and PBHK services.

GAMING Attributes

```
[ //localhost/Radius/UserLists/Common-Services/GAMING/Attributes ]
    Cisco-AVPair = "ip:traffic-class=in access-group name GAMING_ACL_IN"
    Cisco-AVPair = "ip:traffic-class=in default drop"
    Cisco-AVPair = "ip:traffic-class=out access-group name GAMING_ACL_OUT"
    Cisco-AVPair = "ip:traffic-class=out default drop"
    Cisco-SSG-Service-Info = IGAMING
    Cisco-SSG-Service-Info = R10.10.10.0;255.255.255.0
```

INTERNET Attributes

```
[ //localhost/Radius/UserLists/Common-Services/INTERNET/Attributes ]
    Cisco-AVPair = "ip:traffic-class=in access-group name INTERNET_ACL_IN"
    Cisco-AVPair = "ip:traffic-class=in default drop"
```

```
    Cisco-AVPair = "ip:traffic-class=out access-group name INTERNET_ACL_OUT"
    Cisco-AVPair = "ip:traffic-class=out default drop"
    Cisco-SSG-Service-Info = IINTERNET
    Cisco-SSG-Service-Info = R10.10.10.0;255.255.255.0
```

VOIP Attributes

```
[ //localhost/Radius/UserLists/Common-Services/VOIP/Attributes ]
    Cisco-AVPair = "ip:traffic-class=in access-group name VOIP_ACL_IN"
    Cisco-AVPair = "ip:traffic-class=in default drop"
    Cisco-AVPair = "ip:traffic-class=out access-group name VOIP_ACL_OUT"
    Cisco-AVPair = "ip:traffic-class=out default drop"
    Cisco-SSG-Service-Info = IVOIP
    Cisco-SSG-Service-Info = R10.10.10.0;255.255.255.0
```

PBHK_SERVICE Attributes

```
[ //localhost/Radius/UserLists/Common-Services/PBHK_SERVICE/Attributes ]
    Cisco-AVpair = ip:portbundle=enable
```

Configuring the DHCP Server and VRF Classes

Automatic DHCP address allocation is typically based on an IP address, whether it be the gateway or the incoming interface IP address. In some networks, it is necessary to use additional information to further determine which IP addresses to allocate. By using the relay agent information option (option 82), the Cisco IOS relay agent can include additional information about itself when forwarding client-originated DHCP packets to a DHCP server.

The **ip dhcp relay information option** command supports this functionality. The relay agent will automatically add the circuit identifier suboption and the remote ID suboption to the relay agent information option and forward them to the DHCP server. The DHCP server can use this information to assign IP addresses, perform access control, and set security policies (or other parameter-assignment policies) for each subscriber of a service provider network.

Cisco routers running Cisco IOS software include DHCP server and relay agent software. The Cisco IOS DHCP server assigns and manages IP addresses from specified address pools within the router to DHCP clients. If the Cisco IOS DHCP server cannot satisfy a DHCP request from its own database, it can forward the request to one or more secondary DHCP servers defined by the network administrator. DHCP supports three mechanisms for IP address allocation: automatic allocation of a permanent address, dynamic allocation for a limited period of time, and manual allocation where the network administrator assigns an IP address to a client and DHCP is used simply to convey the assigned address to the client.

The best effort network access deployment model uses manual allocation, as shown in the following configuration example:

```
!
no ip domain lookup
ip dhcp relay information option vpn
ip dhcp relay information option
ip dhcp relay information trust-all
ip dhcp use vrf connected
ip dhcp binding cleanup interval 600
!
!
```

```
ip dhcp pool P73-1
   vrf VPN73-1
   relay source 10.100.1.0 255.255.255.0
   relay destination global 10.12.12.56
   class C73-1
!
ip dhcp pool P73-2
   vrf VPN73-2
   relay source 10.100.2.0 255.255.255.0
   relay destination global 10.12.12.56
   class C73-2
!
ip dhcp pool 73-1
   relay source 10.1.1.0 255.255.255.0
   relay destination 10.12.12.56
   class 73-1
!
ip dhcp class C73-1
!
ip dhcp class C73-2
!
ip dhcp class 73-1
!
ip vrf VPN73-1
 rd 10:1
 route-target export 10:1
 route-target import 10:1
!
ip vrf VPN73-2
 rd 10:2
 route-target export 10:2
 route-target import 10:2
!
ip cef
!
```

Configuring the Remote PE Side

The PE is configured to assign subscribers to a VRF and to allow subscribers to access the Cisco SESM.

```
ip vrf VPN73-1
 rd 10:1
 route-target export 10:1
 route-target import 10:1
!
ip vrf VPN73-2
 rd 10:2
 route-target export 10:2
 route-target import 10:2
!

router bgp 100
 no synchronization
 bgp router-id 10.11.11.9
 bgp log-neighbor-changes
 neighbor 10.11.11.2 remote-as 100
 neighbor 10.11.11.2 update-source Loopback0
 neighbor 10.11.11.3 remote-as 100
 neighbor 10.11.11.3 update-source Loopback0
 neighbor 10.11.11.4 remote-as 100
```

```
 neighbor 10.11.11.4 update-source Loopback0
 no auto-summary
!
! Enables BGP VPNv4 neighbors
 address-family vpnv4
 neighbor 10.11.11.2 activate
 neighbor 10.11.11.2 send-community both
 neighbor 10.11.11.3 activate
 neighbor 10.11.11.3 send-community both
 neighbor 10.11.11.4 activate
 neighbor 10.11.11.4 send-community both
 exit-address-family
!
! Allows VRF routes into the BGP routing table.
 address-family ipv4 vrf VPN73-1
 redistribute connected
 redistribute static
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family ipv4 vrf VPN73-1
 redistribute connected
 redistribute static
 no auto-summary
 no synchronization
 exit-address-family
 !
```

Configuration Verification

The following sections provides examples of how to verify correct configuration and operating of the GE-based best effort access network:

- ISG Configuration Information Verification, page 21
- Basic ISG Operation Verification, page 23
- Subscriber Service Verification, page 25

ISG Configuration Information Verification

Use the **show running-configuration** EXEC command with the interface number to check interface configuration.

```
GE-7301-BRAS# show running-config interface gigabitEthernet 0/0.4039

Building configuration...

Current configuration : 369 bytes
!
interface GigabitEthernet0/0.4039
 encapsulation dot1Q 4039
 ip address 10.100.251.1 255.255.255.0 secondary vrf VPN73-251
 ip address 10.100.252.1 255.255.255.0 secondary vrf VPN73-252
 ip address 10.1.254.1 255.255.255.0
 ip subscriber
  initiator dhcp class-aware
 ip vrf autoclassify source
```

```
 no snmp trap link-status
 service-policy type control IP_RULE1
```

Use **show ip dhcp binding** command on the Cisco ISG/BRAS to verify that IP sessions have received IP addresses from the assigned pool correctly, that they have the correct binding with the assigned IP addresses, and that the binding type is relay.

```
GE-7301-BRAS# show ip dhcp binding

Bindings from all pools not associated with VRF:
IP address          Client-ID/     Lease expiration        Type
           Hardware address/
           User name

Bindings from VRF pool VPN73-1:
IP address          Client-ID/     Lease expiration        Type
           Hardware address/
           User name
10.100.1.52        0000.0000.0001          Feb 18 2006 11:31 PM    Relay
10.100.1.106       0000.0000.0091          Feb 18 2006 11:32 PM    Relay
10.100.1.107       0000.0000.0121          Feb 18 2006 11:31 PM    Relay
10.100.1.108       0000.0000.01b1          Feb 18 2006 11:31 PM    Relay
10.100.1.109       0000.0000.0241          Feb 18 2006 11:31 PM    Relay
10.100.1.110       0000.0000.02d1          Feb 18 2006 11:31 PM    Relay
10.100.1.111       0000.0000.0361          Feb 18 2006 11:31 PM    Relay
10.100.1.112       0000.0000.03f1          Feb 18 2006 11:31 PM    Relay
10.100.1.113       0000.0000.0481          Feb 18 2006 11:31 PM    Relay
10.100.1.114       0000.0000.0511          Feb 18 2006 11:31 PM    Relay
10.100.1.115       0000.0000.05a1          Feb 18 2006 11:31 PM    Relay
10.100.1.116       0000.0000.0631          Feb 18 2006 11:31 PM    Relay
10.100.1.117       0000.0000.06c1          Feb 18 2006 11:31 PM    Relay
10.100.1.118       0000.0000.0751          Feb 18 2006 11:31 PM    Relay
10.100.1.119       0000.0000.07e1          Feb 18 2006 11:31 PM    Relay
10.100.1.120       0000.0000.0871          Feb 18 2006 11:31 PM    Relay
10.100.1.121       0000.0000.0901          Feb 18 2006 11:31 PM    Relay
10.100.1.122       0000.0000.0991          Feb 18 2006 11:31 PM    Relay
10.100.1.123       0000.0000.0a21          Feb 18 2006 11:31 PM    Relay
10.100.1.124       0000.0000.0ab1          Feb 18 2006 11:31 PM    Relay
10.100.1.125       0000.0000.0b41          Feb 18 2006 11:31 PM    Relay
10.100.1.126       0000.0000.0bd1          Feb 18 2006 11:32 PM    Relay
10.100.1.127       0000.0000.0c61          Feb 18 2006 11:32 PM    Relay
10.100.1.128       0000.0000.0cf1          Feb 18 2006 11:32 PM    Relay
10.100.1.129       0000.0000.0d81          Feb 18 2006 11:32 PM    Relay
10.100.1.130       0000.0000.0e11          Feb 18 2006 11:32 PM    Relay
10.100.1.131       0000.0000.0ea1          Feb 18 2006 11:32 PM    Relay
10.100.1.132       0000.0000.0f31          Feb 18 2006 11:32 PM    Relay
10.100.1.133       0000.0000.0fc1          Feb 18 2006 11:32 PM    Relay
10.100.1.134       0000.0000.1051          Feb 18 2006 11:32 PM    Relay
10.100.1.135       0000.0000.10e1          Feb 18 2006 11:32 PM    Relay
10.100.1.136       0000.0000.1171          Feb 18 2006 11:32 PM    Relay
10.100.1.137       0000.0000.1291          Feb 18 2006 11:32 PM    Relay
10.100.1.138       0000.0000.1321          Feb 18 2006 11:32 PM    Relay
10.100.1.139       0000.0000.13b1          Feb 18 2006 11:32 PM    Relay
10.100.1.140       0000.0000.1441          Feb 18 2006 11:32 PM    Relay
10.100.1.141       0000.0000.14d1          Feb 18 2006 11:32 PM    Relay
10.100.1.142       0000.0000.1561          Feb 18 2006 11:32 PM    Relay
10.100.1.143       0000.0000.15f1          Feb 18 2006 11:32 PM    Relay
10.100.1.144       0000.0000.1681          Feb 18 2006 11:32 PM    Relay
10.100.1.145       0000.0000.1711          Feb 18 2006 11:32 PM    Relay
10.100.1.146       0000.0000.17a1          Feb 18 2006 11:32 PM    Relay
10.100.1.147       0000.0000.1831          Feb 18 2006 11:32 PM    Relay
10.100.1.148       0000.0000.18c1          Feb 18 2006 11:32 PM    Relay
10.100.1.149       0000.0000.1951          Feb 18 2006 11:32 PM    Relay
10.100.1.150       0000.0000.19e1          Feb 18 2006 11:32 PM    Relay
```

```
10.100.1.151       0000.0000.1a71          Feb 18 2006 11:32 PM    Relay
10.100.1.152       0000.0000.1b01          Feb 18 2006 11:32 PM    Relay
10.100.1.153       0000.0000.1b91          Feb 18 2006 11:33 PM    Relay
```

Basic ISG Operation Verification

Use the **show subscriber statistics** command to show a summary of the number of active sessions and a brief history of session activity.

```
GE-7301-BRAS# show subscriber statistics

Current Subscriber Statistics:

Number of sessions currently up: 1
Number of sessions currently pending: 0
Number of sessions currently authenticated: 1
Number of sessions currently unauthenticated: 0
Highest number of sessions ever up at one time: 14401
Mean up-time duration of sessions: 23:45:42
Total number of sessions up so far: 14405
Mean call rate per minute: 5, per hour: 335
Number of sessions failed to come up: 0
Access type based session count:
Traffic-Class sessions = 3
IP sessions = 1
```

Use the **show subscriber sessions** command to show basic information for all active subscribers.

```
GE-7301-BRAS# show subscriber sessions

Current Subscriber Information: Total sessions 1

Uniq ID Interface  State         Service      Identifier           Up-time
14417   IP         authen        Local Term   00e0.8121.799a       00:11:05
14418   Traffic-Cl unauthen      Ltm Internal                      00:11:05
14419   Traffic-Cl unauthen      Ltm Internal                      00:11:05
14420   Traffic-Cl unauthen      Ltm Internal                      00:11:05
```

Enable conditional debugging based on subinterfaces and the VLAN ID using the **debug condition interface** command. Verify in the DHCP debug that you are receiving DHCP option 82 information from the DSLAM. An example debug follows:

```
00:07:35: DHCPD: Searching for a match to 'relay-information
020e020a00000c0a0164120000000000' in class one
```

Verify in the **debug radius** output that all accounting packets for the IP session contain the attribute Acct-Session-Id [44] and should show debugs only for the specified VLANs. The bold text in the following output is for purposes of example only:

```
GE-7301-BRAS# debug radius

Radius protocol debugging is on
Radius protocol brief debugging is off
Radius protocol verbose debugging is off
Radius packet hex dump debugging is off
Radius packet protocol debugging is on
Radius packet retransmission debugging is off
Radius server fail-over debugging is off
Radius elog debugging is off
```

```
GE-7301-BRAS# show debugging

Radius protocol debugging is on
Radius packet protocol debugging is on
GE-7301-BRAS#
GE-7301-BRAS#
Feb 15 19:10:40.401: RADIUS/ENCODE(00003846):Orig. component type = IEDGE_IP_SIP
Feb 15 19:10:40.401: RADIUS(00003846): Config NAS IP: 10.11.11.2
Feb 15 19:10:40.401: RADIUS/ENCODE(00003846): acct_session_id: 14418
Feb 15 19:10:40.401: RADIUS(00003846): sending
Feb 15 19:10:40.401: RADIUS(00003846): Send Access-Request to 10.12.12.58:1812 id 1645/87,
len 230
Feb 15 19:10:40.401: RADIUS:  authenticator 1F 02 A4 58 08 4C 7F 52 - E9 CA F1 B4 29 DA DB
2B
Feb 15 19:10:40.401: RADIUS:  User-Name           [1]   16  "00e0.8121.799a"
Feb 15 19:10:40.401: RADIUS:  User-Password       [2]   18  *
Feb 15 19:10:40.401: RADIUS:  Calling-Station-Id  [31]  16  "00e0.8121.799a"
Feb 15 19:10:40.401: RADIUS:  NAS-Port-Type       [61]  6   Virtual                   [5]
Feb 15 19:10:40.401: RADIUS:  Vendor, Cisco       [26]  35
Feb 15 19:10:40.401: RADIUS:   Cisco AVpair       [1]   29  "circuit-id-tag=ffffffffciK "
Feb 15 19:10:40.401: RADIUS:  Vendor, Cisco       [26]  46
Feb 15 19:10:40.401: RADIUS:   Cisco AVpair       [1]   40
"remote-id-tag=020a00009601fe0100000fc7"
Feb 15 19:10:40.401: RADIUS:  NAS-Port            [5]   6   0
Feb 15 19:10:40.401: RADIUS:  NAS-Port-Id         [87]  39
"020a00009601fe0100000fc7:ffffffffciK "
Feb 15 19:10:40.401: RADIUS:  Service-Type        [6]   6   Outbound                  [5]
Feb 15 19:10:40.401: RADIUS:  NAS-IP-Address      [4]   6   10.11.11.2
Feb 15 19:10:40.401: RADIUS:  Acct-Session-Id     [44]  10  "00003852"
Feb 15 19:10:40.401: RADIUS:  Event-Timestamp     [55]  6   1140030640
Feb 15 19:10:40.405: RADIUS: Received from id 1645/87 10.12.12.58:1812, Access-Accept, len
195
Feb 15 19:10:40.405: RADIUS:  authenticator 72 33 9B 94 0F F6 7A 19 - AD C4 38 42 BE 3A 47
87
Feb 15 19:10:40.405: RADIUS:  User-Name           [1]   16  "User1"
Feb 15 19:10:40.405: RADIUS:  Vendor, Cisco       [26]  17
Feb 15 19:10:40.405: RADIUS:   ssg-account-info   [250] 11  "AINTERNET"
Feb 15 19:10:40.405: RADIUS:  Vendor, Cisco       [26]  17
Feb 15 19:10:40.405: RADIUS:   ssg-account-info   [250] 11  "NINTERNET"
Feb 15 19:10:40.405: RADIUS:  Vendor, Cisco       [26]  15
Feb 15 19:10:40.405: RADIUS:   ssg-account-info   [250] 9   "AGAMING"
Feb 15 19:10:40.405: RADIUS:  Vendor, Cisco       [26]  15
Feb 15 19:10:40.405: RADIUS:   ssg-account-info   [250] 9   "NGAMING"
Feb 15 19:10:40.405: RADIUS:  Vendor, Cisco       [26]  13
Feb 15 19:10:40.405: RADIUS:   ssg-account-info   [250] 7   "AVOIP"
Feb 15 19:10:40.405: RADIUS:  Vendor, Cisco       [26]  13
Feb 15 19:10:40.405: RADIUS:   ssg-account-info   [250] 7   "NVOIP"
Feb 15 19:10:40.405: RADIUS:  Vendor, Cisco       [26]  36
Feb 15 19:10:40.405: RADIUS:   Cisco AVpair       [1]   30  "subscriber:classname=C73-251"
Feb 15 19:10:40.405: RADIUS:  Vendor, Cisco       [26]  33
Feb 15 19:10:40.405: RADIUS:   Cisco AVpair       [1]   27  "accounting-list=AAA-MLIST"
Feb 15 19:10:40.405: RADIUS(00003846): Received from id 1645/87
Feb 15 19:10:40.409: RADIUS/ENCODE(00003846):Orig. component type = IEDGE_IP_SIP
Feb 15 19:10:40.409: RADIUS/ENCODE: format NAS port, no type set; WARNING
Feb 15 19:10:40.409: RADIUS(00003846): Config NAS IP: 10.11.11.2
Feb 15 19:10:40.409: RADIUS/ENCODE(00003846): acct_session_id: 14418
.
.
.
```

Subscriber Service Verification

Use the **show subscriber sessions uid** command with a user ID to show information about the specified subscriber. Use the **detailed** keyword to display an extensive report with the **show subscriber sessions uid** command.

```
GE-7301-BRAS# show subscriber sessions uid 14417

Unique Session ID: 14417
Identifier: 00e0.8121.799a
SIP subscriber access type(s): IP
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 00:11:32, Last Changed: 00:11:32

Policy information:
  Authentication status: authen
  Active services associated with session:
    name "INTERNET"
    name "GAMING"
    name "VOIP"
    name "PBHK_SERVICE", applied before account logon
  Rules, actions and conditions executed:
    subscriber rule-map IP_RULE1
      condition always event session-start
        1 service-policy type service name PBHK_SERVICE
        2 authorize identifier mac-address

Session inbound features:
 Feature: Session accounting
  Method List: AAA-MLIST
  Packets = 51, Bytes = 6906

Traffic classes:
  Traffic class session ID: 14418
   ACL Name: VOIP_ACL_IN, Packets = 0, Bytes = 0
  Traffic class session ID: 14419
   ACL Name: GAMING_ACL_IN, Packets = 0, Bytes = 0
  Traffic class session ID: 14420
   ACL Name: INTERNET_ACL_IN, Packets = 51, Bytes = 6906
 Default traffic is dropped
 Unmatched Packets (dropped) = 0, Re-classified packets (redirected) = 0

 Feature: Portbundle Hostkey
 Portbundle IP = 10.11.11.203     Bundle Number = 1365

Session outbound features:
 Feature: Session accounting
  Method List: AAA-MLIST
  Packets = 1, Bytes = 56

Traffic classes:
  Traffic class session ID: 14418
   ACL Name: VOIP_ACL_OUT, Packets = 0, Bytes = 0
  Traffic class session ID: 14419
   ACL Name: GAMING_ACL_OUT, Packets = 0, Bytes = 0
  Traffic class session ID: 14420
   ACL Name: INTERNET_ACL_OUT, Packets = 1, Bytes = 56
 Default traffic is dropped
 Unmatched Packets (dropped) = 0, Re-classified packets (redirected) = 0

Configuration sources associated with this session:
Service: INTERNET, Active Time = 00:11:34
  AAA Service ID = 1467652436
```

```
Service: GAMING, Active Time = 00:11:34
Service: VOIP, Active Time = 00:11:34
Service: PBHK_SERVICE, Active Time = 00:11:34
Interface: GigabitEthernet0/0.4039, Active Time = 00:11:34
```

Note Portbundle Hostkey and Traffic class cannot be configured under the same policy group.

Configuration Example

The following is a complete running configuration of a best effort access network that was tested in a lab at Cisco Systems. For the sake of brevity, repetitive portions of the configuration have been truncated and are noted by vertical ellipses.

```
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname GE-7301-BRAS
!
boot-start-marker
boot system disk0:c7301-js-mz.122-28.5.42.SB
boot system disk0:c7301-js-mz.122-28.5.35.SB
boot-end-marker
!
logging buffered 32000 debugging
no logging console
enable password lab
!
aaa new-model
!
!
aaa group server radius AAA-SERVERS-2
 server 10.12.12.58 auth-port 1812 acct-port 1813
!
aaa group server radius AAA-SERVERS-1
 server 10.12.12.57 auth-port 1812 acct-port 1813
!
aaa authentication login default none
aaa authentication login WEB_LOGON group AAA-SERVERS-2
aaa authentication ppp default group AAA-SERVERS-2
aaa authorization network default group AAA-SERVERS-2
aaa authorization subscriber-service default local group AAA-SERVERS-2
aaa accounting update periodic 71582
aaa accounting network default start-stop group AAA-SERVERS-2
aaa accounting network AAA-MLIST start-stop group AAA-SERVERS-2
aaa accounting network AAA_ACCNT_LIST start-stop group AAA-SERVERS-2
!
aaa attribute list IDMGR-Session-DB
!
aaa server radius sesm
 client 10.12.12.55
 key cisco
 message-authenticator ignore
!
!
aaa session-id common
```

```
ip subnet-zero
!
!
no ip domain lookup
ip dhcp smart-relay
ip dhcp relay information option vpn
ip dhcp relay information option
ip dhcp relay information trust-all
ip dhcp use vrf connected
!
ip dhcp pool P73-1
   vrf VPN73-1
   relay source 10.100.1.0 255.255.255.0
   relay destination global 10.12.12.56
   class C73-1
!
ip dhcp pool P73-2
   vrf VPN73-2
   relay source 10.100.2.0 255.255.255.0
   relay destination global 10.12.12.56
   class C73-2
!
ip dhcp pool P73-3
   vrf VPN73-3
   relay source 10.100.3.0 255.255.255.0
   relay destination global 10.12.12.56
   class C73-3
!
ip dhcp pool P73-4
   vrf VPN73-4
   relay source 10.100.4.0 255.255.255.0
   relay destination global 10.12.12.56
   class C73-4
.
.
.
ip dhcp pool 73-254
   relay source 10.1.254.0 255.255.255.0
   relay destination 10.12.12.56
   class 73-254
!
!
ip dhcp class C73-1
!
ip dhcp class C73-2
!
ip dhcp class C73-3
!
ip dhcp class C73-4
!
ip dhcp class C73-5
.
.
.
ip dhcp class 73-252
!
ip vrf VPN73-1
 rd 10:1
 route-target export 10:1
 route-target import 10:1
!
ip vrf VPN73-10
 rd 10:10
 route-target export 10:10
```

```
 route-target import 10:10
!
ip vrf VPN73-100
 rd 10:100
 route-target export 10:100
 route-target import 10:100
!
ip vrf VPN73-101
 rd 10:101
 route-target export 10:101
 route-target import 10:101
!
ip vrf VPN73-102
 rd 10:102
 route-target export 10:102
 route-target import 10:102
!
ip vrf VPN73-103
 rd 10:103
 route-target export 10:103
 route-target import 10:103
!
ip vrf VPN73-104
 rd 10:104
 route-target export 10:104
 route-target import 10:104
!
ip vrf VPN73-105
 rd 10:105
 route-target export 10:105
 route-target import 10:105
.
.
.
ip vrf VPN73-DATA
 rd 73:199
 route-target export 73:199
 route-target import 73:199
!
ip cef
!
!
subscriber policy recording rules limit 64
subscriber authorization enable
vpdn enable
!
redirect server-group DASHBOARD
 server ip 10.12.12.55 port 8090
!
no mpls traffic-eng auto-bw timers frequency 0
mpls ldp router-id Loopback0
no mpls ip propagate-ttl forwarded
call rsvp-sync
!
!
class-map type control match-all IP-UNAUTH-COND
 match timer IP-UNAUTH-TIMER
 match authen-status unauthenticated
!
!
policy-map type service PBHK_SERVICE_LOCAL
 ip portbundle
!
policy-map type service L4_REDIRECT_SERVICE_LOCAL
```

```
 class type traffic IP_AUTHEN
  redirect list 199 to group DASHBOARD

!
!
policy-map type control IP_RULE_LOCAL
 class type control IP-UNAUTH-COND event timed-policy-expiry
  1 service disconnect
!
 class type control always event session-start
  1 service-policy type service name PBHK_SERVICE_LOCAL
  2 authorize aaa password lab identifier mac-address
  3 service-policy type service name L4_REDIRECT_SERVICE_LOCAL
  4 set-timer IP-UNAUTH-TIMER 5
!
 class type control always event account-logon
  1 authenticate aaa list WEB_LOGON
  2 service-policy type service unapply name L4_REDIRECT_SERVICE_LOCAL
!
!
policy-map type control IP_RULE1
 class type control IP-UNAUTH-COND event timed-policy-expiry
  1 service disconnect
!
 class type control always event session-start
  1 service-policy type service name PBHK_SERVICE
  2 authorize aaa password lab identifier mac-address
  3 service-policy type service name L4_REDIRECT_SERVICE
  4 set-timer IP-UNAUTH-TIMER 5
!
 class type control always event account-logon
  1 authenticate aaa list WEB_LOGON
  2 service-policy type service unapply name L4_REDIRECT_SERVICE
!
!
!
interface Loopback0
 ip address 10.11.11.2 255.255.255.255
!
interface Loopback2
 ip address 10.1.1.1 255.255.255.255
!
interface Loopback201
 ip address 10.11.11.201 255.255.255.255
!
interface Loopback202
 ip address 10.11.11.202 255.255.255.255
!
interface Loopback203
 ip address 10.11.11.203 255.255.255.255
!
interface Loopback204
 ip address 10.11.11.204 255.255.255.255
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
 media-type gbic
 negotiation auto
!
interface GigabitEthernet0/0.1
 encapsulation dot1Q 101
 ip address 10.100.1.1 255.255.255.0 secondary vrf VPN73-1
```

```
 ip address 10.100.2.1 255.255.255.0 secondary vrf VPN73-2
 ip address 10.1.1.1 255.255.255.0
 ip subscriber
  initiator dhcp class-aware
 ip vrf autoclassify source
 no snmp trap link-status
 service-policy type control IP_RULE_LOCAL
!
interface GigabitEthernet0/0.2
 encapsulation dot1Q 102
 ip address 10.100.3.1 255.255.255.0 secondary vrf VPN73-3
 ip address 10.100.4.1 255.255.255.0 secondary vrf VPN73-4
 ip address 10.1.2.1 255.255.255.0
 ip subscriber
  initiator dhcp class-aware
 ip vrf autoclassify source
 no snmp trap link-status
 service-policy type control IP_RULE_LOCAL
!
interface GigabitEthernet0/0.3
 encapsulation dot1Q 103
 ip address 10.100.5.1 255.255.255.0 secondary vrf VPN73-5
 ip address 10.100.6.1 255.255.255.0 secondary vrf VPN73-6
 ip address 10.1.3.1 255.255.255.0
 ip subscriber
  initiator dhcp class-aware
 ip vrf autoclassify source
 no snmp trap link-status
 service-policy type control IP_RULE1
!
interface GigabitEthernet0/0.4
 encapsulation dot1Q 104
 ip address 10.100.7.1 255.255.255.0 secondary vrf VPN73-7
 ip address 10.100.8.1 255.255.255.0 secondary vrf VPN73-8
 ip address 10.1.4.1 255.255.255.0
 ip subscriber
  initiator dhcp class-aware
 ip vrf autoclassify source
 no snmp trap link-status
 service-policy type control IP_RULE1
!
interface GigabitEthernet0/0.5
 encapsulation dot1Q 105
 ip address 10.100.10.1 255.255.255.0 secondary vrf VPN73-10
 ip address 10.100.9.1 255.255.255.0 secondary vrf VPN73-9
 ip address 10.1.5.1 255.255.255.0
 ip subscriber
  initiator dhcp class-aware
 ip vrf autoclassify source
 no snmp trap link-status
 service-policy type control IP_RULE1
.
.
.
interface GigabitEthernet0/1.40
 encapsulation dot1Q 180
 ip address 10.100.159.1 255.255.255.0 secondary vrf VPN73-159
 ip address 10.100.160.1 255.255.255.0 secondary vrf VPN73-160
 ip address 10.1.80.1 255.255.255.0
 ip subscriber
  initiator dhcp class-aware
 ip vrf autoclassify source
 no snmp trap link-status
 service-policy type control IP_RULE1
```

```
!
interface GigabitEthernet0/2
 mtu 1508
 ip address 10.50.1.2 255.255.255.0
 ip portbundle outside
 duplex auto
 speed auto
 media-type gbic
 negotiation auto
 mpls label protocol ldp
 mpls ip
!
!
router ospf 100
 router-id 10.11.11.2
 log-adjacency-changes
 redistribute connected
 network 10.11.11.2 0.0.0.0 area 73
 network 10.11.11.201 0.0.0.0 area 73
 network 10.11.11.202 0.0.0.0 area 73
 network 10.11.11.203 0.0.0.0 area 73
 network 10.11.11.204 0.0.0.0 area 73
 network 10.50.0.0 0.0.255.255 area 73
 network 10.1.1.0 0.0.0.255 area 73
 network 10.1.2.0 0.0.0.255 area 73
 network 10.1.3.0 0.0.0.255 area 73
.
.
.
network 10.1.254.0 0.0.0.255 area 73
!
router bgp 100
 no synchronization
 bgp router-id 10.11.11.2
 bgp log-neighbor-changes
 neighbor 10.11.11.9 remote-as 100
 neighbor 10.11.11.9 update-source Loopback0
 no auto-summary
 !
 address-family vpnv4
 neighbor 10.11.11.9 activate
 neighbor 10.11.11.9 send-community both
 exit-address-family
 !
 address-family ipv4 vrf VPN73-DATA
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family ipv4 vrf VPN73-99
 redistribute connected
 redistribute static
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family ipv4 vrf VPN73-98
 redistribute connected
 redistribute static
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family ipv4 vrf VPN73-97
```

```
 redistribute connected
 redistribute static
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family ipv4 vrf VPN73-96
 redistribute connected
 redistribute static
 no auto-summary
 no synchronization
 exit-address-family
 !
.
.
.

 address-family ipv4 vrf VPN73-2
 redistribute connected
 redistribute static
 no auto-summary
 no synchronization
 exit-address-family
!
 address-family ipv4 vrf VPN73-1
 redistribute connected
 redistribute static
 no auto-summary
 no synchronization
 exit-address-family
!
!
ip portbundle
 match access-list 101
 source Loopback0
 source Loopback201
 source Loopback202
 source Loopback203
 source Loopback204
!
ip classless
!
no ip http server
!
!
!
ip access-list extended GAMING_ACL_IN
 permit ip 192.168.0.0 0.0.255.255 10.100.199.0 0.0.0.255
ip access-list extended GAMING_ACL_OUT
 permit ip 10.100.199.0 0.0.0.255 192.168.0.0 0.0.255.255
ip access-list extended INTERNET_ACL_IN
 deny   ip 10.0.0.0 0.255.255.255 any
 permit ip any any
ip access-list extended INTERNET_ACL_OUT
 deny   ip 10.0.0.0 0.255.255.255 any
 permit ip any any
ip access-list extended VOIP_ACL_IN
 permit ip 172.16.0.0 0.0.255.255 10.100.199.0 0.0.0.255
ip access-list extended VOIP_ACL_OUT
 permit ip 10.100.199.0 0.0.0.255 172.16.0.0 0.0.255.255
ip radius source-interface Loopback0
logging source-interface Loopback0
logging 10.12.12.55
access-list 101 permit ip any host 10.12.12.55
```

```
access-list 101 deny   ip any any
access-list 199 deny   tcp any host 10.12.12.55 eq www
access-list 199 deny   tcp any host 10.12.12.55 eq 8080
access-list 199 permit tcp any any eq www
access-list 199 deny   tcp host 10.12.12.55 any
!
snmp-server community cisco RO
snmp-server community public RO
snmp-server community private RW
snmp-server chassis-id 7301-bras
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps ds1
snmp-server enable traps tty
snmp-server enable traps eigrp
snmp-server enable traps gatekeeper
snmp-server enable traps isdn call-information
snmp-server enable traps isdn layer2
snmp-server enable traps isdn chan-not-avail
snmp-server enable traps isdn ietf
snmp-server enable traps atm subif
snmp-server enable traps channel
snmp-server enable traps flash insertion removal
snmp-server enable traps hsrp
snmp-server enable traps config
snmp-server enable traps outage
snmp-server enable traps entity
snmp-server enable traps cpu threshold
snmp-server enable traps config-copy
snmp-server enable traps fru-ctrl
snmp-server enable traps envmon
snmp-server enable traps aaa_server
snmp-server enable traps bgp
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps pim neighbor-change rp-mapping-change invalid-pim-message
snmp-server enable traps ipmulticast
snmp-server enable traps msdp
snmp-server enable traps rsvp
snmp-server enable traps frame-relay
snmp-server enable traps frame-relay subif
snmp-server enable traps syslog
snmp-server enable traps rtr
snmp-server enable traps mpls traffic-eng
snmp-server enable traps mpls ldp
snmp-server enable traps dlsw
snmp-server enable traps pppoe
snmp-server enable traps l2tun session
snmp-server enable traps l2tun pseudowire status
snmp-server enable traps dial
snmp-server enable traps mpls vpn
snmp-server enable traps voice poor-qov
snmp-server enable traps xgcp
snmp-server host 10.12.12.55 public
!
radius-server attribute 44 include-in-access-req
radius-server attribute 8 include-in-access-req
radius-server attribute 55 access-request include
radius-server attribute 25 access-request include
```

```
radius-server host 10.12.12.58 auth-port 1812 acct-port 1813 key cisco
radius-server host 10.12.12.57 auth-port 1812 acct-port 1813 key cisco
radius-server timeout 300
radius-server vsa send accounting
radius-server vsa send authentication
!
control-plane
!
!
dial-peer cor custom
!
!
!
!
gatekeeper
 shutdown
!
alias exec sss show subscriber sessions
alias exec sir show ip route
alias exec siib show ip int brief
alias exec sib show ip bgp
alias exec ct config term
alias exec sri show run int
alias exec sr show run
alias exec ss sh subscr sess
alias exec cssa cle subsc sess all
alias exec sipb sho ip portbundle status
alias exec cidb cle ip dhcp binding *
alias exec sidb sh ip dhcp binding
alias exec ssstat sh subscr stat
alias exec showdb show database data IDMGR-Session-DB 2
alias exec spc show proc cpu
alias exec sms show mem sum
alias exec spms show proc mem sort
alias exec smat show mem alloc totals
!
line con 0
 exec-timeout 0 0
 length 0
 international
 transport output lat pad v120 mop telnet rlogin udptn nasi
 stopbits 1
line aux 0
 transport input all
 transport output lat pad v120 mop telnet rlogin udptn nasi
 stopbits 1
line vty 0 4
 exec-timeout 0 0
 transport input lat pad v120 mop telnet rlogin udptn nasi
 transport output lat pad v120 mop telnet rlogin udptn nasi
line vty 5 15
 exec-timeout 0 0
 transport input lat pad v120 mop telnet rlogin udptn nasi
 transport output lat pad v120 mop telnet rlogin udptn nasi
!
ntp clock-period 17179870
ntp source Loopback0
ntp server 10.11.11.11
!
end
```

Additional References

The following sections provide references related to configuring the ISG in an GE-based broadband network:

Related Documents

Related Topic	Document Title
Broadband and DSL configuration	*Cisco IOS Broadband and DSL Configuration Guide*, Release 12.4
CAR configuration procedure	*Cisco CNS Access Registrar Installation and Configuration Guide*, 3.5
CNR configuration procedure	*Cisco CNS Network Registrar User's Guide*, 6.2 at *http://www.cisco.com/en/US/partner/products/sw/netmgtsw/ps1982/tsd_products_support_series_home.html*
ISG software configuration	*Cisco IOS Intelligent Service Gateway Configuration Guide*, Release 12.2 SB
Layer 2 Tunnel Protocol (L2TP) virtual private dialup network (VPDN) for dialin and dialout configuration	*Cisco IOS VPDN Configuration Guide*, Release 12.4
RADIUS attributes	*RADIUS Attribute-Value Pairs and Dictionary Management* *RADIUS Vendor-Proprietary Attributes* "RADIUS Service and User Profile Attributes" in the *Cisco SSG-to-ISG DSL Broadband Migration Guide*
Virtual template interface configuration	"Configuring Virtual Template Interfaces" in the *Cisco IOS Dial Technologies Configuration Guide*, Release 12.4

Standards

Standard	Title
AAL5/SNAP	• ATM adaptation layer 5—AAL5 is one of four AALs recommended by the ITU-T. • Subnetwork Access Protocol—SNAP specifies a standard method of encapsulating IP datagrams and ARP messages on IEEE networks.
IEEE 802.3 Ethernet Standard	• *LAN/MAN CSMA/CD Access Method*

RFCs

RFC	Title
RFC 1541	*Dynamic Host Configuration Protocol*

Technical Assistance

Description	Link
The Cisco Technical Support and Documentation website contains thousands of 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.	http://www.cisco.com/techsupport

Glossary

AAA—authentication, authorization, and accounting

AAL5/SNAP—ATM adaptation Layer 5/Subnetwork Access Protocol

ACL—access control list or access list

ATU-R—ADSL Transmission Unit—remote

BRAS—Broadband Remote Access Server

CAR—Cisco CNR Access Registrar

CE—customer edge

CNR—Cisco Network Registrar

CPE—customer premises equipment

DHCP—Dynamic Host Configuration Protocol

DNS—Domain Name System

DSL—digital subscriber line

DSLAM—Digital Subscriber Line Access Multiplexer

ISG—Intelligent Service Gateway

ISP—Internet service provider

L2TP—Layer 2 Tunnel Protocol

MAC—Media Access Control

MPLS—Multiprotocol Label Switching

PBHK—Port-Bundle Host Key

PE—provider edge

PPPoE—PPP over Ethernet

PVC—permanent virtual circuit

SESM—Subscriber Edge Services Manager

SSG—Service Selection Gateway

TAL—Transparent Autologin

VoIP—Voice over IP

VPDN—virtual private dialup network

VPN—Virtual Private Network

VRF—VPN routing and forwarding instance

VSA—vendor-specific attribute

Note See *Internetworking Terms and Acronyms* for terms not included in this glossary.