Cisco ISG Design and Deployment Guide: ATM to ISG Aggregation

Version History

Version Number	Date	Notes
1	May 21, 2005	This document was created.

The Intelligent Service Architecture (ISA) is a Cisco IOS feature set that enables the provisioning and maintaining of broadband networks that have multiple types of edge devices, many subscribers, and many services. ISA combines real-time session and flow control with programmable, dynamic policy control to deliver flexible and highly scalable subscriber session management capabilities.

A Cisco device that is running a Cisco IOS image with ISA is called an Intelligent Service Gateway (ISG). An ISG is used to control subscriber access at the edge of an IP network. An ISG is deployed at network access control points, and subscribers access services through ISG. The role of ISA is to execute policies that identify and authenticate subscribers and provide access to the services that the subscriber is entitled to access.

This document describes how to design and deploy an ISA network using the Cisco 7200 series or 7301 as an ISG and ATM as the aggregation technology. The following four deployment models are described:

- Deployment Model 1: Basic Internet Access Service Bundle over L2TP
- Deployment Model 2: Multiservice Service Bundle over PPPoE
- Deployment Model 3: Triple Play Plus Service Bundle over IP and PPPoE
- Deployment Model 4: Triple Play Plus Service Bundle over IP and L2TP

These deployment models are designed to simulate the most common ISP deployments. They combine a specific service bundle, which is a logical combination of features, with specific network topologies. ISPs can configure a single deployment model, or any combination of the four deployment models simultaneously, depending on their needs.

This document contains the following sections:

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

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

Designing ATM to ISG Aggregation

The ISA network described in this document uses the Cisco 7200 series and 7301 as an ISG in a network that uses ATM aggregation. This document covers the following access technologies:

- IP sessions
- PPP over Ethernet (PPPoE) sessions
- PPPoE over L2TP session

The IP and PPPoE deployments simulate the network of a single ISP. The PPPoE over L2TP deployments simulate two ISPs working together:

- ISP-1 offers wholesale service to other ISPs.
- ISP-2 contracts with ISP-1 to receive wholesale service, which it then offers to retail customers.

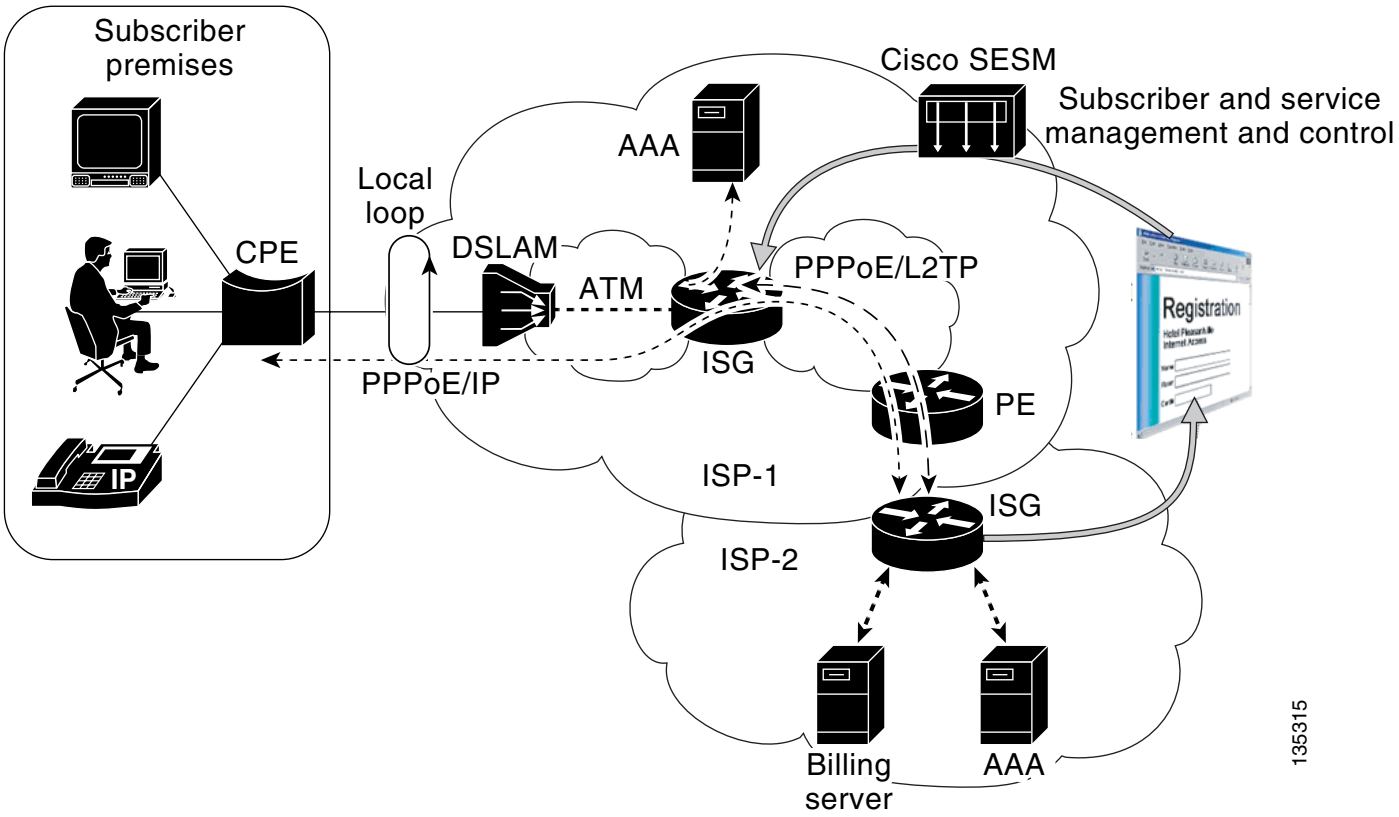
The following sections describe the design of the ISA network:

Network Topology

Figure 1 shows a high-level network topology.

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

Figure 1 High-Level Topology



Network Elements

The following elements play key roles in the network:

CPE

The customer premises equipment (CPE) router is a small router (such as the Cisco 800 series) that is used either as a bridge or to initiate PPPoE connections from the customer PC to the L2TP Access Concentrator LAC.

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

DSLAM

The Digital Subscriber Line Access Multiplexer (DSLAM) aggregates multiple incoming DSL connections into a single ATM line. It is maintained at a point of presence (POP) separate from the ISP's central network.

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

ISG

An Intelligent Service Gateway (ISG) is used to control subscriber access at the edge of an IP/Multiprotocol Label Switching (MPLS) network. An ISG is deployed at network access control points, and subscribers access services through ISG. The role of ISA is to execute policies that identify and authenticate subscribers and provide access to the services that the subscriber is entitled to access. In the L2TP deployments in this document, the ISG also serves as a LAC.

ISG LAC

In the L2TP deployments in this document, the ISG also serves as a LAC. It is maintained by the ISP as part of its central network. It receives incoming sessions from the DSLAM and forwards them to the appropriate retail ISP by establishing an L2TP tunnel with the LNS. The LAC contacts the ISP's Authentication, Authorization, and Accounting (AAA) server to determine the forwarding information based on the subscriber's domain name.

ISG LNS

The ISG L2TP Network Server (LNS) is used only in the L2TP deployments. The ISG LNS terminates the L2TP tunnel from the LAC and the PPPoE session from the subscriber. It is maintained by the ISP on its central network. The ISG LNS authenticates the user by contacting the AAA server for ISP, and assigns the user a VPN routing/forwarding instance (VRF). The ISG LNS also communicates with the AAA server when the user requests additional services.

PE

The provider edge (PE) router is responsible for maintaining 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.

AAA Servers

In the IP and PPPoE deployments, the network utilizes a single AAA server. The AAA server maintains user authentication information as well as information on the services available to users. When the ISG receives a user's username and password, it forwards it to the AAA server for authentication. When a user activates a service, the ISG contacts the AAA server, which replies with information on the service to the ISG.

In the L2TP deployments, each ISP maintains its own AAA server:

- The AAA server for ISP-1 (known as AAA-1) maintains forwarding information for the retail ISPs. When queried by the ISG LAC, it sends forwarding information based on the user's domain name.

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

- The AAA server for ISP-2 (known as AAA-2) maintains user authentication information as well as information on the services available to users. When the LNS receives a user's username and password, it forwards it to AAA-2 for authentication. When a user activates a service, the LNS contacts AAA-2. AAA-2 then replies with information on the service to the LNS.

Instead of using single AAA servers, SPs can maintain multiple AAA servers to be used for separate domains, or for round robin load balancing.

SESM

The Cisco Subscriber Edge Services Manager (SESM) provides service selection and connection management in broadband and mobile wireless networks. The Cisco SESM provides a web portal for users to access services. ISPs can customize the web portal to their needs.

Note Configuring the Cisco SESM is beyond the scope of this document. A detailed *Installation and Configuration Guide for the Cisco SESM* is at the following URL: http://www.cisco.com/univercd/solution/sesm/sesm_320/index.htm

Billing Server

The billing server maintains user account information, including the amount of credit remaining for prepaid services. When users initiate services, the ISG contacts the billing server to determine if the user has credit available.

DHCP Server

A Dynamic Host Control Protocol (DHCP) server can be used to dynamically assign reusable IP addresses to devices in the network. Using a DHCP server can simplify device configuration and network management by centralizing network addressing. In the deployments described in this document a Cisco CNS Network Registrar (CNR) server is used as the DHCP server.

Note Configuring the Cisco CNR is beyond the scope of this document. For information on configuring the Cisco CNR, see the Cisco CNS Network Registrar, 6.1.1 documentation at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/ciscoasu/nr/nr611/index.htm

Deployment Models

The following sections provide an overview of the four deployment models:

- Deployment Model 1: Basic Internet Access Service Bundle over L2TP, page 6
- Deployment Model 2: Multiservice Service Bundle over PPPoE, page 7
- Deployment Model 3: Triple Play Plus Service Bundle over IP and PPPoE, page 9
- Deployment Model 4: Triple Play Plus Service Bundle over IP and L2TP, page 11

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

Deployment Model 1: Basic Internet Access Service Bundle over L2TP

The Basic Internet Access Service Bundle over L2TP deployment is a traditional L2TP network offering basic DSL service, with no advanced ISA services. It is used as a baseline to establish basic connectivity before deploying the ISA services. In this network ISP-2 contracts with ISP-1 to receive wholesale DSL service, which it then offers to its retail customers.

PPP is tunneled from the ISG LAC to the LNS. At the LNS, the PPP session is terminated, and the encapsulated IP traffic is routed on through the ISP's network. The identity of the customer is uniquely maintained only by the PPP session. Figure 2 shows how the PPP session is routed across the network.

In this deployment, subscribers are automatically connected to the appropriate L2TP tunnel on the basis of their domain names. The retail ISP (ISP-2) performs authentication on the far end of the L2TP tunnel.

Figure 2 Deployment Model 1 Protocol Flow

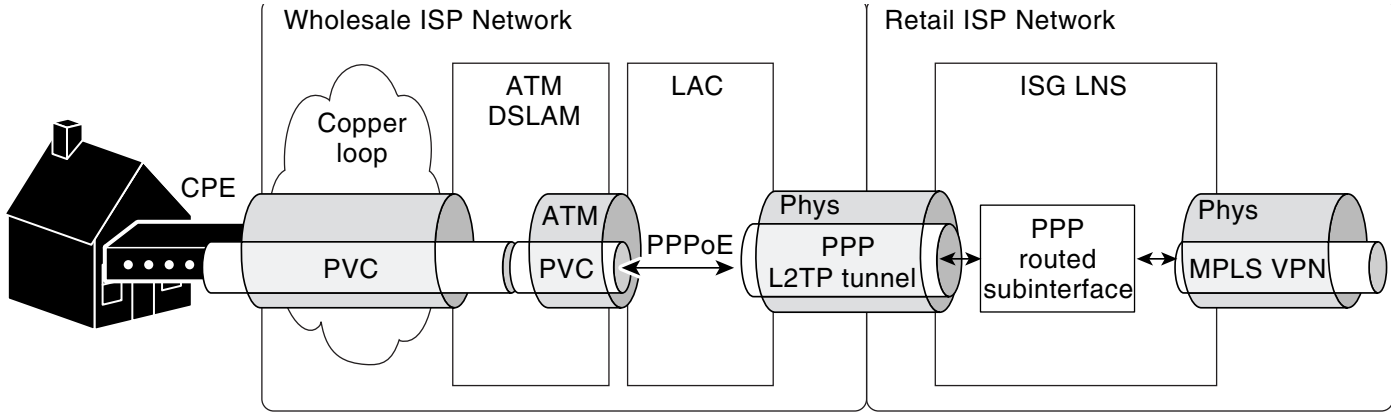


Figure 3 shows all the protocols that are active at each device in the network.

Figure 3 Deployment model 1 Protocol Stacks

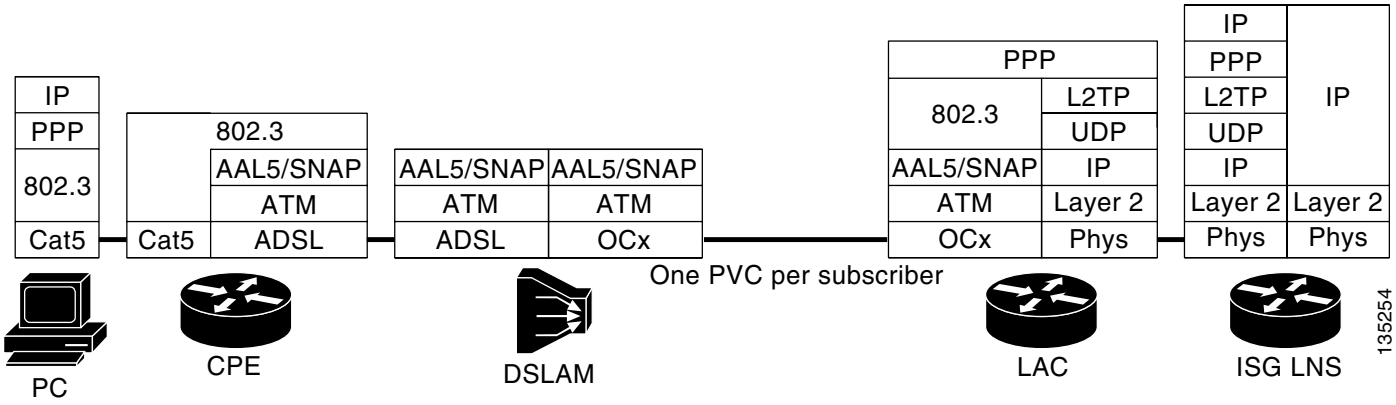


Figure 4 shows all the interfaces in the network where Quality of Service (QoS) could potentially be configured. Here, "Up" refers to the upstream interface between the two devices, and "Dw" refers to the downstream interface. The interfaces in bold are where QoS is configured for this deployment.

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

Figure 4 QoS Interfaces

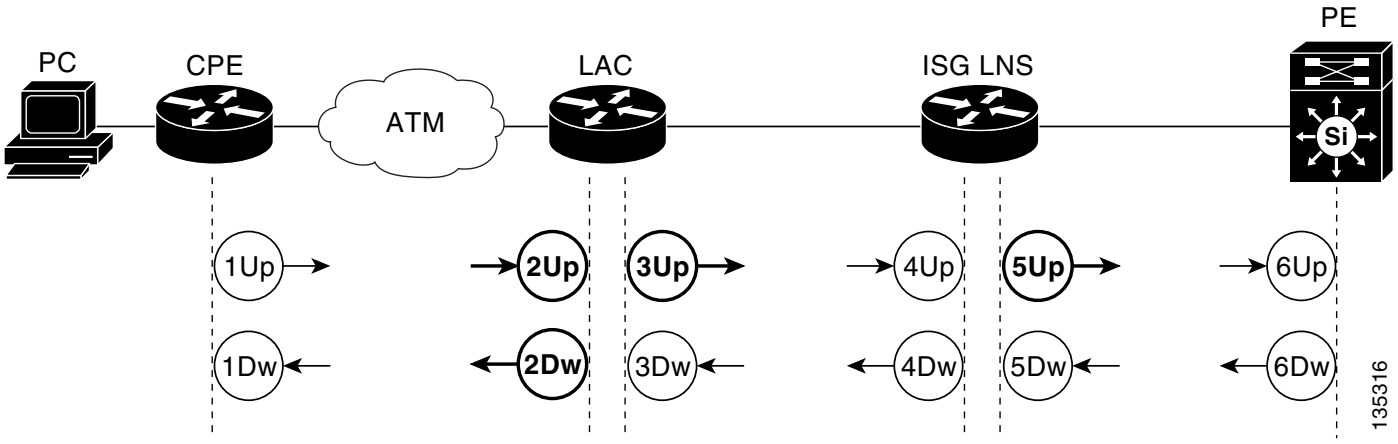


Table 1 describes the QoS strategy that is deployed on each of the interfaces shown in Figure 4.

Table 1 QoS Strategy

Interface	Device	Traffic Origin	Traffic Destination	QoS Strategy
2Up	ISG LAC	CPE	ISG LAC	Virtual circuit (VC) shaping parameters are defined by a domain profile on AAA-1 using the Dynamic Bandwidth Selection (DBS) feature.
2Dw	ISG LAC	ISG LAC	CPE	VC shaping parameters are defined by a domain profile on AAA-1 using the DBS feature.
3Up	ISG LAC	ISG LAC	LNS	All traffic is reclassified as best effort (DiffServ Code Point (DSCP) is set to 0).
4Up	LNS	ISG LAC	LNS	VC shaping parameters are defined by a Domain Profile on AAA-1 using the DBS feature.
4Dw	LNS	LNS	ISG LAC	VC shaping parameters are defined by a Domain Profile on AAA-1 using the DBS feature.
5Up	LNS	LNS	PE	Upstream traffic is marked as the default service, MPLS EXP 0, by the service policy governing the outbound Gigabit Ethernet interface.

Deployment Model 2: Multiservice Service Bundle over PPPoE

In the Multiservice Service Bundle over PPPoE deployment, an ISP expands its traditional, static DSL service by deploying the multiservice service bundle, which consists of the bandwidth-on-demand and Prepaid Services features. When customers activate these services, the network allocates additional bandwidth to them, based on either time or volume of bandwidth. The management of the available minutes will be done via a billing server external to the ISG.

This network involves a single ISP. The DSLAM delivers traffic to the ISG using PPPoE. The ISG terminates PPPoE and routes the IP traffic through the ISP network. Subscriber identities are maintained through PPPoE authentication, and the uniqueness of the DSL line is maintained by a dedicated Layer 2 path to the ISG over an ATM PVC that is cross-connected to the subscriber at the DSLAM.

It is best if services are applied at the ISG. It is possible—but more difficult—to apply services at the DSLAM; however, the services at the DSLAM are not part of the PPP link.

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

This deployment offers to methods for subscriber authentication. Subscribers can be authenticated based on their username on the local AAA server. Or subscribers can be automatically connected to a service domain based on the domain downloaded from an initial local AAA lookup. Subscriber authentication then takes place within the domain of the ISP by a remote AAA server lookup. Figure 5 shows how traffic is routed across the network.

Figure 5 Deployment Model 2 Protocol Flow

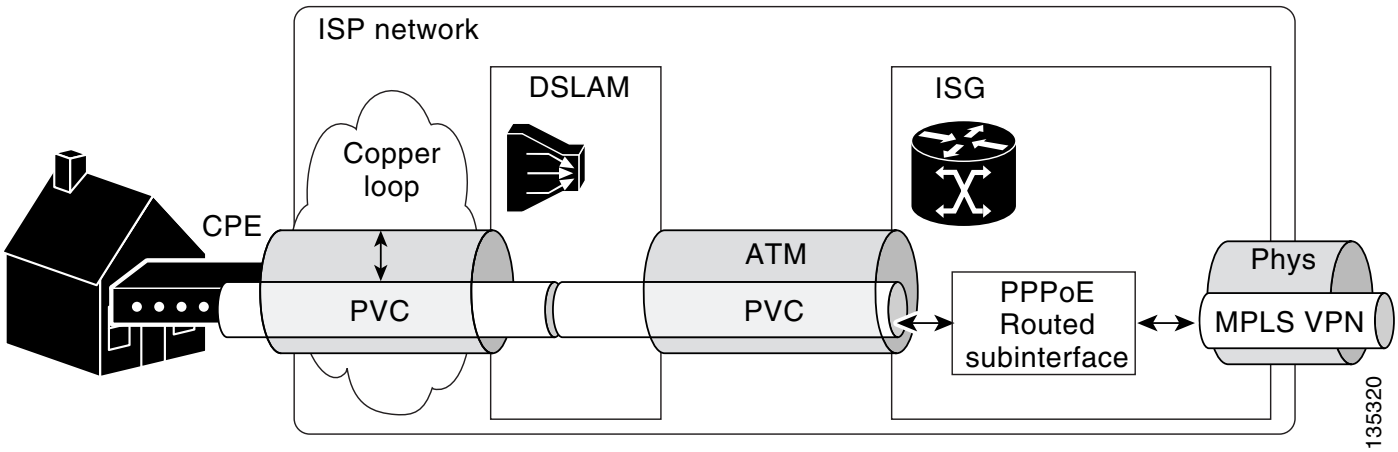


Figure 6 shows all of the protocols that are active at each device in the network.

Figure 6 Deployment Model 2 Traffic Flow

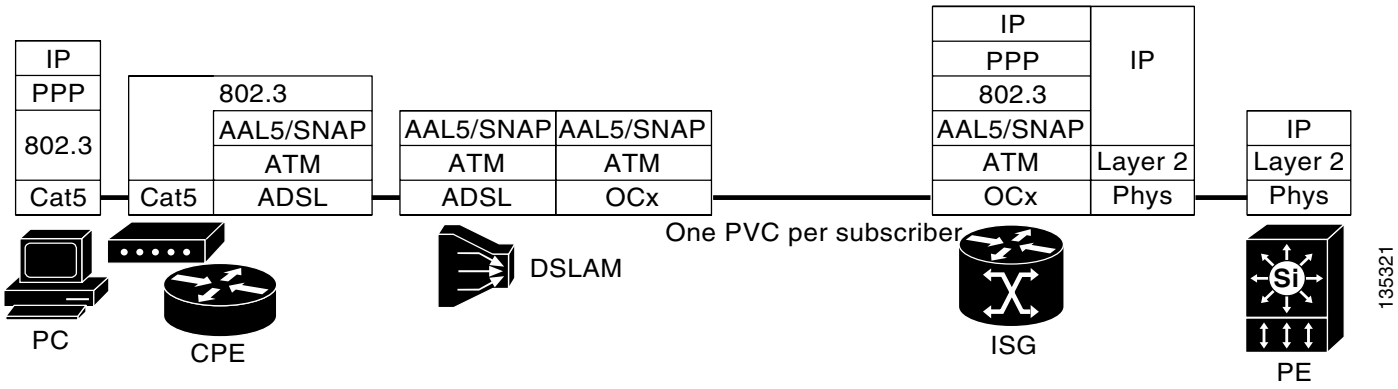


Figure 7 shows all the interfaces in the network where QoS could potentially be configured. Here "Up" refers to the upstream interface between the two devices, and "Dw" refers to the downstream interface. The interfaces in bold are where QoS is configured for this deployment.

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

Figure 7 QoS Interfaces

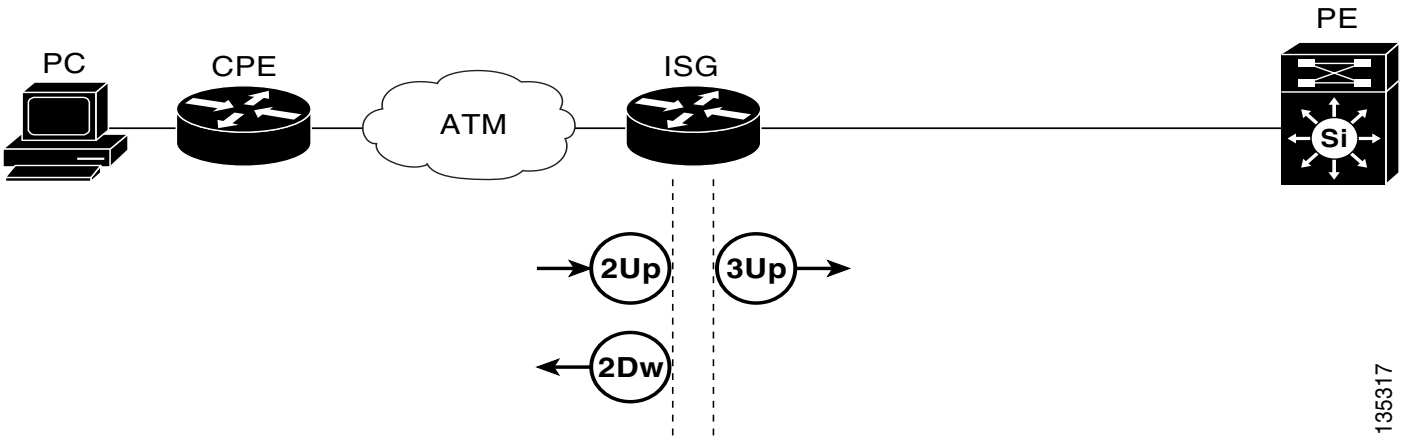


Table 2 describes the QoS strategy that is deployed on each of the interfaces shown in Figure 7.

Table 2 QoS Strategy

Interface	Device	Traffic Origin	Traffic Destination	QoS Strategy
2Up	ISG	CPE	ISG	QoS is not configured on this interface; therefore, upstream traffic must be limited by the DSLAM modem train rate.
2Dw	ISG	ISG	CPE	DBS is configured to shape downstream traffic by using the **dbs enable maximum** command.
3Up	ISG	ISG	PE	Upstream traffic is marked as the default service, MPLS EXP 0, by the service policy governing the outbound Gigabit Ethernet interface.

Deployment Model 3: Triple Play Plus Service Bundle over IP and PPPoE

In the Triple Play Plus Service Bundle over IP and PPPoE deployment, an ISP offers the Triple Play Plus Service Bundle, which consists of advanced services designed for gaming subscribers. The services include voice over IP (VoIP), Broadcast Video, as well as prioritized traffic to the ISP's own gaming servers. This deployment involves a single ISP.

In this deployment, two peering IP interfaces are configured between the CPE and the ISG: one for IP connections and one for PPPoE connections. This configuration allows all subscribers to use PPPoE for data traffic, regardless of where they are subscribing to the basic service or to the triple-play package. This dual-purpose approach eases support and conversion issues and allows the ISP to gradually convert to a full IP Routed scheme.

This deployment supports transparent auto-login (TAL) based on the subscriber's MAC address, which requres that subscriber MAC addresses be configured manually. If MAC address-based authentication fails, subscribers are redirected to the web portal maintained by the Cisco SESM, where they can manually log in. Figure 8 shows how traffic is routed across the network.

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

Figure 8 Deployment Model 3 Protocol Flow

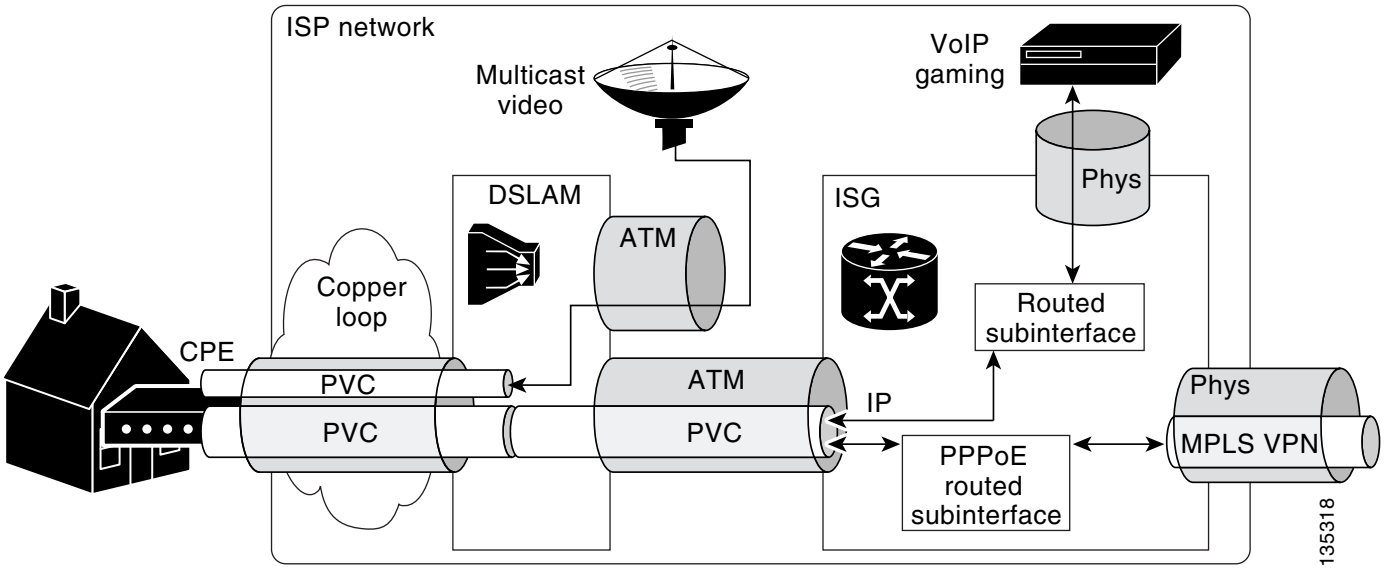


Figure 9 Deployment Model 3 Protocol Stack

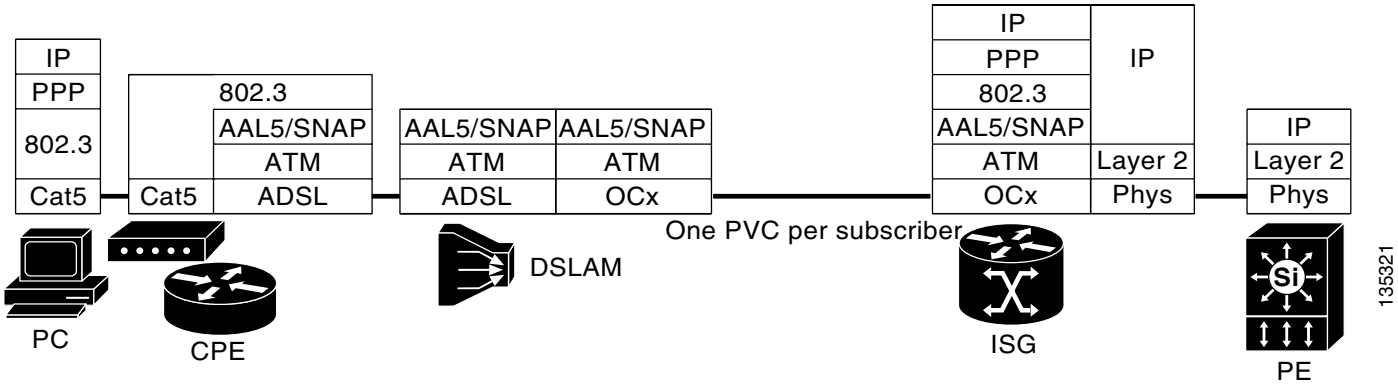


Figure 10 shows all of the interfaces in the network where QoS could potentially be configured. Here, "Up" refers to the upstream interface between the two devices, and "Dw" refers to the downstream interface. The interfaces in bold are where QoS is configured for this deployment.

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

Figure 10 QoS Interfaces

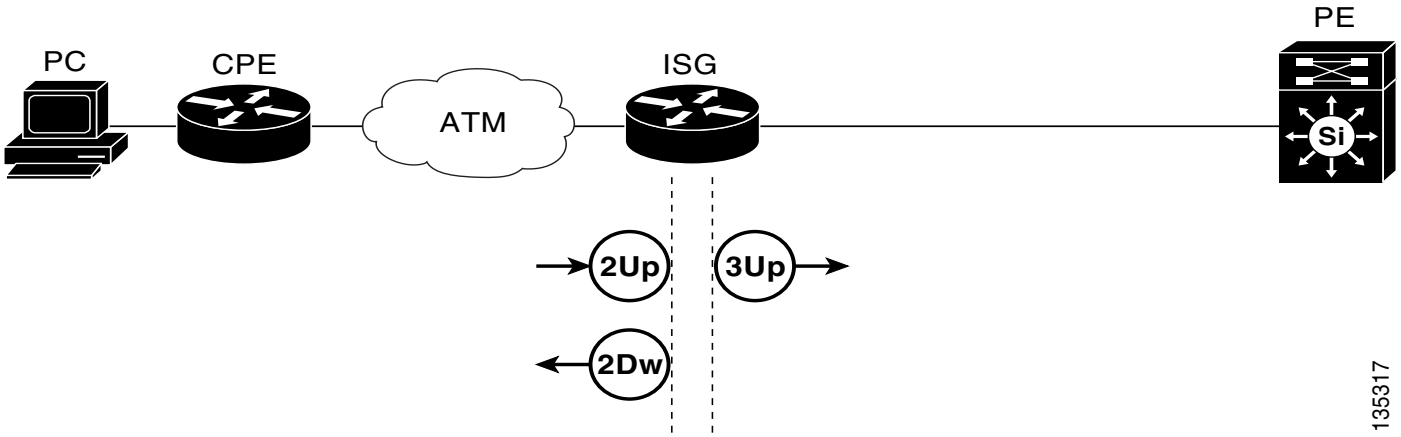


Table 3 describes the QoS strategy that is deployed on each of the interfaces shown in Figure 10.

Table 3 QoS Strategy

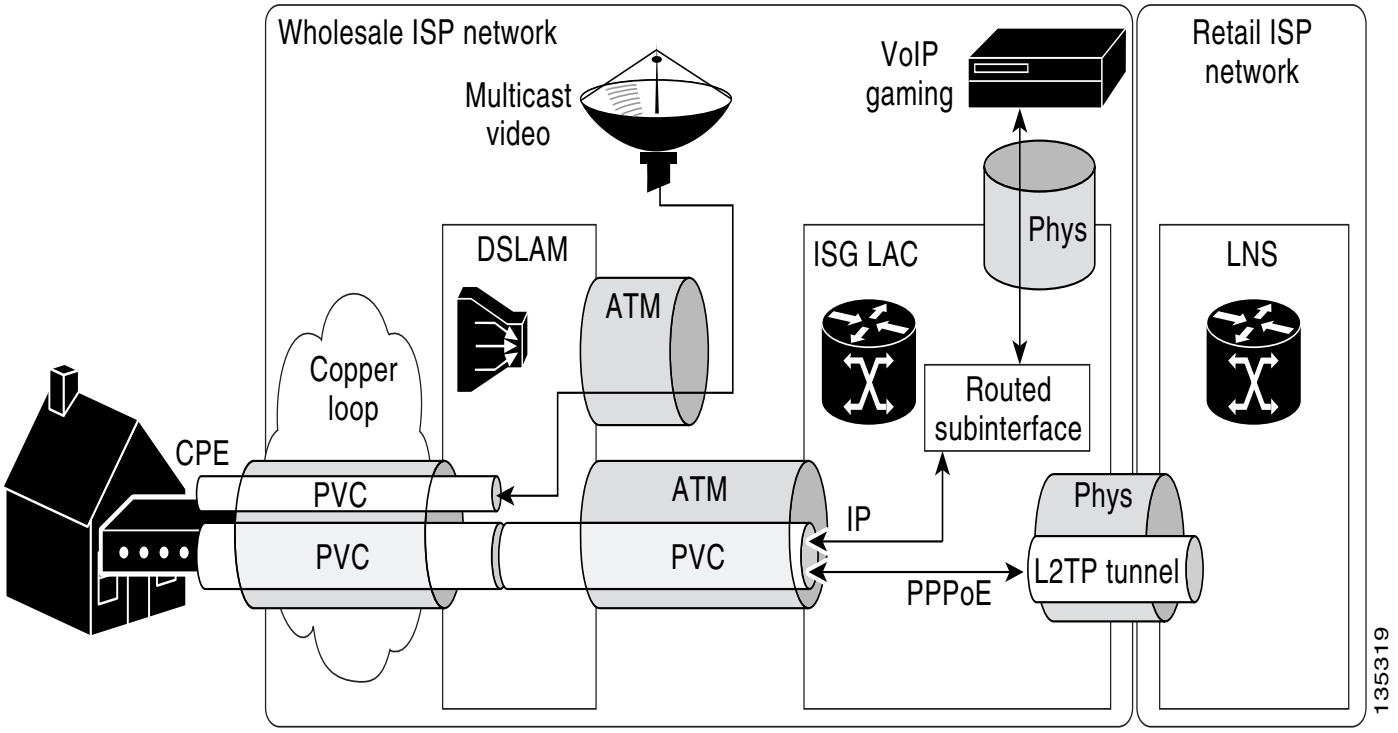
Interface	Device	Traffic Origin	Traffic Destination	QoS Strategy
2Up	ISG	CPE	ISG	Upstream traffic is policed to an aggregate rate using a parent policy. A child policy then applies Class Based Policing on VoIP, Call Control, and gaming. DSCP is mapped to the appropriate MPLS EXP.
2Dw	ISG	ISG	CPE	LLQ is applied to VoIP streams, and class-based weighted fair queueing (CBWFQ) is applied to Call Control and gaming.
3Up	ISG	ISG	LNS	DSCP is mapped to the appropriate MPLS EXP.

Deployment Model 4: Triple Play Plus Service Bundle over IP and L2TP

This deployment is very similar to Deployment Model 3: Triple Play Plus Service Bundle over IP and PPPoE. The IP segments of the two deployments are identical. The difference in this deployment is that PPPoE sessions are delivered to ISP-2's network over L2TP tunnels. Figure 11 shows how traffic is routed across the network.

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

Figure 11 Deployment Model 4 Protocol Flow



Deployment Model 4 QoS Strategy

The QoS strategy for the IP segment is the same as that for the IP segment of Deployment Model 3: Triple Play Plus Service Bundle over IP and PPPoE deployment model.

The QoS strategy for the PPPoE over L2TP segment of the network is the same as that for the Deployment Model 1: Basic Internet Access Service Bundle over L2TP deployment model.

Network Design Options

The following sections describe the various options the ISP must consider in deploying the network:

- Aggregation Technology, page 12
- Routing Technology, page 12

Aggregation Technology

ISA supports ATM for use as the aggregation technology.

Routing Technology

In all cases the DSLAM delivers traffic to the first ISG using an ATM PVC. When designing the network, you have three basic choices for how to deliver traffic from the ISG at the wholesale ISP to the retail ISP:

- IP sessions—Traffic is IP routed from the ISG to the retail ISP.

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

- PPP terminated—The DSLAM delivers traffic to the ISG using PPPoE. The ISG terminates the PPPoE and then IP routes traffic to the retail ISP.
- L2TP tunneled—The DSLAM delivers traffic to the ISG LAC using PPPoE. The ISG LAC then establishes an L2TP tunnel with an LNS on ISP-2's network. The LNS terminates the PPPoE, and IP is used to route the traffic in the retail ISP's network.

Service Bundles

Because of the large number of features available for ISA services, in the design and deployment guides we have grouped the features into service bundles. The following service bundles are deployed in the network:

- Basic Internet Access Service Bundle, page 13
- Multiservice Service Bundle, page 13
- Triple Play Plus Service Bundle, page 14

Basic Internet Access Service Bundle

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

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

Multiservice Service Bundle

The Multiservice service bundle consists of the following features:

- Layer 3 VPN Access
- Bandwidth on Demand
- Prepaid Services

Layer 3 VPN Access

The default service for subscribers in the Multiservice service bundle is Layer 3 VPN access. This is the same basic DSL connectivity described above, where the bandwidth for all users is capped at a static 128 kbps upstream and 256 kbps downstream.

Bandwidth on Demand

The Bandwidth on Demand feature enables subscribers to temporarily increase their upstream and downstream bandwidths for either a set duration of time or a set volume of bandwidth. Subscribers first establish basic connectivity with a default cap on bandwidth, and then access a website (maintained by the Cisco SESM) where they trigger a request for the Bandwidth on Demand. The ISP authorizes the subscriber for the service and bills the subscriber's account. Bandwidth on Demand can be either prepaid or post-paid. The service remains active until either the subscriber deactivates the service or the subscriber terminates the session.

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

Prepaid Services

The Prepaid Services feature allows subscribers to debit their service against a previously credited account. The Prepaid Services payment method can be applied to Bandwidth on Demand, or any of the other ISG services. When subscribers activate a service, the billing server charges the subscriber's account based on either the time the service is active, or the bandwidth the subscriber uses. The service remains active until either the subscriber's account is depleted or the subscriber deactivates the service or terminates the session.

Triple Play Plus Service Bundle

The Triple Play Plus service bundle provides advanced QoS services. It consists of the following services:

- Basic Broadband Connectivity
- VoIP
- Video on Demand (VoD)
- Gaming

When subscribers initiate a session, they are granted basic broadband connectivity. If subscribers wish to activate one of the advanced services (VoIP, VoD and gaming), they go the web portal maintained by the Cisco SESM and select the service. The advanced services are granted a higher level of QoS to ensure that subscribers can maintain the necessary level of bandwidth for the activity they select.

Note In the deployments described in this document, the advanced services are deployed only for IP sessions; however, ISA supports these services on both IP and PPPoE.

Deploying the Cisco ISG with ATM Aggregation

The following sections describe the process of deploying the Cisco ISG with ATM aggregation:

Deployment Models

The following deployment models are deployed in the network. ISPs can chose to deploy an individual deployment model or any combination of models that meet their requirements.

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

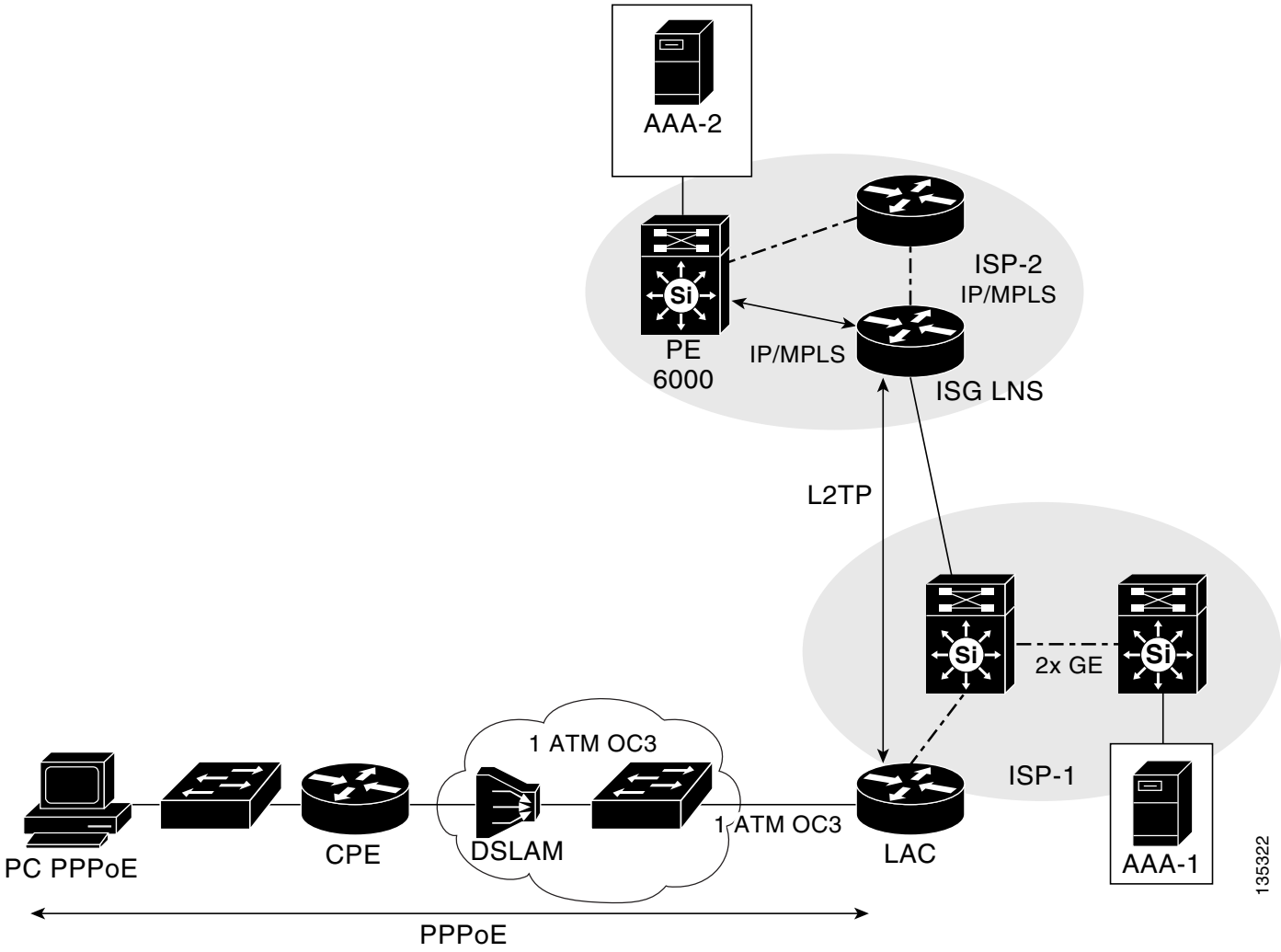
Deployment Model 1: Basic Internet Access Service Bundle over L2TP

The following sections describe the deployment model:

Network Topology

Figure 12 shows the network topology of this deployment.

Figure 12 Deployment Model 1 Network Topology

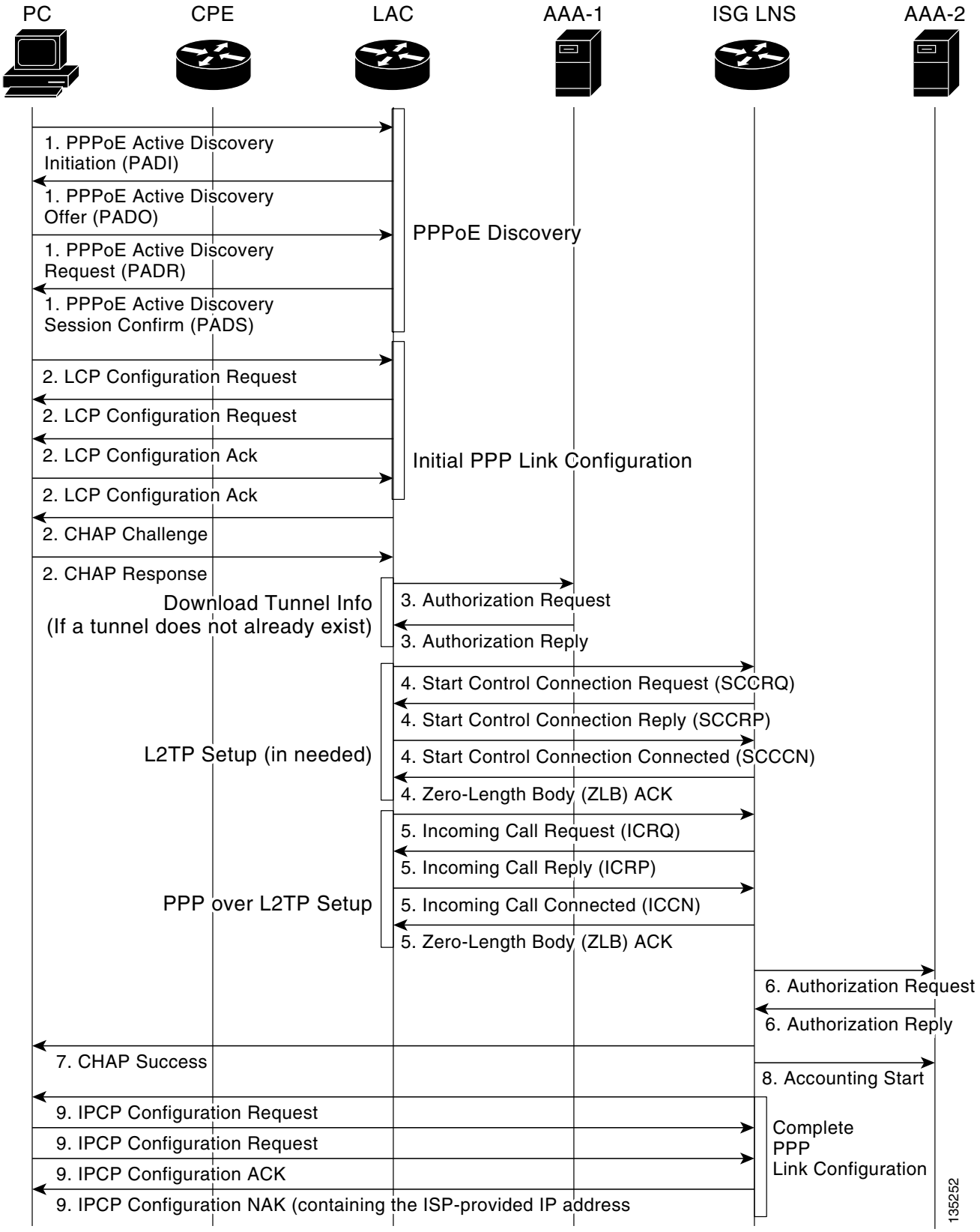


Basic Layer 3 VPN Access Call Flow for L2TP Sessions

Figure 13 shows the call flow process that occurs when a subscriber establishes basic Layer 3 VPN access to the network.

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

Figure 13 Layer 3 VPN Access Call Flow



(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

The following describes the sequence of events in Figure 13:

1. The subscriber initiates a PPPoE connection from the PC to the ISG LAC by way of the CPE.
2. The PC and the ISG LAC establish a PPP connection.
3. The ISG LAC contacts the AAA-1 server to retrieve domain authentication information for L2TP.
4. The ISG LAC establishes an L2TP tunnel with the LNS. This step is necessary only if an L2TP tunnel does not already exist.
5. The ISG LAC forwards the subscriber PPP session and associated information to the LNS.
6. The LNS contacts the AAA-2 server to authenticate the subscriber. Once the subscriber is authenticated, the LNS clones a virtual-access interface from the virtual template.
7. The LNS sends a CHAP response to the subscriber. The IP Control Protocol (IPCP) phase is performed, and the route to the LNS is installed. The PPP session now runs between the subscriber and the LNS, while the ISG forwards the PPP traffic over the L2TP tunnel.
8. The LNS sends an accounting start message to the AAA-2 server.
9. The subscriber and the LNS use IPCP to negotiate the link details, including the IP address. IPCP is responsible for configuring, enabling, and disabling the IP protocol modules on both ends of the PPP link. IPCP uses the same packet exchange mechanism as the Link Control Protocol (LCP). IPCP packets may not be exchanged until PPP has reached the Network-Layer Protocol phase.

Device Characteristics Table for Deployment Model 1

Table 4 describes details of the devices in the network.

Table 4 Device Characteristics

Device	Platform	Software
CPE	Cisco 837	12.3(2)XC2
ISG LAC	Cisco 7206	12.2(27)SBA
LNS	Cisco 7206	12.2(27)SBA
PE	Cisco 6509	12.2(18)SXD1
AAA for ISP1	UNIX server	CAR
AAA for ISP2	UNIX Server	CAR

Deployment Model 2: Multiservice Service Bundle over PPPoE

The following sections describe the deployment model:

In this deployment, the user's PC connects to a CPE, which initiates a PPPoE session to the ISG across the ATM network. The ISG then forwards the subscriber session to the PE over an MPLS VPN. The PE assigns the user a VRF and assigns the user the default service, which is a capped bandwidth of 256 kbps. The following advanced ISA services are then available to the user:

- BOD1MVOLUME: 1 Mbps downstream, 256 kbps upstream
- BOD1MTIME: 1 Mbps downstream, 256 kbps upstream

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

- BOD2MVOLUME: 2 Mpbs downstream, 512 kbps upstream
- BOD2MTIME: 2 Mbps downstream, 512 kbps upstream

For volume-based service, subscribers are billed according to the amount of bandwidth they use. For time-based service, subscribers are billed according to the length of time the service is active.

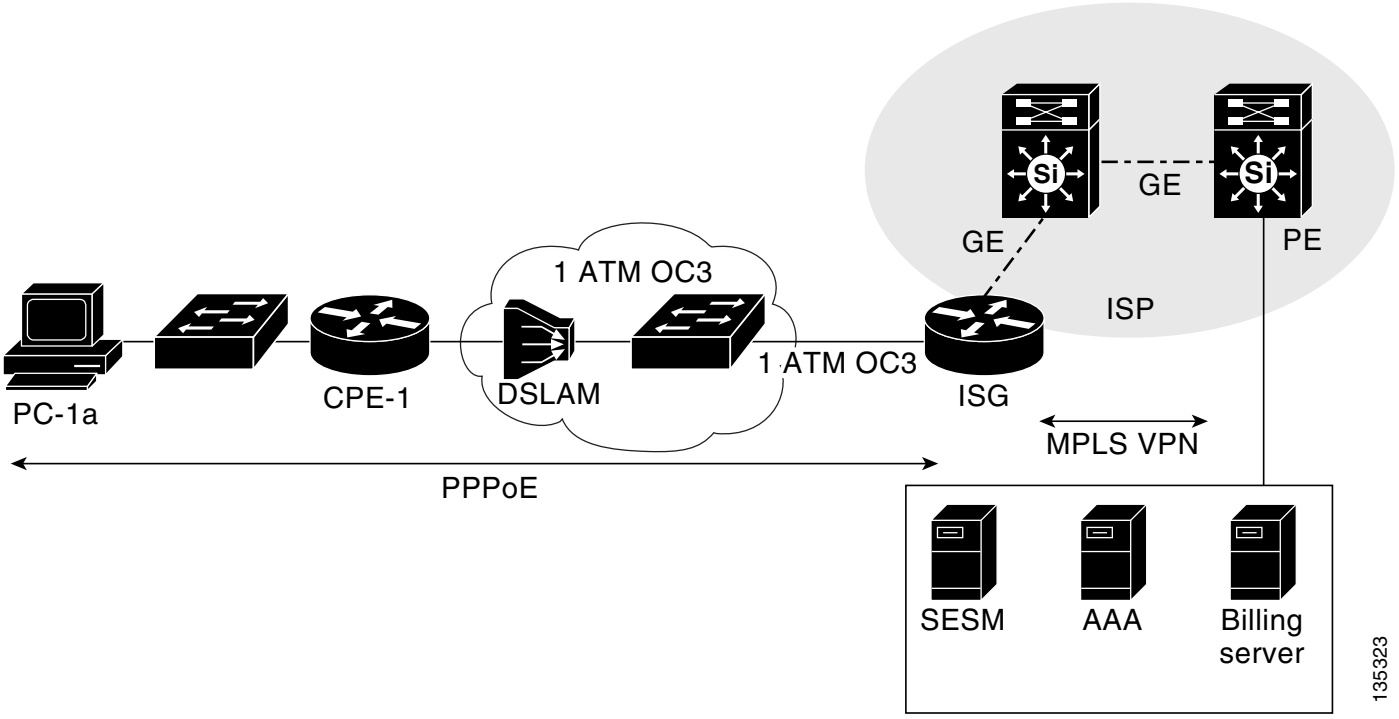
Note The specific bandwidths described in this document are only used as examples. SPs are free to configure any bandwidth levels that their service requires.

Note In this deployment subscribers will not be able to switch from a time-based prepaid service to a volume-based prepaid service or vice versa. In this deployment, SPs can offer both time-based and volume-based services; however, individual subscribers can access one or the other, but not both. This is done to describe the full range of ISA services available. Typically, ISPs will only deploy either time-based or volume-based services for subscribers, but not both simultaneously.

Network Topology

Figure 14 shows the network topology of this deployment.

Figure 14 Deployment Model 2 Network Topology



Call Flows

The following call flows describe the operation of the network:

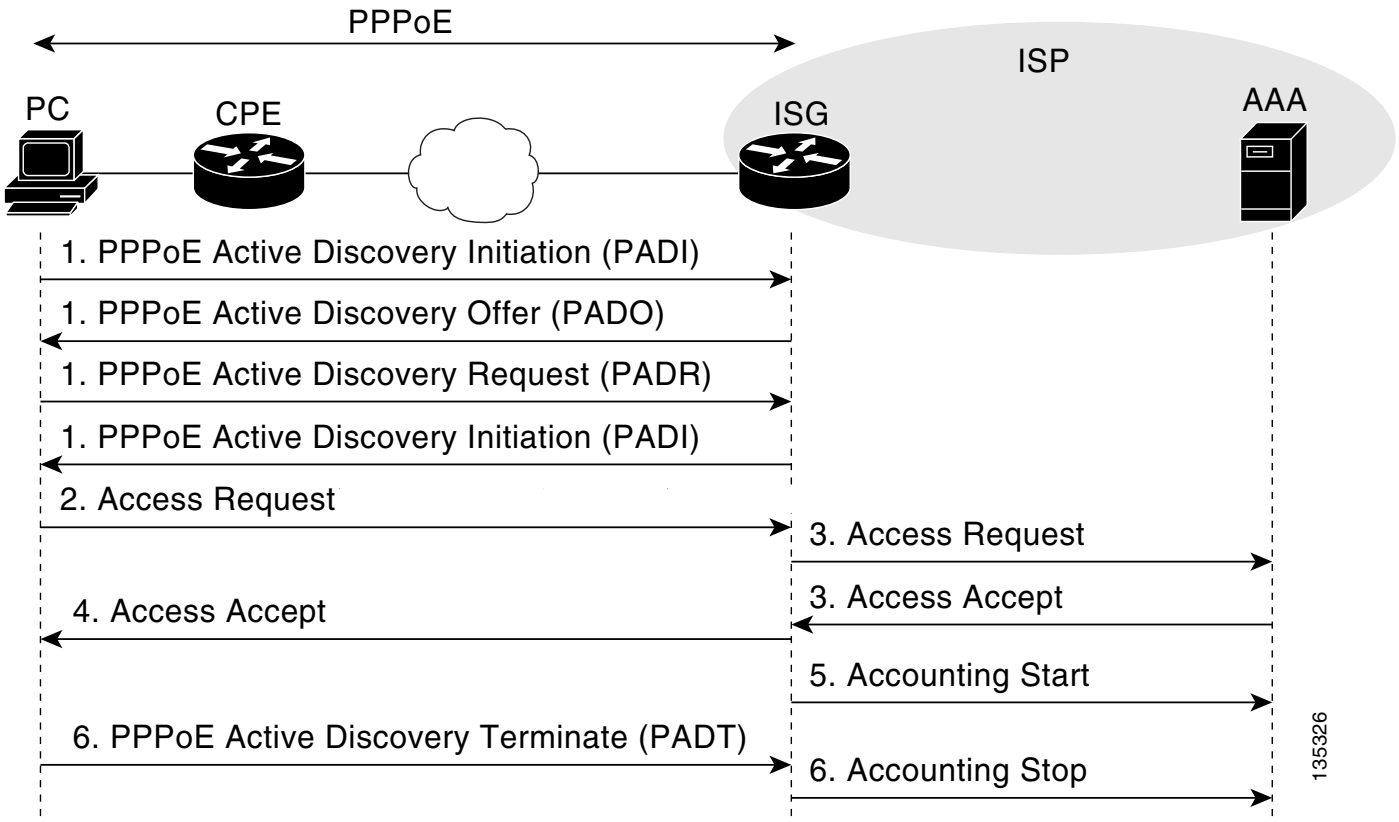
- Basic Layer 3 VPN Access Call Flow for PPPoE Sessions
- Prepaid Services Call Flow

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

Basic Layer 3 VPN Access Call Flow for PPPoE Sessions

Figure 15 shows the call flow process of establishing basic Layer 3 VPN access. Every user session begins with this process before initiating advanced ISA services.

Figure 15 Layer 3 VPN Access Call Flow



The following describes the sequence of events in Figure 15:

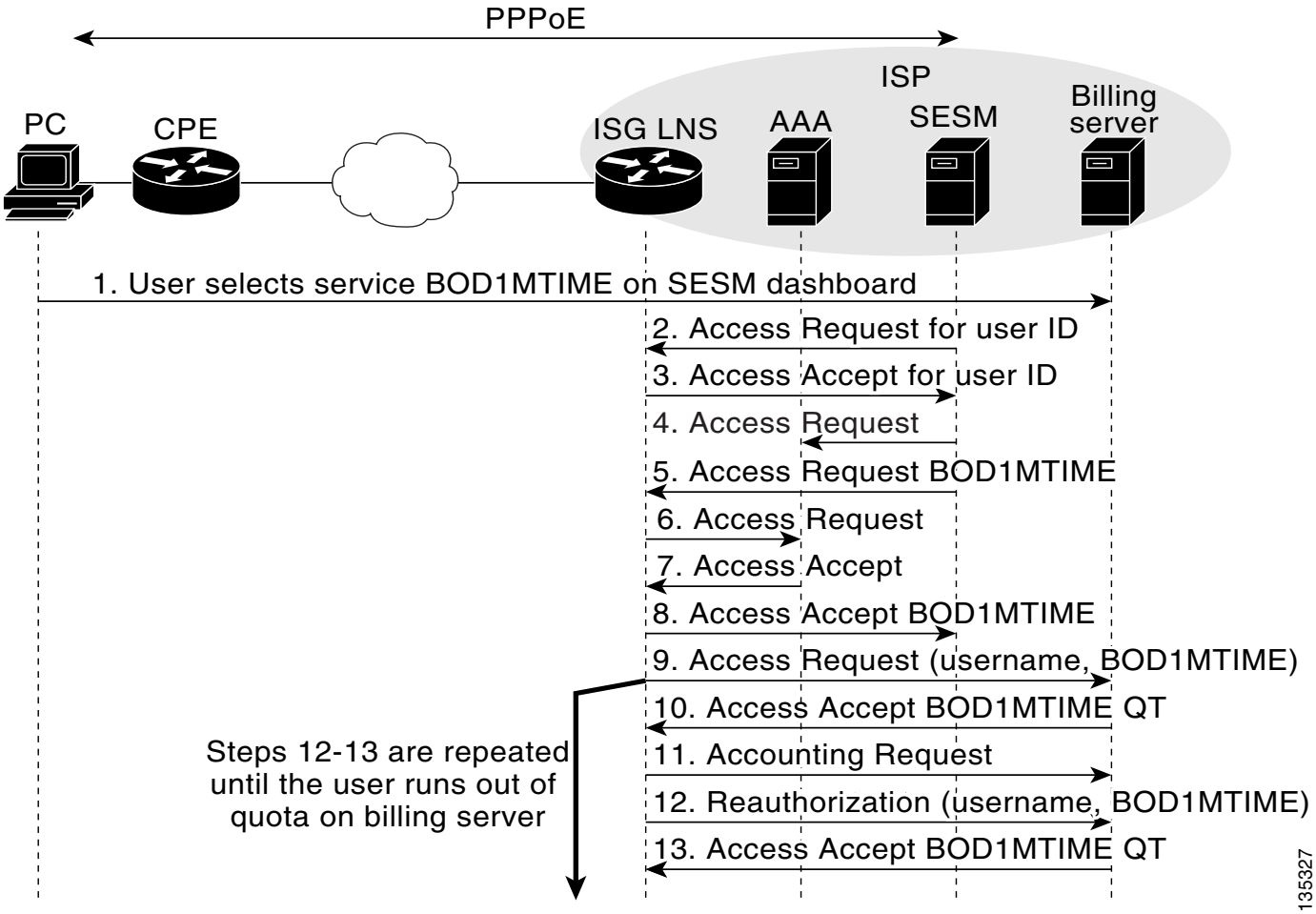
1. The subscriber initiates a PPPoE connection from the PC to the ISG by way of the CPE.
2. The client initiates the session by sending an Access-Request message to the ISG. In this deployment, the ISG is configured for auto-domain operation, and the Access-Request is not transparently forwarded to the AAA server.
3. The ISG sends the subscriber information to the AAA server. The AAA server authenticates the user and sends the ISG the appropriate service profile to the ISG.
4. After the user has been successfully authenticated, the ISG sends an Access-Accept message to the client.
5. The ISG sends an Accounting_Start message to the AAA server.
6. When the subscriber ends the session, the client sends a PPPoE Terminate message to the ISG, and the ISG terminates the session and sends an Accounting_Stop message to the AAA server.

Prepaid Services Call Flow

Figure 16 shows the call flow process of establishing prepaid services. In this example, a subscriber initiates the BOD1MTIME service.

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

Figure 16 Prepaid Services Call Flow



The following describes the sequence of events in Figure 16:

1. The subscribers selects the BOD1MTIME service on the Cisco SESM web interface.
2. The Cisco SESM sends an Access-Request message to the ISG for the subscriber's information.
3. The ISG replies to the Cisco SESM with an Access-Accept message containing the subscriber's information.
4. The Cisco SESM sends an Access-Request message to the ISG requesting information about the BOD1MTIME service.
5. The ISG sends an Access-Request message to the AAA server requesting information about the BOD1MTIME service.
6. The AAA server replies to the ISG with an access-accept message containing the traffic class, BOD1MTIME profile, and the prepaid configuration.
7. The ISG sends an Access-Accept message to the AAA server containing the details of the BOD1MTIME service.
8. The ISG sends an Access-Request message to the billing server, notifying it that the subscriber has initiated the BOD1MTIME service.

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

9. The billing server replies with an Access-Accept message that authorizes the subscriber for a set quota of time.
10. The ISG sends an accounting request to the billing server with the subscriber's username and an event timestamp.
11. After the subscriber quota is depleted, the ISG sends a re-uthorization request to renew the quota.
12. The billing server re-authorizes the subscriber and sends a renewed quota to the ISG.

Steps 8 through 12 are repeated until either the subscriber terminates the BOD1MTIME service or the subscriber runs out of quota on the billing server.

Device Characteristics Table

Table 5 describes details of the devices in the network.

Table 5 Device Characteristics for Deployment Model 2

Device	Platform	Software
CPE	Cisco 837	12.3(2)XC2
ISG	Cisco 7206 or Cisco 7301	12.2(27)SBA
PE	Cisco 6509	12.2(18)SXD1
AAA Server	UNIX server	CAR

Deployment Model 3: Triple Play Plus Service Bundle over IP and PPPoE

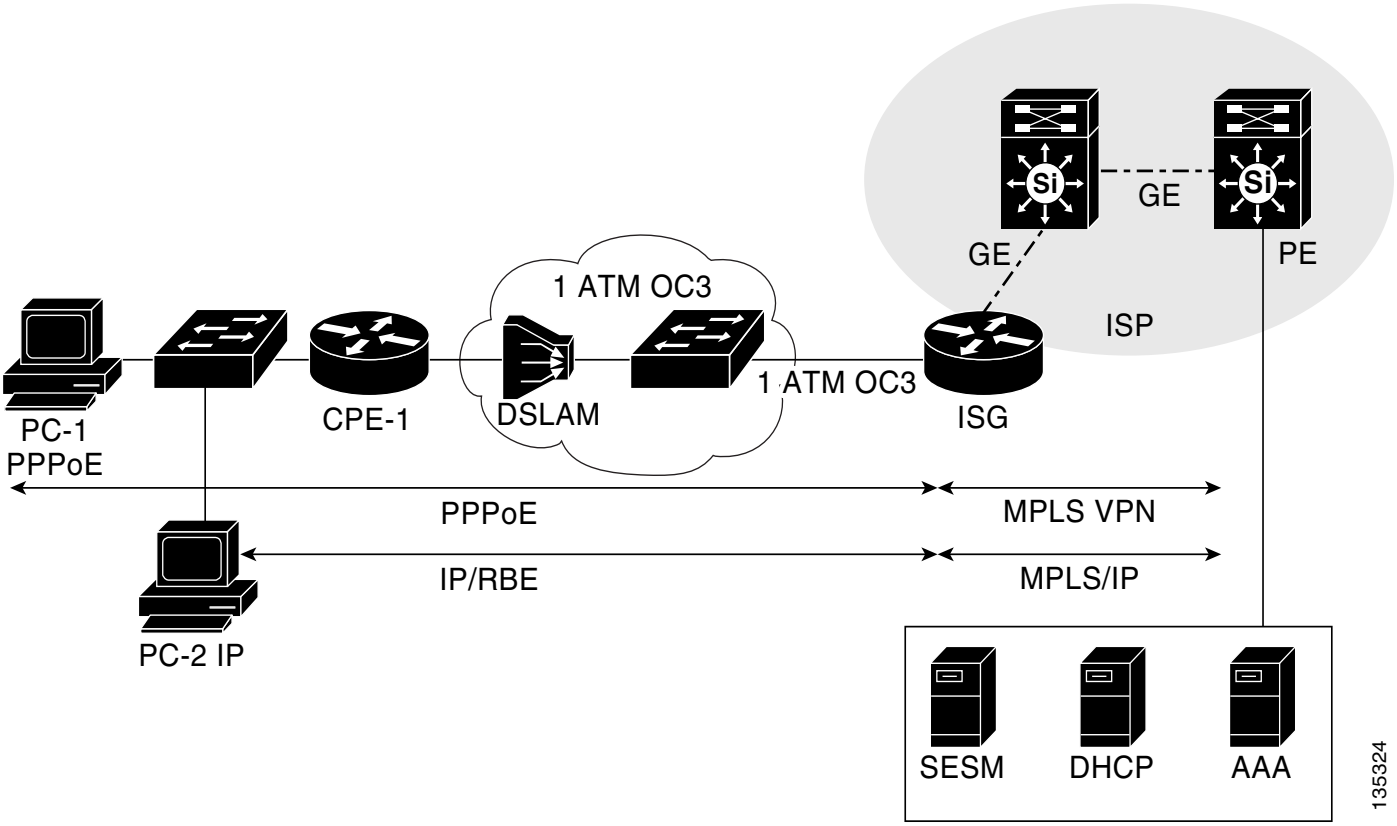
The following sections describe the deployment model:

Network Topology

Figure 17 shows the network topology of this deployment.

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

Figure 17 Deployment Model 3 Network Topology



Call Flows

The following call flows describe the operation of the network:

- Basic Layer 3 VPN Access Call Flow for PPPoE Sessions
- Basic Layer 3 VPN Access Call Flow for IP Sessions

Basic Layer 3 VPN Access Call Flow for PPPoE Sessions

For PPPoE sessions, the process of establishing basic Layer 3 VPN access is the same as the process in Deployment Model 1: Basic Internet Access Service Bundle over L2TP. For details of that process, see the "Basic Layer 3 VPN Access Call Flow for PPPoE Sessions" section.

Basic Layer 3 VPN Access Call Flow for IP Sessions

For IP Sessions, the ISA architecture supports multiple methods of authenticating the user, which lead to multiple call flows. The authentication method used depends on whether or not the ISP configures the Transparent Autologon (TAL) feature. TAL enables the ISG to authenticate subscribers on the basis either source IP address or MAC address.

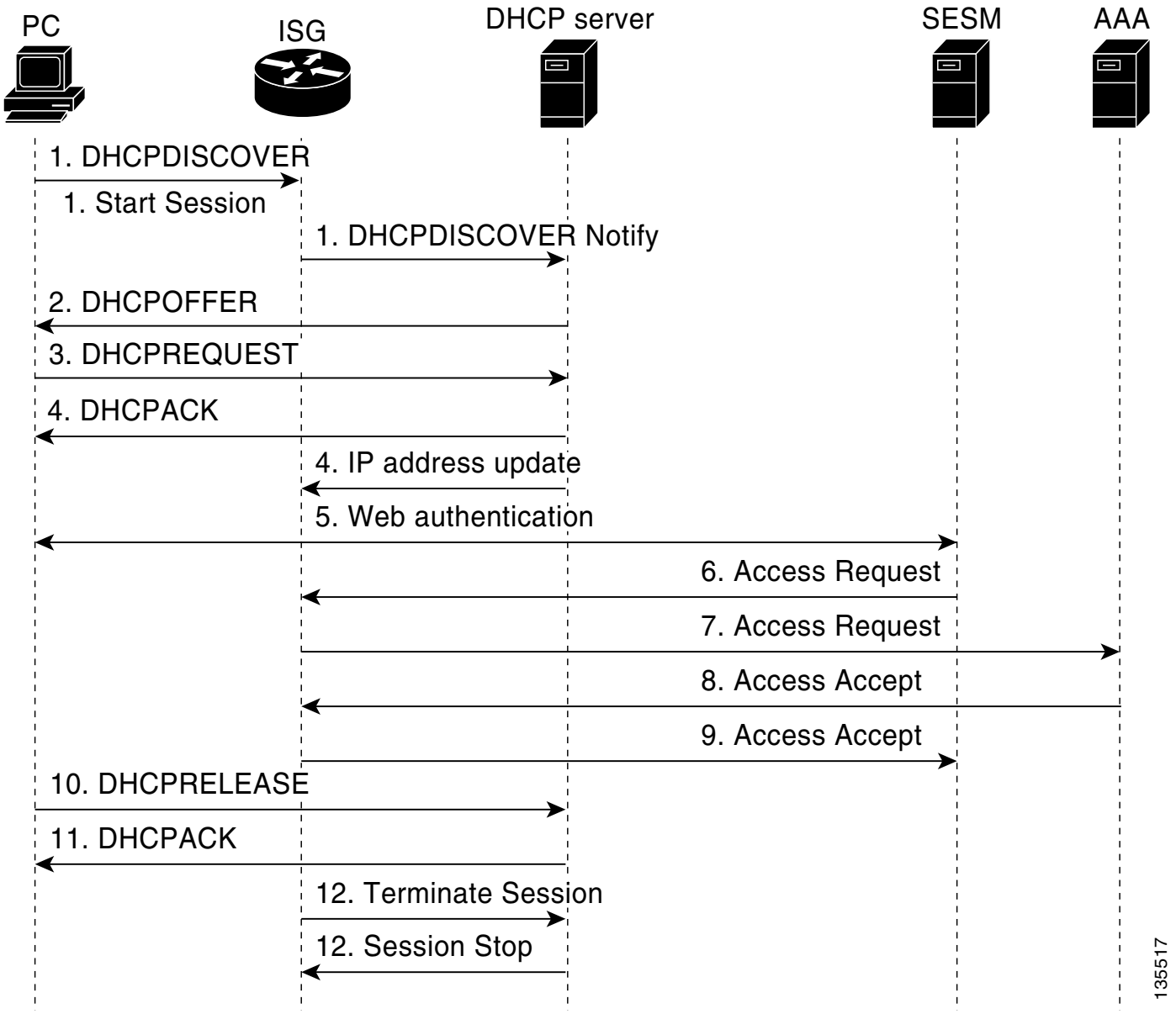
Note If DHCP is used (instead of static IP addresses), TAL can only authenticate subscribers on the basis MAC address.

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

When TAL is not enabled, subscribers are authenticated manually. When subscribers initiate a session, the ISG sends them to the Cisco SESM (using the Layer 4 Redirect feature). Subscribers then enter their usernames and passwords.

Figure 18 shows the call flow process of establishing basic Layer 3 VPN access for IP sessions with non-TAL authentication.

Figure 18 Non-TAL Layer 3 VPN Access Call Flow for IP Sessions



The following describes the sequence of events in Figure 18:

1. The client sends a DHCP Discover message to the ISG, and the sends a DHCP Discover notify message to the DHCP server. The DHCP server then creates a session and identify the class name from a default service assigned to the session, which will be used to allocate the IP address to the client. The DHCP server then sends a start session message to the ISG.

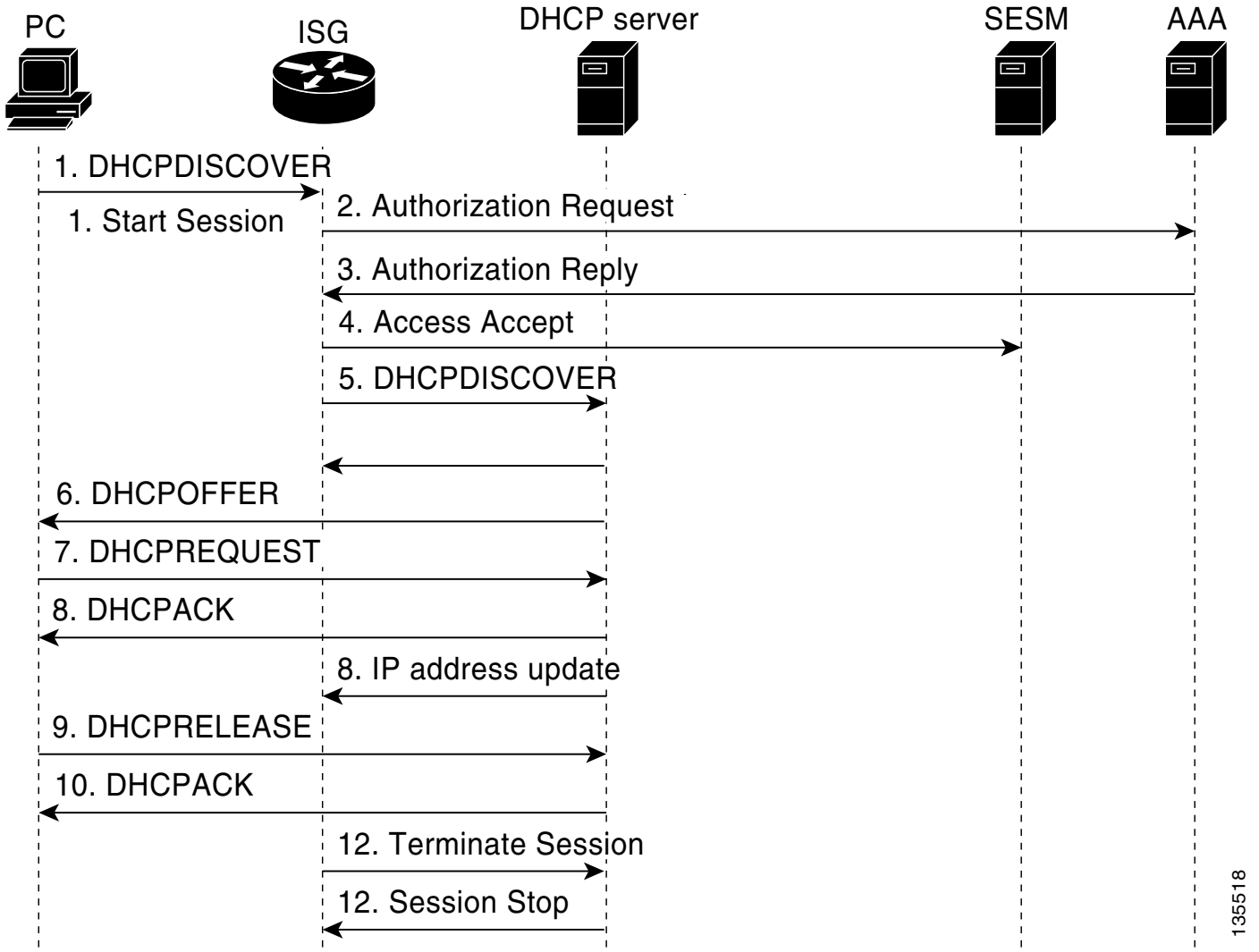
(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

2. The DHCP server sends a DHCP offer message to the client.
3. The client sends a DHCP request message to the DHCP server.
4. The DHCP server assigns the client an IP address and sends it in a DHCP ACK message to the client. The DHCP server sends an Ipaddress Update message to the ISG to notify it of the IP address allocation.
5. The subscriber's port is now allowed to connect only over HTTP to an IP address for the Cisco SESM. Other HTTP requests are sent to the Cisco SESM by the Layer 4 Redirect feature. The subscriber then enters username and password information.
6. The Cisco SESM sends the username and password to the ISG in an Access-Request message.
7. The ISG sends an Access-Request message to the AAA server.
8. The AAA server authenticates the subscriber and sends an Access-Accept message to the ISG.
9. The ISG sends an Access-Accept message to the Cisco SESM, authorizing it to begin service for the subscriber.
10. When the subscriber terminates the session, the client sends a DHCP Release message to the DHCP server.
11. The DHCP server responds with a DHCK ACK message.
12. The ISG sends a terminate session message to the DHCP server, and the DHCP server confirms that the session is ended by sending a session stop message to the ISG.

Figure 19 shows the call flow process of establishing basic Layer 3 VPN access for IP sessions with TAL authentication.

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

Figure 19 TAL-Based Layer 3 VPN Access Call Flow for IP Sessions



The following describes the sequence of events in Figure 18:

1. The client sends a DHCP Discover message to the ISG.
2. The ISG sends an Authorization Request to the AAA server.
3. The AAA server performs TAL authentication based on either the clients' IP address or MAC address and sends an Authorization Reply message to the ISG.
4. If the client is successfully authenticated, the ISG sends an Access Accept message to the Cisco SESM. If the client fails TAL authentication, the subscriber will be sent to the Cisco SESM by Layer 4 redirect to manually login.
5. The ISG sends a DHCP Discover notify message to the DHCP server. The DHCP server then creates a session and identify the class name from a default service assigned to the session, which will be used to allocate the IP address to the client. The DHCP server then sends a Start Session message to the ISG.
6. The DHCP server sends a DHCP offer message to the client.
7. The client sends a DHCP request message to the DHCP server.

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

8. The DHCP server assigns the client an IP address and sends it in a DHCP ACK message to the client. The DHCP server sends an Ipaddress Update message to the ISG to notify it of the IP address allocation.
9. When the subscriber terminates the session, the client sends a DHCP Release message to the DHCP server.
10. The DHCP serverresponds with a DHCP ACK message.
11. The ISG sends a terminate session message to the DHCP server, and the DHCP server confirms that the session is ended by sending a session stop message to the ISG.

Device Characteristics Table

Table 6 describes details of the devices in the network.

Table 6 Device Characteristics for Deployment Model 3

Device	Platform	Software
CPE	Cisco 837	12.3(2)XC2
ISG	Cisco 7206 or Cisco 7301	12.2(27)SBA
PE	Cisco 6509	12.2(18)SXD1
AAA Server	UNIX server	CAR

Deployment Model 4: Triple Play Plus Service Bundle over IP and L2TP

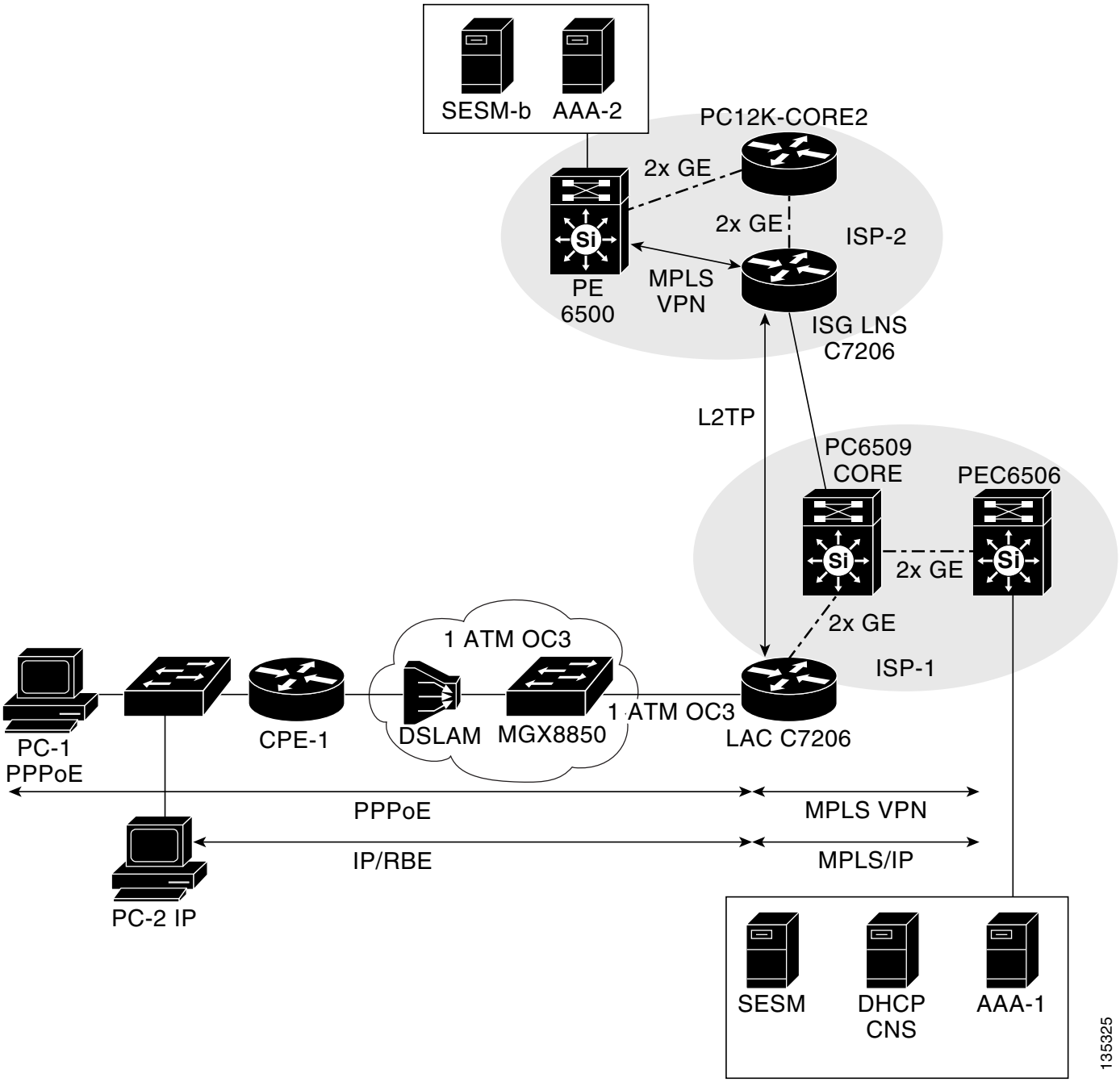
The following sections describe the deployment model:

Network Topology

Figure 20 shows the network topology of this deployment.

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

Figure 20 Deployment Model 4 Network Topology



Call Flows

The following call flows describe the operation of the network.

Basic Layer 3 VPN Access Call Flow for IP Sessions

For IP sessions, the process of establishing basic Layer 3 VPN access is the same as the process in Deployment Model 2: Multiservice Service Bundle over PPPoE. For details of that process, see the "Basic Layer 3 VPN Access Call Flow for IP Sessions" section.

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

Basic Layer 3 VPN Access Call Flow for L2TP Sessions

For L2TP session, the process of establishing basic Layer 3 VPN access is the same as the process in Deployment Model 1: Basic Internet Access Service Bundle over L2TP. For details of that process, see the "Basic Layer 3 VPN Access Call Flow for L2TP Sessions" section.

Device Characteristics Table

Table 7 describes details of the devices in the network.

Table 7 Device Characteristics for Deployment Model 3

Device	Platform	Software
CPE	Cisco 837	12.3(2)XC2
ISG LAC	Cisco 7206	12.2(27)SBA
LNS	Cisco 7206	12.2(27)SBA
PE	Cisco 6509	12.2(18)SXD1
AAA for ISP1	UNIX server	CAR
AAA for ISP2	UNIX Server	CAR

Configuring the Network

The configuration of this deployment is divided into the following sections:

- Prerequisites, page 28
- Baseline Configuration, page 29
- Deployment Model 1: Basic Internet Access Service Bundle over L2TP Configuration, page 31
- Deployment Model 2: Multiservice Service Bundle over PPPoE, page 37
- Deployment Model 3: Triple Play Plus Service Bundle over IP and PPPoE, page 46
- Deployment Model 4: Triple Play Plus Service Bundle over IP and L2TP, page 53

Prerequisites

Before the ISA configuration begins, the following baseline network operations must be configured:

- Basic IP connectivity must be established across the entire network
- L2TP must be configured between the ISG LAC and LNS
- Subscribers must be able to establish a PPPoE connection over the L2TP tunnel to the LNS.

Network administrators should be familiar with the following topics:

- CAR configuration procedure:
  http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cnsar/3_5/install/config.htm
- CNR configuration procedure:
  http://www.cisco.com/en/US/products/sw/netmgtsw/ps1982/products_user_guide_book09186a008022745c.html

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

- Basic broadband (PPP and L2TP) configuration:
  - http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca72a.html
  - http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca724.html
  - http://www.cisco.com/en/US/partner/tech/tk801/tk703/technologies_configuration_example09186a0080093c2a.shtml

Baseline Configuration

The following devices are configured to enable baseline network operation. The baseline configuration establishes basic connectivity across the network and enables the user to establish basic Layer 3 VPN access.

- CPE Configuration for PPPoE Deployments, page 29
- CPE Configuration for IP Deployments, page 30
- PE, page 31

CPE Configuration for PPPoE Deployments

This configuration is for the CPE when used in the PPPoE deployments (Deployment Models 1 and 2). The following baseline configuration tasks are performed on the CPE:

- Configuring the Ethernet Interface and DHCP
- Configuring the Outbound Interface
- Configuring the Dialer Interface and NAT

Configuring the Ethernet Interface and DHCP

Interface Ethernet 0 is configured to connect to the user PC, and DHCP is enabled for incoming sessions.

```
interface Ethernet0
 ip address 10.10.10.1 255.255.255.0
 ip nat inside
 load-interval 30
 ip tcp adjust-mss 1452
 hold-queue 100 out
!

ip dhcp excluded-address 10.10.10.1
!
! DHCP configuration for interface Ethernet 0 users
ip dhcp pool CLIENT
   import all
   network 10.10.10.0 255.255.255.0
   default-router 10.10.10.1
   lease 0 2
```

Configuring the Outbound Interface

ATM interface 0.5 is configured as a PVC. This is the outbound interface from the CPE to the DSLAM.

```
interface ATM0.5 point-to-point
! This is the PVC which is going to the ATM DSLAM
  pvc 5/45
 pppoe max-sessions 100
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
! This associates the PVC with dialer 1
  pppoe-client dial-pool-number 1
```

Configuring the Dialer Interface and NAT

Dialer interface 1 is configured to receive incoming connections from the user. CHAP is used for the CPE's username and password, and NAT is enabled for outbound traffic.

```
interface Dialer1
 ip address negotiated
 ip nat outside
! using PPP
 encapsulation ppp
 ip route-cache flow
 dialer pool 1
 dialer-group 1
 ppp authentication chap callin
!The username and password are set for CHAP
 ppp chap hostname C73_DM1_01@L2TP_DM1_101.com
 ppp chap password 0 lab
!
! Enables users on the inside of E0 to access outside using NAT
ip nat inside source list 23 interface Dialer1 overload
!
ip classless
! set the default gateway out the dialer 1 interface
ip route 0.0.0.0 0.0.0.0 Dialer1

!
! allow E0 users to be NAT translated
access-list 23 permit 10.10.10.0 0.0.0.255
```

CPE Configuration for IP Deployments

The following configuration is for the CPE when used in the IP deployments (Deployment Models 3 and 4). This configures the CPE to bridge subscriber sessions from the user PC on to the DSLAM. IP routing is disabled, and a bridge group is configured on the outbound interface (interface ATM 0.3).

```
! Disabling IP routing instructs the CPE to bridge IP traffic.
no ip routing

interface Ethernet0
 no ip address
 no ip route-cache
 load-interval 30
 bridge-group 1
 hold-queue 100 out


interface ATM0
 no ip address
 no ip route-cache
 load-interval 30
 no atm ilmi-keepalive
 dsl operating-mode auto
!
! This is the outbound interface to the DSLAM.
interface ATM0.3 point-to-point
 no ip route-cache
 pvc 3/43
  encapsulation aal5snap
!
!Bridge group 1 is configured on the interface.
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
 bridge-group 1
!
interface Dialer1
 ip address negotiated
 ip nat outside
 encapsulation ppp
 dialer pool 1
 dialer-group 1
 ppp authentication chap callin
 ppp chap hostname C73_DM4_01@L2TP_DM4_101.com
 ppp chap password 0 lab
```

PE

The following basic configuration is required for all four of the deployment models. First, the PE is configured to assign subscribers to a VRF and to allow users to access the Cisco SESM.

```
! Configures the VRF to which subscribers are assigned.
ip vrf VPN10003
 rd 100:3
 route-target export 100:3
 route-target import 100:3
!
!
router bgp 100
 no synchronization
 bgp router-id 10.200.1.45
 bgp log-neighbor-changes
 redistribute connected
 redistribute static
 neighbor 10.200.1.41 remote-as 100
 neighbor 10.200.1.41 update-source Loopback0
 no auto-summary
!
!
! Allows VRF routes into the BGP routing table.
 address-family ipv4 vrf VPN10003
 redistribute connected
 redistribute static
 no auto-summary
 no synchronization
 network 42.2.103.0 mask 255.255.255.0
 aggregate-address 42.2.103.0 255.255.255.0 summary-only
 exit-address-family
!
!
! Redistributes a route for subscribers in VRF VPN10003 from the global routing table into
! the VRF routing domain. This route is used for subscribers to access the Cisco SESM.
! This command is only necessary when the PBHK feature is enabled.
ip route vrf VPN10003 10.100.3.34 255.255.255.255 GigabitEthernet3/14 10.100.3.34
```

Deployment Model 1: Basic Internet Access Service Bundle over L2TP Configuration

The following devices are configured to enable the Basic Internet Access Service Bundle over L2TP deployment model:

- Deployment Model 1: ISG LAC, page 32
- Deployment Model 1: AAA Server for ISP-1, page 33
- Deployment Model 1: LNS, page 34
- Deployment Model 1: AAA Server for ISP-2, page 37

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

Deployment Model 1: ISG LAC

The following baseline configuration tasks are performed on the ISG LAC:

- Configuring AAA and the Connection to the RADIUS Server
- Configuring the Connection to the LNS and PPPoE

Configuring AAA and the Connection to the RADIUS Server

A basic AAA configuration is entered, and the connection to the RADIUS server is configured, including vendor-specific attribute (VSA) accounting and authentication.

```
aaa new-model
!
! Configures the connection to the AAA server and identifies it as CAR_SERVER
aaa group server radius CAR_SERVER
 server 10.100.1.35 auth-port 1812 acct-port 1813
!
aaa authentication login default none
! Configures the AAA server for authentication, authorization, and accounting.
aaa authentication login IP_AUTHEN_LIST group CAR_SERVER
aaa authentication ppp default group CAR_SERVER
aaa authorization network default group CAR_SERVER
aaa authorization subscriber-service default local group radius
aaa accounting network default start-stop group CAR_SERVER
!
aaa session-id common
!
!
interface Loopback0
 ip address 10.200.1.53 255.255.255.255
!
! Use Loopback 0 to communicate with radius server
ip radius source-interface Loopback0
!
!
radius-server host 10.100.1.35 auth-port 1812 acct-port 1813 key cisco
radius-server retransmit 5
radius-server timeout 15
radius-server vsa send accounting
radius-server vsa send authentication
```

Configuring the Connection to the LNS and PPPoE

The connection to the LNS is configured. The ISG LAC uses VPDN to initiate L2TP tunnels to the LNS, which are used to carry the subscriber PPPoE sessions. An ISA control policy map is used to instruct L2TP to authenticate on the basis domain name, and a BBA group is used to configure PPPoE.

```
no ip dhcp use vrf connected
!
! This command is enabled by default. It sets the number of ISA rules that are displayed
! in the show subscriber session detail command.
subscriber policy recording rules limit 64
subscriber authorization enable

! Enables VPDN globally, which is used for PPPoE.
vpdn enable
vpdn ip udp ignore checksum
vpdn search-order domain
!
no mpls traffic-eng auto-bw timers frequency 0
call rsvp-sync
!
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
!
! This control policy map instructs L2TP to authenticate based on domain name.
policy-map type control RULE_L2TP_LM_ATM3
 class type control always event session-start
  1 collect identifier unauthenticated-domain
  2 authorize identifier unauthenticated-domain
!
!
! The BBA group method is used to configure PPPoE (alternatively, the vpdn-group
! method could be used).
bba-group pppoe BBA_LM_ATM3
 virtual-template 3
!
! This virtual circuit (VC) class is applied to the ATM PVC.
vc-class atm VC_LM_ATM3
! Associates the VC class with the above bba-group.
  protocol pppoe group BBA_LM_ATM3
! Enables dynamic bandwidth selection.
  dbs enable maximum
  encapsulation aal5snap
! Applies the L2TP rule above to the VC class.
  service-policy type control RULE_L2TP_LM_ATM3
!
! Interface Gigabit Ethernet 0/3 points to the LNS.
interface GigabitEthernet0/3
 ip address 40.40.1.53 255.255.255.0
 load-interval 30
 duplex full
 speed 1000
 media-type gbic
 negotiation auto
 mpls mtu 1522
 mpls ip
 ip rsvp bandwidth 100000
!
!
interface ATM1/0.101 multipoint
 description ATM Deployment Model 1
 no atm enable-ilmi-trap
 pvc 101/41
! The VC class is associated with the PVC.
  class-vc VC_LM_ATM3
!
!
! The PPP CHAP configuration is entered on the virtual template.
interface Virtual-Template3
 description VT for LM_ATM3
 no ip address
 no peer default ip address
 no keepalive
 ppp authentication chap
 ppp timeout aaa
```

Deployment Model 1: AAA Server for ISP-1

The following profile configures L2TP forwarding from the ISG LAC to the LNS. The IP address 10.200.1.56 is the address of the loopback interface on the LNS.

```
[ //localhost/Radius/UserLists/L2TPDOMAIN/L2TP_DM1_101.com/Attributes ]
    Cisco-AVpair = vpdn:tunnel-id=L2TP_DM1_101
    Cisco-AVpair = vpdn:l2tp-tunnel-password=cisco
    Cisco-AVpair = vpdn:tunnel-type=l2tp
    Cisco-AVpair = vpdn:ip-addresses=10.200.1.56
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
Cisco-AVpair = atm:peak-cell-rate=1024
Cisco-AVpair = atm:sustainable-cell-rate=512
```

Deployment Model 1: LNS

The following baseline configuration tasks are performed on the LNS:

- Configuring AAA and the Connection to the RADIUS Server
- Configuring PPPoE and the Connection to the ISG LAC
- Configuring Baseline ISA Subscriber Services
- Configuring Inbound and Outbound Access Lists

Configuring AAA and the Connection to the RADIUS Server

In this AAA configuration, connections to the CAR AAA server, the Cisco SESM, and two billing servers are configured. VSA accounting and authentication are enabled, and the loopback interface 0 is used for AAA communications.

```
aaa new-model
!
! Configures the AAA server group for the CAR AAA server.
aaa group server radius CAR_SERVER
 server 10.100.2.36 auth-port 1812 acct-port 1813
!

! Configures AAA for the CAR AAA server.
aaa authentication login default none
aaa authentication login IP_AUTHEN_LIST group CAR_SERVER
aaa authentication ppp default group CAR_SERVER
aaa authorization network default group CAR_SERVER
aaa authorization subscriber-service default local group radius
aaa accounting network default start-stop group CAR_SERVER
! Configures the connection to the Cisco SESM
aaa server radius sesm
 client 10.100.4.38
 key cisco
 port 1812
 message-authenticator ignore
!

! Loopback 0 is used for communicating with AAA, the billing servers, and SESM.
interface Loopback0
 ip address 10.200.1.56 255.255.255.255
 ip router isis Remote_ISP_7301

! Instructs the router to use loopback 0 to communicate with the AAA RADIUS servers.
ip radius source-interface Loopback0
!
! The CAR AAA server.
radius-server host 10.100.2.36 auth-port 1812 acct-port 1813 key Cisco
radius-server retransmit 5
radius-server key cisco
radius-server vsa send accounting
radius-server vsa send authentication
```

Configuring PPPoE and the Connection to the ISG LAC

VPDN is configured to receive L2TP tunnels from the ISG LAC over which the PPPoE sessions are sent. A PPP local pool and MPLS virtual routing forwarding (VRF) tables are created for incoming subscribers.

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
no ip dhcp use vrf connected
!
! Globally enables MPLS VRFs for incoming subscribers.
ip vrf VPN_C72_DM1_1001
 rd 200:1001
 route-target export 200:1001
 route-target import 200:1001
!
!
ip cef
!
vpdn enable
vpdn ip udp ignore checksum
!
! VPDN group L2TP_DM1_101 terminates PPPoE clients that come in from the ISG LAC over L2TP
! tunnels.
vpdn-group L2TP_DM1_101
 accept-dialin
  protocol l2tp
  virtual-template 5
 terminate-from hostname L2TP_DM1_101
 local name L2TP_DM1_101
 l2tp tunnel password 0 cisco
!
!

! Gigabit Ethernet interface 0/1 points to the PE.
interface GigabitEthernet0/1
 ip address 27.27.1.56 255.255.255.0
! The PBHK feature is enabled on this interface.
 ip portbundle outside
 ip router isis Remote_ISP_7301
 load-interval 30
 duplex auto
 speed auto
 media-type gbic
 negotiation auto
 mpls label protocol ldp
 mpls ip
!
! Gigabit Ethernet interface 0/2 points to the ISG LAC.
interface GigabitEthernet0/2
 ip address 26.26.1.56 255.255.255.0
 ip router isis Remote_ISP_7301
 load-interval 30
 duplex auto
 speed auto
 media-type gbic
 negotiation auto
!
! PPPoE subscribers terminated from L2TP tunnels use this virtual template.
interface Virtual-Template5
 no ip address
 load-interval 30
 no peer default ip address
 no keepalive
 ppp mtu adaptive
 ppp authentication chap
!
! The DHCP pool that is assigned to subscribers.
ip local pool C73_DM1_3001 1.3.1.2 1.3.255.254
!
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

Configuring Baseline ISA Subscriber Services

Basic ISA subscriber services are configured, including Layer 4 redirect to the Cisco SESM and the PBHK feature. When the PBHK feature is enabled, TCP packets from subscribers are mapped to a local IP address for the ISA gateway and a range of ports. This mapping allows the portal to identify the ISA gateway from which the session originated. The PBHK mapping only occurs when the Layer 4 traffic matches the access list configured under the **ip portbundle** command.

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

! Configures the connection to the Cisco SESM for Layer 4 Redirect functionality.
redirect server-group SESM-Server
 server ip 10.100.4.38 port 8080
!
!
! This command is enabled by default. It sets the number of ISA rules that are displayed
! in the show subscriber session detail command.
subscriber policy recording rules limit 64

! Enables port bundle host key (PBHK) access to the Cisco SESM. Each loopback interface
! can support up to 4031 bundles. If additional capacity is required, configure additional
! loopback interfaces.
ip portbundle
 match access-list 135
! The Loopback 0 interface is used to communicate with the Cisco SESM.
 source Loopback0
```

Configuring Inbound and Outbound Access Lists

Basic access lists are configured to govern subscribers' Internet access, and an access list is created for the PBHK feature.

```
! This access list is referenced in the AAA subscriber profile. It governs incoming
! Internet traffic. The Internet access lists should prevent subscribers from accessing
! the Cisco SESM and other management devices to help prevent Denial of Service attacks.
!
ip access-list extended Internet-in-acl
 deny   ip any 223.0.0.0 0.255.255.255
 deny   ip any 20.0.0.0 0.255.255.255
 deny   ip any 40.0.0.0 0.255.255.255
 deny   ip any 21.0.0.0 0.255.255.255
 deny   ip any 22.0.0.0 0.255.255.255
 deny   ip any 41.0.0.0 0.255.255.255
 deny   ip any 80.0.0.0 0.255.255.255
 deny   ip any 81.0.0.0 0.255.255.255
 deny   ip any 82.0.0.0 0.255.255.255
 deny   ip any 10.200.0.0 0.0.255.255
 permit ip any any
!
! This access list is called out in the AAA subscriber profile. It governs outgoing
! Internet traffic. The Internet access lists should prevent subscribers from accessing
! the Cisco SESM and other management devices to help prevent Denial of Service attacks.
!
ip access-list extended Internet-out-acl
 deny   ip 223.0.0.0 0.255.255.255 any
 deny   ip 10.200.0.0 0.0.255.255 any
 deny   ip 20.0.0.0 0.255.255.255 any
 deny   ip 40.0.0.0 0.255.255.255 any
 deny   ip 21.0.0.0 0.255.255.255 any
 deny   ip 22.0.0.0 0.255.255.255 any
 deny   ip 41.0.0.0 0.255.255.255 any
 deny   ip 80.0.0.0 0.255.255.255 any
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
 deny   ip 81.0.0.0 0.255.255.255 any
 deny   ip 82.0.0.0 0.255.255.255 any
 permit ip any any
!
! This access list is used in the ip portbundle configuration above.
access-list 135 permit ip any host 10.100.4.38
access-list 135 deny ip any any
```

Deployment Model 1: AAA Server for ISP-2

The following baseline configuration tasks are performed on the AAA server for ISP-2:

- Configuring Layer 4 Redirect
- Configuring PBHK
- Configuring the Basic Internet Access ISA Subscriber Service
- Configuring the Subscriber's Profile

Configuring Layer 4 Redirect

The following attribute enables the Layer 4 Redirect feature.

```
[ Attributes ]
! Instructs Layer 4 redirect to send traffic to ACL 111 on the LNS.
    Cisco-AVPair = "ip:l4redirect=redirect list 111 to group SESM-Server duration 30
frequency 180"
```

Configuring PBHK

The following attribute enable the PBHK feature on the AAA server, which enables access to the SESM by way of the PBHK feature.

```
[ Attributes ]
    Cisco-AVPair = ip:portbundle=enable
```

Configuring the Basic Internet Access ISA Subscriber Service

The following profile configures the basic Internet access service.

```
[ //localhost/Radius/UserLists/SERVICES/INTERNET_SERVICE/Attributes ]
! Specifies the ACLs that govern this service.
    Cisco-AVPair = ip:inacl=Internet-in-acl
    Cisco-AVPair = ip:outacl=Internet-out-acl
! The "I" before "INTERNET_SERVICE" tells the Cisco SESM what the name of the service is.
! The Cisco SESM will display this service by the name "INTERNET_SERVICE".
    Cisco-SSG-Service-Info = IINTERNET_SERVICE
! The "R" in this attribute identifies this as a service to the Cisco SESM.
    Cisco-SSG-Service-Info = R42.1.1.0;255.255.255.0
```

Configuring the Subscriber's Profile

This profile configures the PPP profile that is used in the subscriber's base profile.

```
[ //localhost/Radius/UserLists/ie2-C7301-LNS/C73_DM1_01@L2TP_DM1_101.com/Attributes ]
    Cisco-AVpair = "ip:ip-unnumbered=loopback 3001"
    Cisco-AVpair = ip:addr-pool=C73_DM1_3001
    Cisco-SSG-Account-Info = AINTERNET_SERVICE
```

Deployment Model 2: Multiservice Service Bundle over PPPoE

The following devices are configured to enable Deployment Model 2: Multiservice Service Bundle over PPPoE deployment model:

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

Deployment Model 2: ISG Baseline Configuration

The following baseline configuration tasks are performed on the LNS:

- Configuring AAA and the Connection to the RADIUS Server
- Configuring PPPoE and the Connections to the CPE and PE
- Configuring Baseline ISA Subscriber Services
- Configuring Inbound and Outbound Access Lists

Configuring AAA and the Connection to the RADIUS Server

In this AAA configuration, connections to the CAR AAA server, the Cisco SESM, and two billing servers are configured. VSA accounting and authentication are enabled, and the loopback interface 0 is used for AAA communications.

```
aaa new-model
!
! Configures the AAA server group for the CAR AAA server.
aaa group server radius CAR_SERVER
 server 10.100.2.36 auth-port 1812 acct-port 1813
!
! Configures the AAA server group for the RSIM_SERVER billing server.
aaa group server radius RSIM_SERVER
 server 10.100.12.89 auth-port 1645 acct-port 1646


! Configures AAA for the CAR AAA server.
aaa authentication login default none
aaa authentication ppp default group CAR_SERVER
! Configures authentication for prepaid customers on the RSIM_SERVER billing server.
aaa authentication ppp PREPAID_AUTHEN_LIST group RSIM_SERVER
aaa authorization network default group CAR_SERVER
! Configures authorization for prepaid customers on the RSIM_SERVER billing server.
aaa authorization network PREPAID_AUTHOR_LIST group RSIM_SERVER
aaa authorization subscriber-service default local group radius
aaa accounting network default start-stop group CAR_SERVER
! Configures accounting for prepaid customers on the RSIM_SERVER billing server.
aaa accounting network PREPAID_ACCNT_LIST start-stop group RSIM_SERVER
! Configures the connection to the Cisco SESM
aaa server radius sesm
 client 10.100.4.38
 key cisco
 port 1812
 message-authenticator ignore
!

! Loopback 0 is used for communicating with AAA, the billing servers, and SESM.
interface Loopback0
 ip address 10.200.1.53 255.255.255.255

! Instructs the router to use loopback 0 to communicate with the AAA RADIUS servers.
ip radius source-interface Loopback0
!
! These RADIUS attributes are required for prepaid services.
radius-server attribute 44 include-in-access-req
radius-server attribute 8 include-in-access-req
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
radius-server attribute 55 access-request include
radius-server attribute 25 access-request include
! The CAR AAA server.
radius-server host 10.100.1.35 auth-port 1812 acct-port 1813 key cisco
! The RSIM_SERVER billing server.
radius-server host 10.100.12.89 auth-port 1645 acct-port 1646 key cisco
radius-server retransmit 5
radius-server timeout 15
radius-server vsa send accounting
radius-server vsa send authentication
```

Configuring PPPoE and the Connections to the CPE and PE

The LNS is configured to receive PPPoE sessions from the CPE by way of the DSLAM. A PPP local pool and MPLS VRF tables are created for incoming subscribers.

```
no ip dhcp use vrf connected
!
! Globally enables MPLS VRFs for incoming subscribers.
ip vrf VPN10005
 rd 100:5
 route-target export 100:5
 route-target import 100:5!
!
ip cef
!
!
! The BBA group method is used to configure PPPoE.
bba-group pppoe BBA_LM_ATM5
 virtual-template 8
 sessions per-vc limit 1
!
! This virtual circuit (VC) class is applied to the ATM PVC.
vc-class atm VC_LM_ATM8
! Associates the VC class with the above bba-group.
  protocol pppoe group BBA_LM_ATM8
! Enables dynamic bandwidth selection.
  dbs enable maximum
  encapsulation aal5snap
!

! Gigabit Ethernet interface 0/3 points to the PE.
interface GigabitEthernet0/3
 ip address 40.40.1.53 255.255.255.0
! The PBHK feature is enabled on this interface.
 ip portbundle outside
 load-interval 30
 duplex full
 speed 1000
 media-type gbic
 negotiation auto
 mpls mtu 1522
 mpls ip
 service-policy output QOS_OUT_MPLS_UPLINK
 ip rsvp bandwidth 100000
!
! ATM interface 1/0.105 points to the CPE.
interface ATM1/0.105 point-to-point
 description Deployment Model 2
 atm pppatm passive
 no atm enable-ilmi-trap
 pvc 105/45
! The VC class is associated with the PVC.
  class-vc VC_LM_ATM8
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
! This can be changed to restrict PPPoE sessions on the PVC.
  pppoe max-sessions 1
!
! PPPoE subscribers use this virtual template.
interface Virtual-Template8
 description LM ATM8 PTA Subscriber
 no ip address
 no peer default ip address
 no keepalive
 ppp timeout authentication 100
 ppp timeout aaa
 load-interval 30
 ppp mtu adaptive
 ppp authentication chap
 service-policy control RULE_PTA_LM_ATM8
!
! The DHCP pool that is assigned to subscribers.
ip local pool cpe3_pool-53-VPN10005 200.53.3.210 200.53.3.250
```

Configuring Baseline ISA Subscriber Services

Basic ISA subscriber services are configured, including Layer 4 redirect to the Cisco SESM and the PBHK feature. When the PBHK feature is enabled, TCP packets from subscribers are mapped to a local IP address for the ISA gateway and a range of ports. This mapping allows the portal to identify the ISA gateway from which the session originated.

```
! Configures the connection to the Cisco SESM for Layer 4 Redirect functionality.
redirect server-group SESM-Server
 server ip 10.100.4.38 port 8080
!
!

! Enables port bundle host key (PBHK) access to the Cisco SESM. Each loopback interface
! can support up to 4031 bundles. If additional capacity is required, configure additional
! loopback interfaces.
ip portbundle
 match access-list 135
! The Loopback 0 interface is used to communicate with the Cisco SESM.
 source Loopback0
!
!
! This command is enabled by default. It sets the number of ISA rules that are displayed
! in the show subscriber session detail command.
subscriber policy recording rules limit 64
```

Configuring Inbound and Outbound Access Lists

Basic access lists are configured to govern subscribers' Internet access, and an access list is created for the PBHK feature.

```
! This access list is referenced in the AAA subscriber profile. It governs incoming
! Internet traffic. The Internet access lists should prevent subscribers from accessing
! the Cisco SESM and other management devices to help prevent Denial of Service attacks.
!
ip access-list extended Internet-in-acl
 deny   ip any 223.0.0.0 0.255.255.255
 deny   ip any 20.0.0.0 0.255.255.255
 deny   ip any 40.0.0.0 0.255.255.255
 deny   ip any 21.0.0.0 0.255.255.255
 deny   ip any 22.0.0.0 0.255.255.255
 deny   ip any 41.0.0.0 0.255.255.255
 deny   ip any 80.0.0.0 0.255.255.255
 deny   ip any 81.0.0.0 0.255.255.255
 deny   ip any 82.0.0.0 0.255.255.255
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
 deny   ip any 84.0.0.0 0.255.255.255
 deny   ip any 10.200.0.0 0.0.255.255
 permit ip any any
!
! This access list is called out in the AAA subscriber profile. It governs outgoing
! Internet traffic. The Internet access lists should prevent subscribers from accessing
! the Cisco SESM and other management devices to help prevent Denial of Service attacks.
!
ip access-list extended Internet-out-acl
 deny   ip 223.0.0.0 0.255.255.255 any
 deny   ip 10.200.0.0 0.0.255.255 any
 deny   ip 20.0.0.0 0.255.255.255 any
 deny   ip 40.0.0.0 0.255.255.255 any
 deny   ip 21.0.0.0 0.255.255.255 any
 deny   ip 22.0.0.0 0.255.255.255 any
 deny   ip 41.0.0.0 0.255.255.255 any
 deny   ip 80.0.0.0 0.255.255.255 any
 deny   ip 81.0.0.0 0.255.255.255 any
 deny   ip 82.0.0.0 0.255.255.255 any
 deny   ip 84.0.0.0 0.255.255.255 any
 permit ip any any
!
! This access list is used in the ip portbundle configuration above. It only permits
! traffic to the Cisco SESM.
access-list 135 permit ip any host 10.100.4.38
access-list 135 deny ip any any
```

Deployment Model 2: ISG Configuration for ISA Services

The following configuration tasks are performed on the LNS to enable the advanced ISA subscriber services:

- Configuring the Global Prepaid Services Configuration
- Configuring the BOD1MTIME Service
- Configuring the BOD2MTIME Service
- Configuring the BOD1MVOLUME Service
- Configuring the BOD2MVOLUME Service

Configuring the Global Prepaid Services Configuration

The global attributes of the prepaid services are configured for each of the two billing servers.

```
! This is the global configuration for the PREPAID_RSIM prepaid billing server.
subscriber feature prepaid PREPAID_RSIM
   threshold time 20 seconds
! Specifies the size of the threshold the ISG requests from the billing server. The
! threshold is an increment of the user's quota. When the threshold  (in this case 1000
! bytes) is exhausted, the ISG requests another 1000 bytes from the subscriber's account.
! This continues until the subscriber terminates the session, or the subscriber's account
! is depleted.
   threshold volume 1000 bytes
   interim-interval 3 minutes
! References the authorization list in the above AAA configuration.
   method-list author PREPAID_AUTHOR_LIST
! References the accounting list in the above AAA configuration.
   method-list accounting PREPAID_ACCNT_LIST
! This is the prepaid password that is configured on the billing servers.
   password cisco
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

Note If you configure only default values for a prepaid service, the configuration will not appear in **show running-config** command output, but the configuration will be active.

```
! This is the global configuration for the default prepaid service.
subscriber feature prepaid default
   threshold time 20 seconds
! The quota size for this service is set at 200 bytes.
   threshold volume 200 bytes
   interim-interval 3 minutes
   method-list author default
   method-list accounting default
   password cisco
!
! 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

! Creates the policy map that is used for time based service.
policy-map type control RULE_PTA_TIME_LM_ATM8
! When a session is initiated, PBHK is applied and the subscriber is redirected to the
! Cisco SESM to select a service.
 class type control always event session-start
  1 service-policy type service name PBHK_SERVICE
  2 service-policy type service name L4REDIRECT_SERVICE
!
! The quota-depleted event is triggered when either a prepaid threshold is not configured,
! or if the quota is depleted before the billing server replenishes the quota.
 class type control always event quota-depleted
! Specifies that traffic won't be dropped when the quota is depleted.
  1 set-param drop-traffic FALSE
!
! The credit-exhausted event is triggered when the subscriber's account is empty.
 class type control always event credit-exhausted
! Redirects subscriber's whose accounts are depleted to the Cisco SESM.
  1 service-policy type service name L4REDIRECT_SERVICE
!
! Creates the policy map for volume-based service. The same global configuration is
! applied as that for the time-based policy map.
policy-map type control RULE_PTA_VOLUME_LM_ATM8
 class type control always event session-start
  1 service-policy type service name PBHK_SERVICE
  2 service-policy type service name L4REDIRECT_SERVICE
!
 class type control always event quota-depleted
  1 set-param drop-traffic FALSE
!
 class type control always event credit-exhausted
  1 service-policy type service name L4REDIRECT_SERVICE
```

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

Configuring the BOD1MTIME Service

For each of the additional services to be configured , a control class map is configured to define matching conditions that the policy map uses to trigger events that start and stop the service..

```
! This control class map defines the BOD1MTIME_CLASS service.
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
class-map type control match-all BOD1MTIME_CLASS
 match service-name BOD1MTIME
!

! When subscribers start the service, the other services are unapplied.
policy-map control RULE_PTA_TIME_LM_ATM8
 class type control BOD1MTIME_CLASS_DM2 event service-start
  1 service-policy type service unapply name L4REDIRECT_SERVICE
  2 service-policy type service unapply name BOD2MTIME_DM2
  3 service-policy type service identifier service-name
! When subscribers stop the service, it is unapplied, and Layer 4 redirect is applied to
! redirect the subscriber to the Cisco SESM.
 class type control BOD1MTIME_CLASS_DM2 event service-stop
  1 service-policy type service unapply identifier service-name
  2 service-policy type service name L4REDIRECT_SERVICE
```

Configuring the BOD2MTIME Service

The same method is used as for BOD1MTTIME to configure the BOD2MTIME service.

```
class-map type control match-all BOD2MTIME_CLASS
 match service-name BOD2MTIME
!
policy-map type control RULE_PTA_TIME_LM_ATM8
 class type control BOD2MTIME_CLASS_DM2 event service-start
  1 service-policy type service unapply name L4REDIRECT_SERVICE
  2 service-policy type service unapply name BOD1MTIME_DM2
  3 service-policy type service identifier service-name
!
 class type control BOD2MTIME_CLASS_DM2 event service-stop
  1 service-policy type service unapply identifier service-name
  2 service-policy type service name L4REDIRECT_SERVICE
```

Configuring the BOD1MVOLUME Service

The same method as for BOD1MTTIME is used to configure the BOD1MVOLUME service.

```
class-map type control match-all BOD1MVOLUME_CLASS
 match service-name BOD1MVOLUME

policy-map type control RULE_PTA_VOLUME_LM_ATM8
 class type control BOD1MVOLUME_CLASS_DM2 event service-start
  1 service-policy type service unapply name L4REDIRECT_SERVICE
  2 service-policy type service unapply name BOD2MVOLUME_DM2
  3 service-policy type service identifier service-name
!
 class type control BOD1MVOLUME_CLASS_DM2 event service-stop
  1 service-policy type service unapply identifier service-name
  2 service-policy type service name L4REDIRECT_SERVICE
```

Configuring the BOD2MVOLUME Service

The same method as for BOD1MTTIME is used to configure the BOD2MVOLUME service.

```
class-map type control match-all BOD2MVOLUME_CLASS
 match service-name BOD2MVOLUME
!
policy-map control RULE_PTA_VOLUME_LM_ATM8
 class type control BOD2MVOLUME_CLASS_DM2 event service-start
  1 service-policy type service unapply name L4REDIRECT_SERVICE
  2 service-policy type service unapply name BOD1MVOLUME_DM2
  3 service-policy type service identifier service-name
!
 class type control BOD2MVOLUME_CLASS_DM2 event service-stop
  1 service-policy type service unapply identifier service-name
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
  2 service-policy type service name L4REDIRECT_SERVICE
```

Deployment Model 2: AAA Server

The following baseline configuration tasks are performed on the AAA server for ISP-2:

- Configuring the Time-Based ISA Subscriber Services
- Configuring the Volume-Based ISA Services
- Configuring Layer 4 Redirect
- Configuring PBHK
- Configuring User profiles for Time-Based and Volume-Based Customers

Configuring the Time-Based ISA Subscriber Services

This profile specifies the detalis of the BOD1MTIME service. For all of the ISA services, a priority level must be configured in order for the Layer 4 Redirect feature to work properly. If priority levels are not configured, when the subscriber's credit is exhausted, the Layer 4 Redirect feature is added to the subscriber's existing service (such as BOD1MTIME), but it is not applied.

```
[ BOD1MTIME_DM2/Attributes ]
! All of the user-selectable services are given the priority level 10.
    Cisco-AVPair = "ip:traffic-class=in access-group name INTERNET_IN_ACL priority 10"
    Cisco-AVPair = "ip:traffic-class=in default drop"
    Cisco-AVPair = "ip:traffic-class=out access-group name INTERNET_OUT_ACL priority 10"
    Cisco-AVPair = "ip:traffic-class=out default drop"
    Cisco-AVPair = subscriber:accounting-list=PREPAID_ACCNT_LIST
    Cisco-AVPair = prepaid-config=PREPAID_RSIM
    Cisco-AVPair = atm:peak-cell-rate=1024
    Cisco-AVPair = atm:sustainable-cell-rate=1024
! The "I" in the attribute tells the Cisco SESM that the name of this service is
! "IBOD1MTIME".
    Cisco-SSG-Service-Info = IBOD1MTIME_DM2
! The "R" in the attribute tells the Cisco SESM that this is a user-selectable service.
    Cisco-SSG-Service-Info = R42.1.1.0;255.255.255.0
```

This profile specifies the detalis of the BOD2MTIME service.

```
[ BOD2MTIME_DM2/Attributes ]
    Cisco-AVPair = "ip:traffic-class=in access-group name INTERNET_IN_ACL priority 10"
    Cisco-AVPair = "ip:traffic-class=in default drop"
    Cisco-AVPair = "ip:traffic-class=out access-group name INTERNET_OUT_ACL priority 10"
    Cisco-AVPair = "ip:traffic-class=out default drop"
    Cisco-AVPair = subscriber:accounting-list=PREPAID_ACCNT_LIST
    Cisco-AVPair = prepaid-config=PREPAID_RSIM
    Cisco-AVPair = atm:peak-cell-rate=2048
    Cisco-AVPair = atm:sustainable-cell-rate=2048
    Cisco-SSG-Service-Info = IBOD2MTIME_DM2
    Cisco-SSG-Service-Info = R42.1.1.0;255.255.255.0
```

Configuring the Volume-Based ISA Services

This profile specifies the detalis of the BOD1MVOLUME service.

```
[ BOD1MVOLUME_DM2/Attributes ]
    Cisco-AVPair = "ip:traffic-class=in access-group name INTERNET_IN_ACL priority 10"
    Cisco-AVPair = "ip:traffic-class=in default drop"
    Cisco-AVPair = "ip:traffic-class=out access-group name INTERNET_OUT_ACL priority 10"
    Cisco-AVPair = "ip:traffic-class=out default drop"
    Cisco-AVPair = subscriber:accounting-list=PREPAID_ACCNT_LIST
    Cisco-AVPair = prepaid-config=PREPAID_RSIM
    Cisco-AVPair = atm:peak-cell-rate=1024
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
    Cisco-AVPair = atm:sustainable-cell-rate=1024
    Cisco-SSG-Service-Info = IBOD1MVOLUME_DM2
    Cisco-SSG-Service-Info = R42.1.1.0;255.255.255.0
```

This profile specifies the detalis of the BOD2MVOLUME service.

```
    Cisco-AVPair = "ip:traffic-class=in access-group name INTERNET_IN_ACL priority 10"
    Cisco-AVPair = "ip:traffic-class=in default drop"
    Cisco-AVPair = "ip:traffic-class=out access-group name INTERNET_OUT_ACL priority 10"
    Cisco-AVPair = "ip:traffic-class=out default drop"
    Cisco-AVPair = subscriber:accounting-list=PREPAID_ACCNT_LIST
    Cisco-AVPair = prepaid-config=PREPAID_RSIM
    Cisco-AVPair = atm:peak-cell-rate=2048
    Cisco-AVPair = atm:sustainable-cell-rate=2048
    Cisco-SSG-Service-Info = IBOD2MVOLUME_DM2
    Cisco-SSG-Service-Info = R42.1.1.0;255.255.255.0
```

Configuring Layer 4 Redirect

This attribute enables the Layer 4 Redirect feature.

```
[ //localhost/Radius/UserLists/SERVICES/L4REDIRECT_SERVICE/Attributes ]
! The Layer 4 Redirect feature is given the priority level 5, which is a higher priority
! than the user-selectable features. This ensures that subscribers are redirected when
! their accounts are exhausted.
    Cisco-AVPair = "ip:traffic-class=in access-group name IP_REDIRECT_ACL priority 5"
    Cisco-AVPair = "ip:traffic-class=in default drop"
    Cisco-AVPair = "ip:traffic-class=out access-group name IP_REDIRECT_ACL priority 5"
    Cisco-AVPair = "ip:traffic-class=out default drop"
    Cisco-AVPair = "ip:l4redirect=redirect to group SESM_SERVER_GROUP"
    Cisco-SSG-Service-Info = IL4REDIRECT_SERVICE
```

Configuring PBHK

This profile enables the PBHK feature on the AAA server, which enables access to the SESM by way of the PBHK feature.

```
[ //localhost/Radius/UserLists/SERVICES/PBHK_SERVICE/Attributes ]
    Cisco-AVPair = ip:portbundle=enable
! The "I" in the attribute tells the Cisco SESM that the name of this service is
! "PBHK_SERVICE". But because there an attribute beginning with "R" is not included,
! customers cannot select this service.
    Cisco-SSG-Service-Info = IPBHK_SERVICE
```

Configuring User profiles for Time-Based and Volume-Based Customers

This profile configures a user profile for time-based customers.

```
[ //localhost/Radius/UserLists/ie2-C7206-ATM/C72_DM2_3640/Attributes ]
    Cisco-AVpair = ip:vrf-id=VPN_C72_DM2_1001
    Cisco-AVpair = "ip:ip-unnumbered=loopback 8001"
    Cisco-AVpair = ip:addr-pool=C72_DM2_8001
! The "N" at the beginning of these two attributes specifies that these are services that
! that customers can activate. Time-based subscribers are authorized to access the
! BOD1MTIME and BOD2MTTIME services.
    Cisco-SSG-Account-Info = NBOD1MTIME_DM2
    Cisco-SSG-Account-Info = NBOD2MTIME_DM2
    idle-timeout = 1800
    session-timeout = 18000
```

This profile configures a user profile for a time-based customer with the static IP address 1.108.1.201.

```
[ //localhost/Radius/UserLists/ie2-C7206-ATM/C72_DM2_5640/Attributes ]
    Cisco-AVpair = ip:vrf-id=VPN_C72_DM2_1098
    Cisco-AVpair = "ip:ip-unnumbered=loopback 8002"
    Cisco-SSG-Account-Info = NBOD1MTIME_DM2
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
    Cisco-SSG-Account-Info = NBOD2MTIME_DM2
    Framed-IP-Address = 1.108.1.201
    idle-timeout = 1800
    session-timeout = 18000
```

This profile configures a user profile for volume-based customers.

```
[ //localhost/Radius/UserLists/ie2-C7206-ATM/C72_DM2_4640/Attributes ]
    Cisco-AVpair = ip:vrf-id=VPN_C72_DM2_1001
    Cisco-AVpair = "ip:ip-unnumbered=loopback 8001"
    Cisco-AVpair = ip:addr-pool=C72_DM2_8001
! The "N" at the beginning of these two attributes specifies that these are services that
! these customers are authorized for. Time-based subscribers are authorized to access the
! BOD1MVOLUME and BOD2MVOLUME services.
    Cisco-SSG-Account-Info = NBOD1MVOLUME_DM2
    Cisco-SSG-Account-Info = NBOD2MVOLUME_DM2
    idle-timeout = 1800
    session-timeout = 18000
```

Deployment Model 3: Triple Play Plus Service Bundle over IP and PPPoE

The following devices are configured to enable Deployment Model 3 Triple Play Plus Service Bundle over IP and PPPoE deployment model:

- Deployment Model 3: ISG, page 46
- Deployment Model 3: AAA Server, page 52

Deployment Model 3: ISG

The following baseline configuration tasks are performed on the LNS:

- Configuring AAA and the Connection to the RADIUS Server
- Configuring PPPoE and the Connections to the CPE and PE
- Configuring Baseline ISA Subscriber Services
- Configuring Inbound and Outbound Access Lists
- Configuring QoS for Triple Play Plus

Configuring AAA and the Connection to the RADIUS Server

In this AAA configuration, connections to the CAR AAA server, the Cisco SESM, and two billing servers are configured. VSA accounting and authentication are enabled, and the loopback interface 0 is used for AAA communications.

```
aaa new-model
!
! Configures the AAA server group for the CAR AAA server.
aaa group server radius CAR_SERVER
 server 10.100.2.36 auth-port 1812 acct-port 1813
!
! Configures the AAA server group for the RSIM_SERVER billing server.
aaa group server radius RSIM_SERVER
 server 10.100.12.89 auth-port 1645 acct-port 1646


! Configures AAA for the CAR AAA server.
aaa authentication login default none
aaa authentication login IP_AUTHEN_LIST group CAR_SERVER
aaa authentication ppp default group CAR_SERVER
! Configures the connection to the Cisco SESM
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
aaa server radius sesm
 client 10.100.4.38
 key cisco
 port 1812
 message-authenticator ignore
!

! Loopback 0 is used for communicating with AAA, the billing servers, and SESM.
interface Loopback0
 ip address 10.200.1.53 255.255.255.255

! Instructs the router to use loopback 0 to communicate with the AAA RADIUS servers.
ip radius source-interface Loopback0
!
! These RADIUS attributes are required for prepaid services.
radius-server attribute 44 include-in-access-req
radius-server attribute 8 include-in-access-req
radius-server attribute 55 access-request include
radius-server attribute 25 access-request include
! The CAR AAA server.
radius-server host 10.100.1.35 auth-port 1812 acct-port 1813 key cisco
! The RSIM_SERVER billing server.
radius-server host 10.100.12.89 auth-port 1645 acct-port 1646 key cisco
radius-server retransmit 5
radius-server timeout 15
radius-server vsa send accounting
radius-server vsa send authentication
```

Configuring PPPoE and the Connections to the CPE and PE

The ISG is configured to receive PPPoE sessions from the CPE by way of the DSLAM, and MPLS VRF tables are created for incoming subscribers.

```
no ip dhcp use vrf connected
!
! Globally enables MPLS VRFs for incoming subscribers.
ip vrf VPN10003
 rd 100:3
 route-target export 100:3
 route-target import 100:3
!
ip cef
!
!

! The BBA group method is used to configure PPPoE.
bba-group pppoe BBA_LM_ATM2
 virtual-template 2
!
! This virtual circuit (VC) class is applied to the ATM PVC.
vc-class atm VC_LM_ATM2
! Associates the VC class with the above bba-group.
  protocol pppoe group BBA_LM_ATM2
! Enables dynamic bandwidth selection.
  dbs enable maximum
  encapsulation aal5snap
  service-policy control RULE_PTA_LM_ATM2
!

! Gigabit Ethernet interface 0/3 points to the PE.
interface GigabitEthernet0/3
 ip address 40.40.1.53 255.255.255.0
! The PBHK feature is enabled on this interface.
 ip portbundle outside
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
 load-interval 30
 duplex full
 speed 1000
 media-type gbic
 negotiation auto
 mpls mtu 1522
 mpls ip
 service-policy output QOS_OUT_MPLS_UPLINK
 ip rsvp bandwidth 100000
!
! ATM interface 1/0.103 points to the CPE.
interface ATM1/0.103 point-to-point
 ip unnumbered Loopback3
 ip verify unicast reverse-path
 ip helper-address 10.100.1.37
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip subscriber
  initiator dhcp
 atm route-bridged ip
 no atm enable-ilmi-trap
 ntp disable
 pvc 103/43
! The VC class is associated with the PVC.
  class-vc VC_LM_ATM2
 service-policy input QOS_IN_LM_ATM2
 service-policy output QOS_OUT_LM_ATM2
 service-policy control RULE_IP_LM_ATM2


! PPPoE subscribers use this virtual template.
interface Virtual-Template2
 description LM ATM2 PTA Subscriber
 no ip address
 no peer default ip address
 no keepalive
 ppp authentication chap
 ppp timeout authentication 100
 ppp timeout aaa
!
! The PPPoE pool that is assigned to subscribers.
ip local pool cpe3_pool-53 200.53.3.2 200.53.3.100
```

Configuring Baseline ISA Subscriber Services

The baseline ISA services, Layer 4 redirect, ISA authentication methods, and PBHK are configured. When the PBHK feature is enabled, TCP packets from subscribers are mapped to a local IP address for the ISA gateway and a range of ports. This mapping allows the portal to identify the ISA gateway from which the session originated.

```
! Configures the connection to the Cisco SESM for Layer 4 Redirect functionality.
redirect server-group SESM_SERVER_GROUP
 server ip 10.100.3.34 port 8080
!
! This policy map governs authentication.
policy-map control RULE_IP_LM_ATM2
! Unauthenticated traffic is dropped after the timer expires.
 class control IP_UNAUTH_COND event timed-policy-expiry
  1 service disconnect
!
 class control always event session-start
! PBHK must be applied before authorization, because if subscribers are authorized first,
! ISA will skip the remaining steps and PBHK won't be applied.
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
  1 service-policy service name PBHK_SERVICE
! Authorizes subscribers based on their MAC address. If authorization is successful, the
! remaining steps are skipped.
  2 authorize aaa password lab identifier mac-address
! If authorization fails, subscribers are redirected to the Cisco SESM.
  3 service-policy service name L4REDIRECT_SERVICE
! When users are redirected, the IP_UNAUTH_TIMER gives them 5 minutes to manually
! authenticate at the Cisco SESM before the session is dropped.
  4 set-timer IP_UNAUTH_TIMER 5
!
 class control always event account-logon
! Authorization is performed based on the IP_AUTHEN_LIST.
  1 authenticate aaa list IP_AUTHEN_LIST
! If authorization fails, users are redirected to the Cisco SESM.
  2 service-policy service unapply name L4REDIRECT_SERVICE
!
!
policy-map control RULE_PTA_LM_ATM2
 class control always event session-start
  1 service-policy service name PBHK_SERVICE
!
!
! Enables port bundle host key (PBHK) access to the Cisco SESM. Each loopback interface
! can support up to 4031 bundles. If additional capacity is required, configure additional
! loopback interfaces.
ip portbundle
 match access-list 135
! The Loopback 0 interface is used to communicate with the Cisco SESM.
 source Loopback0
!
! This class map specifies that a timer is initiated for unauthenticated sessions. If the
! subscriber does not authenticate before the timer expires, the session is dropped.
class-map control match-all IP_UNAUTH_COND
 match timer IP_UNAUTH_TIMER
 match authen-status unauthenticated
```

Configuring Inbound and Outbound Access Lists

Basic access lists are configured to govern subscribers' Internet access, and an access list is created for the PBHK feature.

```
! This access list is referenced in the AAA subscriber profile. It governs incoming
! Internet traffic. The Internet access lists should prevent subscribers from accessing
! the Cisco SESM and other management devices to help prevent Denial of Service attacks.
!
ip access-list extended Internet-in-acl
 deny   ip any 223.0.0.0 0.255.255.255
 deny   ip any 20.0.0.0 0.255.255.255
 deny   ip any 40.0.0.0 0.255.255.255
 deny   ip any 21.0.0.0 0.255.255.255
 deny   ip any 22.0.0.0 0.255.255.255
 deny   ip any 41.0.0.0 0.255.255.255
 deny   ip any 80.0.0.0 0.255.255.255
 deny   ip any 81.0.0.0 0.255.255.255
 deny   ip any 82.0.0.0 0.255.255.255
 deny   ip any 84.0.0.0 0.255.255.255
 deny   ip any 10.200.0.0 0.0.255.255
 permit ip any any
!
! This access list is called out in the AAA subscriber profile. It governs outgoing
! Internet traffic. The Internet access lists should prevent subscribers from accessing
! the Cisco SESM and other management devices to help prevent Denial of Service attacks.
!
ip access-list extended Internet-out-acl
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
 deny   ip 223.0.0.0 0.255.255.255 any
 deny   ip 10.200.0.0 0.0.255.255 any
 deny   ip 20.0.0.0 0.255.255.255 any
 deny   ip 40.0.0.0 0.255.255.255 any
 deny   ip 21.0.0.0 0.255.255.255 any
 deny   ip 22.0.0.0 0.255.255.255 any
 deny   ip 41.0.0.0 0.255.255.255 any
 deny   ip 80.0.0.0 0.255.255.255 any
 deny   ip 81.0.0.0 0.255.255.255 any
 deny   ip 82.0.0.0 0.255.255.255 any
 deny   ip 84.0.0.0 0.255.255.255 any
 permit ip any any
!
! This access list is used in the ip portbundle configuration above.
access-list 135 permit ip any host 10.100.4.38
access-list 135 deny ip any any
```

Configuring QoS for Triple Play Plus

The Triple Play Plus service bundle is configured by specifying different levels of QoS for each of the user-selectable services. Three DSCP levels are configured: gaming, call control, and voice. The VoD service uses the same DSCP as the voice service. Policy maps are then used to apply this QoS configuration to the inbound and outbound interfaces.

```
! These class maps specify the various DSCP levels.
class-map match-any QOS_GROUP_CALL_CONTROL
  match qos-group 2
class-map match-any GAMING
  match ip dscp af21
class-map match-any QOS_GROUP_GAMING
  match qos-group 3
class-map match-any CALL_CONTROL
  match ip dscp cs3
class-map match-any QOS_GROUP_VOICE
  match qos-group 1
class-map match-any VOICE
  match ip dscp ef
!

!
! This policy map governs QoS for the outbound interface to the CPE.
policy-map QOS_OUT_LM_ATM2
  class VOICE
    priority 128
  class CALL_CONTROL
    bandwidth percent 5
  class GAMING
    bandwidth percent 20

! This policy map governs QoS for the outbound interface to the PE.
policy-map QOS_OUT_MPLS_UPLINK
  class QOS_GROUP_VOICE
   set mpls experimental topmost 5
  class QOS_GROUP_CALL_CONTROL
   set mpls experimental topmost 3
  class QOS_GROUP_GAMING
   set mpls experimental topmost 2
  class class-default
   set mpls experimental topmost 0

! This policy map governs QoS for the inbound interface from the CPE.
policy-map QOS_IN_LM_ATM2
  class VOICE
! Caps bandwidth for VoIP and VoD traffic at 128 kbps.
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
    police cir 128000
      exceed-action drop
    set qos-group 1
  class CALL_CONTROL
! Caps bandwidth for call control traffic at 12.5 kbps.
    police cir 12500
      exceed-action drop
    set qos-group 2
  class GAMING
! Caps bandwidth for gaming traffic at 75 kbps.
    police cir 75000
      exceed-action drop
    set qos-group 3

! This policy map governs QoS for the default service.
policy-map QOS_IN_LM_ATM2_256K
  class class-default
! Caps bandwidth for basic connectivity traffic at 256 kbps.
    police cir 256000
      exceed-action drop
    set qos-group 1
    service-policy QOS_IN_LM_ATM2
```

Configuring Triple Play Plus Access Lists

The following access lists govern the access of subscribers who have activated the various services.

```
! The gaming access-lists allow gaming subscribers to access only the gaming server.
ip access-list extended GAMING_IN_ACL
 permit ip any 42.5.0.0 0.0.255.255
 deny   ip any any
ip access-list extended GAMING_OUT_ACL
 permit ip 42.5.0.0 0.0.255.255 any
 deny   ip any any
! The opengarden access lists govern the access of users who have not activated an
! advanced service.
ip access-list extended OPENGARDEN_IN_ACL
 permit ip any 10.100.0.0 0.0.255.255
 permit ip any 42.8.0.0 0.0.255.255
 permit ip any 200.53.3.0 0.0.0.255
ip access-list extended OPENGARDEN_OUT_ACL
 permit ip 10.100.0.0 0.0.255.255 any
 permit ip 42.8.0.0 0.0.255.255 any
 permit ip 200.53.3.0 0.0.0.255 any
ip access-list extended SESM-in-acl
 permit ip any host 10.100.3.34
 deny   ip any any
ip access-list extended SESM-out-acl
 permit ip host 10.100.3.34 any
 deny   ip any any
! The VoD access lists allow VoD subscribers to access only the VoD server.
ip access-list extended VOD_IN_ACL
 permit ip any 42.4.0.0 0.0.255.255
 deny   ip any any
ip access-list extended VOD_OUT_ACL
 permit ip 42.4.0.0 0.0.255.255 any
 deny   ip any any
! The VoIP access lists allow VoIP subscribers to access only the VoD server.
ip access-list extended VOIP_IN_ACL
 permit ip any 42.3.0.0 0.0.255.255
 deny   ip any any
ip access-list extended VOIP_OUT_ACL
 permit ip 42.3.0.0 0.0.255.255 any
 deny   ip any any
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

Deployment Model 3: AAA Server

The following configuration tasks are performed on the AAA server.

- Configuring Layer 4 Redirect
- Configuring PBHK
- Service Profiles
- User Profiles

Configuring Layer 4 Redirect

This attribute enables the Layer 4 Redirect feature.

```
[ //localhost/Radius/UserLists/SERVICES/L4REDIRECT_SERVICE/Attributes ]
! The Layer 4 Redirect feature is given the priority level 5, which is a higher priority
! than the user-selectable features. This ensures that subscribers are redirected when
! their accounts are exhausted.
    Cisco-AVPair = "ip:traffic-class=in access-group name IP_REDIRECT_ACL priority 5"
    Cisco-AVPair = "ip:traffic-class=in default drop"
    Cisco-AVPair = "ip:traffic-class=out access-group name IP_REDIRECT_ACL priority 5"
    Cisco-AVPair = "ip:traffic-class=out default drop"
    Cisco-AVPair = "ip:l4redirect=redirect to group SESM_SERVER_GROUP"
    Cisco-SSG-Service-Info = IL4REDIRECT_SERVICE
```

Configuring PBHK

This profile enables the PBHK feature on the AAA server, which enables access to the SESM by way of the PBHK feature.

```
[ //localhost/Radius/UserLists/SERVICES/PBHK_SERVICE/Attributes ]
    Cisco-AVPair = ip:portbundle=enable
! The “I” in the attribute tells the Cisco SESM that the name of this service is
! “PBHK_SERVICE”. But because there an attribute beginning with “R” is not included,
! customers cannot select this service.
    Cisco-SSG-Service-Info = IPBHK_SERVICE
```

Service Profiles

The following service profile enables the GAMING_SERVICE service.

```
[ //localhost/Radius/UserLists/SERVICES/GAMING_SERVICE/Attributes ]
    Cisco-AVPair = "ip:traffic-class=in access-group name GAMING_IN_ACL"
    Cisco-AVPair = "ip:traffic-class=in default drop"
    Cisco-AVPair = "ip:traffic-class=out access-group name GAMING_OUT_ACL"
    Cisco-AVPair = "ip:traffic-class=out default drop"
! The “I” in the attribute tells the Cisco SESM that the name of this service is
! “IGAMING_SERVICE”.
    Cisco-SSG-Service-Info = IGAMING_SERVICE
! The “R” in the attribute tells the Cisco SESM that this is a user-selectable service.
    Cisco-SSG-Service-Info = R42.1.1.0;255.255.255.0
```

The following service profile enables the OPENGARDEN_SERVICE service. “Opengarden” is the SSG term for the default service, basic Internet access.

```
[ //localhost/Radius/UserLists/SERVICES/OPENGARDEN_SERVICE/Attributes ]
    Cisco-AVPair = "ip:traffic-class=in access-group name OPENGARDEN_IN_ACL"
    Cisco-AVPair = "ip:traffic-class=in default drop"
    Cisco-AVPair = "ip:traffic-class=out access-group name OPENGARDEN_OUT_ACL"
    Cisco-AVPair = "ip:traffic-class=out default drop"
    Cisco-SSG-Service-Info = IOPENGARDEN_SERVICE
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

The following service profile enables the VOIP_SERVICE service.

```
[ //localhost/Radius/UserLists/SERVICES/VOIP_SERVICE/Attributes ]
    Cisco-AVPair = "ip:traffic-class=in access-group name VOIP_IN_ACL"
    Cisco-AVPair = "ip:traffic-class=in default drop"
    Cisco-AVPair = "ip:traffic-class=out access-group name VOIP_OUT_ACL"
    Cisco-AVPair = "ip:traffic-class=out default drop"
    Cisco-SSG-Service-Info = IVOIP_SERVICE
    Cisco-SSG-Service-Info = R42.1.1.0;255.255.255.0
```

The following service profile enables the VOD_SERVICE service.

```
[ //localhost/Radius/UserLists/SERVICES/VOD_SERVICE/Attributes ]
    Cisco-AVPair = "ip:traffic-class=in access-group name VOD_IN_ACL"
    Cisco-AVPair = "ip:traffic-class=in default drop"
    Cisco-AVPair = "ip:traffic-class=out access-group name VOD_OUT_ACL"
    Cisco-AVPair = "ip:traffic-class=out default drop"
    Cisco-SSG-Service-Info = IVOD_SERVICE
    Cisco-SSG-Service-Info = R42.1.1.0;255.255.255.0
```

The following service profile enables the INTERNET_SERVICE service. Subscribers select this service to return to the default service, basic Internet access.

```
[ //localhost/Radius/UserLists/SERVICES/INTERNET_SERVICE/Attributes ]
    Cisco-AVPair = ip:inacl=Internet-in-acl
    Cisco-AVPair = ip:outacl=Internet-out-acl
    Cisco-SSG-Service-Info = IINTERNET_SERVICE
    Cisco-SSG-Service-Info = R42.1.1.0;255.255.255.0
```

User Profiles

The following user profile is for IP sessions that use MAC address-based TAL:

```
[ //localhost/Radius/UserLists/ie2-C7206-ATM/0000.1001.1014/Attributes ]
    Cisco-SSG-Account-Info = AOPENGARDEN_SERVICE
    Cisco-SSG-Account-Info = AVOIP_SERVICE
    Cisco-SSG-Account-Info = AVOD_SERVICE
    Cisco-SSG-Account-Info = AGAMING_SERVICE
```

The following user profile is for PPPoE users:

```
[ //localhost/Radius/UserLists/ie2-C7206-ATM/C72_DM3_1188/Attributes ]
    Cisco-AVpair = ip:vrf-id=VPN_C72_DM3_2038
    Cisco-AVpair = "ip:ip-unnumbered=loopback 2001"
    Cisco-AVpair = ip:addr-pool=C72_DM3_2001
    Cisco-SSG-Account-Info = AINTERNET_SERVICE
```

Deployment Model 4: Triple Play Plus Service Bundle over IP and L2TP

The following devices are configured to enable Deployment Model 4: Triple Play Plus Service Bundle over IP and L2TP deployment model:

- Deployment Model 4: ISG LAC, page 53
- Deployment Model 4: AAA Server for ISP-1, page 58
- Deployment Model 4: LNS, page 59
- Deployment Model 4: AAA server for ISP-2, page 62

Deployment Model 4: ISG LAC

The following baseline configuration tasks are performed on the ISG LAC:

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

Configuring AAA and the Connection to the RADIUS Server

A basic AAA configuration is entered, and the connection to the RADIUS server is configured, including VSA accounting and authentication.

```
aaa new-model
!
! Configures the connection to the AAA server and identifies it as CAR_SERVER
aaa group server radius CAR_SERVER
 server 10.100.1.35 auth-port 1812 acct-port 1813
!
aaa authentication login default none
! Configures the AAA server for authentication, authorization, and accounting.
aaa authentication login IP_AUTHEN_LIST group CAR_SERVER
aaa authentication ppp default group CAR_SERVER
aaa authorization network default group CAR_SERVER
aaa authorization subscriber-service default local group radius
aaa accounting network default start-stop group CAR_SERVER
! Configures the connection to the Cisco SESM
aaa server radius sesm
 client 10.100.3.34
 key cisco
 port 1812
 message-authenticator ignore
!
aaa session-id common
!
!
interface Loopback0
 ip address 10.200.1.53 255.255.255.255
!
! Use Loopback 0 to communicate with radius server
ip radius source-interface Loopback0
!
!
radius-server attribute 44 include-in-access-req
radius-server attribute 8 include-in-access-req
radius-server attribute 55 access-request include
radius-server attribute 25 access-request include
radius-server host 10.100.1.35 auth-port 1812 acct-port 1813 key cisco
radius-server retransmit 5
radius-server timeout 15
radius-server vsa send accounting
radius-server vsa send authentication
```

Configuring the Connection to the LNS and PPPoE

The connection to the LNS is configured. The ISG LAC uses VPDN to initiate L2TP tunnels to the LNS, which are used to carry the subscriber PPPoE sessions. An ISA control policy map is used to instruct L2TP to authenticate on the basis of domain name, and a BBA group is used to configure PPPoE.

```
no ip dhcp use vrf connected
!
! This command is enabled by default. It sets the number of rules that are displayed in
! the show subscriber session detail command.
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
subscriber policy recording rules limit 64
subscriber authorization enable

! Enables VPDN globally, which is used for PPPoE.
vpdn enable
vpdn ip udp ignore checksum
vpdn search-order domain
!
! This control policy map instructs L2TP to authenticate based on domain name.
policy-map type control RULE_L2TP_LM_ATM7
 class type control always event session-start
  1 collect identifier unauthenticated-domain
  2 authorize identifier unauthenticated-domain
!
!
! The BBA group method is used to configure PPPoE (alternatively, the vpdn-group
! method could be used).
bba-group pppoe BBA_LM_ATM7
 virtual-template 7
!
! This virtual circuit (VC) class is applied to the ATM PVC.
vc-class atm VC_LM_ATM7
! Associates the VC class with the above bba-group.
  protocol pppoe group BBA_LM_ATM7
  vbr-nrt 2000 2000 94
  encapsulation aal5snap
! Applies the L2TP rule above to the VC class.
  service-policy type control RULE_L2TP_LM_ATM7
!
! Interface Gigabit Ethernet 0/3 points to the LNS.
interface GigabitEthernet0/3
 ip address 40.40.1.53 255.255.255.0
 load-interval 30
 duplex full
 speed 1000
 media-type gbic
 negotiation auto
 mpls mtu 1522
 mpls ip
 service-policy output QOS_OUT_MPLS_UPLINK
 ip rsvp bandwidth 100000
!
!
interface ATM1/0.107 point-to-point
 description ATM Deployment Model 4
 ip unnumbered Loopback7
 ip verify unicast reverse-path
 ip helper-address 10.100.1.37
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip subscriber
  identifier ip src-addr match 107
  initiator dhcp
 atm route-bridged ip
 no atm enable-ilmi-trap
 ntp disable
 pvc 107/47
! The VC class is associated with the PVC.
  class-vc VC_LM_ATM7
 service-policy input QOS_IN_LM_ATM7
 service-policy output QOS_OUT_LM_ATM7
 service-policy control RULE_IP_LM_ATM7
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
!
!
! The PPP CHAP configuration is entered on the virtual template.
interface Virtual-Template7
 description LM ATM7 L2TP Subscriber
 no ip address
 no peer default ip address
 no keepalive
 ppp authentication chap
 ppp timeout authentication 100
 ppp timeout aaa
```

Configuring Baseline ISA Services

The baseline ISA services, Layer 4 redirect, ISA authentication methods, and PBHK are configured. When the PBHK feature is enabled, TCP packets from subscribers are mapped to a local IP address for the ISA gateway and a range of ports. This mapping allows the portal to identify the ISA gateway from which the session originated.

```
redirect server-group SESM_SERVER_GROUP
 server ip 10.100.3.34 port 8080
!
! TAL is configured to authenticate the subscriber static IP address 200.53.7.128.
class-map control match-any TAL_STATIC_DM4
 match source-ip-address 200.53.7.128 255.255.255.128
!
! This policy map governs subscriber authentication.
policy-map control RULE_IP_LM_ATM7
 class control TAL_STATIC_DM4 event session-start
! PBHK must be applied before authorization, because if subscribers are authorized first,
! ISA will skip the remaining steps and PBHK won't be applied.
  1 service-policy service name PBHK_SERVICE
! Authorizes subscribers based on their IP address. If authorization is successful,
! the remaining steps are skipped.
  2 authorize aaa password lab identifier source-ip-address
! If authorization fails, subscribers are redirected to the Cisco SESM.
  3 service-policy service name L4REDIRECT_SERVICE
! When users are redirected, the IP_UNAUTH_TIMER gives them 5 minutes to manually
! authenticate at the Cisco SESM before the session is dropped.
  4 set-timer IP_UNAUTH_TIMER 5
!
 class control IP_UNAUTH_COND event timed-policy-expiry
! Unauthenticated traffic is dropped after the timer expires.
  1 service disconnect
!
 class control always event session-start
  1 service-policy service name PBHK_SERVICE
! Authorizes subscribers based on their MAC address. If authorization is successful, the
! remaining steps are skipped.
  2 authorize aaa password lab identifier mac-address
  3 service-policy service name L4REDIRECT_SERVICE
  4 set-timer IP_UNAUTH_TIMER 5
!
 class control always event account-logon
  1 authenticate aaa list IP_AUTHEN_LIST
  2 service-policy service unapply name L4REDIRECT_SERVICE
!
!
! Enables port bundle host key (PBHK) access to the Cisco SESM. Each loopback interface
! can support up to 4031 bundles. If additional capacity is required, configure additional
! loopback interfaces.
ip portbundle
 match access-list 135
 source Loopback0
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
!
! This class map specifies that a timer is initiated for unauthenticated sessions. If the
! subscriber does not authenticate before the timer expires, the session is dropped.
class-map control match-all IP_UNAUTH_COND
 match timer IP_UNAUTH_TIMER
 match authen-status unauthenticated
```

Configuring QoS for Triple Play Plus

The Triple Play Plus service bundle is configured by specifying different levels of QoS for each of the user-selectable services. Three DSCP levels are configured: gaming, call control, and voice. The VoD service uses the same DSCP as the voice service. Policy maps are then used to apply this QoS configuration to the inbound and outbound interfaces.

```
! These class maps specify the various DSCP levels.
class-map match-any QOS_GROUP_CALL_CONTROL
  match qos-group 2
class-map match-any GAMING
  match ip dscp af21
class-map match-any QOS_GROUP_GAMING
  match qos-group 3
class-map match-any CALL_CONTROL
  match ip dscp cs3
class-map match-any QOS_GROUP_VOICE
  match qos-group 1
class-map match-any VOICE
  match ip dscp ef
!
!
!
! This policy map governs QoS for the outbound interface to the CPE.
policy-map QOS_OUT_LM_ATM7
  class VOICE
    priority 128
  class CALL_CONTROL
    bandwidth percent 5
  class GAMING
    bandwidth percent 20

! This policy map governs QoS for the outbound interface to the LNS.
policy-map QOS_OUT_MPLS_UPLINK
  class QOS_GROUP_VOICE
   set mpls experimental topmost 5
  class QOS_GROUP_CALL_CONTROL
   set mpls experimental topmost 3
  class QOS_GROUP_GAMING
   set mpls experimental topmost 2
  class class-default
   set mpls experimental topmost 0

! This policy map governs QoS for the inbound interface from the CPE.
policy-map QOS_IN_LM_ATM7
  class VOICE
! Caps bandwidth for VoIP and VoD traffic at 128 kbps.
   police cir 128000
     exceed-action drop
   set qos-group 1
  class CALL_CONTROL
! Caps bandwidth for call control traffic at 12.5 kbps.
   police cir 12500
     exceed-action drop
   set qos-group 2
  class GAMING
! Caps bandwidth for gaming traffic at 75 kbps.
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
   police cir 75000
     exceed-action drop
   set qos-group 3

! This policy map governs QoS for the default service.
policy-map QOS_IN_LM_ATM7_256K
  class class-default
! Caps bandwidth for basic connectivity traffic at 256 kbps.
   police cir 256000
     exceed-action drop
   service-policy QOS_IN_LM_ATM7
```

Configuring Triple Play Plus Access Lists

The following access lists govern the access of subscribers who have activated the various services.

```
! The gaming access-lists allow gaming subscribers to access only the gaming server.
ip access-list extended GAMING_IN_ACL
 permit ip any 42.5.0.0 0.0.255.255
 deny   ip any any
ip access-list extended GAMING_OUT_ACL
 permit ip 42.5.0.0 0.0.255.255 any
 deny   ip any any
! The opengarden access lists govern the access of users who have not activated an
! advanced service.
ip access-list extended OPENGARDEN_IN_ACL
 permit ip any 10.100.0.0 0.0.255.255
 permit ip any 42.8.0.0 0.0.255.255
 permit ip any 200.53.3.0 0.0.0.255
ip access-list extended OPENGARDEN_OUT_ACL
 permit ip 10.100.0.0 0.0.255.255 any
 permit ip 42.8.0.0 0.0.255.255 any
 permit ip 200.53.3.0 0.0.0.255 any
ip access-list extended SESM-in-acl
 permit ip any host 10.100.3.34
 deny   ip any any
ip access-list extended SESM-out-acl
 permit ip host 10.100.3.34 any
 deny   ip any any
! The VoD access lists allow VoD subscribers to access only the VoD server.
ip access-list extended VOD_IN_ACL
 permit ip any 42.4.0.0 0.0.255.255
 deny   ip any any
ip access-list extended VOD_OUT_ACL
 permit ip 42.4.0.0 0.0.255.255 any
 deny   ip any any
! The VoIP access lists allow VoIP subscribers to access only the VoD server.
ip access-list extended VOIP_IN_ACL
 permit ip any 42.3.0.0 0.0.255.255
 deny   ip any any
ip access-list extended VOIP_OUT_ACL
 permit ip 42.3.0.0 0.0.255.255 any
 deny   ip any any

! This access list is used in the ip portbundle configuration above.
access-list 135 permit ip any host 10.100.4.38
access-list 135 deny ip any any
```

Deployment Model 4: AAA Server for ISP-1

The following profile configures L2TP forwarding from the ISG LAC to the LNS. The IP address 10.200.1.56 is the address of the loopback interface on the LNS.

```
[ //localhost/Radius/UserLists/L2TPDOMAIN/L2TP_DM4_101.com/Attributes ]
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
Cisco-AVpair = vpdn:tunnel-id=L2TP_DM4_101
Cisco-AVpair = vpdn:l2tp-tunnel-password=cisco
Cisco-AVpair = vpdn:tunnel-type=l2tp
Cisco-AVpair = vpdn:ip-addresses=10.200.1.56
Cisco-AVpair = atm:peak-cell-rate=1024
Cisco-AVpair = atm:sustainable-cell-rate=512
```

Deployment Model 4: LNS

The following baseline configuration tasks are performed on the LNS:

- Configuring AAA and the Connection to the RADIUS Server
- Configuring PPPoE and the Connection to the ISG LAC
- Configuring Baseline ISA Subscriber Services
- Configuring Inbound and Outbound Access Lists

Configuring AAA and the Connection to the RADIUS Server

In this AAA configuration, connections to the CAR AAA server, the Cisco SESM, and two billing servers are configured. VSA accounting and authentication are enabled, and the loopback interface 0 is used for AAA communications.

```
aaa new-model
!
! Configures the AAA server group for the CAR AAA server.
aaa group server radius CAR_SERVER
 server 10.100.2.36 auth-port 1812 acct-port 1813
!

! Configures AAA for the CAR AAA server.
aaa authentication login default none
aaa authentication login IP_AUTHEN_LIST group CAR_SERVER
aaa authentication ppp default group CAR_SERVER
aaa authorization network default group CAR_SERVER
aaa authorization subscriber-service default local group radius
aaa accounting network default start-stop group CAR_SERVER
! Configures the connection to the Cisco SESM
aaa server radius sesm
 client 10.100.4.38
 key cisco
 port 1812
 message-authenticator ignore
!

! Loopback 0 is used for communicating with AAA, the billing servers, and SESM.
interface Loopback0
 ip address 10.200.1.56 255.255.255.255
 ip router isis Remote_ISP_7301

! Instructs the router to use loopback 0 to communicate with the AAA RADIUS servers.
ip radius source-interface Loopback0
!
! These RADIUS attributes are required for prepaid services.
radius-server attribute 44 include-in-access-req
radius-server attribute 8 include-in-access-req
radius-server attribute 55 include-in-acct-req
radius-server attribute 55 access-request include
radius-server attribute 25 access-request include
! The CAR AAA server.
radius-server host 10.100.2.36 auth-port 1812 acct-port 1813 key Cisco
radius-server retransmit 5
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
radius-server key cisco
radius-server vsa send accounting
radius-server vsa send authentication
```

Configuring PPPoE and the Connection to the ISG LAC

VPDN is configured to receive L2TP tunnels from the ISG LAC over which the PPPoE sessions are sent. A PPP local pool and MPLS VRF tables are created for incoming subscribers.

```
no ip dhcp use vrf connected
!
! Globally enables MPLS VRFs for incoming subscribers.
ip vrf VPN_C72_DM4_1001
 rd 200:71001
 route-target export 200:71001
 route-target import 200:71001
!
!
ip cef
!
! This command is enabled by default. It sets the number of ISA rules that are displayed
! in the show subscriber session detail command.
subscriber policy recording rules limit 64
vpdn enable
vpdn ip udp ignore checksum
!
! VPDN group L2TP_DM1_101 terminates PPPoE clients that come in from the ISG LAC over L2TP
! tunnels.
vpdn-group L2TP_DM1_101
 accept-dialin
  protocol l2tp
  virtual-template 5
 terminate-from hostname L2TP_DM1_101
 local name L2TP_DM1_101
 l2tp tunnel password 0 cisco
!
!

! Gigabit Ethernet interface 0/1 points to the PE.
interface GigabitEthernet0/1
 ip address 27.27.1.56 255.255.255.0
! The PBHK feature is enabled on this interface.
 ip portbundle outside
 ip router isis Remote_ISP_7301
 load-interval 30
 duplex auto
 speed auto
 media-type gbic
 negotiation auto
 mpls label protocol ldp
 mpls ip
!
! Gigabit Ethernet interface 0/2 points to the ISG LAC.
interface GigabitEthernet0/2
 ip address 26.26.1.56 255.255.255.0
 ip router isis Remote_ISP_7301
 load-interval 30
 duplex auto
 speed auto
 media-type gbic
 negotiation auto
!
! PPPoE subscribers terminated from L2TP tunnels use this virtual template.
interface Virtual-Template5
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
 no ip address
 load-interval 30
 no peer default ip address
 no keepalive
 ppp mtu adaptive
 ppp authentication chap
!
! Enables IS-IS routing in the network.
router isis Remote_ISP_7301
 net 01.0011.5dd1.f01b.00
 redistribute connected
!
! The DHCP pool that is assigned to subscribers.
ip local pool C73_DM4_7001 1.7.1.2 1.7.255.254
!
```

Configuring Baseline ISA Subscriber Services

Basic ISA subscriber services are configured, including Layer 4 redirect to the Cisco SESM and the PBHK feature. When the PBHK feature is enabled, TCP packets from subscribers are mapped to a local IP address for the ISA gateway and a range of ports. This mapping allows the portal to identify the ISA gateway from which the session originated.

```
! Configures the connection to the Cisco SESM for Layer 4 Redirect functionality.
redirect server-group SESM-Server
 server ip 10.100.4.38 port 8080
!
!

! Enables port bundle host key (PBHK) access to the Cisco SESM. Each loopback interface
! can support up to 4031 bundles. If additional capacity is required, configure additional
! loopback interfaces.
ip portbundle
 match access-list 135
! The Loopback 0 interface is used to communicate with the Cisco SESM.
 source Loopback0
```

Configuring Inbound and Outbound Access Lists

Basic access lists are configured to govern subscribers' Internet access, and an access list is created for the PBHK feature.

```
! This access list is referenced in the AAA subscriber profile. It governs incoming
! Internet traffic. The Internet access lists should prevent subscribers from accessing
! the Cisco SESM and other management devices to help prevent Denial of Service attacks.
!
ip access-list extended Internet-in-acl
 deny   ip any 223.0.0.0 0.255.255.255
 deny   ip any 20.0.0.0 0.255.255.255
 deny   ip any 40.0.0.0 0.255.255.255
 deny   ip any 21.0.0.0 0.255.255.255
 deny   ip any 22.0.0.0 0.255.255.255
 deny   ip any 41.0.0.0 0.255.255.255
 deny   ip any 80.0.0.0 0.255.255.255
 deny   ip any 81.0.0.0 0.255.255.255
 deny   ip any 82.0.0.0 0.255.255.255
 deny   ip any 10.200.0.0 0.0.255.255
 permit ip any any
!
! This access list is called out in the AAA subscriber profile. It governs outgoing
! Internet traffic. The Internet access lists should prevent subscribers from accessing
! the Cisco SESM and other management devices to help prevent Denial of Service attacks.
!
ip access-list extended Internet-out-acl
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
 deny   ip 223.0.0.0 0.255.255.255 any
 deny   ip 10.200.0.0 0.0.255.255 any
 deny   ip 20.0.0.0 0.255.255.255 any
 deny   ip 40.0.0.0 0.255.255.255 any
 deny   ip 21.0.0.0 0.255.255.255 any
 deny   ip 22.0.0.0 0.255.255.255 any
 deny   ip 41.0.0.0 0.255.255.255 any
 deny   ip 80.0.0.0 0.255.255.255 any
 deny   ip 81.0.0.0 0.255.255.255 any
 deny   ip 82.0.0.0 0.255.255.255 any
 permit ip any any
!
! This access list is used in the ip portbundle configuration above.
access-list 135 permit ip any host 10.100.4.38
access-list 135 deny ip any any
```

Deployment Model 4: AAA server for ISP-2

The following configuration tasks are performed on the AAA server for ISP-2:

- Configuring Layer 4 Redirect
- Configuring PBHK
- Configuring the Basic Internet Access ISA Subscriber Service
- Configuring the Subscriber's Profile

Configuring Layer 4 Redirect

This attribute enables the Layer 4 Redirect feature.

```
[ Attributes ]
! Instructs Layer 4 redirect to send traffic to ACL 111 on the LNS.
    Cisco-AVPair = "ip:l4redirect=redirect list 111 to group SESM-Server duration 30
frequency 180"
```

Configuring PBHK

This attribute enables the PBHK feature on the AAA server, which enables access to the SESM by way of the PBHK feature.

```
[ Attributes ]
    Cisco-AVPair = ip:portbundle=enable
```

Configuring the Basic Internet Access ISA Subscriber Service

This profile configures the basic Internet access service.

```
[ //localhost/Radius/UserLists/SERVICES/INTERNET_SERVICE/Attributes ]
! Specifies the ACLs that govern this service.
    Cisco-AVPair = ip:inacl=Internet-in-acl
    Cisco-AVPair = ip:outacl=Internet-out-acl
! The "I" before "INTERNET_SERVICE" tells the Cisco SESM what the name of the service is.
! The Cisco SESM will display this service by the name "INTERNET_SERVICE".
    Cisco-SSG-Service-Info = IINTERNET_SERVICE
! The "R" in this attribute specifies that this is a subscriber-selectable service.
    Cisco-SSG-Service-Info = R42.1.1.0;255.255.255.0
```

Configuring the Subscriber's Profile

This profile configures the PPP profile that is used in the subscriber's base profile.

```
[ //localhost/Radius/UserLists/ie2-C7301-LNS/C73_DM1_01@L2TP_DM1_101.com/Attributes ]
    Cisco-AVpair = "ip:ip-unnumbered=loopback 3001"
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
Cisco-AVpair = ip:addr-pool=C73_DM1_3001
Cisco-SSG-Account-Info = AINTERNET_SERVICE
```

Verifying the Cisco 7206 ISG with ATM Aggregation

The following sections provide sample show command output:

ISG Configuration Information Verification

The **show subscr policy condition** command shows the number of times each policy has been executed.

```
ie2-C7206-ATM# show subscriber policy condition
Class-map                     Action                           Exec Hit Miss Comp
---------                     ------                           ---- --- ---- ----
match-any TAL_STATIC_DM3      match identifier source-ip-addr36131   036131    0
match-any TAL_STATIC_DM3      match identifier source-ip-addr3613128932 719928932
match-all IP_UNAUTH_COND      match identifier timer IP_UNAUT1662416624    0    0
match-all IP_UNAUTH_COND      match identifier authen-status 1662454261119811198
match-any TAL_STATIC_DM4      match identifier source-ip-addr23502   023502    0
match-any TAL_STATIC_DM4      match identifier source-ip-addr2350222902  60022902
match-all BOD2MVOLUME_CLASS_L match identifier service-name B    0   0    0    0
match-all BOD1MVOLUME_CLASS_L match identifier service-name B    0   0    0    0
match-all BOD2MTIME_CLASS_DM2 match identifier service-name B    1   0    1    1
match-all BOD1MTIME_CLASS_DM2 match identifier service-name B4632546325    0    0

Key:
  "Exec" - The number of times this line was executed
  "Hit"  - The number of times this line evaluated to TRUE
  "Miss" - The number of times this line evaluated to FALSE
  "Comp" - The number of times this line completed the execution of its
           condition without a need to continue on to the end
```

The **clear subscriber policy conditions** command can be used to clear the statistics of subscriber policy changes.

```
ie2-C7206-ATM# clear subscriber policy conditions
ie2-C7206-ATM#
ie2-C7206-ATM# show subscriber policy conditions

Class-map                     Action                           Exec Hit Miss Comp
---------                     ------                           ---- --- ---- ----
match-any TAL_STATIC_DM3      match identifier source-ip-addr    0   0    0    0
match-any TAL_STATIC_DM3      match identifier source-ip-addr    0   0    0    0
match-all IP_UNAUTH_COND      match identifier timer IP_UNAUT    0   0    0    0
match-all IP_UNAUTH_COND      match identifier authen-status     0   0    0    0
match-any TAL_STATIC_DM4      match identifier source-ip-addr    0   0    0    0
match-any TAL_STATIC_DM4      match identifier source-ip-addr    0   0    0    02
match-all BOD2MVOLUME_CLASS_L match identifier service-name B    0   0    0    0
match-all BOD1MVOLUME_CLASS_L match identifier service-name B    0   0    0    0
match-all BOD2MTIME_CLASS_DM2 match identifier service-name B    1   0    1    1
match-all BOD1MTIME_CLASS_DM2 match identifier service-name B    0   0    0    0

Key:
  "Exec" - The number of times this line was executed
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
  "Hit"  - The number of times this line evaluated to TRUE
  "Miss" - The number of times this line evaluated to FALSE
  "Comp" - The number of times this line completed the execution of its
           condition without a need to continue on to the end
```

The **show subscriber service** command shows details of all of the services configured on the ISG.

```
ie2-C7206-ATM# show subscriber service
  Service "PBHK_SERVICE":
    Version 1:
      SVM ID                : 47000002
      Locked by             : SVM-Feature-Info       [196]
      Locked by             : SVM-Printer            [1]
      Locked by             : PM-Service             [3626]
      Locked by             : PM-Info                [3626]
      Locked by             : FM-Bind                [3430]
      Profile               : 21E3C738
        Profile name: PBHK_SERVICE, 3628 references
          portbundle           "enable"
          ssg-service-info     "IPBHK_SERVICE"
      Feature               : Portbundle Hostkey
          Feature IDB type      : Sub-if or not required

  Service "GAMING_SERVICE":
    Version 1:
      SVM ID                : 5E000003
      Child ID              : FB000007
      Locked by             : SVM-Feature-Info       [4]
      Locked by             : SVM-Printer            [1]
      Locked by             : PM-Service             [722]
      Locked by             : PM-Info                [722]
      Locked by             : FM-Bind                [718]
      Locked by             : TC-Child               [1]
      Locked by             : Accounting-Feature     [718]
      Profile               : 21E3AE18
        Profile name: GAMING_SERVICE, 1440 references
          idletime             1800 (0x708)
          traffic-class        "in access-group name GAMING_IN_ACL priority 10"
          traffic-class        "in default drop"
          traffic-class        "out access-group name GAMING_OUT_ACL priority 10"
          traffic-class        "out default drop"
          accounting-list      "CAR_ACCNT_LIST"
          ssg-service-info     "IGAMING_SERVICE"
          ssg-service-info     "R42.1.1.0;255.255.255.0"
      Feature               : TC
          Feature IDB type      : Sub-if or not required
          Feature Data          : 28 bytes:
                                : 000000 00 00 FB 00 00 07 00 00  ........
                                : 000008 00 0A 01 00 00 00 21 D2  ......!.
                                : 000010 F4 F8 00 00 00 0A 01 00  ........
                                : 000018 00 00 64 BD              ..d.
      Version 1:
        SVM ID                : FB000007
        Parent ID             : 5E000003
        Locked by             : SVM-Printer            [1]
        Locked by             : FM-Bind                [719]
        Locked by             : TC-Parent              [1]
        Feature               : Idle Timeout
          Feature IDB type      : Sub-if or not required
          Feature Data          : 8 bytes:
                                : 000000 00 00 00 1B 77 40 01 01  ....w@..
        Feature               : Accounting
          Feature IDB type      : Sub-if or not required
          Feature Data          : 24 bytes:
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
                                : 000000 00 00 5E 00 00 03 64 BE  ..^...d.
                                : 000008 03 B0 00 00 00 0F 00 00  ........
                                : 000010 00 01 00 00 00 00 00 00  ........

Service "VOD_SERVICE":
  Version 1:
    SVM ID                  : AB000004
    Child ID                : 41000008
    Locked by               : SVM-Feature-Info       [4]
    Locked by               : SVM-Printer            [1]
    Locked by               : PM-Service             [720]
    Locked by               : PM-Info                [720]
    Locked by               : FM-Bind                [716]
    Locked by               : TC-Child               [1]
    Locked by               : Accounting-Feature     [716]
    Profile                 : 21E3AD58
      Profile name: VOD_SERVICE, 1442 references
        idletime             1800 (0x708)
        traffic-class        "in access-group name VOD_IN_ACL priority 10"
        traffic-class        "in default drop"
        traffic-class        "out access-group name VOD_OUT_ACL priority 10"
        traffic-class        "out default drop"
        accounting-list      "CAR_ACCNT_LIST"
        ssg-service-info     "IVOD_SERVICE"
        ssg-service-info     "R42.1.1.0;255.255.255.0"
    Feature                 : TC
        Feature IDB type       : Sub-if or not required
        Feature Data           : 28 bytes:
                               : 000000 00 00 41 00 00 08 00 00  ..a.....
                               : 000008 00 0A 01 00 00 00 53 18  ......s.
                               : 000010 C0 28 00 00 00 0A 01 00  .(......
                               : 000018 00 00 53 19              ..s.
    Version 1:
      SVM ID                : 41000008
      Parent ID             : AB000004
      Locked by             : SVM-Printer            [1]
      Locked by             : FM-Bind                [716]
      Locked by             : TC-Parent              [1]
      Feature               : Idle Timeout
        Feature IDB type       : Sub-if or not required
        Feature Data           : 8 bytes:
                               : 000000 00 00 00 1B 77 40 01 01  ....w@..
      Feature               : Accounting
        Feature IDB type       : Sub-if or not required
        Feature Data           : 24 bytes:
                               : 000000 00 00 AB 00 00 04 52 30  ......r0
                               : 000008 4C B8 00 00 00 0F 00 00  l.......
                               : 000010 00 01 00 00 00 00 00 00  ........

Service "VOIP_SERVICE":
  Version 1:
    SVM ID                  : 39000005
    Child ID                : E2000009
    Locked by               : SVM-Feature-Info       [4]
    Locked by               : SVM-Printer            [1]
    Locked by               : PM-Service             [719]
    Locked by               : PM-Info                [719]
    Locked by               : FM-Bind                [715]
    Locked by               : TC-Child               [1]
    Locked by               : Accounting-Feature     [716]
    Profile                 : 21E3AD38
      Profile name: VOIP_SERVICE, 1440 references
        idletime             1800 (0x708)
        traffic-class        "in access-group name VOIP_IN_ACL priority 10"
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
        traffic-class        "in default drop"
        traffic-class        "out access-group name VOIP_OUT_ACL priority 10"
        traffic-class        "out default drop"
        accounting-list      "CAR_ACCNT_LIST"
        ssg-service-info     "IVOIP_SERVICE"
        ssg-service-info     "R42.1.1.0;255.255.255.0"
    Feature               : TC
        Feature IDB type      : Sub-if or not required
        Feature Data          : 28 bytes:
                              : 000000 00 00 E2 00 00 09 00 00  ........
                              : 000008 00 0A 01 00 00 00 23 2C  ......#,
                              : 000010 33 B0 00 00 00 0A 01 00  3.......
                              : 000018 00 00 52 0C              ..r.
    Version 1:
      SVM ID                : E2000009
      Parent ID             : 39000005
      Locked by             : SVM-Feature-Info       [3]
      Locked by             : SVM-Printer            [1]
      Locked by             : FM-Bind                [716]
      Locked by             : SM-SIP-Apply           [3]
      Locked by             : TC-Parent              [1]
      Feature               : Idle Timeout
        Feature IDB type      : Sub-if or not required
        Feature Data          : 8 bytes:
                              : 000000 00 00 00 1B 77 40 01 01  ....w@..
      Feature               : Accounting
        Feature IDB type      : Sub-if or not required
        Feature Data          : 24 bytes:
                              : 000000 00 00 39 00 00 05 51 12  ..9...q.
                              : 000008 60 F0 00 00 00 0F 00 00  `.......
                              : 000010 00 01 00 00 00 00 00 00  ........

Service "OPENGARDEN_SERVICE":
  Version 1:
    SVM ID                : 77000006
    Child ID              : E300000A
    Locked by             : SVM-Feature-Info       [5]
    Locked by             : SVM-Printer            [1]
    Locked by             : PM-Service             [722]
    Locked by             : PM-Info                [722]
    Locked by             : FM-Bind                [717]
    Locked by             : TC-Child               [1]
    Profile               : 21E3AD18
      Profile name: OPENGARDEN_SERVICE, 1446 references
        traffic-class        "in access-group name OPENGARDEN_IN_ACL"
        traffic-class        "in default drop"
        traffic-class        "out access-group name OPENGARDEN_OUT_ACL"
        traffic-class        "out default drop"
        ssg-service-info     "IOPENGARDEN_SERVICE"
    Feature               : TC
        Feature IDB type      : Sub-if or not required
        Feature Data          : 28 bytes:
                              : 000000 00 00 E3 00 00 0A 00 00  ........
                              : 000008 00 00 01 00 00 00 51 0F  ......q.
                              : 000010 28 C0 00 00 00 00 01 00  (.......
                              : 000018 00 00 51 12              ..q.
    Version 1:
      SVM ID                : E300000A
      Parent ID             : 77000006
      Locked by             : SVM-Feature-Info       [3]
      Locked by             : SVM-Printer            [1]
      Locked by             : FM-Bind                [717]
      Locked by             : SM-SIP-Apply           [3]
      Locked by             : TC-Parent              [1]
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
Service "L4REDIRECT_SERVICE":
  Version 1:
    SVM ID                : AC000030
    Child ID              : 6D000031
    Locked by             : SVM-Printer            [1]
    Locked by             : PM-Service             [267]
    Locked by             : PM-Info                [2707]
    Locked by             : FM-Bind                [268]
    Locked by             : TC-Child               [1]
    Profile               : 242C1A08
      Profile name: L4REDIRECT_SERVICE, 5149 references
        traffic-class        "in access-group name IP_REDIRECT_ACL priority 5"
        traffic-class        "in default drop"
        traffic-class        "out access-group name IP_REDIRECT_ACL priority 5"
        traffic-class        "out default drop"
        l4redirect           "redirect to group SESM_SERVER_GROUP"
        ssg-service-info     "IL4REDIRECT_SERVICE"
    Feature               : TC
        Feature IDB type      : Sub-if or not required
        Feature Data          : 28 bytes:
                              : 000000 00 00 6D 00 00 31 00 00  ..m..1..
                              : 000008 00 05 01 00 00 00 53 B8  ......s.
                              : 000010 CF C0 00 00 00 05 01 00  ........
                              : 000018 00 00 24 19              ..$.
    Version 1:
      SVM ID                : 6D000031
      Parent ID             : AC000030
      Locked by             : SVM-Printer            [1]
      Locked by             : FM-Bind                [267]
      Locked by             : TC-Parent              [1]
      Feature               : L4 Redirect
        Feature IDB type      : Sub-if or not required
        Feature Data          : 20 bytes:
                              : 000000 00 00 64 72 B7 F8 64 72  ..dr..dr
                              : 000008 B7 F8 00 00 00 01 00 00  ........
                              : 000010 00 00 00 00              ....

Service "BOD1MTIME_DM2":
  Version 1:
    SVM ID                : 19000053
    Child ID              : 13000054
    Locked by             : SVM-Printer            [1]
    Locked by             : PM-Service             [2440]
    Locked by             : PM-Info                [2440]
    Locked by             : FM-Bind                [2440]
    Locked by             : TC-Child               [1]
    Locked by             : Accounting-Feature     [2440]
    Profile               : 242C1A48
      Profile name: BOD1MTIME_DM2, 4882 references
        traffic-class        "in access-group name INTERNET_IN_ACL priority 10"
        traffic-class        "in default drop"
        traffic-class        "out access-group name INTERNET_OUT_ACL priority 10"
        traffic-class        "out default drop"
        accounting-list      "PREPAID_ACCNT_LIST"
        peak-cell-rate       1024 (0x400)
        sustainable-cell-rat 1024 (0x400)
        ssg-service-info     "IBOD1MTIME_DM2"
        ssg-service-info     "R42.1.1.0;255.255.255.0"
    Feature               : TC
        Feature IDB type      : Sub-if or not required
        Feature Data          : 28 bytes:
                              : 000000 00 00 13 00 00 54 00 00  .....t..
                              : 000008 00 0A 01 00 00 00 56 B7  ......v.
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
                                : 000010 49 80 00 00 00 0A 01 00  i.......
                                : 000018 00 00 24 62              ..$b
          SIP                   : Info 23E85AB8 access: PPPoE info: PPPoE
      Version 1:
        SVM ID                : 13000054
        Parent ID             : 19000053
        Locked by             : SVM-Printer            [1]
        Locked by             : FM-Bind                [2440]
        Locked by             : TC-Parent              [1]
        Feature               : Accounting
          Feature IDB type      : Sub-if or not required
          Feature Data          : 24 bytes:
                                : 000000 00 00 19 00 00 53 24 70  .....s$p
                                : 000008 61 68 00 00 00 0F 00 00  ah......
                                : 000010 00 01 00 00 00 00 00 00  ........

  Service "INTERNET_SERVICE":
    Version 1:
      SVM ID                : EE000055
      Locked by             : SVM-Printer            [1]
      Locked by             : PM-Service             [200]
      Locked by             : PM-Info                [200]
      Locked by             : FM-Bind                [200]
      Profile               : 21E3AC78
        Profile name: INTERNET_SERVICE, 402 references
          inacl               "INTERNET_IN_ACL"
          outacl              "INTERNET_OUT_ACL"
          ssg-service-info    "IINTERNET_SERVICE"
          ssg-service-info    "R42.1.1.0;255.255.255.0"
      Feature               : Per-User ACL
          Feature IDB type      : Sub-if or not required
          Feature Data          : 52 bytes:
                                : 000000 00 00 26 0C 07 A6 00 00  ..&.....
                                : 000008 00 00 00 00 00 00 F6 01  ........
                                : 000010 07 B3 00 00 00 00 00 00  ........
                                : 000018 00 00 00 00 00 01 00 00  ........
                                : 000020 00 00 00 00 00 00 00 00  ........
                                : 000028 00 01 00 00 00 00 00 00  ........
                                : 000030 00 00 00 00              ....
```

The **show subscriber policy rule** command shows all of the rules that are configured on the ISG and the number of times they have been executed.

```
ie2-C7206-ATM# show subscriber policy rule
Rule: internal-rule-acct-logon
  Class-map:  always event account-logon
    Action: 1 authenticate aaa list default
    Executed0

Rule: RULE_L2TP_LM_ATM7
  Class-map:  always event session-start
    Action: 1 collect identifier unauthenticated-domain
    Executed0
    Action: 2 authorize identifier unauthenticated-domain
    Executed0

Rule: RULE_L2TP_LM_ATM3
  Class-map:  always event session-start
    Action: 1 collect identifier unauthenticated-domain
    Executed0
    Action: 2 authorize identifier unauthenticated-domain
    Executed0

Rule: RULE_IP_LM_ATM2
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
  Class-map:  IP_UNAUTH_COND event timed-policy-expiry
    Action: 1 service disconnect
    Executed5388
  Class-map:  TAL_STATIC_DM3 event session-start
    Action: 1 service-policy type service name PBHK_SERVICE
    Executed29007
    Action: 2 authorize identifier source-ip-address
    Executed28662
    Action: 3 service-policy type service name L4REDIRECT_SERVICE
    Executed5588
    Action: 4 set-timer IP_UNAUTH_TIMER 5
    Executed5588
  Class-map:  always event session-start
    Action: 1 service-policy type service name PBHK_SERVICE
    Executed7199
    Action: 2 authorize identifier mac-address
    Executed6004
    Action: 3 service-policy type service name L4REDIRECT_SERVICE
    Executed5999
    Action: 4 set-timer IP_UNAUTH_TIMER 5
    Executed5999
  Class-map:  always event account-logon
    Action: 1 authenticate aaa list IP_AUTHEN_LIST
    Executed0
    Action: 2 service-policy type service unapply name L4REDIRECT_SERVICE
    Executed0

Rule: RULE_PTA_LM_ATM2
  Class-map:  always event session-start
    Action: 1 service-policy type service name PBHK_SERVICE
    Executed0

Rule: RULE_IP_LM_ATM7
  Class-map:  TAL_STATIC_DM4 event session-start
    Action: 1 service-policy type service name PBHK_SERVICE
    Executed22957
    Action: 2 authorize identifier source-ip-address
    Executed22902
    Action: 3 service-policy type service name L4REDIRECT_SERVICE
    Executed37
    Action: 4 set-timer IP_UNAUTH_TIMER 5
    Executed37
  Class-map:  IP_UNAUTH_COND event timed-policy-expiry
    Action: 1 service disconnect
    Executed38
  Class-map:  always event session-start
    Action: 1 service-policy type service name PBHK_SERVICE
    Executed600
    Action: 2 authorize identifier mac-address
    Executed200
    Action: 3 service-policy type service name L4REDIRECT_SERVICE
    Executed1
    Action: 4 set-timer IP_UNAUTH_TIMER 5
    Executed1
  Class-map:  always event account-logon
    Action: 1 authenticate aaa list IP_AUTHEN_LIST
    Executed0
    Action: 2 service-policy type service unapply name L4REDIRECT_SERVICE
    Executed0

Rule: RULE_PTA_TIME_LM_ATM8
  Class-map:  BOD1MTIME_CLASS_DM2 event service-start
    Action: 1 service-policy type service unapply name L4REDIRECT_SERVICE
    Executed47256
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
      Action: 2 service-policy type service unapply name BOD2MTIME_DM2
      Executed47256
      Action: 3 service-policy type service identifier service-name
      Executed47256
    Class-map:  BOD2MTIME_CLASS_DM2 event service-start
      Action: 1 service-policy type service unapply name L4REDIRECT_SERVICE
      Executed0
      Action: 2 service-policy type service unapply name BOD1MTIME_DM2
      Executed0
      Action: 3 service-policy type service identifier service-name
      Executed0
    Class-map:  BOD2MTIME_CLASS_DM2 event service-stop
      Action: 1 service-policy type service unapply identifier service-name
      Executed0
      Action: 2 service-policy type service name L4REDIRECT_SERVICE
      Executed0
    Class-map:  BOD1MTIME_CLASS_DM2 event service-stop
      Action: 1 service-policy type service unapply identifier service-name
      Executed1
      Action: 2 service-policy type service name L4REDIRECT_SERVICE
      Executed1
    Class-map:  always event session-start
      Action: 1 service-policy type service name PBHK_SERVICE
      Executed49636
      Action: 2 service-policy type service name L4REDIRECT_SERVICE
      Executed48636
    Class-map:  always event quota-depleted
      Action: 1 set-param drop-traffic FALSE
      Executed0
    Class-map:  always event credit-exhausted
      Action: 1 service-policy type service name L4REDIRECT_SERVICE
      Executed0
    Class-map:  always event internal-event-cre-t-exp
      Action: 1 service-policy type service unapply name L4REDIRECT_SERVICE
      Executed0

  Rule: RULE_PTA_VOLUME_LM_ATM8
    Class-map:  BOD1MVOLUME_CLASS_DM2 event service-start
      Action: 1 service-policy type service unapply name L4REDIRECT_SERVICE
      Executed0
      Action: 2 service-policy type service unapply name BOD2MVOLUME_DM2
      Executed0
      Action: 3 service-policy type service identifier service-name
      Executed0
    Class-map:  BOD2MVOLUME_CLASS_DM2 event service-start
      Action: 1 service-policy type service unapply name L4REDIRECT_SERVICE
      Executed0
      Action: 2 service-policy type service unapply name BOD1MVOLUME_DM2
      Executed0
      Action: 3 service-policy type service identifier service-name
      Executed0
    Class-map:  BOD2MVOLUME_CLASS_DM2 event service-stop
      Action: 1 service-policy type service unapply identifier service-name
      Executed0
      Action: 2 service-policy type service name L4REDIRECT_SERVICE
      Executed0
    Class-map:  BOD1MVOLUME_CLASS_DM2 event service-stop
      Action: 1 service-policy type service unapply identifier service-name
      Executed0
      Action: 2 service-policy type service name L4REDIRECT_SERVICE
      Executed0
    Class-map:  always event session-start
      Action: 1 service-policy type service name PBHK_SERVICE
      Executed0
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
    Action: 2 service-policy type service name L4REDIRECT_SERVICE
    Executed0
  Class-map:  always event quota-depleted
    Action: 1 set-param drop-traffic FALSE
    Executed0
  Class-map:  always event credit-exhausted
    Action: 1 service-policy type service name L4REDIRECT_SERVICE
    Executed0
  Class-map:  always event internal-event-cre-t-exp
    Action: 1 service-policy type service unapply name L4REDIRECT_SERVICE
    Executed0

Key:
  "Exec" - The number of times this rule action line was executed
ie2-C7206-ATM#
```

Basic ISG Operation Verification

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

```
ie2-C7206-ATM# show subscriber statistics

Current Subscriber Statistics:

Number of sessions currently up: 3227
Number of sessions currently pending: 193
Number of sessions currently authenticated: 3101
Number of sessions currently unauthenticated: 0
Highest number of sessions ever up at one time: 3760
Mean up-time duration of sessions: 00:05:12
Total number of sessions up so far: 105408
Mean call rate per minute: 484, per hour: 35200
Number of sessions failed to come up: 3401
Access type based session count:
PPPoE sessions = 2640
Traffic-Class sessions = 4594
IP sessions = 780
```

The **show subscriber session** command shows basic information for all active subscribers.

```
ie2-C7206-LNS# show subscriber session
Current Subscriber Information: Total sessions 3370

Uniq ID Interface  State         Service      Identifier           Up-time
! This is the VID for the subscriber
4910    Vi2.2122   authen        Local Term   C72_DM2_3021         00:03:41
! This is the VID for the subscriber's traffic classes
1748    Traffic-Cl unauthen      Ltm Internal                      00:04:27
10709   Traffic-Cl unauthen      Ltm Internal                      00:04:23
6514    Vi2.78     authen        Local Term   C72_DM2_1078         00:04:55
5650    Traffic-Cl unauthen      Ltm Internal C72_DM2_1446         00:04:46
3771    Traffic-Cl unauthen      Ltm Internal                      00:01:01
2601    Vi2.1558   authen        Local Term   C72_DM2_2097         00:04:12
3508    Traffic-Cl unauthen      Ltm Internal                      00:01:16
9767    Traffic-Cl unauthen      Ltm Internal C72_DM2_1390         00:04:48
```

The **show ip route vrf VPN11006** command shows routing table information for the VRF. In the following output, there is one active subscriber session.

```
ie2-C7206-LNS# show ip route vrf VPN11006
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
Routing Table: VPN11006
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     84.0.0.0/24 is subnetted, 1 subnets
B       84.1.206.0 [200/0] via 10.200.1.43, 4d19h
     100.0.0.0/32 is subnetted, 1 subnets
C       100.6.6.6 is directly connected, Loopback1
     200.53.6.0/32 is subnetted, 1 subnets
! This shows that the subscriber is connected and part of vrf VPN11006
C       200.53.6.2 is directly connected, Virtual-Access3
     200.6.6.0/32 is subnetted, 1 subnets
B       200.6.6.6 [200/0] via 10.200.1.56, 4d19h
     10.0.0.0/32 is subnetted, 1 subnets
B       10.100.4.38 [200/0] via 10.200.1.43, 4d19h
ie2-C7206-LNS#
```

Subscriber Service Verification

The **show subscriber session username c72_DM2_1078** command shows detailed information for the subscriber with the username c72_DM2_1078. The following output is for a subscriber with the BOD1MTIME_DM2 service.

```
ie2-C7206-ATM# show subscriber session username C72_DM2_1078
Unique Session ID: 6514
Identifier: C72_DM2_1078
SIP subscriber access type(s): PPPoE/PPP
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 00:06:17, Last Changed: 00:06:17
AAA unique ID: 102346
Interface: Virtual-Access2.78

Policy information:
  Context 25559F94: Handle 310104C8
  Authentication status: authen
  Active services associated with session:
! Indicates the services that the subscriber is using.
    name "BOD1MTIME_DM2"
    name "PBHK_SERVICE", applied outwith active session
  Rules, actions and conditions executed:
    subscriber rule-map RULE_PTA_TIME_LM_ATM8
      condition always event session-start
        1 service-policy type service name PBHK_SERVICE
        2 service-policy type service name L4REDIRECT_SERVICE
    subscriber rule-map RULE_PTA_TIME_LM_ATM8
      condition BOD1MTIME_CLASS_DM2 event service-start
        subscriber condition-map match-all BOD1MTIME_CLASS_DM2
          match identifier service-name BOD1MTIME_DM2 [TRUE]
    subscriber rule-map RULE_PTA_TIME_LM_ATM8
      condition BOD1MTIME_CLASS_DM2 event service-start
        1 service-policy type service unapply name L4REDIRECT_SERVICE
        2 service-policy type service unapply name BOD2MTIME_DM2
        3 service-policy type service identifier service-name
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
Session inbound features:
 Feature: PPP Idle Timeout
  Timeout value is 1800
  Idle time is 00:06:25
 Feature: Layer 4 Redirect
  Rule table is empty
Traffic classes:
  Traffic class session ID: 3947
   ACL Name: INTERNET_IN_ACL, Packets = 0, Bytes = 0
 Default traffic is dropped
 Unmatched Packets (dropped) = 0, Re-classified packets (redirected) = 0
! Portbound Hostkey information for the subscriber.
 Feature: Portbundle Hostkey
 Portbundle IP = 10.200.1.53     Bundle Number = 1229

Session outbound features:
 Feature: PPP Idle Timeout
  Timeout value is 1800
  Idle time is 00:06:25
Traffic classes:
  Traffic class session ID: 3947
! Identifies the ACL that restricts inbound traffic. The ACL is configured on the ISG,
! and it is applied to the subscriber based on the subscriber profile on the AAA server.
   ACL Name: INTERNET_OUT_ACL, Packets = 0, Bytes = 0
 Default traffic is dropped
 Unmatched Packets (dropped) = 0, Re-classified packets (redirected) = 0

Non-datapath features:
 Feature: Session Timeout
  Timeout value is 18000 seconds
! Indicates the amount of time remaining before the session times out.
  Time remaining is 04:53:33
 Feature: IP Config
  Peer IP Address: 0.0.0.0 (F/F)
  Address Pool: C72_DM2_8003 (F)
  Unnumbered Intf: Lo8001
Configuration sources associated with this session:
! Indicates how long the BOD1MTIME_DM2 service has been active.
Service: BOD1MTIME_DM2, Active Time = 00:06:26
  AAA Service ID = 1441613880
Service: PBHK_SERVICE, Active Time = 00:06:27
Interface: Virtual-Template8, Active Time = 00:06:27
```

The **show subscriber session username C72_DM2_1078 detail** shows further details about the subscriber's session.

```
ie2-C7206-ATM# show subscriber session username C72_DM2_1078 detail
Unique Session ID: 6514
Identifier: C72_DM2_1078
SIP subscriber access type(s): PPPoE/PPP
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 00:06:32, Last Changed: 00:06:32
AAA unique ID: 102346
Interface: Virtual-Access2.78

Policy information:
  Context 25559F94: Handle 310104C8
  Authentication status: authen
  Downloaded User profile, excluding services:
    service-type          2 [Framed]
    Framed-Protocol       1 [PPP]
    routing               False
    Framed-MTU            1500 (0x5DC)
    timeout               18000 (0x4650)
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
    idletime             1800 (0x708)
! The "A" stands for auto-login, which indicates that BOD1MTIME_DM2 is the default
! service.
    ssg-account-info     "ABOD1MTIME_DM2"
! The "N" indicates that the subscriber is allowed access the BOD2MTIME_DM2 service based
! on the subscriber's AAA profile.
    ssg-account-info     "NBOD2MTIME_DM2"
    idletime             1800 (0x708)
    vrf-id               "VPN_C72_DM2_1003"
    ip-unnumbered        "loopback 8001"
    addr-pool            "C72_DM2_8003"
  Downloaded User profile, including services:
    portbundle           "enable"
    service-type         2 [Framed]
    Framed-Protocol      1 [PPP]
    routing              False
    Framed-MTU           1500 (0x5DC)
    timeout              18000 (0x4650)
    idletime             1800 (0x708)
    ssg-account-info     "ABOD1MTIME_DM2"
    ssg-account-info     "NBOD2MTIME_DM2"
    idletime             1800 (0x708)
    vrf-id               "VPN_C72_DM2_1003"
    ip-unnumbered        "loopback 8001"
    addr-pool            "C72_DM2_8003"
    traffic-class        "in access-group name INTERNET_IN_ACL priority 10"
    traffic-class        "in default drop"
    traffic-class        "out access-group name INTERNET_OUT_ACL priority 10"
    traffic-class        "out default drop"
    accounting-list      "PREPAID_ACCNT_LIST"
    peak-cell-rate       1024 (0x400)
    sustainable-cell-rat 1024 (0x400)
    ssg-service-info     "IBOD1MTIME_DM2"
    ssg-service-info     "R42.1.1.0;255.255.255.0"
  Config history for session (recent to oldest):
    Access-type: Web-service-logon Client: SM
     Policy event: Process Config (Service)
      Profile name: BOD1MTIME_DM2, 4882 references
        traffic-class        "in access-group name INTERNET_IN_ACL priority 10"
        traffic-class        "in default drop"
        traffic-class        "out access-group name INTERNET_OUT_ACL priority 10"
        traffic-class        "out default drop"
        accounting-list      "PREPAID_ACCNT_LIST"
        peak-cell-rate       1024 (0x400)
        sustainable-cell-rat 1024 (0x400)
        ssg-service-info     "IBOD1MTIME_DM2"
        ssg-service-info     "R42.1.1.0;255.255.255.0"
    Access-type: Max Client: SM
! Describers the Layer 4 Reidrect service, which is not currently applied.
     Policy event: Process Config (Unapplied) (Service)
      Profile name: L4REDIRECT_SERVICE, 5082 references
        traffic-class        "in access-group name IP_REDIRECT_ACL priority 5"
        traffic-class        "in default drop"
        traffic-class        "out access-group name IP_REDIRECT_ACL priority 5"
        traffic-class        "out default drop"
        l4redirect           "redirect to group SESM_SERVER_GROUP"
        ssg-service-info     "IL4REDIRECT_SERVICE"
    Access-type: PPP Client: SM
     Policy event: Process Config
      Profile name: apply-config-only, 28 references
        service-type         2 [Framed]
        Framed-Protocol      1 [PPP]
        routing              False
        Framed-MTU           1500 (0x5DC)
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
        timeout              18000 (0x4650)
        idletime             1800 (0x708)
        ssg-account-info     "ABOD1MTIME_DM2"
        ssg-account-info     "NBOD2MTIME_DM2"
        idletime             1800 (0x708)
        vrf-id               "VPN_C72_DM2_1003"
        ip-unnumbered        "loopback 8001"
        addr-pool            "C72_DM2_8003"
    Access-type: PPPoE Client: SM
     Policy event: Service Selection Request (Service)
      Profile name: L4REDIRECT_SERVICE, 5082 references
        traffic-class        "in access-group name IP_REDIRECT_ACL priority 5"
        traffic-class        "in default drop"
        traffic-class        "out access-group name IP_REDIRECT_ACL priority 5"
        traffic-class        "out default drop"
        l4redirect           "redirect to group SESM_SERVER_GROUP"
        ssg-service-info     "IL4REDIRECT_SERVICE"
    Access-type: PPPoE Client: SM
     Policy event: Service Selection Request (Service)
      Profile name: PBHK_SERVICE, 3379 references
        portbundle           "enable"
        ssg-service-info     "IPBHK_SERVICE"
  Active services associated with session:
    name "BOD1MTIME_DM2"
    name "PBHK_SERVICE", applied outwith active session
  Rules, actions and conditions executed:
    subscriber rule-map RULE_PTA_TIME_LM_ATM8
      condition always event session-start
        1 service-policy type service name PBHK_SERVICE
        2 service-policy type service name L4REDIRECT_SERVICE
    subscriber rule-map RULE_PTA_TIME_LM_ATM8
      condition BOD1MTIME_CLASS_DM2 event service-start
        subscriber condition-map match-all BOD1MTIME_CLASS_DM2
! Services that are active are identified as "TRUE."
          match identifier service-name BOD1MTIME_DM2 [TRUE]
    subscriber rule-map RULE_PTA_TIME_LM_ATM8
      condition BOD1MTIME_CLASS_DM2 event service-start
        1 service-policy type service unapply name L4REDIRECT_SERVICE
        2 service-policy type service unapply name BOD2MTIME_DM2
        3 service-policy type service identifier service-name

Session inbound features:
 Feature: PPP Idle Timeout
  Timeout value is 1800
  Idle time is 00:06:35
 Feature: Layer 4 Redirect
  Rule table is empty
Traffic classes:
  Traffic class session ID: 3947
! Identifies the ACL that restricts inbound traffic. The ACL is configured on the ISG LNS,
! and it is applied to the subscriber based on the subscriber profile on the AAA server.
   ACL Name: INTERNET-IN-ACL, Packets = 0, Bytes = 0
 Default traffic is dropped
 Unmatched Packets (dropped) = 0, Re-classified packets (redirected) = 0

 Feature: Portbundle Hostkey
! Identifies the PBHK IP address and the bundle number. This information can be used to
! troubleshoot PBHK with the show ip portbundle command.
 Portbundle IP = 10.200.1.53     Bundle Number = 1229

Session outbound features:
 Feature: PPP Idle Timeout
  Timeout value is 1800
  Idle time is 00:06:35
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
Traffic classes:
  Traffic class session ID: 3947
   ACL Name: INTERNET_OUT_ACL, Packets = 0, Bytes = 0
 Default traffic is dropped
 Unmatched Packets (dropped) = 0, Re-classified packets (redirected) = 0

Non-datapath features:
 Feature: Session Timeout
  Timeout value is 18000 seconds
  Time remaining is 04:53:23
 Feature: IP Config
  Peer IP Address: 0.0.0.0 (F/F)
  Address Pool: C72_DM2_8003 (F)
  Unnumbered Intf: Lo8001
Configuration sources associated with this session:
Service: BOD1MTIME_DM2, Active Time = 00:06:35
  AAA Service ID = 1441613880
Service: PBHK_SERVICE, Active Time = 00:06:36
Interface: Virtual-Template8, Active Time = 00:06:36
```

Complete Running Configurations

The following sections contain complete running configurations for the devices in the various deployments:

- Deployment Model 1: Basic Internet Access Service Bundle over L2TP, page 77
- Deployment Model 2: Multiservice Service Bundle over PPPoE, page 86
- Deployment Model 3: Triple Play Plus Service Bundle over IP and PPPoE, page 96
- Deployment Model 4: Triple Play Plus Service Bundle over IP and L2TP, page 105

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

Deployment Model 1: Basic Internet Access Service Bundle over L2TP

The following sections contain the complete running configurations for the devices in Deployment Model 1:

Deployment Model 1: CPE

```
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log uptime
no service password-encryption
!
hostname ie2-C837-CPE5
!
!
no aaa new-model
ip subnet-zero
no ip domain lookup
ip dhcp excluded-address 10.10.10.1
!
ip dhcp pool CLIENT
   import all
   network 10.10.10.0 255.255.255.0
   default-router 10.10.10.1
   lease 0 2
!
!
ip audit notify log
ip audit po max-events 100
vpdn enable
!
vpdn-group ppoe
 request-dialin
  protocol pppoe
!
no ftp-server write-enable
!
!
!
!
!
!
!
interface Ethernet0
 ip address 10.10.10.1 255.255.255.0
 ip nat inside
 ip tcp adjust-mss 1452
 load-interval 30
 hold-queue 100 out
!
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
interface ATM0
 no ip address
 shutdown
 no atm ilmi-keepalive
 dsl operating-mode auto
!
interface ATM0.5 point-to-point
 pvc 5/45
  pppoe max-sessions 100
  pppoe-client dial-pool-number 1
 !
!
interface FastEthernet1
 no ip address
 duplex auto
 speed auto
!
interface Dialer1
 ip address negotiated
 ip nat outside
 encapsulation ppp
 dialer pool 1
 dialer-group 1
 ppp authentication chap callin
 ppp chap hostname C73_DM1_01@L2TP_DM1_101.com
 ppp chap password 0 lab
!
!
ip nat inside source list 23 interface Dialer1 overload
ip classless
ip route 0.0.0.0 0.0.0.0 Dialer1
ip http server
no ip http secure-server
!
access-list 23 permit 10.10.10.0 0.0.0.255
!
line con 0
 exec-timeout 0 0
 no modem enable
 stopbits 1
line aux 0
line vty 0 4
 access-class 23 in
 exec-timeout 120 0
 login local
```

Deployment Model 1: ISG LAC

```
version 12.2
no service pad
service config
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname ie2-C7206-ATM
!
boot-start-marker
boot host tftp ie2/configs/tc5xx/isg_add_tc5xx_pta.dat 223.255.12.34
boot system disk2:c7200-js-mz.122-27.1.11.SIE7
boot-end-marker
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
!
logging buffered 1000000 debugging
no logging console
enable password lab
!
aaa new-model
!
!
!
aaa group server radius CAR_SERVER
 server 10.100.1.35 auth-port 1812 acct-port 1813
!
aaa authentication login default none
aaa authentication login IP_AUTHEN_LIST group CAR_SERVER
aaa authentication ppp default group CAR_SERVER
aaa authorization network default group CAR_SERVER
aaa authorization subscriber-service default local group radius
aaa accounting network default start-stop group CAR_SERVER
!
aaa session-id common
clock timezone Pacific -8
ip subnet-zero
!
!
ip ftp username root
ip ftp password lab
ip dhcp smart-relay
ip dhcp relay information option vpn
ip dhcp relay information option
ip dhcp relay information trust-all
no ip dhcp use vrf connected
!
ip cef
!
subscriber policy recording rules limit 64
subscriber authorization enable
vpdn enable
vpdn ip udp ignore checksum
vpdn search-order domain
!
no mpls traffic-eng auto-bw timers frequency 0
call rsvp-sync
!
!
!
policy-map control RULE_L2TP_LM_ATM3
 class control always event session-start
  1 collect identifier unauthenticated-domain
  2 authorize identifier unauthenticated-domain
 !
!
!
bba-group pppoe BBA_LM_ATM3
 virtual-template 3
!
vc-class atm VC_LM_ATM3
  protocol pppoe group BBA_LM_ATM3
  dbs enable maximum
  encapsulation aal5snap
  service-policy control RULE_L2TP_LM_ATM3
!
interface Loopback0
 ip address 10.200.1.53 255.255.255.255
!
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
interface GigabitEthernet0/1
 ip address 223.255.12.53 255.255.255.0
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
!
interface GigabitEthernet0/3
 ip address 40.40.1.53 255.255.255.0
 load-interval 30
 duplex full
 speed 1000
 media-type gbic
 negotiation auto
 mpls mtu 1522
 mpls ip
 ip rsvp bandwidth 100000
!
interface ATM1/0
 no ip address
 load-interval 30
 no atm auto-configuration
 no atm ilmi-keepalive
 no atm address-registration
 no atm ilmi-enable
 no atm enable-ilmi-trap
 bundle-enable
!
interface ATM1/0.101 multipoint
 description ATM Deployment Model 1
 no atm enable-ilmi-trap
 pvc 101/41
  class-vc VC_LM_ATM3
 !
!
interface Virtual-Template3
 description VT for LM_ATM3
 no ip address
 no peer default ip address
 no keepalive
 ppp authentication chap
 ppp timeout aaa
!
router ospf 100
 router-id 10.200.1.53
 log-adjacency-changes
 area 100 range 200.53.0.0 255.255.0.0
 redistribute connected
 redistribute static subnets
 network 10.200.1.53 0.0.0.0 area 100
 network 20.20.1.0 0.0.0.255 area 100
 network 40.40.1.0 0.0.0.255 area 100
 network 200.53.0.0 0.0.255.255 area 100
!
router bgp 100
 no synchronization
 bgp router-id 10.200.1.53
 bgp log-neighbor-changes
 network 200.53.0.0 mask 255.255.0.0
 aggregate-address 200.53.3.0 255.255.255.0 summary-only
 redistribute connected
 redistribute static
 neighbor 10.200.1.41 remote-as 100
 neighbor 10.200.1.41 update-source Loopback0
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
 no auto-summary
 !
 address-family vpnv4
 neighbor 10.200.1.41 activate
 neighbor 10.200.1.41 send-community both
 exit-address-family
 !
!
ip classless
!
no ip http server
!
!
!
ip radius source-interface Loopback0
!
radius-server host 10.100.1.35 auth-port 1812 acct-port 1813 key cisco
radius-server retransmit 5
radius-server timeout 15
radius-server vsa send accounting
radius-server vsa send authentication
!
control-plane
!
!
dial-peer cor custom
!
!
!
!
gatekeeper
 shutdown
!
alias exec showdb show database data IDMGR-Session-DB 2
alias exec sss show subscriber session
alias exec css clear subscriber session
alias exec ss show subscriber statistics
!
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 exec-timeout 0 0
!
ntp clock-period 17179872
ntp server 10.200.1.41 source GigabitEthernet0/3 prefer
!
end
```

Deployment Model 1: LNS

```
version 12.2
no service pad
service timestamps debug datetime msec localtime
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname ie2-C7301-LNS
!
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
boot-start-marker
boot host ftp://223.255.12.34/tftpboot/ie2/configs/tc5xx/isg_add_tc5xx_lns.dat
boot system disk0:c7301-js-mz.122-27.1.11.SIE7
boot-end-marker
!
logging buffered 2000000 debugging
no logging console
enable password lab
!
aaa new-model
!
!
aaa group server radius CAR_SERVER
 server 10.100.2.36 auth-port 1812 acct-port 1813
!
aaa authentication login default none
aaa authentication login IP_AUTHEN_LIST group CAR_SERVER
aaa authentication ppp default group CAR_SERVER
aaa authorization network default group CAR_SERVER
aaa authorization subscriber-service default local group radius
aaa accounting network default start-stop group CAR_SERVER
aaa server radius sesm
 client 10.100.4.38
 key cisco
 port 1812
 message-authenticator ignore
!
!
aaa session-id common
clock timezone Pacific -8
ip subnet-zero
!
!
ip ftp username root
ip ftp password lab
no ip dhcp use vrf connected
!
!
ip cef
!
subscriber policy recording rules limit 64
vpdn enable
vpdn ip udp ignore checksum
!
!
redirect server-group SESM-Server
 server ip 10.100.4.38 port 8080
!
clns routing
no mpls traffic-eng auto-bw timers frequency 0
mpls label protocol ldp
call rsvp-sync
!
ip vrf VPN_C72_DM1_1001
 rd 200:1001
 route-target export 200:1001
 route-target import 200:1001
!
vpdn-group L2TP_DM1_101
 accept-dialin
  protocol l2tp
  virtual-template 5
 terminate-from hostname L2TP_DM1_101
 local name L2TP_DM1_101
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
 l2tp tunnel password 0 cisco
!

!
!
interface Loopback0
 ip address 10.200.1.56 255.255.255.255
 ip router isis Remote_ISP_7301
!
!
interface Loopback5001
 ip address 5.55.1.1 255.255.0.0
!
!
interface GigabitEthernet0/0
 ip address 223.255.12.56 255.255.255.0
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
!
interface GigabitEthernet0/1
 description connection to ISP2 CORE router
 ip address 27.27.1.56 255.255.255.0
 ip portbundle outside
 ip router isis Remote_ISP_7301
 load-interval 30
 duplex auto
 speed auto
 media-type gbic
 negotiation auto
 mpls label protocol ldp
 mpls ip
!
interface GigabitEthernet0/2
 description connection to ISP1 CORE router
 ip address 26.26.1.56 255.255.255.0
 ip router isis Remote_ISP_7301
 load-interval 30
 duplex auto
 speed auto
 media-type gbic
 negotiation auto
!
interface Virtual-Template5
 no ip address
 load-interval 30
 no peer default ip address
 no keepalive
 ppp mtu adaptive
 ppp authentication chap
!
router isis Remote_ISP_7301
 net 01.0011.5dd1.f01b.00
 redistribute connected
!
router bgp 200
 no synchronization
 bgp router-id 10.200.1.56
 bgp log-neighbor-changes
 network 10.100.4.0 mask 255.255.255.0
 network 10.200.1.47 mask 255.255.255.255
 network 10.200.1.55 mask 255.255.255.255
 network 10.200.1.62 mask 255.255.255.255
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
 network 21.21.1.55 mask 255.255.255.0
 network 22.22.1.55 mask 255.255.255.0
 network 23.0.0.0
 network 24.0.0.0 mask 255.255.0.0
 network 24.5.0.0 mask 255.255.0.0
 redistribute connected
 neighbor 10.200.1.41 remote-as 100
 neighbor 10.200.1.41 ebgp-multihop 2
 neighbor 10.200.1.41 update-source Loopback0
 neighbor 10.200.1.47 remote-as 200
 neighbor 10.200.1.47 update-source Loopback0
 no auto-summary
!
 address-family vpnv4
 neighbor 10.200.1.47 activate
 neighbor 10.200.1.47 send-community both
 exit-address-family
!
 address-family ipv4 vrf VPN_C72_DM1_1001
 redistribute connected
 redistribute static
 no auto-summary
 no synchronization
 exit-address-family
 !
!
ip local pool C73_DM1_3001 1.3.1.2 1.3.255.254
!
ip portbundle
 match access-list 135
 source Loopback0
!
ip classless
ip route 10.200.1.41 255.255.255.255 26.26.1.41
!
no ip http server
!
!
!
ip access-list extended Internet-in-acl
 deny   ip any 223.0.0.0 0.255.255.255
 deny   ip any 20.0.0.0 0.255.255.255
 deny   ip any 40.0.0.0 0.255.255.255
 deny   ip any 21.0.0.0 0.255.255.255
 deny   ip any 22.0.0.0 0.255.255.255
 deny   ip any 41.0.0.0 0.255.255.255
 deny   ip any 80.0.0.0 0.255.255.255
 deny   ip any 81.0.0.0 0.255.255.255
 deny   ip any 82.0.0.0 0.255.255.255
 deny   ip any 10.200.0.0 0.0.255.255
 permit ip any any
ip access-list extended Internet-out-acl
 deny   ip 223.0.0.0 0.255.255.255 any
 deny   ip 10.200.0.0 0.0.255.255 any
 deny   ip 20.0.0.0 0.255.255.255 any
 deny   ip 40.0.0.0 0.255.255.255 any
 deny   ip 21.0.0.0 0.255.255.255 any
 deny   ip 22.0.0.0 0.255.255.255 any
 deny   ip 41.0.0.0 0.255.255.255 any
 deny   ip 80.0.0.0 0.255.255.255 any
 deny   ip 81.0.0.0 0.255.255.255 any
 deny   ip 82.0.0.0 0.255.255.255 any
 permit ip any any
ip radius source-interface Loopback0
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
access-list 135 permit ip any host 10.100.4.38
access-list 135 deny ip any any
!
radius-server host 10.100.2.36 auth-port 1812 acct-port 1813 key cisco
radius-server retransmit 5
radius-server key cisco
radius-server vsa send accounting
radius-server vsa send authentication
!
control-plane
!
!
dial-peer cor custom
!
!
!
!
gatekeeper
 shutdown
!
alias exec sss show subscriber session
alias exec css clear subscriber session
alias exec ss show subscriber statistics
!
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 exec-timeout 0 0
!
ntp clock-period 17180035
ntp server 10.200.1.41 prefer
```

Deployment Model 1: PE

```
ip vrf VPN10003
 rd 100:3
 route-target export 100:3
 route-target import 100:3
!
!
router bgp 100
 no synchronization
 bgp router-id 10.200.1.45
 bgp log-neighbor-changes
 redistribute connected
 redistribute static
 neighbor 10.200.1.41 remote-as 100
 neighbor 10.200.1.41 update-source Loopback0
 no auto-summary
!
!
address-family ipv4 vrf VPN10003
 redistribute connected
 redistribute static
 no auto-summary
 no synchronization
 network 42.2.103.0 mask 255.255.255.0
 aggregate-address 42.2.103.0 255.255.255.0 summary-only
 exit-address-family
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
!
!
ip route vrf VPN10003 10.100.3.34 255.255.255.255 GigabitEthernet3/14 10.100.3.34
```

Deployment Model 1: AAA Server for ISP-1

The following profile configures L2TP forwarding from the ISG LAC to the LNS.

```
[ //localhost/Radius/UserLists/L2TPDOMAIN/L2TP_DM1_101.com/Attributes ]
    Cisco-AVpair = vpdn:tunnel-id=L2TP_DM1_101
    Cisco-AVpair = vpdn:l2tp-tunnel-password=cisco
    Cisco-AVpair = vpdn:tunnel-type=l2tp
    Cisco-AVpair = vpdn:ip-addresses=10.200.1.56
    Cisco-AVpair = atm:peak-cell-rate=1024
    Cisco-AVpair = atm:sustainable-cell-rate=512
```

Deployment Model 1: AAA Server for ISP-2

This profile configures the basic Internet access service.

```
[ //localhost/Radius/UserLists/SERVICES/INTERNET_SERVICE/Attributes ]
    Cisco-AVPair = ip:inacl=Internet-in-acl
    Cisco-AVPair = ip:outacl=Internet-out-acl
    Cisco-SSG-Service-Info = IINTERNET_SERVICE
    Cisco-SSG-Service-Info = R42.1.1.0;255.255.255.0
```

This attribute enables the Layer 4 Redirect feature.

```
[ Attributes ]
    Cisco-AVPair = "ip:l4redirect=redirect list 111 to group SESM-Server duration 30
frequency 180"
```

This attribute enable the PBHK feature on the AAA server, which enables access to the SESM by way of the PBHK feature.

```
[ Attributes ]
    Cisco-AVPair = ip:portbundle=enable
```

This profile configures the PPP profile that is used in the subscriber's base profile.

```
[ //localhost/Radius/UserLists/ie2-C7301-LNS/C73_DM1_01@L2TP_DM1_101.com/Attributes ]
    Cisco-AVpair = "ip:ip-unnumbered=loopback 3001"
    Cisco-AVpair = ip:addr-pool=C73_DM1_3001
    Cisco-SSG-Account-Info = AINTERNET_SERVICE
```

Deployment Model 2: Multiservice Service Bundle over PPPoE

The following sections contain the complete running configurations for the devices in Deployment Model 2:

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

Deployment Model 2: CPE

```
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log uptime
no service password-encryption
!
hostname ie2-C837-CPE5
!
!
no aaa new-model
ip subnet-zero
no ip domain lookup
ip dhcp excluded-address 10.10.10.1
!
ip dhcp pool CLIENT
   import all
   network 10.10.10.0 255.255.255.0
   default-router 10.10.10.1
   lease 0 2
!
!
ip audit notify log
ip audit po max-events 100
vpdn enable
!
vpdn-group ppoe
 request-dialin
  protocol pppoe
!
no ftp-server write-enable
!
!
!
!
!
!
!
interface Ethernet0
 ip address 10.10.10.1 255.255.255.0
 ip nat inside
 ip tcp adjust-mss 1452
 load-interval 30
 hold-queue 100 out
!
interface ATM0
 no ip address
 shutdown
 no atm ilmi-keepalive
 dsl operating-mode auto
!
interface ATM0.5 point-to-point
 pvc 5/45
  pppoe max-sessions 100
  pppoe-client dial-pool-number 1
 !
!
interface FastEthernet1
 no ip address
 duplex auto
 speed auto
!
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
interface Dialer1
 ip address negotiated
 ip nat outside
 encapsulation ppp
 dialer pool 1
 dialer-group 1
 ppp authentication chap callin
 ppp chap hostname C72_DM2_11111
 ppp chap password 0 lab
!
!
ip nat inside source list 23 interface Dialer1 overload
ip classless
ip route 0.0.0.0 0.0.0.0 Dialer1
ip http server
no ip http secure-server
!
access-list 23 permit 10.10.10.0 0.0.0.255
!
line con 0
 exec-timeout 0 0
 no modem enable
 stopbits 1
line aux 0
line vty 0 4
 access-class 23 in
 exec-timeout 120 0
 login local
```

Deployment Model 2: ISG

```
version 12.2
no service pad
service config
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname ie2-C7206-ATM
!
boot-start-marker
boot host tftp ie2/configs/tc5xx/isg_add_tc5xx_pta.dat 223.255.12.34
boot system disk2:c7200-js-mz.122-27.1.11.SIE7
boot-end-marker
!
logging buffered 1000000 debugging
no logging console
enable password lab
!
aaa new-model
!
!
aaa group server radius CAR_SERVER
 server 10.100.1.35 auth-port 1812 acct-port 1813
!
aaa group server radius RSIM_SERVER
 server 10.100.12.89 auth-port 1645 acct-port 1646
!
aaa authentication login default none
aaa authentication ppp default group CAR_SERVER
aaa authentication ppp PREPAID_AUTHEN_LIST group RSIM_SERVER
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
aaa authorization network default group CAR_SERVER
aaa authorization network PREPAID_AUTHOR_LIST group RSIM_SERVER
aaa authorization subscriber-service default local group radius
aaa accounting network default start-stop group CAR_SERVER
aaa accounting network PREPAID_ACCNT_LIST start-stop group RSIM_SERVER
aaa server radius sesm
 client 10.100.3.34
 key cisco
 port 1812
 message-authenticator ignore
!
!
aaa session-id common
clock timezone Pacific -8
ip subnet-zero
!
!
ip ftp username root
ip ftp password lab
ip dhcp smart-relay
ip dhcp relay information option vpn
ip dhcp relay information option
ip dhcp relay information trust-all
no ip dhcp use vrf connected
!
ip vrf VPN10005
 rd 100:5
 route-target export 100:5
 route-target import 100:5
!
ip cef
!
subscriber feature prepaid PREPAID_RSIM
   threshold time 20 seconds
   threshold volume 5000 bytes
   interim-interval 3 minutes
   method-list author PREPAID_AUTHOR_LIST
   method-list accounting PREPAID_ACCNT_LIST
   password cisco
subscriber feature prepaid default
   threshold time 20 seconds
   threshold volume 200 bytes
   interim-interval 3 minutes
   method-list author default
   method-list accounting default
   password cisco
!
subscriber policy recording rules limit 64
subscriber authorization enable
vpdn enable
vpdn ip udp ignore checksum
vpdn search-order domain
!
redirect server-group SESM_SERVER_GROUP
 server ip 10.100.3.34 port 8080
!
no mpls traffic-eng auto-bw timers frequency 0
call rsvp-sync
!
!
class-map control match-all BOD256K_CLASS
 match service-name BOD256K
!
class-map control match-all BOD2MVOLUME_CLASS
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
 match service-name BOD2MVOLUME
!
class-map control match-all BOD1MVOLUME_CLASS
 match service-name BOD1MVOLUME
!
class-map control match-all BOD2MTIME_CLASS
 match service-name BOD2MTIME
!
class-map control match-all BOD1MTIME_CLASS
 match service-name BOD1MTIME
!
!
policy-map control RULE_PTA_LM_ATM8
 class control BOD1MVOLUME_CLASS event service-start
  1 service-policy service unapply name BOD256K
  2 service-policy service unapply name BOD2MVOLUME
  3 service-policy service identifier service-name
 !
 class control BOD2MVOLUME_CLASS event service-start
  1 service-policy service unapply name BOD256K
  2 service-policy service unapply name BOD1MVOLUME
  3 service-policy service identifier service-name
 !
 class control BOD1MTIME_CLASS event service-start
  1 service-policy service unapply name BOD256K
  2 service-policy service unapply name BOD2MTIME
  3 service-policy service identifier service-name
 !
 class control BOD2MTIME_CLASS event service-start
  1 service-policy service unapply name BOD256K
  2 service-policy service unapply name BOD1MTIME
  3 service-policy service identifier service-name
 !
 class control BOD256K_CLASS event service-start
  1 service-policy service unapply name BOD1MVOLUME
  2 service-policy service unapply name BOD2MVOLUME
  3 service-policy service unapply name BOD1MTIME
  4 service-policy service unapply name BOD2MTIME
  5 service-policy service identifier service-name
 !
 class control BOD2MTIME_CLASS event service-stop
  1 service-policy service unapply identifier service-name
  2 service-policy service name BOD256K
 !
 class control BOD1MTIME_CLASS event service-stop
  1 service-policy service unapply identifier service-name
  2 service-policy service name BOD256K
 !
 class control BOD2MVOLUME_CLASS event service-stop
  1 service-policy service unapply identifier service-name
  2 service-policy service name BOD256K
 !
 class control BOD1MVOLUME_CLASS event service-stop
  1 service-policy service unapply identifier service-name
  2 service-policy service name BOD256K
 !
 class control always event session-start
  1 service local
  2 service-policy service name PBHK_SERVICE
 !
 class control always event quota-depleted
  1 set-param drop-traffic FALSE
 !
 class control always event credit-exhausted
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
  1 service-policy service name L4REDIRECT_SERVICE
 !
!
!
policy-map QOS_OUT_MPLS_UPLINK
  class QOS_GROUP_VOICE
   set mpls experimental topmost 5
  class QOS_GROUP_CALL_CONTROL
   set mpls experimental topmost 3
  class QOS_GROUP_GAMING
   set mpls experimental topmost 2
  class class-default
   set mpls experimental topmost 0
!
bba-group pppoe BBA_LM_ATM8
 virtual-template 8
 sessions per-vc limit 1
!
vc-class atm VC_LM_ATM8
  protocol pppoe group BBA_LM_ATM8
  dbs enable maximum
  encapsulation aal5snap
!
interface Loopback0
 ip address 10.200.1.53 255.255.255.255
!
interface Loopback5
 ip address 200.53.5.1 255.255.255.255
!
interface GigabitEthernet0/3
 ip address 40.40.1.53 255.255.255.0
 ip portbundle outside
 load-interval 30
 duplex full
 speed 1000
 media-type gbic
 negotiation auto
 mpls mtu 1522
 mpls ip
 service-policy output QOS_OUT_MPLS_UPLINK
 ip rsvp bandwidth 100000
!
interface ATM1/0
 no ip address
 load-interval 30
 no atm auto-configuration
 no atm ilmi-keepalive
 no atm address-registration
 no atm ilmi-enable
 no atm enable-ilmi-trap
 bundle-enable
!
interface ATM1/0.105 multipoint
 description Deployment Model 2
 atm pppatm passive
 no atm enable-ilmi-trap
 pvc 105/45
  class-vc VC_LM_ATM8
 !
!
!
interface Virtual-Template8
 description LM ATM8 PTA Subscriber
 no ip address
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
 no peer default ip address
 no keepalive
 ppp timeout authentication 100
 ppp timeout aaa
 load-interval 30
 ppp mtu adaptive
 ppp authentication chap
 service-policy control RULE_PTA_LM_ATM8
!
router ospf 100
 router-id 10.200.1.53
 log-adjacency-changes
 area 100 range 200.53.0.0 255.255.0.0
 redistribute connected
 redistribute static subnets
 network 10.200.1.53 0.0.0.0 area 100
 network 20.20.1.0 0.0.0.255 area 100
 network 40.40.1.0 0.0.0.255 area 100
 network 200.53.0.0 0.0.255.255 area 100
!
router bgp 100
 no synchronization
 bgp router-id 10.200.1.53
 bgp log-neighbor-changes
 network 200.53.0.0 mask 255.255.0.0
 aggregate-address 200.53.3.0 255.255.255.0 summary-only
 redistribute connected
 redistribute static
 neighbor 10.200.1.41 remote-as 100
 neighbor 10.200.1.41 update-source Loopback0
 no auto-summary
 !
 address-family vpnv4
 neighbor 10.200.1.41 activate
 neighbor 10.200.1.41 send-community both
 exit-address-family
 !
 address-family ipv4 vrf VPN10005
 redistribute connected
 redistribute static
 no auto-summary
 no synchronization
 network 200.53.0.0 mask 255.255.0.0
 exit-address-family
 !
!
ip local pool cpe3_pool-53-VPN10005 200.53.3.210 200.53.3.250
!
ip portbundle
 match access-list 135
 source Loopback0
!
ip classless
!
no ip http server
!
!
!
ip access-list extended Internet-in-acl
 deny   ip any 223.0.0.0 0.255.255.255
 deny   ip any 20.0.0.0 0.255.255.255
 deny   ip any 40.0.0.0 0.255.255.255
 deny   ip any 21.0.0.0 0.255.255.255
 deny   ip any 22.0.0.0 0.255.255.255
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
 deny   ip any 41.0.0.0 0.255.255.255
 deny   ip any 80.0.0.0 0.255.255.255
 deny   ip any 81.0.0.0 0.255.255.255
 deny   ip any 82.0.0.0 0.255.255.255
 deny   ip any 84.0.0.0 0.255.255.255
 deny   ip any 10.200.0.0 0.0.255.255
 permit ip any any
ip access-list extended Internet-out-acl
 deny   ip 223.0.0.0 0.255.255.255 any
 deny   ip 10.200.0.0 0.0.255.255 any
 deny   ip 20.0.0.0 0.255.255.255 any
 deny   ip 40.0.0.0 0.255.255.255 any
 deny   ip 21.0.0.0 0.255.255.255 any
 deny   ip 22.0.0.0 0.255.255.255 any
 deny   ip 41.0.0.0 0.255.255.255 any
 deny   ip 80.0.0.0 0.255.255.255 any
 deny   ip 81.0.0.0 0.255.255.255 any
 deny   ip 82.0.0.0 0.255.255.255 any
 deny   ip 84.0.0.0 0.255.255.255 any
 permit ip any any
ip radius source-interface Loopback0
access-list 135 permit ip any host 10.100.4.38
access-list 135 deny ip any any
!
!
radius-server attribute 44 include-in-access-req
radius-server attribute 8 include-in-access-req
radius-server attribute 55 access-request include
radius-server attribute 25 access-request include
radius-server host 10.100.1.35 auth-port 1812 acct-port 1813 key cisco
radius-server host 10.100.12.89 auth-port 1645 acct-port 1646 key cisco
radius-server retransmit 5
radius-server timeout 15
radius-server vsa send accounting
radius-server vsa send authentication
!
control-plane
!
!
dial-peer cor custom
!
!
alias exec showdb show database data IDMGR-Session-DB 2
alias exec sss show subscriber session
alias exec css clear subscriber session
alias exec showpb show ip portbundle status inuse
alias exec ss show subscriber statistics
!
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 exec-timeout 0 0
!
ntp clock-period 17179872
ntp server 10.200.1.41 source GigabitEthernet0/3 prefer
!
end
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

Deployment Model 2: PE

```
ip vrf VPN10005
 rd 100:3
 route-target export 100:3
 route-target import 100:3
!
router bgp 100
 no synchronization
 bgp router-id 10.200.1.45
 bgp log-neighbor-changes
 redistribute connected
 redistribute static
 neighbor 10.200.1.41 remote-as 100
 neighbor 10.200.1.41 update-source Loopback0
 no auto-summary
!
 address-family ipv4 vrf VPN10005
 redistribute connected
 redistribute static
 no auto-summary
 no synchronization
 network 42.2.103.0 mask 255.255.255.0
 aggregate-address 42.2.103.0 255.255.255.0 summary-only
 exit-address-family
!
ip route vrf VPN10005 10.100.3.34 255.255.255.255 GigabitEthernet3/14 10.100.3.34
```

Deployment Model 2: AAA Server

This profile configures the BOD1MTIME service.

```
[ BOD1MTIME_DM2/Attributes ]
    Cisco-AVPair = "ip:traffic-class=in access-group name INTERNET_IN_ACL priority 10"
    Cisco-AVPair = "ip:traffic-class=in default drop"
    Cisco-AVPair = "ip:traffic-class=out access-group name INTERNET_OUT_ACL priority 10"
    Cisco-AVPair = "ip:traffic-class=out default drop"
    Cisco-AVPair = subscriber:accounting-list=PREPAID_ACCNT_LIST
    Cisco-AVPair = prepaid-config=PREPAID_RSIM
    Cisco-AVPair = atm:peak-cell-rate=1024
    Cisco-AVPair = atm:sustainable-cell-rate=1024
    Cisco-SSG-Service-Info = IBOD1MTIME_DM2
    Cisco-SSG-Service-Info = R42.1.1.0;255.255.255.0
```

This profile configures the BOD2MTIME service.

```
[ BOD2MTIME_DM2/Attributes ]
    Cisco-AVPair = "ip:traffic-class=in access-group name INTERNET_IN_ACL priority 10"
    Cisco-AVPair = "ip:traffic-class=in default drop"
    Cisco-AVPair = "ip:traffic-class=out access-group name INTERNET_OUT_ACL priority 10"
    Cisco-AVPair = "ip:traffic-class=out default drop"
    Cisco-AVPair = subscriber:accounting-list=PREPAID_ACCNT_LIST
    Cisco-AVPair = prepaid-config=PREPAID_RSIM
    Cisco-AVPair = atm:peak-cell-rate=2048
    Cisco-AVPair = atm:sustainable-cell-rate=2048
    Cisco-SSG-Service-Info = IBOD2MTIME_DM2
    Cisco-SSG-Service-Info = R42.1.1.0;255.255.255.0
```

This profile configures the BOD1MVOLUME service.

```
[ BOD1MVOLUME_DM2/Attributes ]
    Cisco-AVPair = "ip:traffic-class=in access-group name INTERNET_IN_ACL priority 10"
    Cisco-AVPair = "ip:traffic-class=in default drop"
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
    Cisco-AVPair = "ip:traffic-class=out access-group name INTERNET_OUT_ACL priority 10"
    Cisco-AVPair = "ip:traffic-class=out default drop"
    Cisco-AVPair = subscriber:accounting-list=PREPAID_ACCNT_LIST
    Cisco-AVPair = prepaid-config=PREPAID_RSIM
    Cisco-AVPair = atm:peak-cell-rate=1024
    Cisco-AVPair = atm:sustainable-cell-rate=1024
    Cisco-SSG-Service-Info = IBOD1MVOLUME_DM2
    Cisco-SSG-Service-Info = R42.1.1.0;255.255.255.0
```

This profile configures the BOD2MVOLUME service.

```
    Cisco-AVPair = "ip:traffic-class=in access-group name INTERNET_IN_ACL priority 10"
    Cisco-AVPair = "ip:traffic-class=in default drop"
    Cisco-AVPair = "ip:traffic-class=out access-group name INTERNET_OUT_ACL priority 10"
    Cisco-AVPair = "ip:traffic-class=out default drop"
    Cisco-AVPair = subscriber:accounting-list=PREPAID_ACCNT_LIST
    Cisco-AVPair = prepaid-config=PREPAID_RSIM
    Cisco-AVPair = atm:peak-cell-rate=2048
    Cisco-AVPair = atm:sustainable-cell-rate=2048
    Cisco-SSG-Service-Info = IBOD2MVOLUME_DM2
    Cisco-SSG-Service-Info = R42.1.1.0;255.255.255.0
```

This attribute enables the Layer 4 Redirect feature.

```
[ //localhost/Radius/UserLists/SERVICES/L4REDIRECT_SERVICE/Attributes ]
    Cisco-AVPair = "ip:traffic-class=in access-group name IP_REDIRECT_ACL priority 5"
    Cisco-AVPair = "ip:traffic-class=in default drop"
    Cisco-AVPair = "ip:traffic-class=out access-group name IP_REDIRECT_ACL priority 5"
    Cisco-AVPair = "ip:traffic-class=out default drop"
    Cisco-AVPair = "ip:l4redirect=redirect to group SESM_SERVER_GROUP"
    Cisco-SSG-Service-Info = IL4REDIRECT_SERVICE
```

This profile enables the PBHK feature on the AAA server, which enables access to the SESM by way of the PBHK feature.

```
[ //localhost/Radius/UserLists/SERVICES/PBHK_SERVICE/Attributes ]
    Cisco-AVPair = ip:portbundle=enable
    Cisco-SSG-Service-Info = IPBHK_SERVICE
```

This profile configures a user profile for time-based customers.

```
[ //localhost/Radius/UserLists/ie2-C7206-ATM/C72_DM2_3640/Attributes ]
    Cisco-AVpair = ip:vrf-id=VPN_C72_DM2_1001
    Cisco-AVpair = "ip:ip-unnumbered=loopback 8001"
    Cisco-AVpair = ip:addr-pool=C72_DM2_8001
    Cisco-SSG-Account-Info = NBOD1MTIME_DM2
    Cisco-SSG-Account-Info = NBOD2MTIME_DM2
    idle-timeout = 1800
    session-timeout = 18000
```

This profile configures a user profile for a time-based customer with the static IP address 1.108.1.201.

```
[ //localhost/Radius/UserLists/ie2-C7206-ATM/C72_DM2_5640/Attributes ]
    Cisco-AVpair = ip:vrf-id=VPN_C72_DM2_1098
    Cisco-AVpair = "ip:ip-unnumbered=loopback 8002"
    Cisco-SSG-Account-Info = NBOD1MTIME_DM2
    Cisco-SSG-Account-Info = NBOD2MTIME_DM2
    Framed-IP-Address = 1.108.1.201
    idle-timeout = 1800
    session-timeout = 18000
```

This profile configures a user profile for volume-based customers.

```
[ //localhost/Radius/UserLists/ie2-C7206-ATM/C72_DM2_4640/Attributes ]
    Cisco-AVpair = ip:vrf-id=VPN_C72_DM2_1001
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
Cisco-AVpair = "ip:ip-unnumbered=loopback 8001"
Cisco-AVpair = ip:addr-pool=C72_DM2_8001
Cisco-SSG-Account-Info = NBOD1MVOLUME_DM2
Cisco-SSG-Account-Info = NBOD2MVOLUME_DM2
idle-timeout = 1800
session-timeout = 18000
```

Deployment Model 3: Triple Play Plus Service Bundle over IP and PPPoE

The following sections contain the complete running configurations for the devices in Deployment Model 3:

Deployment Model 3: CPE

```
version 12.3
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname ie2-C837-CPE3
!
enable password 7 12150415
!
no aaa new-model
ip subnet-zero
no ip routing
no ip domain lookup
!
!
ip audit notify log
ip audit po max-events 100
no ftp-server write-enable
!
!
!
!
interface Ethernet0
 no ip address
 no ip route-cache
 load-interval 30
 bridge-group 1
 hold-queue 100 out
!
interface ATM0
 no ip address
 no ip route-cache
 load-interval 30
 no atm ilmi-keepalive
 dsl operating-mode auto
!
interface ATM0.3 point-to-point
 no ip route-cache
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
 pvc 3/43
  encapsulation aal5snap
 !
 bridge-group 1
!
!
ip classless
ip http server
no ip http secure-server
!
bridge 1 protocol ieee
!
line con 0
 exec-timeout 0 0
 no modem enable
 stopbits 1
line aux 0
line vty 0 4
 access-class 23 in
 exec-timeout 0 0
 login local
!
scheduler max-task-time 5000
```

Deployment Model 3: ISG

```
version 12.2
no service pad
service config
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ie2-C7206-ATM
!
boot-start-marker
boot host tftp ie2/configs/tc5xx/isg_add_tc5xx_pta.dat 223.255.12.34
boot system disk2:c7200-js-mz.122-27.1.11.SIE7
boot-end-marker
!
logging buffered 1000000 debugging
no logging console
enable password lab
!
aaa new-model
!
!
aaa group server radius CAR_SERVER
 server 10.100.1.35 auth-port 1812 acct-port 1813
!
aaa group server radius RSIM_SERVER
 server 10.100.12.89 auth-port 1645 acct-port 1646
!
aaa authentication login default none
aaa authentication login IP_AUTHEN_LIST group CAR_SERVER
aaa authentication ppp default group CAR_SERVER
aaa authentication ppp PREPAID_AUTHEN_LIST group RSIM_SERVER
aaa authorization network default group CAR_SERVER
aaa authorization network PREPAID_AUTHOR_LIST group RSIM_SERVER
aaa authorization subscriber-service default local group radius
aaa accounting network default start-stop group CAR_SERVER
aaa accounting network PREPAID_ACCNT_LIST start-stop group RSIM_SERVER
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
aaa server radius sesm
 client 10.100.3.34
 key cisco
 port 1812
 message-authenticator ignore
!
!
aaa session-id common
clock timezone Pacific -8
ip subnet-zero
!
!
ip ftp username root
ip ftp password lab
ip dhcp smart-relay
ip dhcp relay information option vpn
ip dhcp relay information option
ip dhcp relay information trust-all
no ip dhcp use vrf connected
!
!
ip vrf VPN10003
 rd 100:3
 route-target export 100:3
 route-target import 100:3
!
ip cef
!
subscriber policy recording rules limit 64
subscriber authorization enable
vpdn enable
vpdn ip udp ignore checksum
vpdn search-order domain
!
redirect server-group SESM_SERVER_GROUP
 server ip 10.100.3.34 port 8080
!
no mpls traffic-eng auto-bw timers frequency 0
call rsvp-sync
!
!
!
!
!
!
class-map control match-all IP_UNAUTH_COND
 match timer IP_UNAUTH_TIMER
 match authen-status unauthenticated
!
class-map match-any QOS_GROUP_CALL_CONTROL
  match qos-group 2
class-map match-any GAMING
  match ip dscp af21
class-map match-any QOS_GROUP_GAMING
  match qos-group 3
class-map match-any CALL_CONTROL
  match ip dscp cs3
class-map match-any QOS_GROUP_VOICE
  match qos-group 1
class-map match-any VOICE
  match ip dscp ef
!
policy-map control RULE_IP_LM_ATM2
 class control IP_UNAUTH_COND event timed-policy-expiry
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
  1 service disconnect
 !
 class control always event session-start
  1 authorize aaa password lab identifier mac-address
  2 service-policy service name PBHK_SERVICE
  3 service-policy service name L4REDIRECT_SERVICE
  4 set-timer IP_UNAUTH_TIMER 5
 !
 class control always event account-logon
  1 authenticate aaa list IP_AUTHEN_LIST
  2 service-policy service unapply name L4REDIRECT_SERVICE
 !
!
policy-map control RULE_PTA_LM_ATM2
 class control always event session-start
  1 service-policy service name PBHK_SERVICE
 !
!
policy-map QOS_OUT_LM_ATM2
  class VOICE
    priority 128
  class CALL_CONTROL
    bandwidth percent 5
  class GAMING
    bandwidth percent 20
policy-map QOS_OUT_MPLS_UPLINK
  class QOS_GROUP_VOICE
   set mpls experimental topmost 5
  class QOS_GROUP_CALL_CONTROL
   set mpls experimental topmost 3
  class QOS_GROUP_GAMING
   set mpls experimental topmost 2
  class class-default
   set mpls experimental topmost 0
policy-map QOS_IN_LM_ATM2
  class VOICE
   police cir 128000
     exceed-action drop
   set qos-group 1
  class CALL_CONTROL
   police cir 12500
     exceed-action drop
   set qos-group 2
  class GAMING
   police cir 75000
     exceed-action drop
   set qos-group 3
policy-map QOS_IN_LM_ATM2_256K
  class class-default
   police cir 256000
     exceed-action drop
   set qos-group 1
   service-policy QOS_IN_LM_ATM2
!
bba-group pppoe BBA_LM_ATM2
 virtual-template 2
!
vc-class atm VC_LM_ATM2
  protocol pppoe group BBA_LM_ATM2
  dbs enable maximum
  encapsulation aal5snap
  service-policy control RULE_PTA_LM_ATM2
!
interface Loopback0
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
 ip address 10.200.1.53 255.255.255.255
!
interface Loopback3
 ip address 200.53.3.1 255.255.255.0
!
interface GigabitEthernet0/1
 ip address 223.255.12.53 255.255.255.0
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
!
interface GigabitEthernet0/3
 ip address 40.40.1.53 255.255.255.0
 ip portbundle outside
 load-interval 30
 duplex full
 speed 1000
 media-type gbic
 negotiation auto
 mpls mtu 1522
 mpls ip
 service-policy output QOS_OUT_MPLS_UPLINK
 ip rsvp bandwidth 100000
!
interface ATM1/0
 no ip address
 load-interval 30
 no atm auto-configuration
 no atm ilmi-keepalive
 no atm address-registration
 no atm ilmi-enable
 no atm enable-ilmi-trap
 bundle-enable
!
interface ATM1/0.103 point-to-point
 ip unnumbered Loopback3
 ip verify unicast reverse-path
 ip helper-address 10.100.1.37
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip subscriber
  initiator dhcp
 atm route-bridged ip
 no atm enable-ilmi-trap
 ntp disable
 pvc 103/43
  class-vc VC_LM_ATM2
 service-policy input QOS_IN_LM_ATM2
 service-policy output QOS_OUT_LM_ATM2
 service-policy control RULE_IP_LM_ATM2
 !
!
interface Virtual-Template2
 description LM ATM2 PTA Subscriber
 no ip address
 no peer default ip address
 no keepalive
 ppp authentication chap
 ppp timeout authentication 100
 ppp timeout aaa
!
router ospf 100
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
 router-id 10.200.1.53
 log-adjacency-changes
 area 100 range 200.53.0.0 255.255.0.0
 redistribute connected
 redistribute static subnets
 network 10.200.1.53 0.0.0.0 area 100
 network 20.20.1.0 0.0.0.255 area 100
 network 40.40.1.0 0.0.0.255 area 100
 network 200.53.0.0 0.0.255.255 area 100
!
router bgp 100
 no synchronization
 bgp router-id 10.200.1.53
 bgp log-neighbor-changes
 network 200.53.0.0 mask 255.255.0.0
 aggregate-address 200.53.3.0 255.255.255.0 summary-only
 redistribute connected
 redistribute static
 neighbor 10.200.1.41 remote-as 100
 neighbor 10.200.1.41 update-source Loopback0
 no auto-summary
 !
 address-family vpnv4
 neighbor 10.200.1.41 activate
 neighbor 10.200.1.41 send-community both
 exit-address-family
 !
 address-family ipv4 vrf VPN10003
 redistribute connected
 redistribute static
 no auto-summary
 no synchronization
 aggregate-address 200.53.3.0 255.255.255.0 summary-only
 exit-address-family
!
ip local pool cpe3_pool-53 200.53.3.2 200.53.3.100
!
ip portbundle
 match access-list 135
 source Loopback0
!
ip classless
!
no ip http server
!
!
!
ip access-list extended GAMING_IN_ACL
 permit ip any 42.5.0.0 0.0.255.255
 deny   ip any any
ip access-list extended GAMING_OUT_ACL
 permit ip 42.5.0.0 0.0.255.255 any
 deny   ip any any
ip access-list extended Internet-in-acl
 deny   ip any 223.0.0.0 0.255.255.255
 deny   ip any 20.0.0.0 0.255.255.255
 deny   ip any 40.0.0.0 0.255.255.255
 deny   ip any 21.0.0.0 0.255.255.255
 deny   ip any 22.0.0.0 0.255.255.255
 deny   ip any 41.0.0.0 0.255.255.255
 deny   ip any 80.0.0.0 0.255.255.255
 deny   ip any 81.0.0.0 0.255.255.255
 deny   ip any 82.0.0.0 0.255.255.255
 deny   ip any 84.0.0.0 0.255.255.255
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
 deny   ip any 10.200.0.0 0.0.255.255
 permit ip any any
ip access-list extended Internet-out-acl
 deny   ip 223.0.0.0 0.255.255.255 any
 deny   ip 10.200.0.0 0.0.255.255 any
 deny   ip 20.0.0.0 0.255.255.255 any
 deny   ip 40.0.0.0 0.255.255.255 any
 deny   ip 21.0.0.0 0.255.255.255 any
 deny   ip 22.0.0.0 0.255.255.255 any
 deny   ip 41.0.0.0 0.255.255.255 any
 deny   ip 80.0.0.0 0.255.255.255 any
 deny   ip 81.0.0.0 0.255.255.255 any
 deny   ip 82.0.0.0 0.255.255.255 any
 deny   ip 84.0.0.0 0.255.255.255 any
 permit ip any any
ip access-list extended OPENGARDEN_IN_ACL
 permit ip any 10.100.0.0 0.0.255.255
 permit ip any 42.8.0.0 0.0.255.255
 permit ip any 200.53.3.0 0.0.0.255
ip access-list extended OPENGARDEN_OUT_ACL
 permit ip 10.100.0.0 0.0.255.255 any
 permit ip 42.8.0.0 0.0.255.255 any
 permit ip 200.53.3.0 0.0.0.255 any
ip access-list extended SESM-in-acl
 permit ip any host 10.100.3.34
 deny   ip any any
ip access-list extended SESM-out-acl
 permit ip host 10.100.3.34 any
 deny   ip any any
ip access-list extended VOD_IN_ACL
 permit ip any 42.4.0.0 0.0.255.255
 deny   ip any any
ip access-list extended VOD_OUT_ACL
 permit ip 42.4.0.0 0.0.255.255 any
 deny   ip any any
ip access-list extended VOIP_IN_ACL
 permit ip any 42.3.0.0 0.0.255.255
 deny   ip any any
ip access-list extended VOIP_OUT_ACL
 permit ip 42.3.0.0 0.0.255.255 any
 deny   ip any any
ip radius source-interface Loopback0
access-list 135 permit ip any host 10.100.4.38
access-list 135 deny ip any any
!
!
radius-server attribute 44 include-in-access-req
radius-server attribute 8 include-in-access-req
radius-server attribute 55 access-request include
radius-server attribute 25 access-request include
radius-server host 10.100.1.35 auth-port 1812 acct-port 1813 key cisco
radius-server host 10.100.12.89 auth-port 1645 acct-port 1646 key cisco
radius-server retransmit 5
radius-server timeout 15
radius-server vsa send accounting
radius-server vsa send authentication
!
control-plane
!
!
dial-peer cor custom
!
!
!
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
!
!
alias exec showdb show database data IDMGR-Session-DB 2
alias exec sss show subscriber session
alias exec css clear subscriber session
alias exec showpb show ip portbundle status inuse
alias exec ss show subscriber statistics
!
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 exec-timeout 0 0
!
ntp clock-period 17179872
ntp server 10.200.1.41 source GigabitEthernet0/3 prefer
!
end
```

Deployment Model 3: PE

```
ip vrf VPN10003
 rd 100:3
 route-target export 100:3
 route-target import 100:3
!
router bgp 100
 no synchronization
 bgp router-id 10.200.1.45
 bgp log-neighbor-changes
 redistribute connected
 redistribute static
 neighbor 10.200.1.41 remote-as 100
 neighbor 10.200.1.41 update-source Loopback0
 no auto-summary
!
 address-family ipv4 vrf VPN10003
 redistribute connected
 redistribute static
 no auto-summary
 no synchronization
 network 42.2.103.0 mask 255.255.255.0
 aggregate-address 42.2.103.0 255.255.255.0 summary-only
 exit-address-family
!
ip route vrf VPN10003 10.100.3.34 255.255.255.255 GigabitEthernet3/14 10.100.3.34
```

Deployment Model 3: AAA Server

This attribute enables the Layer 4 Redirect feature.

```
[ //localhost/Radius/UserLists/SERVICES/L4REDIRECT_SERVICE/Attributes ]
    Cisco-AVPair = "ip:traffic-class=in access-group name IP_REDIRECT_ACL priority 5"
    Cisco-AVPair = "ip:traffic-class=in default drop"
    Cisco-AVPair = "ip:traffic-class=out access-group name IP_REDIRECT_ACL priority 5"
    Cisco-AVPair = "ip:traffic-class=out default drop"
    Cisco-AVPair = "ip:l4redirect=redirect to group SESM_SERVER_GROUP"
    Cisco-SSG-Service-Info = IL4REDIRECT_SERVICE
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

This profile enables the PBHK feature on the AAA server, which enables access to the SESM by way of the PBHK feature.

```
[ //localhost/Radius/UserLists/SERVICES/PBHK_SERVICE/Attributes ]
    Cisco-AVPair = ip:portbundle=enable
    Cisco-SSG-Service-Info = IPBHK_SERVICE
```

The following service profile enables the GAMING_SERVICE service.

```
[ //localhost/Radius/UserLists/SERVICES/GAMING_SERVICE/Attributes ]
    Cisco-AVPair = "ip:traffic-class=in access-group name GAMING_IN_ACL"
    Cisco-AVPair = "ip:traffic-class=in default drop"
    Cisco-AVPair = "ip:traffic-class=out access-group name GAMING_OUT_ACL"
    Cisco-AVPair = "ip:traffic-class=out default drop"
    Cisco-SSG-Service-Info = IGAMING_SERVICE
    Cisco-SSG-Service-Info = R42.1.1.0;255.255.255.0
```

The following service profible enables the OPENGARDEN_SERVICE service. “Opengarden” is the SSG term for the default service, basic Internet access.

```
[ //localhost/Radius/UserLists/SERVICES/OPENGARDEN_SERVICE/Attributes ]
    Cisco-AVPair = "ip:traffic-class=in access-group name OPENGARDEN_IN_ACL"
    Cisco-AVPair = "ip:traffic-class=in default drop"
    Cisco-AVPair = "ip:traffic-class=out access-group name OPENGARDEN_OUT_ACL"
    Cisco-AVPair = "ip:traffic-class=out default drop"
    Cisco-SSG-Service-Info = IOPENGARDEN_SERVICE
```

The following service profile enables the VOIP_SERVICE service.

```
[ //localhost/Radius/UserLists/SERVICES/VOIP_SERVICE/Attributes ]
    Cisco-AVPair = "ip:traffic-class=in access-group name VOIP_IN_ACL"
    Cisco-AVPair = "ip:traffic-class=in default drop"
    Cisco-AVPair = "ip:traffic-class=out access-group name VOIP_OUT_ACL"
    Cisco-AVPair = "ip:traffic-class=out default drop"
    Cisco-SSG-Service-Info = IVOIP_SERVICE
    Cisco-SSG-Service-Info = R42.1.1.0;255.255.255.0
```

The following service profile enables the VOD_SERVICE service.

```
[ //localhost/Radius/UserLists/SERVICES/VOD_SERVICE/Attributes ]
    Cisco-AVPair = "ip:traffic-class=in access-group name VOD_IN_ACL"
    Cisco-AVPair = "ip:traffic-class=in default drop"
    Cisco-AVPair = "ip:traffic-class=out access-group name VOD_OUT_ACL"
    Cisco-AVPair = "ip:traffic-class=out default drop"
    Cisco-SSG-Service-Info = IVOD_SERVICE
    Cisco-SSG-Service-Info = R42.1.1.0;255.255.255.0
```

The following service profile enables the INTERNET_SERVICE service.

```
[ //localhost/Radius/UserLists/SERVICES/INTERNET_SERVICE/Attributes ]
    Cisco-AVPair = ip:inacl=Internet-in-acl
    Cisco-AVPair = ip:outacl=Internet-out-acl
    Cisco-SSG-Service-Info = IINTERNET_SERVICE
    Cisco-SSG-Service-Info = R42.1.1.0;255.255.255.0
```

The following user profile is for IP sessions that use MAC address-based TAL:

```
[ //localhost/Radius/UserLists/ie2-C7206-ATM/0000.1001.1014/Attributes ]
    Cisco-SSG-Account-Info = AOPENGARDEN_SERVICE
    Cisco-SSG-Account-Info = AVOIP_SERVICE
    Cisco-SSG-Account-Info = AVOD_SERVICE
    Cisco-SSG-Account-Info = AGAMING_SERVICE
```

The following user profile is for PPPoE users:

```
[ //localhost/Radius/UserLists/ie2-C7206-ATM/C72_DM3_1188/Attributes ]
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
Cisco-AVpair = ip:vrf-id=VPN_C72_DM3_2038
Cisco-AVpair = "ip:ip-unnumbered=loopback 2001"
Cisco-AVpair = ip:addr-pool=C72_DM3_2001
Cisco-SSG-Account-Info = AINTERNET_SERVICE
```

Deployment Model 4: Triple Play Plus Service Bundle over IP and L2TP

The following sections contain the complete running configurations for the devices in Deployment Model 4:

Deployment Model 4: CPE

```
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log uptime
no service password-encryption
!
hostname ie2-C837-CPE5
!
!
no aaa new-model
ip subnet-zero
no ip domain lookup
ip dhcp excluded-address 10.10.10.1
!
ip dhcp pool CLIENT
   import all
   network 10.10.10.0 255.255.255.0
   default-router 10.10.10.1
   lease 0 2
!
!
ip audit notify log
ip audit po max-events 100
vpdn enable
!
vpdn-group ppoe
 request-dialin
  protocol pppoe
!
no ftp-server write-enable
!
!
!
!
!
!
!
interface Ethernet0
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
 ip address 10.10.10.1 255.255.255.0
 ip nat inside
 ip tcp adjust-mss 1452
 load-interval 30
 hold-queue 100 out
!
interface ATM0
 no ip address
 shutdown
 no atm ilmi-keepalive
 dsl operating-mode auto
!
interface ATM0.5 point-to-point
 pvc 5/45
  pppoe max-sessions 100
  pppoe-client dial-pool-number 1
 !
!
interface FastEthernet1
 no ip address
 duplex auto
 speed auto
!
interface Dialer1
 ip address negotiated
 ip nat outside
 encapsulation ppp
 dialer pool 1
 dialer-group 1
 ppp authentication chap callin
 ppp chap hostname C73_DM4_01@L2TP_DM4_101.com
 ppp chap password 0 lab
!
!
ip nat inside source list 23 interface Dialer1 overload
ip classless
ip route 0.0.0.0 0.0.0.0 Dialer1
ip http server
no ip http secure-server
!
access-list 23 permit 10.10.10.0 0.0.0.255
!
line con 0
 exec-timeout 0 0
 no modem enable
 stopbits 1
line aux 0
line vty 0 4
 access-class 23 in
 exec-timeout 120 0
 login local
```

Deployment Model 4: ISG LAC

```
version 12.2
no service pad
service config
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
hostname ie2-C7206-ATM
!
boot-start-marker
boot host tftp ie2/configs/tc5xx/isg_add_tc5xx_pta.dat 223.255.12.34
boot system disk2:c7200-js-mz.122-27.1.11.SIE7
boot-end-marker
!
logging buffered 1000000 debugging
no logging console
enable password lab
!
aaa new-model
!
!
aaa group server radius CAR_SERVER
 server 10.100.1.35 auth-port 1812 acct-port 1813
!
aaa authentication login default none
aaa authentication login IP_AUTHEN_LIST group CAR_SERVER
aaa authentication ppp default group CAR_SERVER
aaa authorization network default group CAR_SERVER
aaa authorization subscriber-service default local group radius
aaa accounting network default start-stop group CAR_SERVER
aaa server radius sesm
 client 10.100.3.34
 key cisco
 port 1812
 message-authenticator ignore
!
!
aaa session-id common
clock timezone Pacific -8
ip subnet-zero
!
!
ip ftp username root
ip ftp password lab
ip dhcp smart-relay
ip dhcp relay information option vpn
ip dhcp relay information option
ip dhcp relay information trust-all
no ip dhcp use vrf connected
!
!
ip cef
!
!
subscriber policy recording rules limit 64
subscriber authorization enable
vpdn enable
vpdn ip udp ignore checksum
vpdn search-order domain
!
redirect server-group SESM_SERVER_GROUP
 server ip 10.100.3.34 port 8080
!
no mpls traffic-eng auto-bw timers frequency 0
call rsvp-sync
!
!
!
!
!
!
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
class-map control match-all IP_UNAUTH_COND
 match timer IP_UNAUTH_TIMER
 match authen-status unauthenticated
!
class-map control match-any TAL_STATIC_DM4
 match source-ip-address 200.53.7.128 255.255.255.128
!
!
class-map match-any QOS_GROUP_CALL_CONTROL
  match qos-group 2
class-map match-any GAMING
  match ip dscp af21
class-map match-any QOS_GROUP_GAMING
  match qos-group 3
class-map match-any CALL_CONTROL
  match ip dscp cs3
class-map match-any QOS_GROUP_VOICE
  match qos-group 1
class-map match-any VOICE
  match ip dscp ef
!
!
policy-map control RULE_L2TP_LM_ATM7
 class control always event session-start
  1 collect identifier unauthenticated-domain
  2 authorize identifier unauthenticated-domain
 !
!
policy-map control RULE_IP_LM_ATM7
 class control TAL_STATIC_DM4 event session-start
  1 authorize aaa password lab identifier source-ip-address
  2 service-policy service name PBHK_SERVICE
  3 service-policy service name L4REDIRECT_SERVICE
  4 set-timer IP_UNAUTH_TIMER 5
 !
 class control IP_UNAUTH_COND event timed-policy-expiry
  1 service disconnect
 !
 class control always event session-start
  1 authorize aaa password lab identifier mac-address
  2 service-policy service name PBHK_SERVICE
  3 service-policy service name L4REDIRECT_SERVICE
  4 set-timer IP_UNAUTH_TIMER 5
 !
 class control always event account-logon
  1 authenticate aaa list IP_AUTHEN_LIST
  2 service-policy service unapply name L4REDIRECT_SERVICE
 !
!
!
policy-map QOS_OUT_LM_ATM7
  class VOICE
    priority 128
  class CALL_CONTROL
    bandwidth percent 5
  class GAMING
    bandwidth percent 20
policy-map QOS_OUT_MPLS_UPLINK
  class QOS_GROUP_VOICE
   set mpls experimental topmost 5
  class QOS_GROUP_CALL_CONTROL
   set mpls experimental topmost 3
  class QOS_GROUP_GAMING
   set mpls experimental topmost 2
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
  class class-default
   set mpls experimental topmost 0
policy-map QOS_IN_LM_ATM7
  class VOICE
   police cir 128000
     exceed-action drop
   set qos-group 1
  class CALL_CONTROL
   police cir 12500
     exceed-action drop
   set qos-group 2
  class GAMING
   police cir 75000
     exceed-action drop
   set qos-group 3
policy-map QOS_IN_LM_ATM7_256K
  class class-default
   police cir 256000
     exceed-action drop
   service-policy QOS_IN_LM_ATM7
!
bba-group pppoe BBA_LM_ATM7
 virtual-template 7
!
vc-class atm VC_LM_ATM7
  protocol pppoe group BBA_LM_ATM7
  vbr-nrt 2000 2000 94
  encapsulation aal5snap
  service-policy control RULE_L2TP_LM_ATM7
!
interface Loopback0
 ip address 10.200.1.53 255.255.255.255
!
interface Loopback7
 ip address 200.53.7.1 255.255.255.0
!

interface GigabitEthernet0/1
 ip address 223.255.12.53 255.255.255.0
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
!
interface GigabitEthernet0/3
 ip address 40.40.1.53 255.255.255.0
 ip portbundle outside
 load-interval 30
 duplex full
 speed 1000
 media-type gbic
 negotiation auto
 mpls mtu 1522
 mpls ip
 service-policy output QOS_OUT_MPLS_UPLINK
 ip rsvp bandwidth 100000
!
interface ATM1/0
 no ip address
 load-interval 30
 no atm auto-configuration
 no atm ilmi-keepalive
 no atm address-registration
 no atm ilmi-enable
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
 no atm enable-ilmi-trap
 bundle-enable
!
!
interface ATM1/0.107 point-to-point
 description ATM DM4
 ip unnumbered Loopback7
 ip verify unicast reverse-path
 ip helper-address 10.100.1.37
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip subscriber
  identifier ip src-addr match 107
  initiator dhcp
 atm route-bridged ip
 no atm enable-ilmi-trap
 ntp disable
 pvc 107/47
  class-vc VC_LM_ATM8
 service-policy input QOS_IN_LM_ATM7
 service-policy output QOS_OUT_LM_ATM7
 service-policy control RULE_IP_LM_ATM7

 !
!
interface Virtual-Template7
 description LM ATM7 L2TP Subscriber
 no ip address
 no peer default ip address
 no keepalive
 ppp authentication chap
 ppp timeout authentication 100
 ppp timeout aaa
!
router ospf 100
 router-id 10.200.1.53
 log-adjacency-changes
 area 100 range 200.53.0.0 255.255.0.0
 redistribute connected
 redistribute static subnets
 network 10.200.1.53 0.0.0.0 area 100
 network 20.20.1.0 0.0.0.255 area 100
 network 40.40.1.0 0.0.0.255 area 100
 network 200.53.0.0 0.0.255.255 area 100
!
router bgp 100
 no synchronization
 bgp router-id 10.200.1.53
 bgp log-neighbor-changes
 network 200.53.0.0 mask 255.255.0.0
 aggregate-address 200.53.3.0 255.255.255.0 summary-only
 redistribute connected
 redistribute static
 neighbor 10.200.1.41 remote-as 100
 neighbor 10.200.1.41 update-source Loopback0
 no auto-summary
 !
 address-family vpnv4
 neighbor 10.200.1.41 activate
 neighbor 10.200.1.41 send-community both
 exit-address-family
 !
!
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
ip portbundle
 match access-list 135
 source Loopback0
!
ip classless
!
no ip http server
!
!
!
ip access-list extended GAMING_IN_ACL
 permit ip any 42.5.0.0 0.0.255.255
 deny   ip any any
ip access-list extended GAMING_OUT_ACL
 permit ip 42.5.0.0 0.0.255.255 any
 deny   ip any any
ip access-list extended OPENGARDEN_IN_ACL
 permit ip any 10.100.0.0 0.0.255.255
 permit ip any 42.8.0.0 0.0.255.255
 permit ip any 200.53.3.0 0.0.0.255
ip access-list extended OPENGARDEN_OUT_ACL
 permit ip 10.100.0.0 0.0.255.255 any
 permit ip 42.8.0.0 0.0.255.255 any
 permit ip 200.53.3.0 0.0.0.255 any
ip access-list extended SESM-in-acl
 permit ip any host 10.100.3.34
 deny   ip any any
ip access-list extended SESM-out-acl
 permit ip host 10.100.3.34 any
 deny   ip any any
ip access-list extended VOD_IN_ACL
 permit ip any 42.4.0.0 0.0.255.255
 deny   ip any any
ip access-list extended VOD_OUT_ACL
 permit ip 42.4.0.0 0.0.255.255 any
 deny   ip any any
ip access-list extended VOIP_IN_ACL
 permit ip any 42.3.0.0 0.0.255.255
 deny   ip any any
ip access-list extended VOIP_OUT_ACL
 permit ip 42.3.0.0 0.0.255.255 any
 deny   ip any any
ip radius source-interface Loopback0
access-list 135 permit ip any host 10.100.4.38
access-list 135 deny ip any any
!
radius-server attribute 44 include-in-access-req
radius-server attribute 8 include-in-access-req
radius-server attribute 55 access-request include
radius-server attribute 25 access-request include
radius-server host 10.100.1.35 auth-port 1812 acct-port 1813 key cisco
radius-server retransmit 5
radius-server timeout 15
radius-server vsa send accounting
radius-server vsa send authentication
!
control-plane
!
!
dial-peer cor custom
!
!
!
!
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
gatekeeper
 shutdown
!
alias exec showdb show database data IDMGR-Session-DB 2
alias exec sss show subscriber session
alias exec css clear subscriber session
alias exec showpb show ip portbundle status inuse
alias exec ss show subscriber statistics
!
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 exec-timeout 0 0
!
ntp clock-period 17179872
ntp server 10.200.1.41 source GigabitEthernet0/3 prefer
!
end
```

Deployment Model 4: LNS

```
version 12.2
no service pad
service timestamps debug datetime msec localtime
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname ie2-C7301-LNS
!
boot-start-marker
boot host ftp://223.255.12.34/tftpboot/ie2/configs/tc5xx/isg_add_tc5xx_lns.dat
boot system disk0:c7301-js-mz.122-27.1.11.SIE7
boot-end-marker
!
logging buffered 2000000 debugging
no logging console
enable password lab
!
aaa new-model
!
!
aaa group server radius CAR_SERVER
 server 10.100.2.36 auth-port 1812 acct-port 1813
!
aaa authentication login default none
aaa authentication login IP_AUTHEN_LIST group CAR_SERVER
aaa authentication ppp default group CAR_SERVER
aaa authorization network default group CAR_SERVER
aaa authorization subscriber-service default local group radius
aaa accounting network default start-stop group CAR_SERVER
aaa server radius sesm
 client 10.100.4.38
 key cisco
 port 1812
 message-authenticator ignore
!
!
aaa session-id common
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
clock timezone Pacific -8
ip subnet-zero
!
!
ip ftp username root
ip ftp password lab
no ip dhcp use vrf connected
!
ip vrf VPN_C73_DM4_1001
 rd 200:71001
 route-target export 200:71001
 route-target import 200:71001
!
ip cef
!
subscriber policy recording rules limit 64
vpdn enable
vpdn ip udp ignore checksum
!
!
redirect server-group SESM-Server
 server ip 10.100.4.38 port 8080
!
clns routing
no mpls traffic-eng auto-bw timers frequency 0
mpls label protocol ldp
call rsvp-sync
!
vpdn-group L2TP_DM1_101
 accept-dialin
  protocol l2tp
  virtual-template 5
 terminate-from hostname L2TP_DM1_101
 local name L2TP_DM1_101
 l2tp tunnel password 0 cisco
!

!
!
interface Loopback0
 ip address 10.200.1.56 255.255.255.255
 ip router isis Remote_ISP_7301
!
!
interface Loopback5001
 ip address 5.55.1.1 255.255.0.0
!
!
interface GigabitEthernet0/0
 ip address 223.255.12.56 255.255.255.0
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
!
interface GigabitEthernet0/1
 description connection to ISP2 CORE router
 ip address 27.27.1.56 255.255.255.0
 ip portbundle outside
 ip router isis Remote_ISP_7301
 load-interval 30
 duplex auto
 speed auto
 media-type gbic
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
 negotiation auto
 mpls label protocol ldp
 mpls ip
!
interface GigabitEthernet0/2
 description connection to ISP1 CORE router
 ip address 26.26.1.56 255.255.255.0
 ip router isis Remote_ISP_7301
 load-interval 30
 duplex auto
 speed auto
 media-type gbic
 negotiation auto
!
interface Virtual-Template5
 no ip address
 load-interval 30
 no peer default ip address
 no keepalive
 ppp mtu adaptive
 ppp authentication chap
!
router isis Remote_ISP_7301
 net 01.0011.5dd1.f01b.00
 redistribute connected
!
router bgp 200
 no synchronization
 bgp router-id 10.200.1.56
 bgp log-neighbor-changes
 network 10.100.4.0 mask 255.255.255.0
 network 10.200.1.47 mask 255.255.255.255
 network 10.200.1.55 mask 255.255.255.255
 network 10.200.1.62 mask 255.255.255.255
 network 21.21.1.55 mask 255.255.255.0
 network 22.22.1.55 mask 255.255.255.0
 network 23.0.0.0
 network 24.0.0.0 mask 255.255.0.0
 network 24.5.0.0 mask 255.255.0.0
 redistribute connected
 neighbor 10.200.1.41 remote-as 100
 neighbor 10.200.1.41 ebgp-multihop 2
 neighbor 10.200.1.41 update-source Loopback0
 neighbor 10.200.1.47 remote-as 200
 neighbor 10.200.1.47 update-source Loopback0
 no auto-summary
!
 address-family vpnv4
 neighbor 10.200.1.47 activate
 neighbor 10.200.1.47 send-community both
 exit-address-family
!
 address-family ipv4 vrf VPN_C73_DM4_1001
 redistribute connected
 redistribute static
 no auto-summary
 no synchronization
 exit-address-family
 !
!
ip local pool C73_DM4_7001 1.7.1.2 1.7.255.254
!
ip portbundle
 match access-list 135
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
 source Loopback0
!
ip classless
ip route 10.200.1.41 255.255.255.255 26.26.1.41
!
no ip http server
!
!
!
ip access-list extended Internet-in-acl
 deny   ip any 223.0.0.0 0.255.255.255
 deny   ip any 20.0.0.0 0.255.255.255
 deny   ip any 40.0.0.0 0.255.255.255
 deny   ip any 21.0.0.0 0.255.255.255
 deny   ip any 22.0.0.0 0.255.255.255
 deny   ip any 41.0.0.0 0.255.255.255
 deny   ip any 80.0.0.0 0.255.255.255
 deny   ip any 81.0.0.0 0.255.255.255
 deny   ip any 82.0.0.0 0.255.255.255
 deny   ip any 10.200.0.0 0.0.255.255
 permit ip any any
ip access-list extended Internet-out-acl
 deny   ip 223.0.0.0 0.255.255.255 any
 deny   ip 10.200.0.0 0.0.255.255 any
 deny   ip 20.0.0.0 0.255.255.255 any
 deny   ip 40.0.0.0 0.255.255.255 any
 deny   ip 21.0.0.0 0.255.255.255 any
 deny   ip 22.0.0.0 0.255.255.255 any
 deny   ip 41.0.0.0 0.255.255.255 any
 deny   ip 80.0.0.0 0.255.255.255 any
 deny   ip 81.0.0.0 0.255.255.255 any
 deny   ip 82.0.0.0 0.255.255.255 any
 permit ip any any
ip radius source-interface Loopback0
access-list 135 permit ip any host 10.100.4.38
access-list 135 deny ip any any
!
radius-server attribute 44 include-in-access-req
radius-server attribute 8 include-in-access-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 10.100.2.36 auth-port 1812 acct-port 1813 key cisco
radius-server retransmit 5
radius-server key cisco
radius-server vsa send accounting
radius-server vsa send authentication
!
control-plane
!
!
dial-peer cor custom
!
!
!
!
gatekeeper
 shutdown
!
alias exec sss show subscriber session
alias exec css clear subscriber session
alias exec ss show subscriber statistics
!
line con 0
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```
 exec-timeout 0 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 exec-timeout 0 0
!
ntp clock-period 17180035
ntp server 10.200.1.41 prefer
```

Deployment Model 4: PE

```
ip vrf VPN_C73_DM4_1001
 rd 200:71001
 route-target export 200:71001
 route-target import 200:71001
!
router bgp 100
 no synchronization
 bgp router-id 10.200.1.45
 bgp log-neighbor-changes
 redistribute connected
 redistribute static
 neighbor 10.200.1.41 remote-as 100
 neighbor 10.200.1.41 update-source Loopback0
 no auto-summary
!
 address-family ipv4 vrf VPN_C73_DM4_1001
 redistribute connected
 redistribute static
 no auto-summary
 no synchronization
 network 42.2.107.0 mask 255.255.255.0
 aggregate-address 42.2.107.0 255.255.255.0 summary-only
 exit-address-family
!
ip route vrf VPN_C73_DM4_1001 10.100.3.34 255.255.255.255 GigabitEthernet3/14 10.100.3.34
```

Deployment Model 4: AAA Server for ISP-1

The following profile configures L2TP forwarding from the ISG LAC to the LNS.

```
[ //localhost/Radius/UserLists/L2TPDOMAIN/L2TP_DM4_101.com/Attributes ]
    Cisco-AVpair = vpdn:tunnel-id=L2TP_DM4_101
    Cisco-AVpair = vpdn:l2tp-tunnel-password=cisco
    Cisco-AVpair = vpdn:tunnel-type=l2tp
    Cisco-AVpair = vpdn:ip-addresses=10.200.1.56
    Cisco-AVpair = atm:peak-cell-rate=1024
    Cisco-AVpair = atm:sustainable-cell-rate=512
```

Deployment Model 4: AAA Server for ISP-2

This attribute enables the Layer 4 Redirect feature.

```
[ Attributes ]
    Cisco-AVPair = "ip:l4redirect=redirect list 111 to group SESM-Server duration 30
frequency 180"
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

This attribute enable the PBHK feature on the AAA server, which enables access to the SESM by way of the PBHK feature.

```
[ Attributes ]
    Cisco-AVPair = ip:portbundle=enable
```

This profile configures the basic Internet access service.

```
[ //localhost/Radius/UserLists/SERVICES/INTERNET_SERVICE/Attributes ]
    Cisco-AVPair = ip:inacl=Internet-in-acl
    Cisco-AVPair = ip:outacl=Internet-out-acl
    Cisco-SSG-Service-Info = IINTERNET_SERVICE
    Cisco-SSG-Service-Info = R42.1.1.0;255.255.255.0
```

This profile configures the PPP profile that is used in the subscriber's base profile.

```
[ //localhost/Radius/UserLists/ie2-C7301-LNS/C73_DM1_01@L2TP_DM1_101.com/Attributes ]
    Cisco-AVpair = "ip:ip-unnumbered=loopback 3001"
    Cisco-AVpair = ip:addr-pool=C73_DM1_3001
    Cisco-SSG-Account-Info = AINTERNET_SERVICE
```

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Copyright © 2005 Cisco Systems, Inc. All rights reserved..

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL