Cisco ISG Design and Deployment Guide: Gigabit Ethernet Aggregation Using Cisco IOS Software Release 12.2(31)SB2

First Published: November 27, 2006
Last Updated: January 25, 2010

This document uses model networks tested in a Cisco laboratory to describe how to deploy a service provider broadband-based network using Cisco 7200, 7300, and 10000 series routers as a Cisco Intelligent Services 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, 7300, and 10000 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 the bandwidth needed to ease response to the demands of increased network traffic. GE provides 1000 Mbps of raw bandwidth and is built upon the existing Institute of IEEE 802.3 Ethernet standard. The installed base of over 70 million Ethernet nodes and GE's adherence to the Ethernet standard make GE 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 and 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 the delivery of higher-bandwidth services at lower cost than other broadband aggregation methods while preserving quality of service (QoS).

The result of configuring an ISG is a collection of powerful and dynamic policies that can be applied to Internet subscriber sessions. 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 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 the subscription services for both use and application, and for advanced accounting for such features as prepaid service. You will also find enhanced distributed conditional debugging that provides the ability to monitor and debug sessions and services based on identity.

GE Aggregation Platform Support

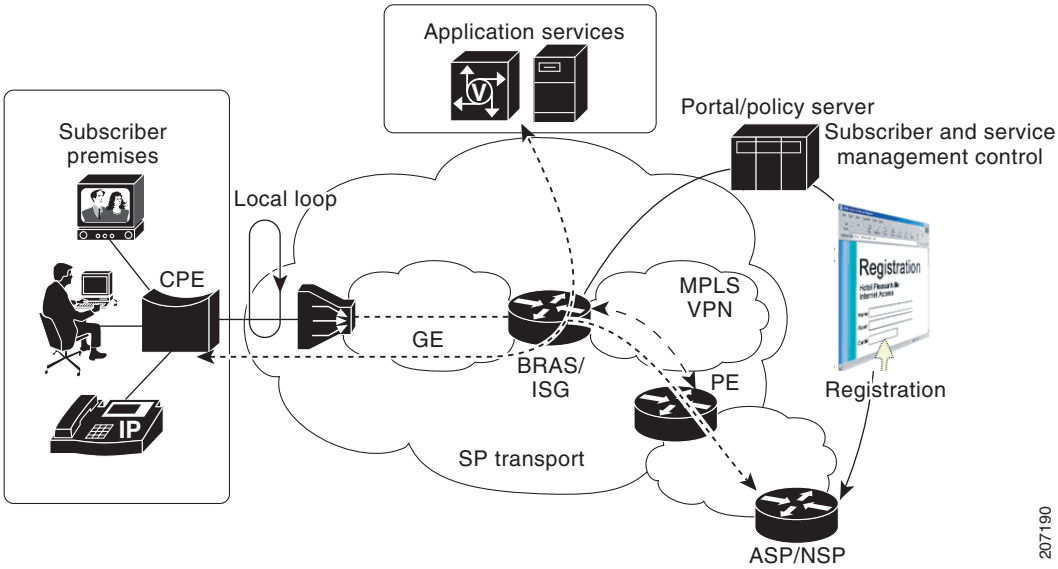
Cisco's broadband aggregation portfolio offers comprehensive solutions that provides innovative technologies for simplified operations, revenue-generating network services, comprehensive management, and proven high availability for broadband service deployment. The aggregation of traffic received from a GE-based DSL network element is supported by the following Cisco hardware:

- The Cisco 7200 series router with the NPE-G1 network processing engine card and the stackable, operationally efficient Cisco 7300 series router 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 broadband aggregation and the network service provider, and they are capable of supporting 8,000 sessions with extended memory configurations.
- The Cisco 10000 series router with the PRE2 or PRE3 performance routing engine card provides carrier-class delivery of over 32,000 simultaneous subscriber sessions.

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 is not discussed in this document.

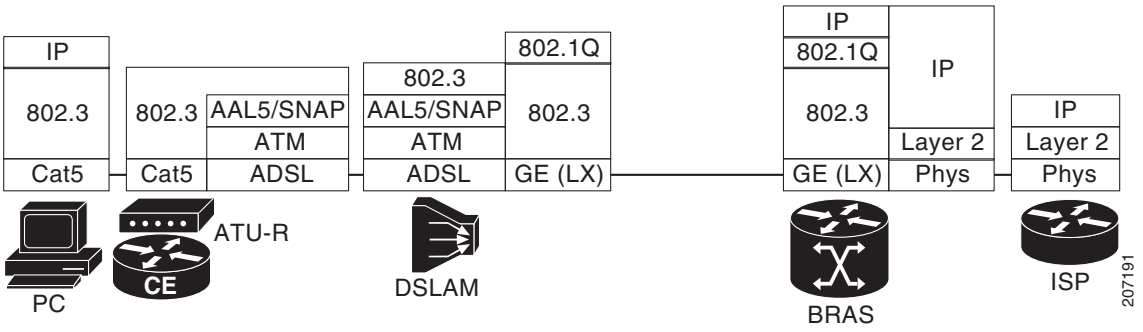
- ISG—A Cisco router such as the Cisco 7200 series is configured as an ISG to control subscriber access at the edge of an IP/MPLS network.
- ISG as BRAS—A Broadband Remote Access Server (BRAS) is a high-density ISG router that supports thousands of simultaneous active sessions for the widest variety 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.
- ASP/NSP—Access and network switch processors.
- 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 Network Registrar (CNR) server is used as the DHCP server.

- Policy/portal server—A policy/portal server is the network element that provides the service control that allows for the management and modification of services in real time.
- Billing server—The billing server maintains user account information, including the amount of credit remaining for prepaid services. When a user initiates 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.

Network Access Models

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 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 Transmission Unit—remote (ATU-R). The CPE communicates to the rest of the network through a customer edge (CE) router.

The following sections summarize the network access types used in the ISG GE network:

- DHCP, page 5
- IP Sessions, page 6
- IEEE 802.1Q, page 7
- IEEE 802.1Q Tunneling (Q-in-Q), page 7
- PPPoE, page 8

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.
- Unrecognized MAC 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 MAC address.
- RADIUS proxy record.

  A new IP session can also be triggered by the appearance of a RADIUS Access-Request packet. The RADIUS proxy record is basically an insertion mechanism that allows an ISG device to be introduced to a network with minimum disruption to the existing AAA servers.

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.
- Session termination using an ISG control policy.
- Idle timeout.

- Session timeout.
- Account logoff.

IEEE 802.1Q

The IEEE 802.1Q protocol was developed to allow multiple bridged networks to share the same physical network link transparently without leakage of information between networks. The standard addresses how to break up large networks so that broadcast and multicast traffic does not take more bandwidth than is necessary. The standard also allows for individual virtual LANs (VLANs) to communicate with one another using a router.

The IEEE 802.1Q protocol establishes a method for inserting virtual VLAN membership information into Ethernet frames. The term VLAN refers to the ability to virtualize a LAN.

IEEE 802.1Q Tunneling (Q-in-Q)

Without VLANs, all subscribers in a switched network would be in the same broadcast domain. Dedicating a VLAN to each customer is possible but impractical because of the 4096 global VLAN limit in the IEEE 802.1Q protocol. It is more common to configure one single VLAN per switch, but this configuration still leaves all users on the same switch in the same broadcast domain. Private VLANs can be used to solve this issue, but another alternative is to use double VLAN encapsulation, where traffic from each subscriber's port is mapped to a different 802.1Q tag, and then each frame is tagged again when it leaves the switch with a tag that uniquely identifies the switch on the Ethernet network.

Double VLAN encapsulation adds another layer of IEEE 802.1Q tag (called metro tag or PE-VLAN) to 802.1Q tagged packets that enter the network. The purpose is to expand the VLAN space by tagging the tagged packets, thus producing a double-tagged frame. The expanded VLAN space allows the service provider to provide certain services, such as Internet access on specific VLANs for specific customers, and yet still allows the service provider to provide other types of services for their other customers on other VLANs.

Another term for this encapsulating functionality is *tunneling*, and another way to note this functionality is "802.1Q-in-802.1Q," or more simply "Q-in-Q."

Generally a service provider's customers require a range of VLANs to handle multiple applications. Service providers can allow their customers to use this feature to safely assign their own VLAN IDs on subinterfaces because these subinterface VLAN IDs are encapsulated within a service-provider-designated VLAN ID for a given customer. Therefore, there is no overlap of VLAN IDs among customers, nor does traffic from different customers become mixed. The double-tagged frame is terminated or assigned on a subinterface with an expanded **encapsulation dot1q** command that specifies the two VLAN ID tags (outer VLAN ID and inner VLAN ID) terminated on the subinterface.

When you configure Q-in-Q, you assign a tunnel port to a VLAN that you dedicate to tunneling, which then becomes a tunnel VLAN. To keep customer traffic segregated requires a separate tunnel VLAN for each customer, but that one tunnel VLAN supports all of the customer's traffic. Q-in-Q is not restricted to point-to-point tunnel configurations. Any tunnel port in a tunnel VLAN is a tunnel entry and exit point. An IEEE 802.1Q tunnel can have as many tunnel ports as needed to connect customer routers.

Q-in-Q is generally used in Metro Ethernet or Ethernet digital subscriber line access multiplexer (DSLAM) environments. Networks using Q-in-Q are commonly found in multi-tenant buildings such as a hotel where Internet services are provided individually to each tenant. Because Ethernet is inherent in Q-in-Q, customers have access to abundant bandwidth, and service providers can easily deliver services to the customer.

Q-in-Q is generally supported on whichever Cisco IOS features or protocols are supported on the subinterface. For example, if you can run PPP over Ethernet (PPPoE) on the subinterface, you can configure a double-tagged frame for PPPoE.

PPPoE

When you deploy ADSL in a network with PPP, you must support PPP-style authentication and authorization over a large installed base of legacy bridging customer premises equipment (CPE). PPPoE provides the ability to connect a network of hosts over a simple bridging access device to a remote access concentrator or aggregation concentrator. With this model, each host uses its own PPP stack, thus providing a familiar user interface. Access control, billing, and type of service can be done on a per-user, rather than a per-site, basis.

As specified in RFC 2516, PPPoE has two distinct stages, a discovery stage and a PPP session stage. When a host initiates a PPPoE session, it must first perform discovery to identify which server can meet the client's request. Then it must identify the Ethernet MAC address of the peer and establish a PPPoE session ID. Although PPP defines a peer-to-peer relationship, discovery is inherently a client-server relationship. In the discovery process, the client discovers the server (access concentrator). Based on the network topology, there may be more than one server with which the host can communicate. The discovery stage allows the host to discover all servers and select one. When the discovery phase completes successfully, both the host and the selected server have the information needed to build their point-to-point connection over Ethernet.

ISG Features Tested

Following are the features that were tested on the platforms—Cisco 7200, 7300, and 10000 series routers—used in the test environments described in this document:

- Accounting: Per Session, Service and Flow; Prepaid
- Flow Redirect (L4, Captive Portal)
- Protocol Event (DHCP)
- Service Profiles
- User Profiles
- Cisco Policy Language
- Triggers (Time, Volume, Duration)
- Change of Authorization (CoA) (QoS, L4 Redirect, User ACL, TimeOut)
- Multi-Service Creation and Flow Control
- Idle Timeout
- Interface IP Session at Layer 2
- Absolute Session Timeout
- Port-Bundle Host Key (PBHK)
- Transparent Autologin (TAL)
- VRF Transfer

Test Software and Equipment

Table 1 lists devices used in the ISG test network.

Table 1 Device List

Function	Description
Portal	BroadHop Service Management Engine
DSL aggregation	Ericsson GE DSLAM
Terminal server	Cisco 2511
Access switches	Catalyst 3550
BRAS	Cisco 7206 router with NPE-G1
BRAS	Cisco 10008 router with PRE2/PRE3
BRAS	Cisco 7301
PE-Agg, MPLS core	Cisco 7600 router with SUP720
MPLS PE	Cisco 6500 router with SUP720

Table 2 lists the software used in the testing.

Table 2 Software Used in Testing

Device	Software
PCs	Windows XP
Sun servers	Sun Solaris 8
Cisco 7206 router as BRAS	Cisco IOS Release 12.2(31)SB2
Cisco 10000 router as BRAS	Cisco IOS Release 12.2(31)SB2
Cisco 7301 router as BRAS	Cisco IOS Release 12.2(31)SB2
Cisco 7600 router	Cisco IOS Release 12.2(18)SXD4
Cisco 6500 router	Cisco IOS Release 12.2(18)SXD4
AAA server	BroadHop Server used as the AAA server
DHCP server	CNR 6.1
Ericsson GE DSLAM	CXC 132 7440 V2.0.7.1
BroadHop Server	v4.1

Configuration Prerequisites

This section describes prerequisites that must be in place before deploying the ISG features described in this document in the following sections:

- Basic Configuration Requirements, page 10
- Configuration Passwords, page 10
- Vendor-Specific Attributes, page 10

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 router; 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 55.

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. See the RADIUS document titles in the "Related Documents" section on page 55 for help in configuring these attributes.

GE Deployment Models for Cisco IOS Software Release 12.2(31)SB2

Numerous configurations using various platforms and features were tested in the Cisco laboratories for Cisco IOS Software Release 12.2(31)SB2. The following network models are presented as representative of the features used most by Cisco customers:

Model 1: Authenticated IP Sessions over a .1Q Interface

This section is organized as follows:

- Call Flow for VRF Transfer, page 14

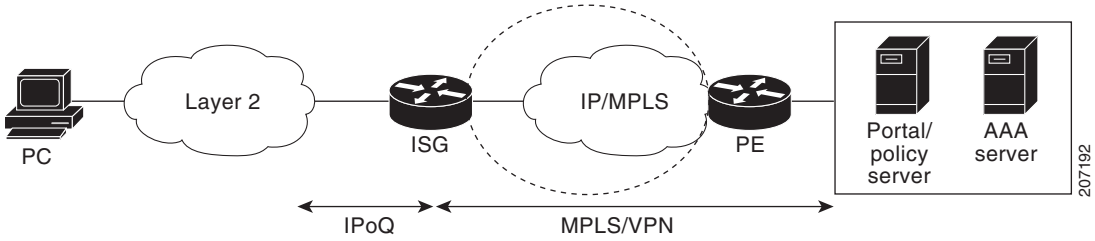
Description of Model 1

Model 1 transports IP sessions over an IEEE 802.1Q interface (IPoQ in Figure 3). The session is initiated based on new DHCP traffic. TAL is used to authorize the session based on the DHCP relay agent information option (option 82) and the user MAC address.

Network subscribers can be authorized by one of two methods: either they log in at the portal using a username and password or the network can admit them transparently based on their MAC address and DHCP option 82 information. The AAA server is configured to force subscribers to log in the first time the network is accessed. The next time subscribers access the network, however, they should be transparently authorized into the network. The AAA server will force subscribers to log in when they do not connect from their usual location and may force login if they have been inactive for some interval of time.

Topology for Model 1

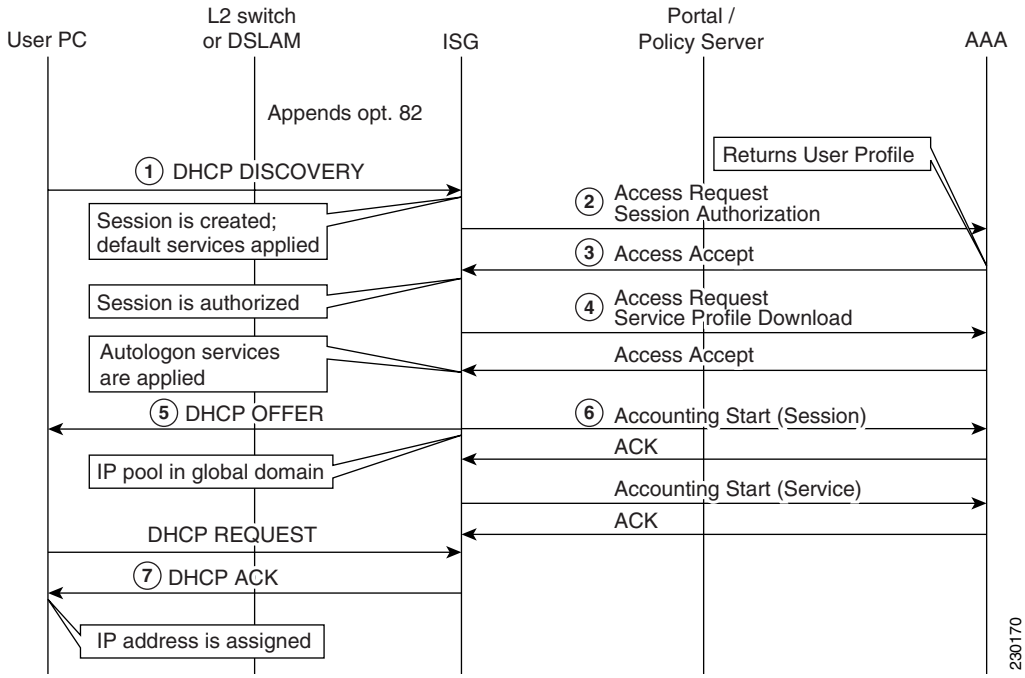
Figure 3 IP Sessions over .1Q Interface



Call Flow for Session Initiation

Figure 4 shows the call flows for the model 1 network. After the first login, the user will transparently be authorized for access to the network.

Figure 4 Session Initiation Call Flow for Model 1



Flow 1

- A DHCP DISCOVERY message is initiated by subscriber.
- An intermediate device (DSLAM or switch) populates DHCP Option-82 information to identify the subscriber's physical location.
- The ISG interface is configured to start a new session using DHCP control traffic.
- Upon starting, the policy starts default service and authorizes the session based on network identifiers.

Flow 2

- The ISG issues an Accept Request to authorize the session at AAA. The request includes DHCP option 82 information and the client's MAC address as a username.

Flow 3

- Upon successful identity verification, the AAA server responds with an Access Request, which includes the user profile and services to be activated. If the AAA server sends an Access Reject message, it means that user authorization failed; the L4 Redirect service will be activated and the subscriber will be forced to log into the account.

Flow 4

- Assuming that services to be activated for the session are not already cached on the ISG, the ISG sends an Access Request to the AAA server to download the service definition.

Flow 5

- TAL is successful, and the DHCP module sends a DHCP OFFER message to the DHCP client.

Flow 6

- Accounting Start Record begins for the parent session and service.

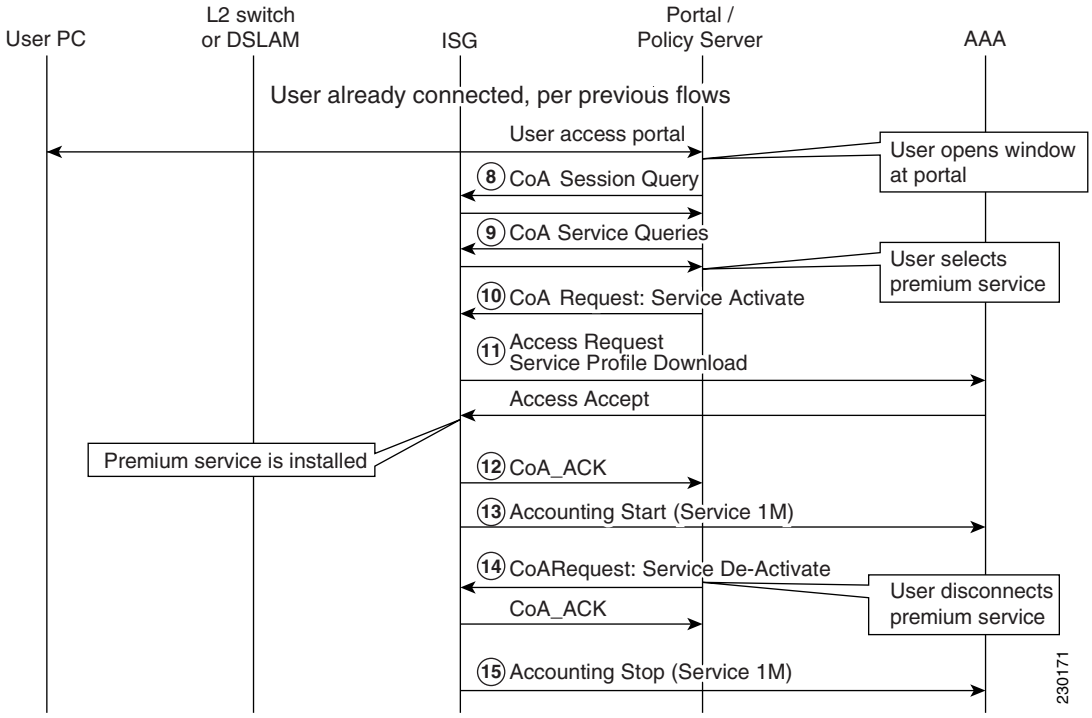
Flow 7

- The ISG assigns an IP address to the client.

Call Flow for Bandwidth Upgrade

Figure 5 depicts the logic that applies when PC users request an upgrade to the amount of bandwidth available for Internet access.

Figure 5 Bandwidth Upgrade Call Flow for Model 1



Flow 8

- The PC user opens a web browser and accesses a portal, causing the policy server to query the ISG about this session.

Flow 9

- The policy server sends a Service Status Query for all subscribed services.

Flow 10

- The PC user selects a new service from the portal. The policy server, in turn, generates a Service Activate request to the ISG.

Flow 11

- If service is not already cached on the ISG, the ISG retrieves the service definition from the AAA server.

Flow 12

- The ISG acknowledges the service activation and installs the service.

Flow 13

- The Accounting Start message is sent to signal the start of the new service.

Flow 14

- The PC user deactivates the service from the portal.

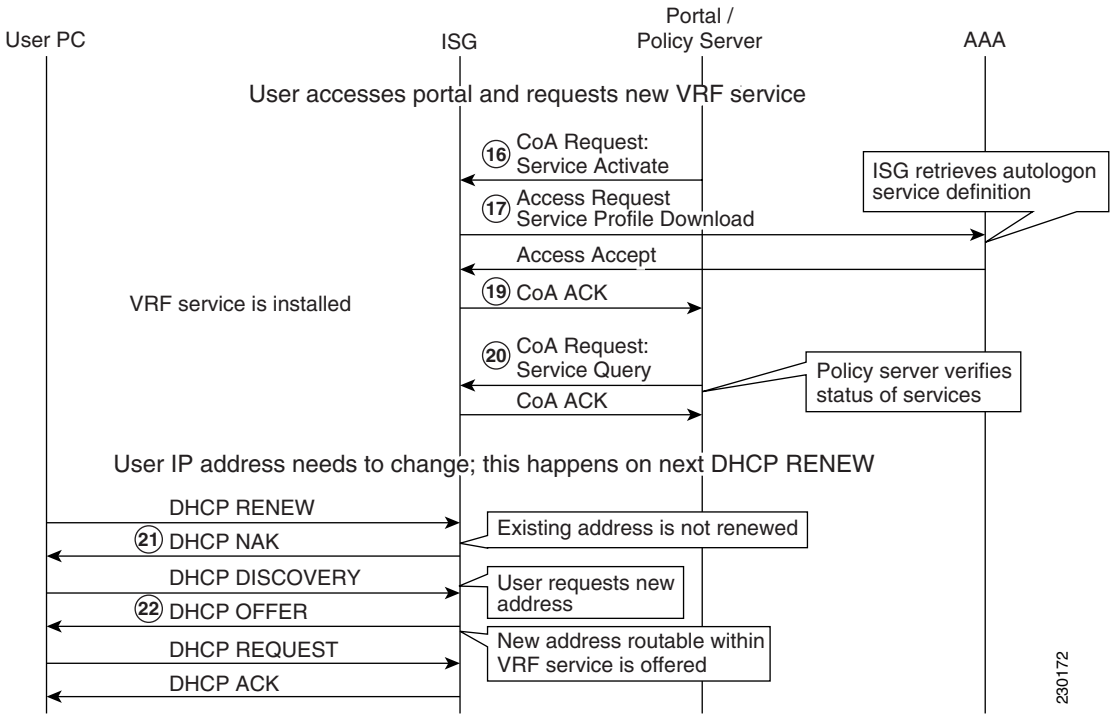
Flow 15:

- The Accounting Stop is recorded for the service.

Call Flow for VRF Transfer

Figure 6 depicts the logic that applies when the ISG activates new VRF service for the PC user.

Figure 6 VRF Transfer Call Flow for Model 1



Flow 16

- The policy server instructs the ISG to activate new VRF service for the PC user.

Flow 17

- The ISG retrieves the VRF service definition.

Flow 18

- The ISG acknowledges the CoA Service Activate request.

Flow 19

- The policy server verifies the status of the subscribed services via a service query message.

Flow 20

- After the DHCP lease expires, the client sends the DHCPREQUEST (RENEW) to the ISG (DHCP server) and gets the DHCP NAK back from the ISG, because the session is now in a VPN with a different class.

Flow 21 and 22

- Upon receiving the DHCPNAK from the ISG, the client sends a new DHCP DISCOVERY message and receives the DHCPOFFER message with the new IP address belonging to the VRF.

Model 2: Authenticated IP Sessions over a Q-in-Q Interface

This section is organized as follows:

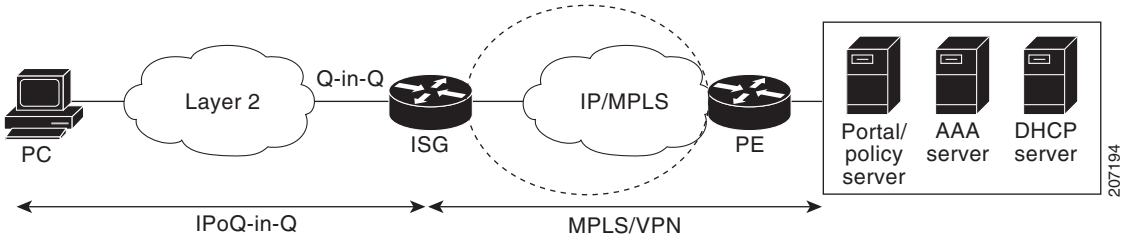
Description of Model 2

Model 2 transports authenticated IP sessions over a Q-in-Q interface. This model uses DHCP-initiated connections (IP sessions, Layer 2-connected). Each subscriber has a unique ID made up of an outer and inner VLAN ID. Session authentication information is based on the inner and outer VLAN tags (Q-in-Q VLANs) that are transported in the RADIUS NAS-Port attribute. User and service profiles are downloaded from the RADIUS server, and users are dynamically assigned to a VRF.

Topology for Model 2

Figure 7 shows the basic topology for network model 2.

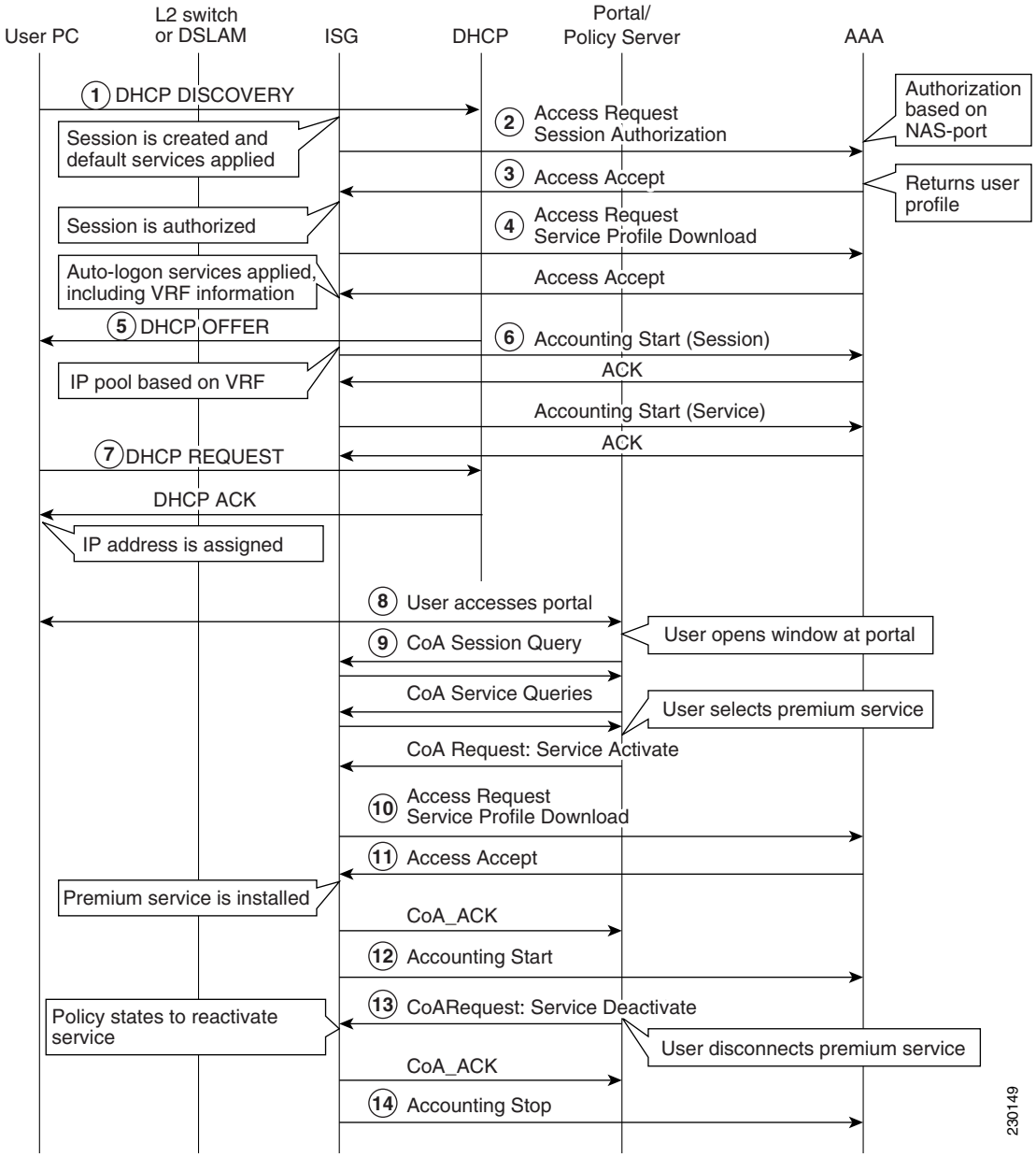
Figure 7 IP Sessions over Q-in-Q Interface



Call Flow for a DHCP-Initiated Session

Figure 8 shows the call flows for DHCP-initiated session using dynamic VPN selection.

Figure 8 DHCP-Initiated Session Call Flow for Model 2



The call flows in Figure 8 can be summarized as follows:

Flow 1

- A DHCP DISCOVERY message is initiated by the subscriber.
- Authorization is done based on the NAS-port ID.
- The ISG interface is configured to start a new session on DHCP control traffic.
- Upon starting, the policy uses the default service and authorizes the session based on network identifiers.

Flow 2

- The ISG issues an Access Request to authorize the session from the AAA server.

Flow 3

- Upon successful identification verification, the AAA server responds with an Access Accept, which includes the user profile and services to be activated.

Flow 4

- The ISG sends an Access Request to the AAA server, to download the service definition.
- The service profile is downloaded by an Access-Request for service.
- The server responds with the service definition for the primary VRF service, and the ISG applies the service to the session.
- The server responds with the service definition for Internet service, and the ISG applies the service to the session.

Flow 5

- TAL is successful; the DHCP module sends a DHCP OFFER message.

Flow 6

- Accounting starts a record for the parent session.

Flow 7

- The ISG assigns an IP address to the client.

Flow 8

- The PC user opens a web browser and accesses the portal, and this causes the policy server to query the ISG about this session.
- The ISG responds with the session's complete ID and service information.

Flow 9

- The service status query message is sent.
- The service status query reply is sent.

Flow 10

- The user selects a new service from the portal, and the portal generates a Service Activate request to the ISG.
- The policy is configured.
- The ISG retrieves the service definition from the AAA server.

Flow 11

The ISG acknowledges the service and activates and installs the service.

Flow 12

An accounting message signals the start of a new service.

Flow 13

The user deactivates the service from the portal.

Flow 14

An accounting Stop Service message is sent.

Refer to the "RFCs" section on page 56 for more information about DHCP and HTTP and call flow logic.

Model 3: Authenticated PPP Sessions over a Q-in-Q Interface

This section is organized as follows:

Description of Model 3

The Model 3 network contains a BRAS or ISG that terminates PPPoE sessions on Q-in-Q subinterfaces.

PPPoE subscribers are authorized to access Internet content and services based on an inner and outer VLAN tag. Information from this tag is transported in the NAS-port attribute. The user and service profiles are downloaded from RADIUS, and users are dynamically assigned to a VRF. The downloaded services can have a prepaid feature enabled.

If the authentication fails, users are redirected to the portal, where they are given options to log in or purchase services.

Once subscribers are authorized in the ISG, they can log into the portal and activate or deactivate services. The following services are defined for the users to select in model 3:

- SERVICE_403_SPECIFIC_PORT_L4R—This service is defined as a traffic class. The corresponding RADIUS profile and access lists are defined in the AAA server and in the ISG. Layer 4 Redirect is applied only to the subscriber traffic destined to TCP port 8080. All other subscriber traffic is handled normally. When a user selects this service from the portal server, it sends a CoA service logon to the ISG to activate the service.
- SERVICE_403_Upgraded_Internet—This service is defined as a traffic class. The corresponding RADIUS profile and access lists are defined in the AAA server and in the ISG. This service is defined with a higher bandwidth than SERVICE_403_INTERNET. Users select this service to receive a faster (upgraded) Internet access speed. The user selects this service from the portal server, and the portal server sends a CoA service logon to the ISG to activate the service.
- SERVICE_403_PL4R—This service is defined as a traffic class. The corresponding RADIUS profile and access lists are defined in the AAA server and in the ISG. This service performs a Layer 4 redirect on all subscriber traffic periodically using a defined time interval. When users select this service, they are redirected to a configured web server that displays advertisements and the like periodically as defined in the L4 Redirect configuration in the RADIUS profile. The user selects this service from the portal server, and the portal server sends a CoA service logon to the ISG to activate the service.
- CoA_403_QOS_UPDATE—This service is configured in the AAA server with VSAs to modify the Modular QoS CLI (MQC) policy on a parent session in the ISG. The user selects this service from the portal server, and the portal server sends a CoA Push to the ISG session with the VSAs to modify the MQC applied on the session.

- CoA_VRF_QOS_UPDATE—This service is configured in the AAA server with VSAs to modify the MQC policy and the VRF for a session in the ISG. The user selects this service from the portal server, and the portal server sends a CoA Push to the ISG session with the VSAs, to modify the MQC applied on the session and the VRF. When there is a VRF change, the ISG tears down down the IP Control Protocol (IPCP) layer of the subscriber's PPP session and renegotiates the session to provide a new IP address in the new VRF domain.
- SERVICE_403_L4R_TC—This service is defined as a traffic class. The corresponding RADIUS profile and access lists are defined in the AAA server and in the ISG. This service performs a Layer 4 redirect on all subscriber traffic. This service is applied to the subscriber session when a prepaid Volume and Time credit is exhausted. Once this service is applied, all subscriber traffic is redirected to a portal server, where the user is instructed to buy more credits to continue the service.
- Once the subscriber buys more credit, software in the ISG unapplies SERVICE_403_L4R_TC for the subscriber the next time the subscriber's quotas are reauthorized. Then user traffic is forwarded.
- SERVICE_403_INTERNET—This is the default automatic service for the subscribers. This service is automatically started by the ISG using information in the subscriber user profile. This service is defined as a traffic class and as a prepaid service. The corresponding RADIUS profile and access lists are defined in AAA, the billing server, and in the ISG.

Topology for Model 3

Figure 9 shows the network topology for model 3.

Figure 9 PPPoE Sessions over QinQ

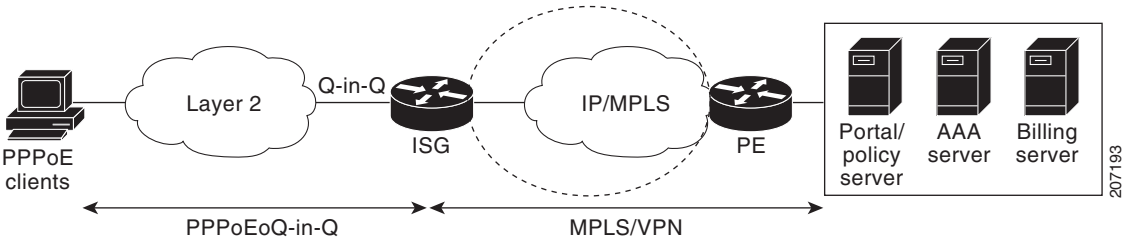


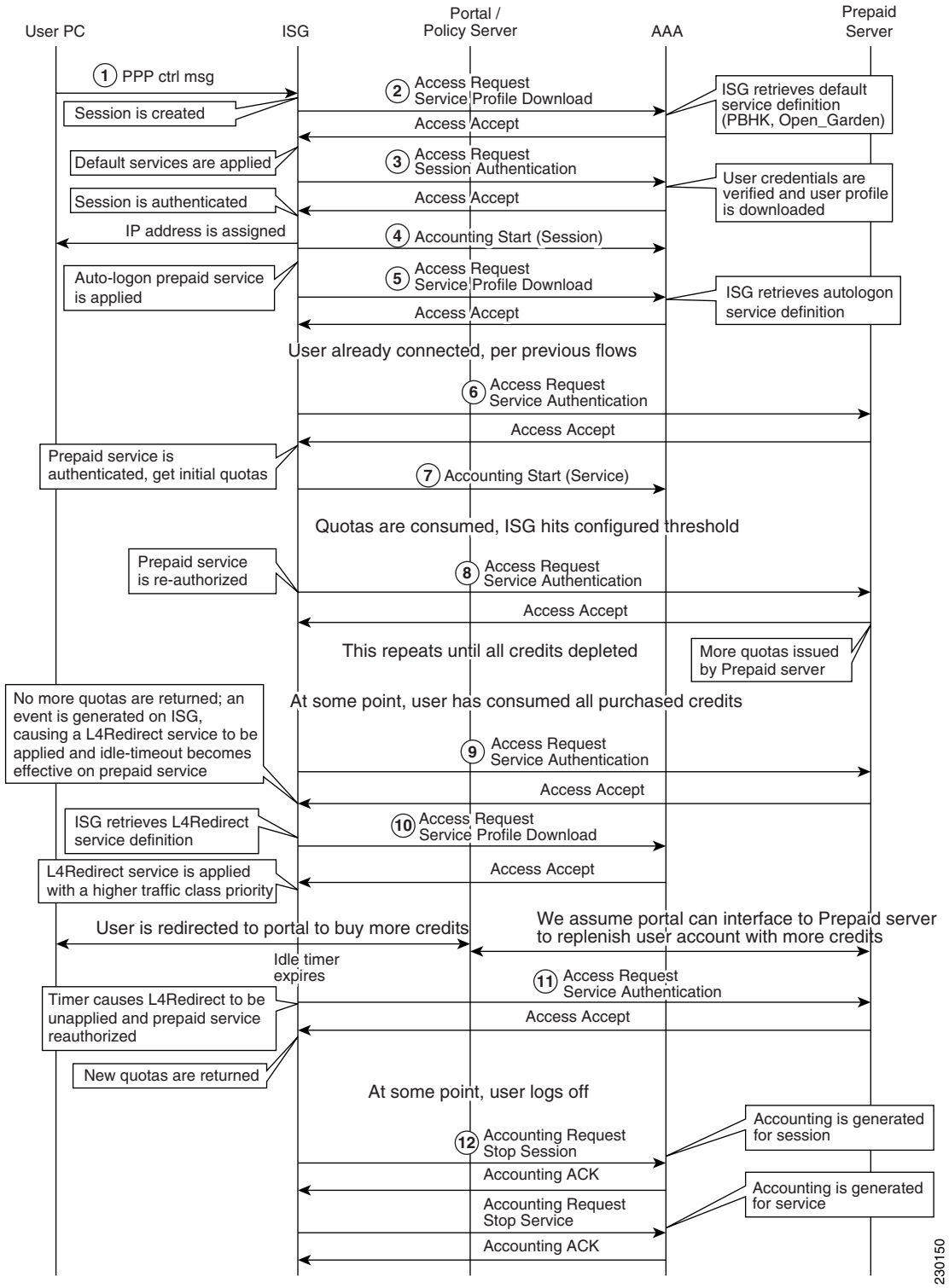
Figure 10 and Figure 11 show call flows for authenticated PPP sessions.

Call Flow for the Prepaid Feature

Figure 10 shows call flows for the following prepaid feature processes:

- PPP session creation
- Default service activation
- PPP authentication
- Prepaid autologon service activation
- Prepaid service reauthorization
- Activation of L4 Redirect service after expiration of prepaid credit
- Accounting for session and prepaid service

Figure 10 Call Flow for the Prepaid Feature



The call flows seen in Figure 10 can be described as follows:

Flow 1

- A PPPoE session is initiated by the user at the PC.
- The ISG starts a new session on PPP control traffic and executes the control policy configured on the virtual template interface.
- The ISG installs default services for this session

Flow 2

- The ISG retrieves the service definition.
- The ISG applies the service definition.

Flow 3

- The user is authenticated by the AAA server.
- The user profile contains a prepaid service that is to be auto started.

Flow 4

- Accounting Start record for the parent session.

Flow 5

- The ISG retrieves the service definition for autologon prepaid service.
- The ISG gets the prepaid service definition and installs it as a traffic-class service to the user's parent session.

Flow 6

- The ISG attempts to authorize the user for the requested service with the billing server.
- The user gets an initial quota of Internet access time/volume.

Flow 7

- Once the service is authorized, an Accounting Start record is sent to the AAA server using the accounting list configured under the prepaid configuration in the ISG.

Flow 8

- The user exhausts the initial quota of Internet access time/volume. In the ISG, a reauthorization request is sent immediately after the threshold value is reached.
- The user gets another incremental quota of time/volume until he reaches his quota limit.

Flow 9

- After so many minutes of continuous traffic from the user PC, the user exhausts the quota of time/volume available in the user's account. The ISG sends the reauthorization request after the limit is reached.
- The prepaid server replies with QV0/QTO and a greater than 0 second idle timeout, which triggers a credit-exhaust event in the ISG. The Layer 4 Redirect service is applied, in accordance with the configured control policy.

Flow 10

- The ISG retrieves the service definition for the redirect service.

- The redirect service definition is applied.

Flow 11

- When the idle timeout expires, the ISG automatically unapplies the L4 Redirect service and tries to reauthorize the prepaid service for more quota.
- Since the user's account has been has replenished, the process is restarted, and more time/volume is allocated.

Flow 12

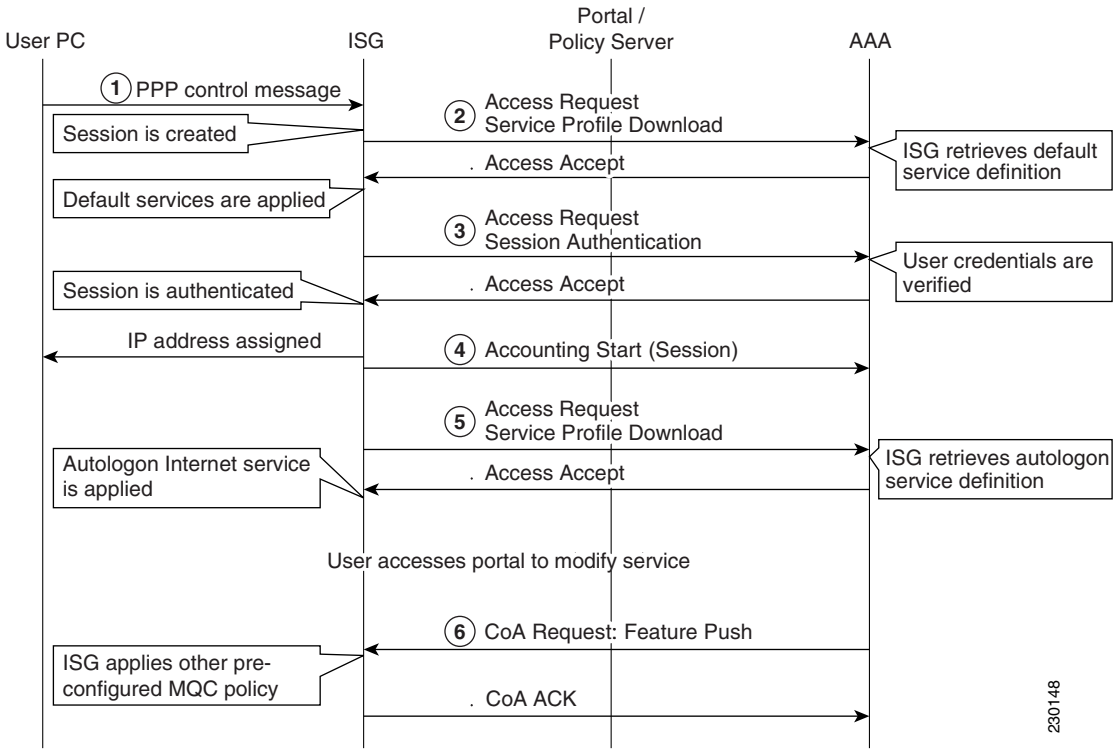
- The user logs off and accounting stop records are sent for parent and for service session.

Call Flow for a Dynamic MQC/QoS Change

The call flows illustrated in Figure 11 are valid only for a PPP session. Figure 11 illustrates call flows for the following dynamic MQC/QoS change processes:

- PPP session creation
- Default service activation
- PPP authentication
- Autologon service and MQC policy activation
- Dynamic modification of MQC policy

Figure 11 Call Flow for a Dynamic MQC/QoS Change



The call flows seen in Figure 11 can be described as follows:

Flow 1

- A PPPoE session is initiated from the PC. The ISG interface automatically starts a new session of PPP control traffic. Upon PPPoE initiation on a virtual template interface, the ISG executes the control policy map applied on the interfaces and installs default services.

Flow 2

- The ISG retrieves the service definition for default services.

Flow 3

- The user is authenticated by the AAA server.
- The user profile contains Internet service and MQC policies to be applied to the session.

Flow 4

- Accounting starts for the session.

Flow 5

- The ISG requests the service definition for auto-service.
- The ISG gets the service definition and installs it.

Flow 6

- The user accesses the portal and activates an upgraded policy from the policy server via CoA. The ISG applies the new QoS policy by the CoA push from the portal server.

Model 1 Configuration: Authenticated IP Sessions over a .1Q Interface

The following sections describe how to configure the model 1 network:

Prerequisites for Model 1

See the "Configuration Prerequisites" section on page 9 for network configurations that must be in place before you begin the tasks described in this section. Network administrators should also be familiar with the topics listed in the "Additional References" section on page 55. See the "Configuration Passwords" section on page 10 for information about configuration passwords. See the "Vendor-Specific Attributes" section on page 10 for information about vendor-specific attributes. Figure 3 shows the devices that are configured.

Configuring Subscriber Access for Model 1

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

```
interface GigabitEthernet1/0/0.400
 description TC406a using Local DHCP server
 encapsulation dot1Q 400
 ip address 10.1.10.1 255.255.255.0
 no snmp trap link-status
 service-policy type control RULE_406a
 ip subscriber l2-connected
  initiator dhcp class-aware
!
```

Configuring ISG to AAA Server Interfaces for Model 1

The following example shows a basic AAA configuration that includes connection to the RADIUS server:

```
aaa new-model
!
!
aaa group server radius SERVER_GROUP1
 server 172.17.10.9 auth-port 1812 acct-port 1813
!
aaa authentication login default none
aaa authentication login AUTHEN_LIST1 group SERVER_GROUP1
aaa authorization network default group SERVER_GROUP1
aaa authorization network AUTHOR_LIST1 group SERVER_GROUP1
aaa authorization subscriber-service default group SERVER_GROUP1
aaa accounting delay-start all
aaa accounting update periodic 5
aaa accounting network default start-stop group SERVER_GROUP1
aaa accounting network BH_ACCNT_LIST1 start-stop group SERVER_GROUP1
!
!
aaa session-id common
!
!
ip subnet-zero

radius-server attribute 44 include-in-access-req vrf default
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 32 include-in-access-req
radius-server attribute 32 include-in-accounting-req
radius-server attribute 55 include-in-acct-req
radius-server attribute 55 access-request include
```

```
radius-server attribute 25 access-request include
radius-server host 172.17.10.9 auth-port 1812 acct-port 1813 key aaacisco
radius-server vsa send authentication
!
radius-server vsa send accounting
!
ip radius source-interface Loopback0 vrf default
!

!
subscriber service password servicecisco
!
```

Configuring the User Profile on the AAA Server for Model 1

Following is the user profile used in network model 1, which is configured on the AAA server:

```
User-Name: tc406auser1
Idle-Timeout: 3000
CiscoAVPair: "subscriber:accounting-list=BH_ACCNT_LIST1"
ssg-account-info: "ABasic_Internet_Service"
ssg-account-info: "NSERVICE_406_BOD1Mc"
ssg-account-info: "NSERVICE_406_VPN_1001c"
```

Configuring Service Profiles on the AAA Server for Model 1

This section contains examples for the following service profiles:

- PBHK_SERVICE, page 26
- SERVICE_406_L4R, page 26
- Basic_Internet_Service, page 26
- SERVICE_406_BOD1Mc, page 27
- SERVICE_406_VPN_1001c, page 27

Note The following configurations are done on the AAA server, not the ISG router.

PBHK_SERVICE

```
Service Name: "PBHK_SERVICE"
CiscoAVPair: ip:portbundle=enable
```

SERVICE_406_L4R

```
Service Name: "SERVICE_406_L4R"
CiscoAVPair: ip:l4redirect=redirect list 199 to group REDIRECT_SERVER_GROUP1
```

Basic_Internet_Service

```
Service Name: "Basic_Internet_Service"
 SERVICE INFO: QD;512000;256000
 SERVICE INFO: QU;256000;128000
```

```
 CiscoAVPair: ip:traffic-class=input access-group name ACL_IN_INTERNET_406 priority 30
 CiscoAVPair: ip:traffic-class=out default drop
 CiscoAVPair: ip:traffic-class=in default drop
 CiscoAVPair: subscriber:accounting-list=BH_ACCNT_LIST1
 CiscoAVPair: ip:traffic-class=output access-group name ACL_OUT_INTERNET_406 priority 30
```

SERVICE_406_BOD1Mc

```
Service Name: "SERVICE_406_BOD1Mc"
 Idle-Timeout.value: 1800
 CiscoAVPair: subscriber:accounting-list=BH_ACCNT_LIST1
 SERVICE INFO: QU;512000;256000;D;1024000;512000
 CiscoAVPair: ip:traffic-class=input access-group name ACL_IN_BOD1M_406 priority 20
 CiscoAVPair: ip:traffic-class=out default drop
 CiscoAVPair: ip:traffic-class=output access-group name ACL_OUT_BOD1M_406 priority 20
 CiscoAVPair: ip:traffic-class=in default drop
```

SERVICE_406_VPN_1001c

```
Service Name: "SERVICE_406_VPN_1001c"
CiscoAVPair: ip:traffic-class=in default drop
 CiscoAVPair: ip:traffic-class=out default drop
 CiscoAVPair: ip:traffic-class=in access-group name ACL_IN_VPN_406_1001
 CiscoAVPair: ip:vrf-id=VPN_406_1001
 CiscoAVPair: subscriber:sg-service-type=primary
 CiscoAVPair: subscriber:accounting-list=BH_ACCNT_LIST1
 CiscoAVPair: ip:traffic-class=out access-group name ACL_OUT_VPN_406_1001
 CiscoAVPair: subscriber:classname=DHCP_CLASS_VPN_406_1001
```

Configuring Inbound and Outbound Access Lists for Model 1

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 portal and other management devices, to help prevent denial-of-service attacks.

```
ip access-list extended ACL_IN_BOD1M_406
 permit ip any any
ip access-list extended ACL_IN_INTERNET_406
 permit ip any any
ip access-list extended ACL_IN_VPN_406_1001
 permit ip any any
ip access-list extended ACL_OUT_BOD1M_406
 permit ip any any
ip access-list extended ACL_OUT_INTERNET_406
 permit ip any any
ip access-list extended ACL_OUT_VPN_406_1001
 permit ip any any
!
```

Configuring the Policy/Portal Server Interface for Model 1

The following examples show how to configure the policy/portal server interface for network model 1:

- Configuring the CoA Interface in the ISG for Model 1, page 28
- Configuring the Policy/Portal Server for CoA for Model 1, page 28

Configuring the CoA Interface in the ISG for Model 1

The following example shows how to configure the ISG with the CoA interface and define the policy and portal servers as clients:

```
aaa server radius dynamic-author
client 172.17.10.9
server-key cisco555
```

Configuring the Policy/Portal Server for CoA for Model 1

The following example defines the secret keys and port (by default, the ISG uses port 1700) to be used for CoA communication between ISG and the policy/portal server:

```
NAS-IP-Address = 10.200.1.1
Dyanmic-author Port number = 1700
Shared Key = "cisco555"
```

Configuring ISG to Support PBHK for Subscriber Access to the Portal for Model 1

When the PBHK feature is enabled, matching TCP packets from subscribers are mapped to the configured local IP address of the ISG gateway and a range of ports. The following configuration allows the policy/portal server to identify a subscriber session in the ISG to do dynamic updates using the CoA interface. It also specifies the loopback address in the ISG that will be used by the policy/portal server while communicating in CoA with ISG.

```
ip portbundle
match access-list 135
source Loopback0
!
interface GigabitEthernet5/0/0
ip address 10.1.50.1 255.255.255.0
ip portbundle outside
negotiation auto
mpls ip
cdp enable

access-list 135 permit ip any host 172.17.10.9
access-list 135 deny ip any any
!
interface Loopback 0
  ip address 10.200.1.1 255.255.255.0
```

The PBHK ID is comprised of the ISG IP used for portbundle and a dynamically assigned port number by ISG.

Configuring Layer 4 Redirect for Model 1

The following commands define redirect server groups in the ISG. These groups will be used by the Layer 4 Redirect services to redirect subscriber traffic.

```
redirect server-group REDIRECT_SERVER_GROUP1
server ip 172.17.10.9 port 8091
!
```

```
! L4 Redirect service access list
access-list 199 deny ip any host 172.17.10.9
access-list 199 permit tcp any any eq www
access-list 199 permit tcp any any eq 8080
access-list 199 permit tcp any any eq 8091
!
```

Configuring ISG Control Policies for Model 1

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:

Step 1 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.

Step 2 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.

Step 3 Apply the control policy map.

The following examples show how to configure control policies used in the model 1 network:

```
! 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 RULE_406a
 class type control IP_UNAUTH_COND event timed-policy-expiry
  1 service disconnect
!
 class type control always event session-start
  10 service-policy type service name PBHK_SERVICE
! TAL uses the remote-id + circuit-id + DHCP client source MAC address, which are
! extracted from the DHCP DISCOVERY message
  20 authorize aaa list AUTHOR_LIST1 password cisco123 identifier remote-id plus
circuit-id plus mac-address
  30 service-policy type service name SERVICE_406_L4R
  40 set-timer IP_UNAUTH_TIMER 5
! The session is disconnected if the session stays in the unauthenticated state for more
```

```
! than the time set (5 minutes) by IP_UNAUTH_TIMER
!
class type control always event session-restart
  10 service-policy type service name PBHK_SERVICE
  20 service-policy type service name SERVICE_406_L4R
  30 set-timer IP_UNAUTH_TIMER 5
!
 class type control always event account-logon
  10 authenticate aaa list AUTHEN_LIST1
  20 service-policy type service unapply name SERVICE_406_L4R
!
! After receiving the Account-Logoff message, the following commands allow the session to
! stay active for another 10 seconds
 class type control always event account-logoff
  10 service disconnect delay 10
!
```

Configuring the DHCP Server and DHCP Classes for Model 1

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 DHCP server and DHCP classes for Model 1 are configured as shown in the following example:

```
ip dhcp relay information policy keep
ip dhcp relay information trust-all
ip dhcp use vrf connected
ip dhcp excluded-address 10.1.11.1
ip dhcp excluded-address 10.1.10.1
!
ip dhcp pool TC406a_DHCP_POOL1
   network 10.1.10.0 255.255.255.0
   default-router 10.1.10.1
   lease 0 0 30
   class default
!
ip dhcp pool VPN_406_1001_POOL1
   vrf VPN_406_1001
   network 10.1.11.0 255.255.255.0
   default-router 10.1.11.1
   lease 0 0 30
   class DHCP_CLASS_VPN_406_1001
!
ip dhcp class default
!
ip dhcp class DHCP_CLASS_VPN_406_1001
```

Configuring the Multiservice Interface for VRF Transfer for Model 1

The following commands configure the multiservice interface:

```
interface multiservice1
 ip vrf forwarding VPN_406_1001
```

```
 ip address 10.1.11.1 255.255.255.0
 no keepalive
!
```

Configuring mBGP and VPNv4 for Model 1

The following example shows a typical configuration to enable routing in the model 1 network:

```
ip vrf VPN_406_1001
 rd 406:1001
 route-target export 406:1001
 route-target import 406:1001
!
ip vrf forwarding

router ospf 100
 router-id 10.200.1.1
 log-adjacency-changes
 network 10.1.50.1 0.0.0.0 area 100
 network 10.1.0.0 0.0.255.255 area 100
 network 10.200.1.1 0.0.0.0 area 100
!
router bgp 100
 no synchronization
 bgp router-id 10.200.1.1
 bgp log-neighbor-changes
 neighbor 10.200.1.9 remote-as 100
 neighbor 10.200.1.9 ebgp-multihop 2
 neighbor 10.200.1.9 update-source Loopback0
 no auto-summary
 !
 address-family vpnv4
  neighbor 10.200.1.9 activate
  neighbor 10.200.1.9 send-community both
 exit-address-family
 !
address-family ipv4 vrf VPN_406_1001
  redistribute connected
  redistribute static
  no auto-summary
  no synchronization
 exit-address-family
```

Configuring the Remote PE Side for Model 1

The PE is configured to assign subscribers to a VRF and to allow subscribers to access the portal. Following is an example:

```
ip vrf VPN_406_1001
 rd 406:1001
 route-target export 406:1001
 route-target import 406:1001
!
!
router bgp 100
 no synchronization
 bgp router-id 10.200.1.9
 bgp log-neighbor-changes
 neighbor SP100 peer-group
 neighbor SP100 remote-as 100
```

```
 neighbor SP100 ebgp-multihop 2
 neighbor SP100 update-source Loopback0
 neighbor 10.200.1.1 peer-group SP100
  no auto-summary
 !
 address-family vpnv4
 neighbor SP100 activate
 neighbor SP100 send-community extended
 neighbor 10.200.1.1 peer-group SP100
  exit-address-family
 !
 address-family ipv4 vrf VPN_406_1001
 redistribute connected
 redistribute static
 no auto-summary
 no synchronization
 exit-address-family
!
ip classless
ip route vrf VPN_406_1001 172.17.10.9 255.255.255.255 GigabitEthernet7/48 172.17.10.1
```

Model 2 Configuration: Authenticated IP Sessions over a Q-in-Q Interface

The following sections describe how to configure the model 2 network:

Prerequisites for Model 2

See the "Configuration Prerequisites" section on page 9 for network configurations that must be in place before you begin the tasks described in this section. Network administrators should also be familiar with the topics listed in the "Additional References" section on page 55. See the "Configuration Passwords" section on page 10 for information about configuration passwords. See the "Vendor-Specific Attributes" section on page 10 for information about vendor-specific attributes.

Figure 7 shows the devices that are configured.

Configuring Subscriber Access for Model 2

The following example configures an interface for IP subscriber sessions using DHCP with class-aware as the session initiator:

```
interface GigabitEthernet1/0/0.111
 encapsulation dot1Q 4020 second-dot1q 4043
 ip address 172.16.1.1 255.255.255.0
 no snmp trap link-status
 service-policy type control RULE-401a-1
 ip subscriber l2-connected
  initiator dhcp class-aware
!
```

Configuring ISG to AAA Server Interfaces for Model 2

The following example shows a basic AAA configuration that includes connection to the RADIUS server:

```
aaa new-model
!
!
aaa group server radius BH_SERVER_GROUP1
 server 172.16.5.45 auth-port 1812 acct-port 1813
!
aaa authentication login default none
aaa authentication login BH_WEB_LOGON group BH_SERVER_GROUP1
aaa authorization network default group BH_SERVER_GROUP1
aaa authorization subscriber-service default local group BH_SERVER_GROUP1
aaa accounting update periodic 5
aaa accounting network default start-stop group BH_SERVER_GROUP1
aaa accounting network BH_ACCNT_LIST start-stop group BH_SERVER_GROUP1
!
aaa session-id common
!
```

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 32 include-in-access-req
radius-server attribute 55 access-request include
radius-server attribute 25 access-request include
radius-server attribute 4 172.16.4.4
radius-server host 172.16.5.45 auth-port 1812 acct-port 1813 key cisco
radius-server vsa send accounting
radius-server vsa send authentication
!
ip radius source-interface Loopback0 vrf default
!
```

Configuring the User Profile on the AAA Server for for Model 2

Following are the commands configured on the AAA server to create the user profile for network model 2:

Subscriber Identities:

```
ISG authorized the subscriber using nas-port-id:
nas-port:172.16.4.4:1/0/0/4043.4020
```

Where:

- 172.16.4.4 is the IP NAS port of the ISG.
- 1/0/0 is the physical interface number of the access interface in the ISG.
- 4043 is the inner VLAN ID in QinQ.
- 4020 is the outer VLAN ID in QinQ.

Complete RADIUS User Profile:

In the following example, the ID is auto-generated by the ISG. The subscriber login identity is defined as 'tc401a1'.

```
nas-port:172.16.4.4:1/0/0/4043.4020 & tc401a1(second identity)
User-Name.value: tc401a1
CiscoAVPair: subscriber:accounting-list=BH_ACCNT_LIST
   Has the following selectable services:
     SERVICE_401_UPGRADED_INTERNET
     SERVICE_401_PERIODIC_L4R
   Has the following auto-started services:
     VPN_401_1001
     SERVICE_401_INTERNET
```

Configuring Service Profiles for Model 2

This section contains the following service profile examples:

L4_REDIRECT_SERVICE

```
CiscoAVPair: ip:l4redirect=redirect list 199 to group BROADHOP
```

PBHK_SERVICE

```
CiscoAVPair: ip:portbundle=enable
```

SERVICE_401_INTERNET

```
CiscoAVPair: ip:traffic-class=in access-group name ACL_IN_INTERNET_401 priority 10
CiscoAVPair: ip:traffic-class=out default drop
CiscoAVPair: ip:traffic-class=out access-group name ACL_OUT_INTERNET_401 priority 10
SERVICE INFO: QD;1024000;1024000
```

```
CiscoAVPair: subscriber:accounting-list=BH_ACCNT_LIST
SERVICE INFO: QU;512000;512000
CiscoAVPair: ip:traffic-class=in default drop
```

SERVICE_401_PERIODIC_L4R

```
CiscoAVPair: ip:traffic-class=out access-group name ACL_OUT_PL4R_401 priority 5
CiscoAVPair: subscriber:accounting-list=BH_ACCNT_LIST
CiscoAVPair: ip:l4redirect=redirect list 199 to group PERIODIC_L4R duration 60 frequency 120
CiscoAVPair: ip:traffic-class=out default drop
CiscoAVPair: ip:traffic-class=in default drop
SERVICE INFO: QD;1024000;1024000
CiscoAVPair: ip:traffic-class=in access-group name ACL_IN_PL4R_401 priority 5
SERVICE INFO: QU;512000;512000
```

SERVICE_401_UPGRADED_INTERNET

```
Idle-Timeout.value: 90
CiscoAVPair: ip:traffic-class=in default drop
CiscoAVPair: subscriber:accounting-list=BH_ACCNT_LIST
CiscoAVPair: ip:traffic-class=in access-group name ACL_IN_UPGRADED_INTERNET_401 priority 10
CiscoAVPair: ip:traffic-class=out default drop
CiscoAVPair: ip:traffic-class=out access-group name ACL_OUT_UPGRADED_INTERNET_401 priority 10
Session-Timeout.value: 300
SERVICE INFO: QU;1024000;1024000
SERVICE INFO: QD;2048000;2048000
```

VPN_401_1001

```
CiscoAVPair: subscriber:classname=VPN_401_1001
CiscoAVPair: subscriber:sg-service-type=primary
CiscoAVPair: ip:vrf-id=VPN_401_1001
```

CoA_Session_Update

```
Session-Timeout.value: 600
Idle-Timeout.value: 120
```

Configuring Inbound and Outbound Access Lists for Model 2

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 portal and other management devices, to help prevent denial-of-service attacks.

```
!
ip access-list extended ACL_IN_INTERNET_401
 deny   ip 10.0.0.0 0.255.255.255 any
 deny   ip 192.168.0.0 0.0.255.255 any
 permit ip any any
ip access-list extended ACL_IN_PL4R_401
 deny   ip 10.0.0.0 0.255.255.255 any
 deny   ip 192.168.0.0 0.0.255.255 any
 permit ip any any
ip access-list extended ACL_IN_UPGRADED_INTERNET_401
 deny   ip 10.0.0.0 0.255.255.255 any
```

```
 deny   ip 192.168.0.0 0.0.255.255 any
 permit ip any any
ip access-list extended ACL_OUT_INTERNET_401
 deny   ip 10.0.0.0 0.255.255.255 any
 deny   ip 192.168.0.0 0.0.255.255 any
 permit ip any any
ip access-list extended ACL_OUT_PL4R_401
 deny   ip 10.0.0.0 0.255.255.255 any
 deny   ip 192.168.0.0 0.0.255.255 any
 permit ip any any
ip access-list extended ACL_OUT_UPGRADED_INTERNET_401
 deny   ip 10.0.0.0 0.255.255.255 any
 deny   ip 192.168.0.0 0.0.255.255 any
 permit ip any any
```

Configuring the Policy/Portal Server Interface for Model 2

The following examples show how to configure the policy/portal server interface for network model 2:

- Configuring the CoA Interface in the ISG for Model 2, page 36
- Configuring the Policy/Portal Server for CoA for Model 2, page 36
- Configuring ISG to Support PortBundle Host Key for Subscriber Access to the Portal for Model 2, page 36

Configuring the CoA Interface in the ISG for Model 2

The following example shows how to configure ISG with CoA interface and define the policy and portal servers as clients. It also specifies the loopback address in the ISG that will be used by the policy/portal server while communicating in CoA with ISG.

```
aaa server radius dynamic-author
 client 172.16.5.45
 server-key cisco
!
interface Loopback0
 ip address 172.16.4.4 255.255.255.255
```

Configuring the Policy/Portal Server for CoA for Model 2

The following example defines the secret keys and port (by default, the ISG uses port 1700) to be used for CoA communication between ISG and the policy/portal servers. Configure the following information on the policy/portal server:

```
NAS-IP-Address = 172.16.4.4
Dyanmic-author Port number = 1700
Shared Key = "cisco"
```

Configuring ISG to Support PortBundle Host Key for Subscriber Access to the Portal for Model 2

When the Port-Bundle Host Key (PBHK) feature is enabled, matching TCP packets from subscribers are mapped to the configured local IP address of the ISG gateway and a range of ports. The mapping allows the policy/portal server to identify a subscriber session in the ISG to do dynamic updates using the CoA interface. The PBHK ID consists of the ISG IP used for the port bundle and a dynamically assigned port number by ISG. The key **ip portbundle** command in this configuration is highlighted in bold text for purpose of example.

```
ip portbundle
match access-list 198
source Loopback0
!
interface GigabitEthernet5/0/0
 description P to c10k link 1 port GE 6/1
 mtu 1508
 ip address 172.16.3.4 255.255.255.0
ip portbundle outside
negotiation auto
mpls label protocol ldp
mpls ip
cdp enable
!
! The PBHK feature is applied only to traffic destined to the portal IP 172.16.5.45
!
access-list 198 permit ip any host 172.16.5.45
access-list 198 deny   ip any any
```

Configuring Layer 4 Redirect for Model 2

The following commands define redirect server groups in the ISG. These groups will be used by the Layer 4 Redirect services to redirect subscriber traffic.

```
redirect server-group PORTAL
server ip 172.16.5.45 port 8091
!
redirect server-group PERIODIC_L4R
server ip 172.16.5.57 port 80
!
! access-List 199 is used by L4_REDIRECT_SERVICE and SERVICE 401 Periodic L4 Redirect.
!
access-list 199 deny   tcp any host 172.16.5.45 eq www
access-list 199 deny   tcp any host 172.16.5.45 eq 8080
access-list 199 deny   tcp any host 172.16.5.57 eq www
access-list 199 permit tcp any any eq www
```

Configuring ISG Control Policies for Model 2

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:

Step 1 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.

Step 2 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.

Step 3 Apply the control policy map.

The following example shows how to configure subscriber rule RULE-401a-1 for IP TAL sessions using NAS-port as the identifier, and then how to apply common services that are configured remotely on the AAA server, such as PBHK_SERVICE, INTERNET, and so on. The L4_REDIRECT_SERVICE 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
!
class-map type control match-all SERVICE_401_PERIODIC_L4_REDIRECT
 match service-name SERVICE_401_PERIODIC_L4R
!
class-map type control match-all SERVICE_401_UPGRADED_INTERNET
 match service-name SERVICE-401_UPGRADED_INTERNET
!

!
policy-map type control RULE-401a-1
 class type control IP_UNAUTH_COND event timed-policy-expiry
  1 service disconnect
 !
 class type control SERVICE_401_UPGRADED_INTERNET event service-stop
  1 service-policy type service unapply identifier service-name
  2 service-policy type service name SERVICE-401-INTERNET
 !
 class type control SERVICE_401_UPGRADED_INTERNET event service-start
  1 service-policy type service unapply name SERVICE-401-INTERNET
  2 service-policy type service unapply name SERVICE_401_PERIODIC_L4R
  3 service-policy type service identifier service-name
 !
 class type control always event session-start
  1 service-policy type service name PBHK_SERVICE
  2 authorize aaa password lab123 identifier nas-port
  3 service-policy type service name L4_REDIRECT_SERVICE
  4 set-timer IP_UNAUTH_TIMER 5
! The session is disconnected if it stays in unauthenticated state for more than the
! time set by IP_UNAUTH_TIMER (5 minutes)
!
 class type control always event account-logon
  1 authenticate aaa list BH_WEB_LOGON
  2 service-policy type service unapply name L4_REDIRECT_SERVICE
!
class type control always event account-logoff
  1 service disconnect delay 5
!
 class type control always event session-restart
  1 service-policy type service name PBHK_SERVICE
  3 service-policy type service name L4_REDIRECT_SERVICE
  4 set-timer IP_UNAUTH_TIMER 5
```

Configuring the DHCP Server and DHCP Classes for Model 2

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. 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.

The **ip dhcp relay information option** command supports the relay agent functionality. The relay agent will automatically add the VPN information 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, whereby the network administrator assigns an IP address to a client, and DHCP is used simply to convey the assigned address to the client.

The model 2 deployment uses DHCP dynamic allocation for a limited period of time, 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 10
!
ip dhcp pool VPN_401_1001
   vrf VPN_401_1001
   relay source 172.16.6.0 255.255.255.0
   relay destination global 172.16.5.56
   class VPN_401_1001
!
ip dhcp pool ISP1
   network 172.16.1.0 255.255.255.0
   default-router 172.16.1.1
   lease 0 0 3
   class default
!
!
ip dhcp class VPN_401_1001
!
ip dhcp class default
!
```

Configuring the Multiservice Interface for VRF Termination for Model 2

The following commands configure the multiservice interface:

```
interface multiservice1
 ip vrf forwarding VPN_401_1001
 ip address 172.16.6.1 255.255.255.0
```

```
 no keepalive
```

Configuring mBGP and VPNv4 for Model 2

The following example shows a typical configuration to enable VRF forwarding and IP routing in the model 2 network:

```
ip vrf VPN_401_1001
 rd 401:1001
 route-target export 401:1001
 route-target import 401:1001
!
router ospf 100
 router-id 172.16.4.4
 log-adjacency-changes
 redistribute connected
 network 172.16.1.0 0.0.0.255 area 10
 network 172.16.4.4 0.0.0.0 area 10
 network 172.16.3.0 0.0.255.255 area 10
!
router bgp 100
 no synchronization
 bgp router-id 172.16.4.4
 bgp log-neighbor-changes
 neighbor 172.16.4.9 remote-as 100
 neighbor 172.16.4.9 update-source Loopback0
 no auto-summary
!
address-family vpnv4
  neighbor 172.16.4.9 activate
  neighbor 172.16.4.9 send-community both
 exit-address-family
!
address-family ipv4 vrf VPN_401_1001
  redistribute connected
  redistribute static
  no auto-summary
  no synchronization
 exit-address-family
!
```

Configuring the Remote PE Side for Model 2

The PE is configured to assign subscribers to a VRF and to allow subscribers to access the portal. Following is an example:

```
ip vrf VPN_401_1001
 rd 401:1001
 route-target export 401:1001
 route-target import 401:1001
!

router bgp 100
 no synchronization
 bgp router-id 172.16.4.9
 bgp log-neighbor-changes
 neighbor 172.16.4.4 remote-as 100
 neighbor 172.16.4.4 update-source Loopback0
 no auto-summary
!
```

```
 address-family vpnv4
 neighbor 172.16.4.4 activate
 neighbor 172.16.4.4 send-community both
 exit-address-family
!
 address-family ipv4 vrf VPN_401_1001
 redistribute connected
 redistribute static
 no auto-summary
 no synchronization
 exit-address-family
!
```

Model 3 Configuration: Authenticated PPP Sessions over a Q-in-Q Interface

The following sections describe how to configure the model 3 network:

Prerequisites for Model 3

See the "Configuration Prerequisites" section on page 9 for network configurations that must be in place before you begin the tasks described in this section. Network administrators should also be familiar with the topics listed in the "Additional References" section on page 55. See the "Configuration Passwords" section on page 10 for information about configuration passwords. See the "Vendor-Specific Attributes" section on page 10 for information about vendor-specific attributes. Figure 9 shows the devices that are configured.

Configuring Subscriber Access for Model 3

The following example configures a PPPoE session:

```
bba-group pppoe PPPOE-GROUP4031
```

```
virtual-template 201
!
interface GigabitEthernet1/0/0.4037
 encapsulation dot1Q 4020 second-dot1q 4037
 pppoe enable group PPPOE-GROUP4031
 no snmp trap link-status
!
interface Virtual-Template201
 no ip address
 peer default ip address pool PPPoE_POOL_403_1
 no keepalive
 service-policy type control RULE-403a-1

ip local pool PPPoE_POOL_403_1 172.16.2.2 172.16.2.254
```

Configuring ISG to AAA Server Interfaces for Model 3

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

```
!
aaa new-model
!
!
! AAA Server Configuration
!
aaa group server radius BH-SERVER
 server 172.16.5.45 auth-port 1812 acct-port 1813
!
! Prepaid Billing and Accounting Server
!
aaa group server radius BILLING-SERVER
 server 172.16.13.2 auth-port 1812 acct-port 1813
!
aaa authentication login default none
aaa authentication login BH_WEB_LOGON group BH-SERVER
aaa authentication ppp default group BH-SERVER
aaa authentication ppp BH-PPP group BH-SERVER
aaa authorization network default group BH-SERVER
aaa authorization network PREPAID_AUTHOR_LIST group BILLING-SERVER
aaa authorization subscriber-service default local group BH-SERVER
aaa accounting update periodic 15
aaa accounting network default start-stop group BH-SERVER
aaa accounting network BH_ACCNT_LIST start-stop group BH-SERVER
aaa accounting network PREPAID_ACCOUNT_LIST start-stop group BILLING-SERVER
```

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 vrf default
radius-server attribute 8 include-in-access-req
radius-server attribute 55 access-request include
radius-server attribute 25 access-request include
radius-server attribute nas-port format d
radius-server attribute 4 172.16.4.13
radius-server host 172.16.13.2 auth-port 1812 acct-port 1813 key cisco
radius-server host 172.16.5.45 auth-port 1812 acct-port 1813 key cisco
radius-server vsa send accounting
radius-server vsa send authentication
```

Configuring the User Profile for Model 3

```
SUBSCRIBER IDENTITIES:
ISG authorizes the subscriber using nas-port-id :
nas-port:172.16.4.13:1/0/0/4020.4037
```

where

- 172.16.4.13 is the NAS-IP address of the ISG.
- 1/0/0 is the physical interface ID of the access interface in the ISG.
- 4020 is the outer VLAN ID in Q-in-Q.
- 4037 is the inner VLAN ID in Q-in-Q.

The ID is auto-generated by the ISG. It requires the **radius-server attribute nas-port format d** command to be configured in the ISG.

The subscriber login or secondary identity is defined as ‘tc403a1’.

User Radius Profile

```
ip:ip-unnumbered=loopback201
User-Name: nas-port:172.16.4.13:1/0/0/4020.4037
subscriber:accounting-list=BH_ACCNT_LIST
ip:outacl=ACL_OUT_PARENT_403
Idle-Timeout: 600
ip:inacl=ACL_IN_PARENT_403
ip:vrf-id=VPN_403_1001
```

Configuring Service Profiles for Model 3

This section contains examples for the following service profiles:

L4_REDIRECT_SERVICE

```
CiscoAVPair: ip:l4redirect=redirect list 199 to group BROADHOP
```

PBHK_SERVICE

```
CiscoAVPair: ip:portbundle=enable
```

SERVICE_403_SPECIFIC_PORT_L4R

```
CiscoAVPair: ip:traffic-class=out default drop
CiscoAVPair: ip:traffic-class=in default drop
CiscoAVPair: ip:traffic-class=out access-group name ACL_OUT_SPECIFIC_PORT_L4R_403 priority 7
CiscoAVPair: ip:l4redirect=redirect list 197 to group SPECIFIC_PORT_L4R
CiscoAVPair: ip:traffic-class=in access-group name ACL_IN_SPECIFIC_PORT_L4R_403 priority 7
```

SERVICE_403_L4R_TC

```
CiscoAVPair: ip:traffic-class=in access-group name ACL_IN_L4R_TC_403 priority 5
CiscoAVPair: ip:l4redirect=redirect to group BROADHOP
CiscoAVPair: ip:traffic-class=out access-group name ACL_OUT_L4R_TC_403 priority 5
```

CoA_403_QOS_UPDATE

```
CiscoAVPair: ip:sub-qos-policy-out=QOS_POLICY_OUT_512_PARENT_403
CiscoAVPair: ip:sub-qos-policy-in=QOS_POLICY_IN_512_PARENT_403
```

CoA_VRF_QOS_UPDATE

```
CiscoAVPair: ip:ip-unnumbered=loopback201
CiscoAVPair: ip:vrf-id=VPN_403_3002
CiscoAVPair: ip:addr-pool=PPPoE_POOL_403_2
CiscoAVPair: ip:inacl=ACL_IN_PARENT_403
CiscoAVPair: ip:inacl=ACL_IN_PARENT_403
CiscoAVPair: ip:sub-qos-policy-out=QOS_POLICY_OUT_512_PARENT_403
CiscoAVPair: ip:sub-qos-policy-in=QOS_POLICY_IN_512_PARENT_403
```

SERVICE_403_INTERNET

```
CiscoAVPair: ip:traffic-class=in access-group name ACL_IN_INTERNET_403 priority 10
CiscoAVPair: ip:traffic-class=in default drop
SERVICE INFO: QD;1024000;1024000
SERVICE INFO: QU;512000;512000
CiscoAVPair: ip:traffic-class=out access-group name ACL_OUT_INTERNET_403 priority 10
CiscoAVPair: prepaid-config=PREPAID_RSIM
CiscoAVPair: subscriber:accounting-list=BH_ACCNT_LIST
CiscoAVPair: ip:traffic-class=out default drop
```

SERVICE_403_Upgraded_Internet

```
CiscoAVPair: ip:traffic-class=in default drop
SERVICE INFO: QD;2048000;2048000
CiscoAVPair: ip:traffic-class=in access-group name ACL_IN_UPGRADED_INTERNET_403 priority 6
CiscoAVPair: ip:traffic-class=out default drop
CiscoAVPair: ip:traffic-class=out access-group name ACL_OUT_UPGRADED_INTERNET_403 priority 6
SERVICE INFO: QU;1024000;1024000
CiscoAVPair: subscriber:accounting-list=BH_ACCNT_LIST
```

SERVICE_403_PL4R: Periodic Layer 4 Redirect Service

```
CiscoAVPair: ip:traffic-class=in access-group name ACL_IN_PL4R_403 priority 5
CiscoAVPair: ip:traffic-class=out default drop
CiscoAVPair: subscriber:accounting-list=BH_ACCNT_LIST
```

```
CiscoAVPair: ip:l4redirect=redirect list 199 to group PERIODIC_L4R duration 60 frequency 120
CiscoAVPair: ip:traffic-class=out access-group name ACL_OUT_PL4R_403 priority 5
CiscoAVPair: ip:traffic-class=in default drop
CiscoAVPair: ip:traffic-class=in access-group name ACL_IN_L4R_TC_403 priority 5
CiscoAVPair: ip:l4redirect=redirect to group BROADHOP
CiscoAVPair: ip:traffic-class=out access-group name ACL_OUT_L4R_TC_403 priority 5
```

Configuring Inbound and Outbound Access Lists for Model 3

Basic access lists are configured to govern subscribers' Internet access. In the following example, the access lists are referenced in the AAA subscriber, and service profiles govern incoming and outgoing Internet traffic.

```
ip access-list extended ACL_IN_INTERNET_403
 deny   ip 10.0.0.0 0.255.255.255 any
 deny   ip 192.168.0.0 0.0.255.255 any
 permit ip any any
ip access-list extended ACL_IN_L4R_TC_403
 deny   ip any host 172.16.5.45
 permit tcp any any eq www
 permit tcp any any eq 8080
 deny   ip any any
ip access-list extended ACL_IN_OPEN_TC_403
 permit ip any host 172.16.5.45
 permit ip any host 172.16.5.49
 permit ip any host 172.16.5.57
 deny   ip any any
ip access-list extended ACL_IN_PARENT_403
 permit ip any any
ip access-list extended ACL_IN_PL4R_403
 deny   ip 10.0.0.0 0.255.255.255 any
 deny   ip 192.168.0.0 0.0.255.255 any
 permit ip any any
ip access-list extended ACL_IN_SPECIFIC_PORT_L4R_403
 deny   ip 10.0.0.0 0.255.255.255 any
 deny   ip 192.168.0.0 0.0.255.255 any
 permit tcp any host 172.16.5.45 eq 443
 permit tcp any host 172.16.5.45 eq www
 permit tcp any host 172.16.5.45 eq 8080
 permit tcp any host 172.16.5.49 eq 443
 permit tcp any host 172.16.5.49 eq www
 permit tcp any host 172.16.5.49 eq 8080
 permit tcp any host 172.16.5.57 eq www
 permit ip any host 172.16.101.1
 permit tcp any any eq 8080
 deny   ip any any
ip access-list extended ACL_IN_UPGRADED_INTERNET_403
 deny   ip 10.0.0.0 0.255.255.255 any
 deny   ip 192.168.0.0 0.0.255.255 any
 permit ip any host 5.5.201.1
 deny   ip any any
ip access-list extended ACL_OUT_INTERNET_403
 deny   ip 10.0.0.0 0.255.255.255 any
 deny   ip 192.168.0.0 0.0.255.255 any
 permit ip any any
ip access-list extended ACL_OUT_L4R_TC_403
 permit ip any any
ip access-list extended ACL_OUT_OPEN_TC_403
 permit ip host 172.16.5.45 any
 permit ip host 172.16.5.49 any
 permit ip host 172.16.5.57 any
```

```
 deny   ip any any
ip access-list extended ACL_OUT_PARENT_403
 permit ip any any
ip access-list extended ACL_OUT_PL4R_403
 deny   ip 10.0.0.0 0.255.255.255 any
 deny   ip 192.168.0.0 0.0.255.255 any
 permit ip any any
ip access-list extended ACL_OUT_SPECIFIC_PORT_L4R_403
 deny   ip 10.0.0.0 0.255.255.255 any
 deny   ip 192.168.0.0 0.0.255.255 any
 permit ip any any
ip access-list extended ACL_OUT_UPGRADED_INTERNET_403
 deny   ip 10.0.0.0 0.255.255.255 any
 deny   ip 192.168.0.0 0.0.255.255 any
 permit ip any any
```

Configuring the Policy/Portal Server Interface for Model 3

This section provides the following configuration examples:

- Configuring the CoA Interface in the ISG in Model 3, page 46
- Configuring the Policy/Portal Server for CoA in Model 3, page 46
- Configuring ISG to Support Port-Bundle Host Key for Subscriber Access to the Portal in Model 3, page 46

Configuring the CoA Interface in the ISG in Model 3

The following example defines the secret keys to be used for CoA communication between ISG and the policy/portal servers. The loopback address is in the ISG, which will be used by the policy/portal server while communicating in CoA with ISG.

```
aaa server radius dynamic-author
 client 172.16.5.45
 server-key cisco

interface Loopback0
 ip address 172.16.4.13 255.255.255.255
```

Configuring the Policy/Portal Server for CoA in Model 3

The following commands configure the policy/portal servers as clients:

```
NAS-IP-Address = 172.16.4.13
Dynamic-author Port number = 1700
Shared Key = "cisco"
```

Configuring ISG to Support Port-Bundle Host Key for Subscriber Access to the Portal in Model 3

When the Port-Bundle Host Key (PBHK) feature is enabled, matching TCP packets from subscribers are mapped to the configured local IP address of the ISG gateway and a range of ports. The mapping allows the policy/portal server to identify a subscriber session in ISG to do dynamic updates using the CoA interface. The PBHK ID consists of the ISG IP address used for the portbundle and a dynamically assigned port number by the ISG.

See "Configuring ISG Port-Bundle Host Key" in the *Cisco IOS Intelligent Services Gateway Configuration Guide* for more information.

```
ip portbundle
match access-list 198
source Loopback0

interface GigabitEthernet5/0/0
mtu 1508
ip address 172.16.9.13 255.255.255.0
ip portbundle outside
negotiation auto
mpls label protocol ldp
mpls ip
cdp enable
!
! PBHK feature applied only to traffic destined to the portal IP 172.16.5.45
!
access-list 198 permit ip any host 172.16.5.45
access-list 198 deny   ip any any
```

Configuring the Prepaid Server for Model 3

Enable the prepaid feature in the ISG by defining the following:

- A prepaid list with the desired thresholds for volume and time monitors.
- The secret key that the ISG should use to communicate with the billing server.
- An authorization and accounting list to be used by the ISG prepaid feature engine.

For detailed information about ISG prepaid billing feature, see "Configuring ISG Support for Prepaid Billing" in the *Cisco IOS Intelligent Services Gateway Configuration Guide*.

Following are the commands to enable the prepaid server feature for model 3:

```
subscriber feature prepaid PREPAID_RSIM
 threshold time 120 seconds
 threshold volume 20000 bytes
 interim-interval 15 minutes
 method-list author PREPAID_AUTHOR_LIST
 method-list accounting PREPAID_ACCOUNT_LIST
 password cisco
```

Configuring Layer 4 Redirect for Model 3

Define redirect server groups in ISG. These groups will be used by the Layer 4 Redirect services to redirect subscriber traffic.

```
redirect server-group BROADHOP
server ip 172.16.5.45 port 8091
!
redirect server-group PERIODIC_L4R
server ip 172.16.5.57 port 80
!
redirect server-group SPECIFIC_PORT_L4R
server ip 172.16.5.57 port 80

!
! ACL 197 is used by SERVICE_403_SPECIFIC_PORT_L4R
access-list 197 deny   tcp any host 172.16.5.45 eq www
access-list 197 deny   tcp any host 172.16.5.45 eq 8080
access-list 197 permit tcp any any eq 8080
!
```

```
! ACL 199 is used by SERVICE_403_PL4R
access-list 199 deny   tcp any host 172.16.5.45 eq www
access-list 199 deny   tcp any host 172.16.5.45 eq 8080
access-list 199 permit tcp any any eq www
```

Configuring ISG Control Policies for Model 3

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:

Step 1 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.

Step 2 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.

Step 3 Apply the control policy map.

The following example shows how to configure subscriber rule RULE-403a-1 for IP TAL sessions using NAS-port as the identifier, 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 SERVICE_403_SPECIFIC_PORT_L4R
 match service-name SERVICE_403_SPECIFIC_PORT_L4R
!
class-map type control match-all SERVICE_403_INTERNET
 match service-name SERVICE_403_INTERNET
!
class-map type control match-all SERVICE_403_PL4R
 match service-name SERVICE_403_PL4R
!
class-map type control match-all IP-UNAUTH-COND
 match timer IP-UNAUTH-TIMER
 match authen-status unauthenticated
!
!
policy-map type control RULE-403a-1
 class type control IP-UNAUTH-COND event timed-policy-expiry
  1 service disconnect
```

```
 !
 class type control SERVICE_403_PL4R event service-start
  1 service-policy type service unapply name SERVICE_403_INTERNET
  2 service-policy type service unapply name SERVICE_403_L4R_TC
  3 service-policy type service unapply name SERVICE_403_OPEN_GARDEN
  4 service-policy type service identifier service-name
 !
 class type control SERVICE_403_PL4R event service-stop
  1 service-policy type service unapply identifier service-name
  2 service-policy type service name SERVICE_403_INTERNET
  3 service-policy type service name SERVICE_403_OPEN_GARDEN
 !
 class type control SERVICE_403_SPECIFIC_PORT_L4R event service-start
  1 service-policy type service unapply name SERVICE_403_INTERNET
  2 service-policy type service unapply name SERVICE_403_L4R_TC
  3 service-policy type service unapply name SERVICE_403_OPEN_GARDEN
  4 service-policy type service identifier service-name
 !
 class type control SERVICE_403_SPECIFIC_PORT_L4R event service-stop
  1 service-policy type service unapply identifier service-name
  2 service-policy type service name SERVICE_403_INTERNET
  3 service-policy type service name SERVICE_403_OPEN_GARDEN
 !
 class type control always event session-start
  1 service-policy type service name PBHK_SERVICE
  2 service-policy type service name SERVICE_403_OPEN_GARDEN
  3 authorize aaa password lab123 identifier nas-port
  4 service-policy type service name L4_REDIRECT_SERVICE
  6 set-timer IP_UNAUTH_TIMER 5
 !
 class type control always event account-logon
  1 authenticate aaa list BH_WEB_LOGON
  2 service-policy type service unapply name L4_REDIRECT_SERVICE
 !
 class type control always event credit-exhausted
  1 service-policy type service name SERVICE_403_L4R_TC
 !
 class type control always event quota-depleted
  1 set-param drop-traffic FALSE
!
! After receiving the Account-Logoff request, allow the session to stay active for
! another 10 seconds for graceful log-off.
class type control always event account-logoff
  1 service-policy disconnect delay 10
```

Configuring QoS Policies for Model 3

Here is how to configure the QoS policies:

```
class-map match-any QOS_CLASS_VOICE_403
  match ip dscp ef

policy-map QOS_POLICY_IN_VOICE_403
  class QOS_CLASS_VOICE_403
   police cir 128000
     exceed-action drop

policy-map QOS_POLICY_IN_512_PARENT_403
  class class-default
   police cir 512000
     exceed-action drop
   service-policy QOS_POLICY_IN_VOICE_403
```

```
policy-map QOS_POLICY_IN_256_PARENT_403
  class class-default
   police cir 256000
     exceed-action drop
   service-policy QOS_POLICY_IN_VOICE_403

policy-map QOS_POLICY_OUT_VOICE_403
  class QOS_CLASS_VOICE_403
    priority 128

policy-map QOS_POLICY_OUT_512_PARENT_403
  class class-default
    shape average 512000
   service-policy QOS_POLICY_OUT_VOICE_403

policy-map QOS_POLICY_OUT_256_PARENT_403
  class class-default
    shape average 256000
     service-policy QOS_POLICY_OUT_VOICE_403
```

Configuring mBGP and VPNv4 for Model 3

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

```
ip vrf VPN_403_1001
 rd 403:1001
 route-target export 403:1001
 route-target import 403:1001
!
ip vrf VPN_403_1002
 rd 403:1002
 route-target export 403:1002
 route-target import 403:1002
!

router ospf 100
 router-id 172.16.4.13
 log-adjacency-changes
 redistribute static metric-type 1 subnets
 network 172.16.3.0 0.0.0.255 area 102
 network 172.16.4.13 0.0.0.0 area 102
 network 172.16.9.0 0.0.255.255 area 102
!
router bgp 100
 no synchronization
 bgp router-id 172.16.4.13
 bgp log-neighbor-changes
 neighbor 172.16.4.9 remote-as 100
 neighbor 172.16.4.9 update-source Loopback0
 no auto-summary
!
 address-family vpnv4
 neighbor 172.16.4.9 activate
 neighbor 172.16.4.9 send-community both
 exit-address-family
!
 address-family ipv4 vrf VPN_403_1002
 redistribute connected
 no auto-summary
 no synchronization
 exit-address-family
```

```
!
 address-family ipv4 vrf VPN_403_1001
 redistribute connected
 no auto-summary
 no synchronization
 exit-address-family
```

Configuring the Remote PE Side for Model 3

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

```
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
!

router bgp 100
 no synchronization
 bgp router-id 172.16.4.9
 bgp log-neighbor-changes
 neighbor 172.16.4.13 remote-as 100
 neighbor 172.16.4.13 update-source Loopback0
 no auto-summary
 !
 address-family vpnv4
 neighbor 172.16.4.13 activate
 neighbor 172.16.4.13 send-community both
 exit-address-family
 !

 address-family ipv4 vrf VPN_403_1002
 redistribute connected
 redistribute static
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family ipv4 vrf VPN_403_1001
 redistribute connected
 redistribute static
 no auto-summary
 no synchronization
 exit-address-family
!
```

Configuration Verification Commands

The following sections list the **show** and **debug** commands that are helpful for verifying and debugging the ISG network configurations:

Show Commands

Use the following **show** commands to verify subscriber configurations:

- **show ip subscriber detail | dangling | mac | vrf**
- **show subscriber session uid | username**

Use the following command to verify service configurations:

- **show subscriber service**

Use the following command to display address bindings on the DHCP server:

- show ip dhcp binding

The **show running-configuration** command is also useful for verifying configurations.

Debug Commands

The following **debug** commands are commonly used for debugging problems for networks using the IP sessions used in the Model 1 and 2 networks:

- **debug ip subscriber all | error | event | fsm | packet**
- **debug ip dhcp server event | packet | class** [1]
- **debug subscriber policy dpm event | error** [1]
- **debug subscriber event | error**
- **debug subscriber policy event | error**
- **debug subscriber policy prepaid**
- **debug radius**

[1] Used mostly for DHCP sessions; also useful to verify for VRF transfer.

The following **debug** commands are commonly used for debugging problems for networks using the PPP sessions used in the model 3 network:

- **debug ppp negotiation**
- **debug ppp authentication**
- **debug pppoe error | event**
- **debug subscriber event | error**
- **debug subscriber policy event | error**
- **debug radius**

Verification Command Examples

This section provides the following examples:

ISG Configuration Information Verification

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

```
GE-10008-BRAS1# show running interface gigE 1/0/0.111

Building configuration...
Current configuration : 244 bytes
!
interface GigabitEthernet1/0/0.111
encapsulation dot1Q 4020 second-dot1q 4043
ip address 172.16.1.1 255.255.255.0
no snmp trap link-status
service-policy type control RULE-401a-1
ip subscriber l2-connected
initiator dhcp class-aware
end
```

Basic ISG Operation Verification

Use the **show subscriber session** command to show a summary of the number of active sessions and their unique identifier, interface, state, service, NAS-port identifier, and up time.

```
GE-10008-BRAS1# show subscriber session

Current Subscriber Information: Total sessions 1

Uniq ID Interface  State Service  Identifier                        Up-time
10      IP         authen         Local Term   nas-port:1/0/0/4020. 00:00:45
11      Traffic-Cl unauthen      Ltm Internal                       00:00:45
```

Subscriber Service Verification

Use the **show ip subscriber** command with the VRF identifier and detailed keyword to verify that a subscriber belongs to a VRF as expected.

```
GE-10008-BRAS1# show ip subscriber vrf VPN_401_1001 detailed

IP subscriber: 000e.0c4a.f197, type connected, status up
display uid: 10, aaa uid: 21
session initiator: dhcp discovery
access address: 172.16.6.2
service address: vrf VPN_401_1001, 172.16.6.2
conditional debug flag: 0x0
control plane state: connected, start time: 00:00:57
data plane state: connected, start time: 00:00:52
```

```
arp entry: [vrf VPN_401_1001] 172.16.6.2, GigabitEthernet1/0/0.111
midchain adj: 172.16.6.2 on multiservice1
forwarding statistics:
packets total: received 14, sent 2
bytes total: received 1520, sent 656
packets dropped: 1, bytes dropped: 98
```

ISG Prepaid Service Verification

Use the **show subscriber session uid** command to verify the prepaid service status.

```
GE-10008-BRAS2# show subscriber session uid 60

Unique Session ID: 60
Identifier: nas-port:172.16.4.13:1/0/0/4020.4037
SIP subscriber access type(s): Traffic-Class
Current SIP options: None
Session Up-time: 00:01:29, Last Changed: 00:00:58

Policy information:
  Authentication status: unauthen
  Prepaid context: PREPAID_RSIM
    threshold time 100 seconds
    threshold volume 500 bytes
    method-list author PREPAID_AUTHOR_LIST
    method-list accounting default
    password cisco
    Interim 3 minutes
    State PREPAID_FEATURE_RUNNING
    Flow idle at last re-author ? NO
    Total idle time 0 seconds
    Are we accounting for time consumed ? YES
    Acct start sent ? YES

Session inbound features:
 Feature: Prepaid Idle Timeout
   Timeout configuration: 120 (seconds)
Feature: Policing
 Upstream Params:
Average rate = 512000, Normal burst = 512000, Excess burst = 0
Config level = Service

 Feature: Prepaid Volume Monitor
   Threshold:500 - Quota:1000
   Usage(since last update):0 - Total:864
   Current states: Start
Session outbound features:
 Feature: Prepaid Idle Timeout
   Timeout configuration: 120 (seconds)
Feature: Policing
 Dnstream Params:
Average rate = 1024000, Normal burst = 1024000, Excess burst = 0
Config level = Service

 Feature: Prepaid Volume Monitor
   Threshold:500 - Quota:1000
   Usage(since last update):0 - Total:864
   Current states: Start
Configuration sources associated with this session:
Service: SERVICE_403_INTERNET, Active Time = 00:01:30
```

DHCP Server Address Bindings

The following example displays address bindings from all pools not associated with a VRF:

```
GE-10008-BRAS1# 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 VPN_401_1001:
IP address          Client-ID/     Lease expiration        Type
            Hardware address/
            User name
172.16.6.2            0100.0e0c.4af1.97       Aug 26 2006 11:10 AM    Automatic

Bindings from VRF pool VPN_401_1002:
IP address          Client-ID/     Lease expiration        Type
            Hardware address/
            User name

Bindings from VRF pool VPN_401_1003:
IP address          Client-ID/     Lease expiration        Type
            Hardware address/
            User name
```

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 Services Gateway Configuration Guide*
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*
RFC 2616	*Hypertext Transfer 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

ADSL2—asymmetric dual-latency modem

ATU-R—ADSL Transmission Unit—remote

BRAS—Broadband Remote Access Server

CAR—Cisco Access Registrar

CE—customer edge

CNR—Cisco Network Registrar

CoA—Change of Authorization

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 Services Gateway

ISP—Internet service provider

IPCP—IP Control Protocol

L2TP—Layer 2 Tunnel Protocol

MAC—Media Access Control

MQC—Modular QoS CLI

MPLS—Multiprotocol Label Switching

PBHK—Port-Bundle Host Key

PE—provider edge

POP—point of presence

PPPoE—PPP over Ethernet

PVC—permanent virtual circuit

QoS—quality of service

SESM—Subscriber Edge Services Manager

SSG—Service Selection Gateway

TAL—Transparent Autologin

VoIP—Voice over IP

VPDN—virtual private dialup network

VLAN—virtual LAN

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.