Configuring ISG Access for IP Subscriber Sessions

Last Updated: December 19, 2012

Intelligent Services Gateway (ISG) provides a structured framework in which edge devices can deliver flexible and scalable services to subscribers. ISG supports IP sessions for subscribers who connect to ISG from Layer 2 or routed Layer 3 access networks. This module describes how to configure ISG to bring up IP subscriber sessions, manage subscriber IP addressing, and configure dynamic VPN selection.

Note This document assumes that network address translation (NAT) is performed on a different Layer 3 gateway other than ISG.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

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

Prerequisites for ISG Access for IP Subscriber Sessions

- The DHCP server must support the DHCP lease protocol.
- For ISG to use DHCP to assign IP addresses, the following conditions must be met:
  - The subscriber must be Layer 2-connected.
  - ISG must be in the path of DHCP requests, serving as a DHCP server or relay.
  - Appropriate IP subnets must be configured on the subscriber interface.

Restrictions for ISG Access for IP Subscriber Sessions

IPv6 Session Restrictions

- Layer 2 connected interfaces are not supported. Only Layer 3-routed inband IPv6 sessions are supported.
- Out-of-band IPv6 sessions are not supported.
- DHCP-initiated or RADIUS proxy-initiated sessions are not supported for IPv6 sessions.
- Dual-stack sessions are not supported. A native IP session can have either an IPv4 or IPv6 address, not both.

Overlapping IP Address Restrictions

- Overlapping IP addresses in the same virtual routing and forwarding (VRF) instance are not supported.
- Overlapping IP subscribers in different VRFs on the same interface are not supported for static and routed IP subscriber sessions. In contrast, overlapping IP subscribers in different VRFs on the same interface are supported for Layer 2-connected DHCP subscriber sessions.

IP Subnet Session Restrictions

IP subnet sessions are not supported on an interface configured with the **ip subscriber l2-connected** command. IP subnet sessions are supported only when the **ip subscriber routed** command is configured on the interface.

ISG DHCP Restrictions

ISG cannot relay DHCP requests when a Layer 3 DHCP relay agent is between an ISG device and subscriber devices.

Dynamic VPN Selection Restrictions

- Dynamic VPN selection is not supported for IP interface sessions, IP subnet sessions, and subscribers connecting on nonglobal VRF interfaces.
- Dynamic VPN selection is not supported for subscribers with a static VPN configuration on the access interface.
- Dynamic VPN selection with address reassignment is not supported for routed IP subscriber sessions that are initiated by DHCP. The IP addresses of routed IP subscribers must be routable in the access network. Because ISP- or VRF-owned private addresses could overlap or be unroutable in the network between subscribers and an ISG device, IP addresses cannot be addressed to subscribers in such networks.

- IP interface sessions do not support dynamic VRF; only static VRF is supported. If an interface is configured with the **ip subscriber interface** command, dynamic VRF through a RADIUS vendor-specific attributes (VSA) is not supported; only static VRF is supported.

General IP Session Restrictions

- Network Address Translation (NAT) configuration is not supported on the access side of ISG.
- Virtual Fragment Reassembly (VFR) configuration is not supported on the virtual-template interface.
- IP subscriber sessions are not supported on ambiguous IEEE 802.1QinQ or IEEE 802.1Q (Dot1Q) subinterfaces.
- IP subscriber sessions are not supported on interfaces that receive Multiprotocol Label Switching (MPLS) packets.
- Modular quality of service (QoS) CLI (MQC) shaping and queueing is supported in the egress direction in the default class for IP subscriber sessions.
- Configuring features on static IP sessions is not supported.
- ISG IP subscriber functionality is not supported on the following types of access interfaces:
  - Generic routing encapsulation (GRE)
  - Gigabit EtherChannel (Port Channel)
  - Layer 2 Tunnel Protocol (L2TP)
  - PPP (virtual template)
- Interface statistics are not generated for ISG multiservice interfaces.
- Stateful switchover (SSO) and In Service Software Upgrade (ISSU) are not supported for DHCP IP sessions (where ISG serves as a relay or server). Upon switchover, a DHCP IP session must be restarted when the session becomes active again.
- The following subscriber features are not supported for Internet Protocol over Ethernet (IPoE) sessions:
  - Per-session firewall
  - Per-session NAT
  - Per-session netflow
  - Per-session network-based application recognition (NBAR)
  - Per-session multicast
  - Per-session policy-based routing (PBR)
- The following PPP session features are not supported for IP sessions:
  - Packet of Disconnect (PoD)
  - Session limit per system, VLAN, or MAC

Multiservice Interface Restrictions

- IP interface features such as QoS and access lists are not supported on multiservice interfaces.
- Only one multiservice interface can belong to a single VRF. For example, the following configuration will not work:

```
interface multiservice 1
 ip vrf forwarding VRF_A
!
interface multiservice 2
 ip vrf forwarding VRF_A
```

Information About ISG Access for IP Subscriber Sessions

Types of IP Subscriber Sessions

ISG supports the types of IP subscriber sessions described in the following sections:

IP Sessions

An IP session includes all the traffic that is associated with a single subscriber IP address. If the IP address is not unique to the system, other distinguishing characteristics such as a VRF or a MAC address form part of the identity of the session. ISG can be configured to create IP sessions when it receives DHCP packets, packets with unclassified IP or MAC addresses, or RADIUS packets. See the “IP Subscriber Session Initiation” section for more information.

IP sessions may be hosted for a connected subscriber device (one routing hop from the ISG) or a subscriber device that is more than one hop from the gateway.

IP Interface Sessions

An IP interface session includes all the IP traffic that is received on a specific physical or virtual interface. IP interface sessions are created when the IP interface session commands are entered. The session remains continuous even when the interface is shut down. By default, IP interface sessions come up in the unauthenticated state with full network access.

IP interface sessions can be used in situations where a subscriber is represented by an interface (with the exception of PPP) and communicates using more than one IP address. For example, a subscriber using a routed bridge encapsulation (RBE) access might have a dedicated ATM virtual circuit (VC) to home customer premises equipment (CPE) that is hosting a number of PCs.

IP Subnet Sessions

An IP subnet session represents all the traffic that is associated with a single IP subnet. IP subnet sessions are used to apply uniform edge processing to packets associated with a particular IP subnet. When an IP subnet session is configured, ISG treats the subnet as a single subscriber, that is ISG features and functionality are applied to the subnet traffic as an aggregate.

IP subnet sessions are supported for routed IP subscriber traffic.

IP subnet sessions are created in the same way as IP sessions, except that when a subscriber is authorized or authenticated and the Framed-IP-Netmask attribute is present in the user or service profile, ISG converts the source-IP-based session into a subnet session with the subnet value in the Framed-IP-Netmask attribute.

Note Where an ingress interface maps to a single subnet, the subnet might be accommodated with an IP interface session. However, if an ISG device is more than one hop away from a subscriber, and multiple subnets could be accessible through the same interface, IP subnet sessions may be defined to distinguish the traffic and apply appropriate edge functionality to each subnet.

Coexistence of Multicast and IP Sessions

The ISG Session Multicast Coexistence feature introduces the ability to host all the subscribers and services (data and multicast) on the same VLAN by enabling multicast and IP sessions to coexist on the same subinterface for Cisco 7600 series routers. ISG IP sessions are supported on nonaccess-type subinterfaces. In the case of an existing session or even when no session exists, this support helps the multicast traffic to pass through the interfaces configured for the IP sessions in both upstream and downstream directions without creating a session.

IP Subscriber Connectivity

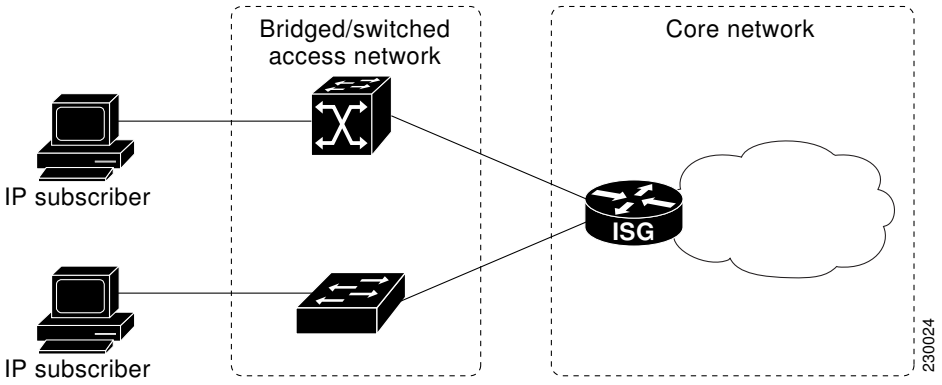
IP subscribers connect to ISG through either Layer 2-connected access networks or routed access networks. The following sections describe these types of IP subscriber connectivity:

- Layer 2-Connected Access Networks, page 5
- Routed Access Networks, page 6

Layer 2-Connected Access Networks

Layer 2-connected subscribers are either directly attached to the physical interfaces of ISG or connected to ISG through a Layer 2 access network, such as a bridged or a switched network. Layer 3 forwarding is either absent or not used to direct subscriber traffic in the Layer 2 access network. IP addresses of the subscribers may or may not be on the same subnet as the Layer 2-connected physical interfaces. The figure below shows an example of a Layer 2-connected access network.

Figure 1 Layer 2-Connected Access Network

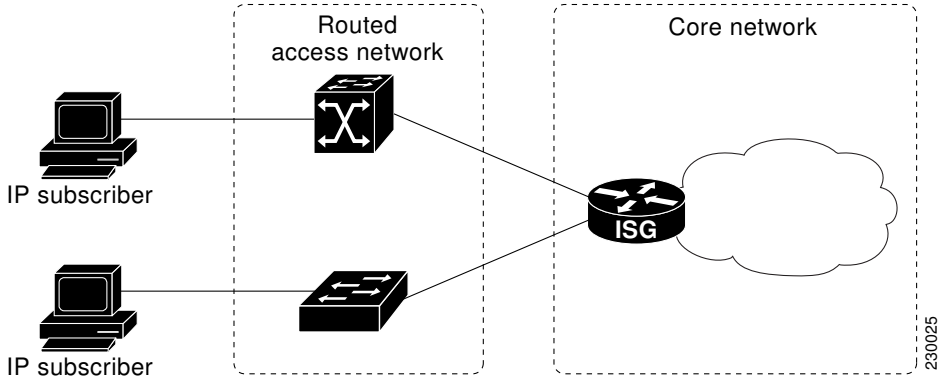


Roaming can be configured on Layer 2-connected IP subscriber sessions by using the **ip subscriber l2-roaming** command. When a Layer 2-connected IP subscriber tries to establish a session with an existing MAC address and a new IP address on an interface that is different from the one that is running the current session, ISG terminates the existing session and creates a new session with a new MAC address-IP address pair. When the subscriber tries to establish a session with an existing MAC address and a new IP address on the same interface that is running the current session, ISG blocks the new session.

Routed Access Networks

For routed access networks, subscriber traffic is routed through a Layer 3 access network with at least one transit router before reaching the ISG. IP addresses of the subscribers are at least routable in the Layer 3 access network. Layer 3 access networks contain a single routing domain and therefore, do not support overlapping IP addresses. The figure below shows an example of a routed access network.

Figure 2 Routed Access Network



IP Subscriber Session Initiation

ISG can be configured to allow one or more of the following events to signal the start of an IP session or IP subnet session on an interface:

- DHCP DISCOVER packet— If the following conditions are met, an IP session is created after ISG receives a DHCP DISCOVER packet:
  - ISG serves as a DHCP relay or a server for new IP address assignments.
  - Subscribers are configured for DHCP.
  - The DHCP DISCOVER packet is the first DHCP request received from the subscriber.
  - Source IP address is unclassified— For routed IP subscribers, a new IP session is triggered when an IP packet with an unclassified source IP address (an IP session does not yet exist for that IP address) is received.
- Unclassified source MAC address— For Layer 2-connected IP subscribers, a new IP session is triggered when an IP packet with an unclassified source MAC address (which means that an IP session does not yet exist for that MAC address) is received.
- RADIUS Access-Request packet— For routed or Layer 2-connected access, a new IP session is triggered by the appearance of a RADIUS Access-Request packet when ISG is serving as a RADIUS proxy.

IP Subscriber Addressing

The following sections provide information about how ISG handles IP addressing for IP subscribers:

Methods of ISG Subscriber IP Address Assignment

IP subscribers either have IP addresses configured statically or obtain IP addresses dynamically through some network protocol that has the ability to assign IP addresses. For a subscriber to be routable within a given IP service domain, the subscriber must present a domain-specific IP address to the network. If a subscriber transfers between IP service domains (including any private domain managed by the access provider), the IP address presented to the network must change to reflect the new domain.

The following sections describe the methods of IP address assignment that ISG supports for each type of Layer 3 session:

IP Interface Sessions

For IP interface sessions, ISG is not involved in (or aware of) the assignment of subscriber IP addresses.

IP Sessions

For IP sessions, ISG supports the following methods of IP address assignment:

- Static IP addresses—If a subscriber's static IP address is configured correctly for the service domain, ISG does not have to be involved in the assignment of an IP address for the subscriber.
- DHCP—If DHCP is being used to assign IP addresses, and the IP address that is assigned by DHCP is correct for the service domain, ISG does not have to be involved in the assignment of an IP address for the subscriber.
  If the IP address that is assigned by DHCP is not correct for the service domain or if the domain changes because of a VRF transfer, ISG can be configured to influence the DHCP IP address assignment.

  The following conditions must be met for ISG to influence DHCP IP address assignment:

  - The subscriber must be Layer 2-connected.
  - The ISG device must be in the path of DHCP requests by serving as a DHCP server or relay.
  - Subscribers must not have statically configured IP addresses.

  For deployments that support it, DHCP is the recommended method of IP address assignment.

IP Subnet Sessions

For IP subnet sessions, the IP subnet is specified in the user profile.

Public and Private IP Addresses

An IP address falls in either the public or the private IP address category, irrespective of the method used to assign the IP address to the IP subscriber. If an IP subscriber is assigned a private IP address and the subscriber has to reach the Internet, a Layer 3 gateway, such as an ISG or a firewall, that is present between the subscriber and the Internet must perform Network Address Translation (NAT) for the subscriber's private IP address.

When the access network is a Layer 2-connected network, a subscriber IP address can be either native or foreign to an access interface. A native subscriber IP address belongs to the subnet provisioned on the access interface. A foreign subscriber IP address does not belong to the subnet provisioned on the access interface. A foreign subscriber IP address could result when a retail ISP assigns an IP address to the IP subscriber from its own IP address allotment, which is different from the wholesale ISPs, or when an IP subscriber with a static IP address that is native in the home access network roams to a foreign access network. To support IP subscribers with foreign IP addresses, ISG must be able to respond to Address Resolution Protocol (ARP) requests that originate from foreign IP addresses with a MAC address of the ISG itself. Because the access network is Layer 2-connected, ISG maintains an adjacency to every subscriber.

When the access network is a routed network, a subscriber IP address must be routable in the access network; otherwise, subscriber traffic will never be able to reach ISG. ISG may not have an adjacency for each subscriber in this case, but has an adjacency of the next hop towards a subscriber. The next hop is determined by the routing process on ISG.

Overlapping IP Addresses

When an access network is deployed without VPN capability, the IP address space in the access network is shared among all IP subscribers. When the IP addresses are assigned dynamically, care must be taken to ensure that these addresses do not overlap. When overlapping IP addresses are assigned to IP subscribers intentionally, the access network should use a Layer 2 separation mechanism to differentiate the IP address spaces. For example, the access network may put each IP address space in a different VLAN.

When the access network serves both local IP subscribers and roaming users, the static private IP address of a roaming subscriber may overlap the native private IP address of another subscriber. For example, a public wireless hotspot that generally assigns dynamic IP addresses may provide access to occasional roaming users with statically configured IP addresses. To support this special overlapping condition, all IP subscribers must be in a Layer 2-connected access network in which overlapping MAC addresses do not exist. In this case, IP subscribers can be distinguished using MAC addresses.

ISG Subscriber IP Address Assignment Using DHCP

When ISG is in the path of DHCP requests (as either a DHCP server or a DHCP relay), ISG can influence the IP address pool and the DHCP server that are used to assign subscriber IP addresses. To enable ISG to influence the IP addresses assigned to subscribers, associate a DHCP address pool class with an address domain. The DHCP address pool class must also be configured in a service policy map, service profile, or user profile that is associated with a subscriber. When a DHCP request is received from a subscriber, DHCP uses the address pool class that is associated with the subscriber to determine which DHCP address pool should be used to service the request. As a result, on a per-request basis, an IP address is either provided by the local DHCP server or relayed to a remote DHCP server that is defined in the selected pool.

IP Subscriber Identity

IP subscriber identity is closely related to IP session initiation because ISG must uniquely identify an IP subscriber at the time that it creates an IP session. However, the need to identify an IP subscriber goes

beyond the session initiation phase. The following sections describe how ISG uniquely identifies IP subscribers:

Routed IP Subscriber Identity

By definition, subscriber IP addresses are at least routable in the access network. If the access network is a routed network, subscriber IP addresses can be used to uniquely identify IP subscribers.

When using a subscriber IP address as the identifier, ISG assumes that the subscriber IP address is unique. If the access network is deployed with Layer 3 load balancing, redundancy, or asymmetric routing, ISG also assumes that IP traffic from the same IP subscriber may arrive at different access interfaces. To support this type of deployment, ISG assumes a single IP address space for all access interfaces connecting to the same access network.

If there is a requirement to support several IP address spaces over a single physical access network, the access network must use some Layer 2 encapsulation to create a separate logical access network for each IP address space. In this case, ISG can still have a single IP address space for all the logical access interfaces that connect to a logical access network.

When subscriber IP addresses are private IP addresses, the access network must be able to route such subscriber traffic. If the subscriber traffic is destined for the Internet, NAT must be performed.

For routed IP subscribers, the subscriber IP address serves as the key for an IP session. ISG associates IP traffic with an IP session as follows:

- In the upstream direction, the source IP address of an IP packet is used to identify the IP session. The source IP address is the subscriber IP address.
- In the downstream direction, the destination IP address of an IP packet is used to identify the IP session. The destination IP address is the subscriber IP address.

If the IP subscriber is a VPN user, the subscriber IP address must be routable in both the global routing table and the VPN routing table on ISG.

For an IP subnet subscriber, a subscriber IP address is defined as an IP prefix address instead of a /32 IP host address. This IP prefix covers a range of IP addresses used by end users but represents a single logical IP subscriber for ISG. In this deployment, all end users share the same connectivity and services provided by ISG.

To normalize the classification of IP subscribers that have different network masks, ISG uses the network mask in conjunction with the subscriber IP address for routed IP subscribers.

MAC Address as Secondary Identity

You must configure the **collect identifier mac-address** command at the start of a session. This instructs the ISG devices to store the MAC address as part of the session identifiers. For routed IP subscriber sessions, the MAC address is collected from the DHCP server using the DHCP lease Query Protocol. For information about configuring the command, see the “Configuring ISG Control Policies” module.

DHCP Lease Query Support

The DHCP Lease Query message is a DHCP message type transmitted from a DHCP relay agent to a DHCP server. A DHCP Lease Query-aware relay agent sends the location of an IP endpoint to the DHCP Lease Query message.

The DHCP Lease Query transaction is a DHCP transaction with special message types that enable clients to query DHCP servers regarding the owner and the lease expiration time of an IP address. For information about configuring DHCP server for Lease Query, see the "Configuring a DHCP Server IP Address" section.

Layer 2-Connected IP Subscriber Identity

A Layer 2-connected access network can provide IP connectivity to IP subscribers with native IP addresses and foreign and overlapping IP addresses. Because subscriber IP addresses might not be unique in such an access network, ISG uses the subscriber MAC address to identify Layer 2-connected IP subscribers.

Traffic that comes from IP subscribers with private or overlapping IP addresses and that is destined to the Internet is subject to NAT.

For Layer 2-connected IP subscribers, both the subscriber MAC address (unique within a VLAN) and the IP address, serve as keys for the IP session and are used in the following directions:

- In the upstream direction, the VLAN ID and source MAC address of an IP packet are used to identify the IP session.
- In the downstream direction, the destination IP address and the VLAN ID of an IP packet are used to identify the IP subscriber context.

Interface IP Subscriber Identity

When access interfaces are used to identify IP subscribers, each access interface corresponds to a single IP subscriber. As soon as the access interface becomes available, ISG creates an IP session using the interface as the key, and associates all IP traffic coming in and going out of this interface with the IP session.

To accurately associate IP traffic with an IP subscriber, ISG must be configured to use interfaces as the method of IP subscriber identification. ISG will then classify IP traffic as follows:

- When receiving IP traffic from the access network (upstream direction), ISG uses the input interface to identify the IP session.
- When receiving IP traffic from the core network (downstream direction), ISG uses the output interface to identify the IP session.

VPN Connectivity and Services for IP Subscribers

Subscriber VPN Membership

Based on the deployment requirements, an IP subscriber may or may not have the VPN service. If an IP subscriber does have the VPN service, the subscriber may belong to only one VPN domain at any time. An IP subscriber is associated with a VPN domain in one of the following ways:

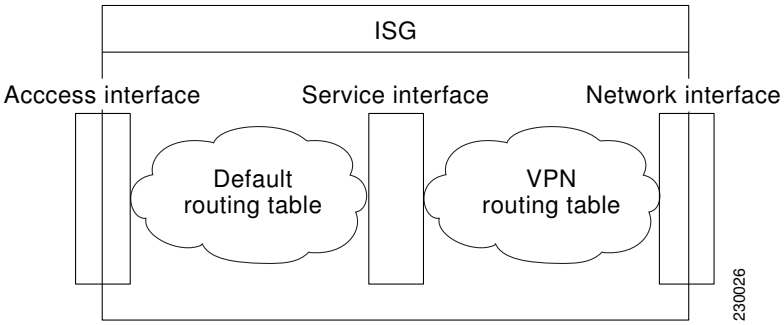
- Static VPN assignment—The VPN IP subscriber belongs to a static VPN domain. Whenever the IP subscriber connects to ISG, the IP subscriber is placed in the preassigned VPN domain.
- Dynamic VPN selection—The VPN IP subscriber can choose and switch among different VPN domains through dynamic service login. Whenever a new VPN domain is selected, VPN services of the current VPN domain must be removed before VPN services of the new VPN domain can be applied to the IP subscriber.

Dynamic VPN selection can be initiated through automatic service login, where the virtual routing and forwarding (VRF) instance is downloaded and applied to the subscriber session at the start of a session. Dynamic VPN selection can also be initiated through subscriber service selection at a web portal, where the subscriber is transferred to the VRF that corresponds to the selected service.

Multiservice Interface Model

For a subscriber without a static VPN configuration, a multiservice interface must be configured on the ISG device to map the IP session to a VRF instance. The multiservice interface represents a boundary between a VPN routing domain and the default routing domain. When an IP subscriber is associated with several routing domains throughout the duration of a connection, multiservice interfaces serve as demarcation points for the IP subscriber to switch from one VPN domain to another VPN domain. One multiservice interface must be configured for each VPN routing domain. The figure below illustrates the multiservice interface model.

Figure 3 Multiservice Interface Model



VPN Addressing

When a subscriber session is transferred from one VPN domain to another, the session enters a new addressing domain that may or may not overlap the previous domain of the subscriber. The network-facing address of the subscriber must be altered accordingly, so that packets can be correctly routed back from within the service domain.

A VRF transfer is necessary when a identity of the subscriber and subscribed services cannot be determined without interaction with a web portal. A local routing context is required, at least initially, so that IP packets may be routed to and from the portal server. After the portal-based service selection, the subscriber

has to be transferred into the VRF that is associated with the selected service domain. After the VRF transfer, the subscriber must also receive an address that is routable in this new domain.

If ISG is adjacent to the subscriber device and serves as a DHCP relay or server, DHCP can be used to assign domain-specific addresses to subscribers.

To support VRF transfers, DHCP should be configured with short initial leases. This is because existing subscriber addresses can be altered only after the current lease has expired. Subscribers will not have access to the selected domain before the next DHCP renew request is received. Using short initial lease times minimizes the interval between a VRF change and a DHCP renewal. If long lease times are used, an out-of-band method of initiating IP address change should be implemented.

When DHCP can be used to assign a new address at the subscriber device, subnet-based VRF selection can be used to bring about the transfer. Subnet-based VRF selection (also known as *VRF autoclassify*) is a feature that selects the VRF at the ingress port on the basis of the source IP subnet address.

Service providers and organizations have public IP address blocks allocated to them that are not overlapping by nature. Therefore, when they are assigned public IP addresses, VPN IP subscribers have no overlapping IP addresses. When VPN IP subscribers of different VPN domains have private IP addresses assigned, they are likely to have overlapping addresses in the access network.

An access network is a single IP address space when there is no Layer 2 encapsulation separating VPN IP subscribers of different VPN domains. Therefore, ISG must be able to handle overlapping IP addresses when deploying VPN IP subscribers. IP connectivity for VPN IP subscribers with overlapping IP addresses is possible only when they are connected to ISG through a Layer 2-connected access network.

VPN IP Subscriber Identity

ISG identifies VPN IP subscribers in the same way that it identifies non-VPN IP subscribers. Upstream IP traffic is defined as the subscriber IP traffic traveling from the access network to the VPN (overlaid on top of the service provider core network). Downstream IP traffic is defined as the subscriber IP traffic traveling from the VPN to the access network.

Service Model for VRF Transfers

A *primary* service contains a network-forwarding policy (such as a VRF) in its service definition. Only one primary service at a time can be activated for a session. A secondary service is any service that does not contain a network-forwarding policy.

When a subscriber for whom a primary service has already been activated tries to select another primary service, ISG deactivates all current services (including the current primary service) and activates the new primary service, and hence, switches the VRF.

When a subscriber for whom a primary service has already been activated tries to select a secondary service, the action taken by ISG depends on whether the secondary service is part of a service group. A service group is a grouping of services that may be simultaneously active for a given session. Typically, a *service group* includes one primary service and one or more secondary services. The table below describes the action that ISG will take when a subscriber selects a secondary service.

Table 1 ISG Activation Policy for Secondary Services

Primary Service Characteristics	Secondary Service Characteristics	Resulting Behavior at ISG
Primary service with no service group attribute	Secondary service with service group	Do not bring up the secondary service.
	Secondary service with no service group	Bring up the secondary service.
Primary service with service group attribute	Secondary service with different service group	Do not bring up the secondary service.
	Secondary service with same service group	Bring up the secondary service.
	Secondary service with no service group	Bring up the secondary service.

Benefits of Dynamic VPN Selection

The need for switching of a subscriber session between routing and forwarding domains (also called *network services*) occurs frequently in markets where equal access networking must be supported. Equal access networking is often mandated by regulatory rules stating that an access provider should allow service providers equal access to a retail subscriber network. ISG dynamic VPN selection facilitates equal access networking by allowing subscribers to transfer between network services.

VRF-Aware Support for CoA Clients

- ISG supports VRF-aware capabilities for CoA clients (RADIUS server), allowing one CoA client to accommodate subscribers in multiple VRFs. Subscriber sessions can be in a different VRF than where the CoA client is configured. To send a CoA message to ISG if the IP subscriber session is in a different VRF, the session identifier must use the vendor-specific attribute (VSA) format shown in the table below.

Table 2 VRF ID VSA Description

Sub-AttrID	Attribute Type	Value	Example
250	account-info	S<*subscriber-ip-address* [:vrf-id=*vrf-name*]> • S--Code for subscriber IP • *vrf-name* --VRF where the Network access server (NAS) will look up the subscriber IP address.	Cisco-Account-Info=S10.0.0.3:vrf-id=subscriber_VRF1

The following example shows the VRF configuration:

RADIUS user profile

```
simulator radius subscriber 401
 authentication smith pap smith
 vsa cisco 250 S10.0.0.3:vrf-id=subscriber_VRF1
 vsa cisco generic 252 binary 015042484b
```

The lookup of the subscriber session is based on the method of providing the VRF. The order of precedence in determining which VRF to use to look up the subscriber IP address is as follows:

1. VRF present in CoA message as part of session-identifier
2. VRF present in client configuration.
3. VRF to which the CoA client belongs

The table below shows the expected behavior when the client sends the CoA message to the server.

Table 3 Expected Behavior Using vrf-id Attribute

If vrf-id is present in...		Then the lookup of the subscriber IP address is done within this VRF
CoA Message	CoA Client Configuration	
Yes	Yes	VRF in CoA message
Yes	No	VRF in CoA message
No	Yes	VRF in client configuration
No	No	VRF in the configuration of the interface facing the client
vrf-id=global	No	VRF in global routing table on server

IP Session Termination

An IP session may be terminated in one of the following ways:

- DHCP lease expiry or DHCP release from client—If DHCP is used to detect a new session, its departure may also be signaled by a DHCP event.
- Application stop—The **application stop** command is typically used to terminate a session when a subscriber initiates an account logout from a web portal. An application stop may also result from the actions of an administrator, such as action taken in response to rogue behavior from a subscriber.
- Idle timeout and session timeout—Idle timeouts and session timeouts can be used to detect or impose termination of an IP session.
- Control policy—A control policy containing the service disconnect action can be used to terminate a session.

IP Session Recovery for DHCP-Initiated IP Sessions

When an IP session is terminated (for example, by account logoff or session timeout) or lost (for example, by router reload), the client may continue to hold an unexpired DHCP lease. When the client continues to hold an unexpired DHCP lease, ISG performs a session restart to prevent the client's IP connection from being nonfunctional until the DHCP lease expires. A control policy can be configured to define the actions that ISG performs when the session restart event occurs. If a policy is not defined, a default policy takes effect. The default policy causes ISG to disconnect the session after 60 seconds after a session restart and is the equivalent of the following configuration:

```
policy-map type control GLOBAL
 class type control always event session-restart
  1 service disconnect delay 60
```

This default policy appears in the output of the **show subscriber policy rules** command, as follows:

```
Rule: internal-rule-session-restart
 Class-map: always event session-restart
  Action: 1 service disconnect delay 60
  Executed: 0
```

Default Services for IP Subscriber Sessions

New IP sessions may require a default service to allow subsequent subscriber packets to be processed appropriately; for example, to permit or force TCP packets to a captive portal where menu-driven authentication and service selection can be performed. A default service policy map or service profile may be configured for IP sessions to redirect traffic, enable port-bundle host-key functionality for session identification, or enable transparent autologin. A default service might also include a network service, which allows subscribers to access a web portal for authentication and service selection.

How to Configure ISG for IP Subscriber Sessions

Creating ISG Sessions for IP Subscribers

An ISG creates IP sessions for IP traffic on subscriber-side interfaces.

Note For the Cisco 7600 router, ISG IP sessions can be configured on both access and nonaccess subinterfaces.

The following tasks enable IP sessions on an interface and indicate how sessions will be identified:

Creating IP Subscriber Sessions for Routed ISG Subscribers

Routed IP subscribers are subscribers that are routed through a Layer 3 access network with at least one transit router before reaching the ISG. Perform this task to configure ISG to create IP sessions for routed IP subscribers.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Do one of the following:
   - **interface** *type number*
   - or
   - **interface** *type number* **access**
4. **ip subscriber routed**
5. **initiator** {**dhcp** [**class-aware**] | **radius-proxy** | **unclassified ip-address**}
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose

Step 3	Do one of the following:
	• **interface** *type number*
	• or
	• **interface** *type number* **access**
	
	Example:
	`Router(config)# interface GigabitEthernet 1/0/0`
	
	Example:
	
	Example:
	`Router(config)# interface GigabitEthernet 1/0/0.100 access`
		Specifies an interface and enters interface configuration mode.
		• **access** --Specifies a subinterface.

Step 4	**ip subscriber routed** **Example:** `Router(config-if)# ip subscriber routed`	Specifies the type of IP subscriber to be hosted on the interface, and enters ISG IP subscriber configuration mode.

	Command or Action	Purpose
Step 5	**initiator** {**dhcp** [**class-aware**] | **radius-proxy** | **unclassified ip-address**} **Example:** `Router(config-subscriber)# initiator dhcp class-aware`	Configures ISG to create an IP subscriber session upon receipt of the specified packet type. • **dhcp** --ISG will initiate an IP session upon receipt of a DHCP DISCOVER packet. The **class-aware** keyword allows ISG to influence the IP address assigned by DHCP by providing DHCP with a class name. • **radius-proxy** --ISG will initiate an IP session upon receipt of a RADIUS Access-Request packet. **Note** The RADIUS proxy feature is not supported on the Cisco 7600 router. • **unclassified ip-address** --ISG will initiate an IP session upon receipt of the first IP packet with an unclassified IP source address. • This command can be entered more than once to specify more than one method of IP session initiation. **Note** If the ISG device serves as either a DHCP relay or DHCP server in the assignment of client IP addresses, ISG must be configured to initiate IP sessions upon receipt of DHCP DISCOVER packets. In other words, the **initiator dhcp** command must be configured instead of the **initiator unclassified ip** or **initiator unclassified mac** command.
Step 6	**end** **Example:** `Router(config-subscriber)# end`	(Optional) Returns to privileged EXEC mode.

Creating IP Subscriber Sessions for Layer 2 Connected ISG Subscribers

Layer 2 connected subscribers are either directly attached to the physical interfaces of an ISG or connected to an ISG through a Layer 2 access network, such as a bridged network or a switched network. Perform this task to configure ISG to create IP sessions for Layer 2 connected IP subscribers.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Do one of the following:
   - **interface** *type number*
   - or
   - **interface** *type number* **access**
4. **ip subscriber l2-connected**
5. **initiator** {**dhcp** [**class-aware**] | **radius-proxy** | **unclassified mac-address**}
6. **arp ignore local**
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

Command or Action	Purpose

Step 3 Do one of the following:
• **interface** *type number*
• or
• **interface** *type number* **access**
 	
Example:
`Router(config)# interface GigabitEthernet 1/0/0`
 	
Example:
 	
Example:
`Router(config)# interface GigabitEthernet 1/0/0.100 access`
	Specifies an interface and enters interface configuration mode.
	• **access** --Specifies a subinterface.

Step 4 **ip subscriber l2-connected** **Example:** `Router(config-if)# ip subscriber l2-connected`	Specifies the type of IP subscriber to be hosted on the interface, and enters ISG IP subscriber configuration mode. **Note** It is recommended that you configure IP sessions for Layer 2 connected subscribers by using the **ip subscriber l2-connected** command. You can also use the **ip subscriber routed** command if subscriber IP addresses are routable in the access domain.

	Command or Action	Purpose
Step 5	**initiator** {**dhcp** [**class-aware**] | **radius-proxy** | **unclassified mac-address**} **Example:** `Router(config-subscriber)# initiator unclassified mac-address`	Configures ISG to create an IP subscriber session upon receipt of the specified packet type. • **dhcp** --ISG initiates an IP session upon receipt of a DHCP DISCOVER packet. The **class-aware** keyword is required when using the **dhcp** keyword. • **radius-proxy** --ISG initiates an IP session upon receipt of a RADIUS packet. **Note** The RADIUS proxy feature is not supported on the Cisco 7600 router. • **unclassified mac-address** --ISG will initiate an IP session upon receipt of the first IP packet with an unclassified MAC source address. • This command can be entered more than once to specify more than one method of IP session initiation. **Note** If the ISG device serves as either a DHCP relay or DHCP server in assigning client IP addresses, ISG must be configured to initiate IP sessions upon receipt of DHCP DISCOVER packets. In other words, the **initiator dhcp** command must be configured instead of the **initiator unclassified ip** or **initiator unclassified mac** command.
Step 6	**arp ignore local** **Example:** `Router(config-subscriber)# arp ignore local`	(Optional) Prevents ISG from replying to incoming Address Resolution Protocol (ARP) requests for destinations on the same interface.
Step 7	**end** **Example:** `Router(config-subscriber)# end`	(Optional) Returns to privileged EXEC mode.

Creating ISG IP Interface Sessions

An ISG IP interface session encompasses all IP packets that cross the specified interface or subinterface. Perform this task to create an ISG IP interface session.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number* [**.** *subinterface-number*]
4. **ip subscriber interface**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* [**.** *subinterface-number*] **Example:** `Router(config)# interface ethernet 0/0.1`	Specifies an interface or subinterface and enters interface configuration mode.
Step 4	**ip subscriber interface** **Example:** `Router(config-if)# ip subscriber interface`	Specifies the type of IP subscriber to be hosted on the interface.
Step 5	**end** **Example:** `Router(config-if)# exit`	(Optional) Returns to privileged EXEC mode.

Creating an ISG Static Session

The ISG Static Session Creation feature enables administrator-initiated static IP sessions. An ISG static session enables you to configure static IP sessions from the CLI. You can create static IP sessions by configuring a group of server addresses.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip subscriber list** *list-name*
4. Do one of the following:
   - **ip source** *ipaddress* **mac** *macaddress*
   -
   - **ip source** *ipaddress* **mask** *subnetmask*
5. **exit**
6. Do one of the following:
   - **interface** *type number*
   -
   - **interface** *type number* **access**
7. Do one of the following:
   - **ip subscriber l2-connected**
   -
   - **ip subscriber routed**
8. **initiator static ip subscriber list list-name**
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip subscriber list** *list-name* **Example:** `Router(config)# ip subscriber list mylist`	Specifies the IP subscriber list name and enters server list configuration mode.

Command or Action	Purpose

Step 4 Do one of the following:
• **ip source** *ipaddress* **mac** *macaddress*
•
• **ip source** *ipaddress* **mask** *subnetmask*
 	
Example:
`Router(config-server-list)# ip source 209.165.200.225 mac 0.7.f`
 	
Example:
 	
Example:
`Router(config-server-list)# ip source 209.165.200.225 mask 255.255.255.224`
	Specifies the static server IP address and MAC address (in the case of L2-connected) or subnet mask (in the case of routed).

Step 5 **exit** **Example:** `Router(config-server-list)# exit`	Returns to global configuration mode.

Step 6 Do one of the following:
• **interface** *type number*
•
• **interface** *type number* **access**
 	
Example:
`Router(config)# interface GigabitEthernet 1/0/0`
 	
Example:
 	
Example:
`Router(config)# interface GigabitEthernet 1/0/0.100 access`
	Specifies an interface and enters interface configuration mode.
	• **access** --Specifies a subinterface.

	Command or Action	Purpose

Step 7	Do one of the following:
	• **ip subscriber l2-connected**
	•
	• **ip subscriber routed**
	Example:
	`Router(config-if)# ip subscriber l2-connected`
	Example:
	Example:
	`Router(config-if)# ip subscriber routed`
		Specifies the type of IP subscriber to be hosted on the interface and enters ISG IP subscriber configuration mode.
		Note It is recommended that you configure IP sessions for Layer 2 connected subscribers by using the **ip subscriber l2-connected** command. However, you can also use the **ip subscriber routed** command if subscriber IP addresses are routable in the access domain.

Step 8	**initiator static ip subscriber list list-name** **Example:** `Router(config-subscriber)# initiator static ip subscriber list mylist`	Creates an IP subscriber session with the packet type as static and attaches the session to the list.
Step 9	**end** **Example:** `Router(config-subscriber)# end`	(Optional) Returns to privileged EXEC mode.

Creating ISG IP Subnet Sessions

An IP subnet session represents all the traffic that is associated with a single IP subnet. IP subnet sessions are used to apply uniform edge processing to packets associated with a particular IP subnet. When an IP subnet session is configured, ISG treats the subnet as a single subscriber, which means that ISG features and functionality are applied to the subnet traffic as an aggregate. Perform this task to configure an IP subnet session.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Do one of the following:
   - **interface** *type number*
   - or
   - **interface** *type number* **access**
4. **ip subscriber routed**
5. **initiator unclassified ip-address**
6. **end**
7. Add the Framed-IP-Netmask attribute to the service or user profile.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose

Step 3	Do one of the following:
	• **interface** *type number*
	• or
	• **interface** *type number* **access**
	
	Example:
	`Router(config)# interface GigabitEthernet 1/0/0`
	
	Example:
	
	Example:
	`Router(config)# interface GigabitEthernet 1/0/0.100 access`
		Specifies an interface and enters interface configuration mode.
		• **access** --Specifies a subinterface.

Step 4	**ip subscriber routed** **Example:** `Router(config-if)# ip subscriber routed`	Specifies the type of IP subscriber to be hosted on the interface, and enters ISG IP subscriber configuration mode.
Step 5	**initiator unclassified ip-address** **Example:** `Router(config-subscriber)# initiator unclassified ip-address`	Configures ISG to create an IP subscriber session upon receipt of an IP packet with an unclassified IP source address.
Step 6	**end** **Example:** `Router(config-subscriber)# end`	(Optional) Returns to privileged EXEC mode.
Step 7	Add the Framed-IP-Netmask attribute to the service or user profile.	Enables an IP subnet session for the subscriber. • When a subscriber is authorized or authenticated and the Framed-IP-Netmask attribute is present in the user or service profile, ISG converts the source-IP-based session into a subnet session with the subnet value in the Framed-IP-Netmask attribute.

Configuring IP Session Recovery for DHCP-Initiated IP Sessions

Perform this task to configure Intelligent Services Gateway (ISG) to take specific actions after the recovery of an IP session when ISG has terminated or reloaded the session. This task applies to DHCP-initiated IP sessions only.

If a policy for session recovery is not configured, ISG applies the following default policy:

```
policy-map type control GLOBAL
 class type control always event session-restart
  1 service disconnect delay 60
```

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type control** *policy-map-name*
4. **class type control** {*control-class-name* | **always**} **event session-restart**
5. *action-number* **authorize** [**aaa list** *list-name*] [**password** *password*] [**upon network-service-found** {**continue** | **stop**}] **identifier** {**authenticated-domain** | **authenticated-username** | **auto-detect** | **circuit-id** [**plus remote-id**] | **dnis** | **mac-address** | **nas-port** | **remote-id** [**plus circuit-id**] | **source-ip-address** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username**}
6. *action-number* **service-policy type service** [**unapply**] [**aaa list** *list-name*] {**name** *service-name* | **identifier** {**authenticated-domain** | **authenticated-username** | **dnis** | **nas-port** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username**}}
7. *action-number* **set-timer** *name-of-timer minutes*
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type control** *policy-map-name* **Example:** `Device(config)# policy-map type control MY-POLICY`	Creates or modifies a control policy map, which is used to define a control policy, and enters control policy-map configuration mode.

	Command or Action	Purpose
Step 4	**class type control** {*control-class-name* | **always**} **event session-restart** **Example:** `Device(config-control-policymap)# class type control always event session-restart`	Specifies a control class that is evaluated when the session-restart event occurs and enters policy-map class control configuration mode. • A policy rule for which the control class is **always** will always be treated as the lowest priority rule within the control policy map.
Step 5	*action-number* **authorize** [**aaa list** *list-name*] [**password** *password*] [**upon network-service-found** {**continue** | **stop**}] **identifier** {**authenticated-domain** | **authenticated-username** | **auto-detect** | **circuit-id** [**plus remote-id**] | **dnis** | **mac-address** | **nas-port** | **remote-id** [**plus circuit-id**] | **source-ip-address** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username**} **Example:** `Device(config-control-policymap-class-control)# 1 authorize identifier source-ip-address`	(Optional) Initiates a request for authorization on the basis of the specified identifier.
Step 6	*action-number* **service-policy type service** [**unapply**] [**aaa list** *list-name*] {**name** *service-name* | **identifier** {**authenticated-domain** | **authenticated-username** | **dnis** | **nas-port** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username**}} **Example:** `Device(config-control-policymap-class-control)# 1 service-policy type service aaa list LISTA name REDIRECT`	(Optional) Activates an ISG service. • Specifying an identifier instead of a service name activates a service that has the same name as the specified identifier.
Step 7	*action-number* **set-timer** *name-of-timer minutes* **Example:** `Device(config-control-policymap-class-control)# 1 set-timer TIMERA 5`	(Optional) Starts a named policy timer. • Expiration of the timer generates the event timed-policy expiry.
Step 8	**end** **Example:** `Device(config-control-policymap-class-control)# end`	(Optional) Returns to privileged EXEC mode.

Verifying ISG IP Subscriber Sessions

Perform this task to verify IP subscriber session configuration and creation. The **show** commands can be used in any order.

SUMMARY STEPS

1. **enable**
2. **show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id* | **username** *name*]
3. **show ip subscriber** [**mac** *mac-address* | [**vrf** *vrf-name*] [[**dangling** *seconds*] [**detail**] | **interface** *interface-name* [**detail** | **statistics**] | **ip** *ip-address* | **static list** *listname* | **statistics** {**arp** | **dangling**}]]
4. **show platform isg session-count** {**all** | *slot*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show subscriber session** [**detailed**] [**identifier** *identifier*	**uid** *session-id*	**username** *name*] **Example:** `Device# show subscriber session detailed`	Displays information about ISG policies and features for subscriber sessions.
Step 3	**show ip subscriber** [**mac** *mac-address*	[**vrf** *vrf-name*] [[**dangling** *seconds*] [**detail**]	**interface** *interface-name* [**detail**	**statistics**]	**ip** *ip-address*	**static list** *listname*	**statistics** {**arp**	**dangling**}]] **Example:** `Device# show ip subscriber ip 10.10.10.10`	Displays information about ISG IP subscriber sessions.
Step 4	**show platform isg session-count** {**all**	*slot*} **Example:** `Device# show platform isg session-count all`	Displays the number of active ISG subscriber sessions by line card.

Clearing ISG IP Subscriber Sessions

SUMMARY STEPS

1. **enable**
2. **show ip subscriber** [**mac** *mac-address* | [**vrf** *vrf-name*] [[**dangling** *seconds*] [**detail**] | **interface** *interface-name* [**detail** | **statistics**] | **ip** *ip-address* | **static list** *listname* | **statistics** {**arp** | **dangling**}]]
3. **clear ip subscriber** [**interface** *interface-name* | **mac** *mac-address* | **slot** *slot-number* **no-hardware** | [**vrf** *vrf-name*] [**dangling** *seconds* | **ip** *ip-address* | **statistics**]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ip subscriber** [**mac** *mac-address* | [**vrf** *vrf-name*] [[**dangling** *seconds*] [**detail**] | **interface** *interface-name* [**detail** | **statistics**] | **ip** *ip-address* | **static list** *listname* | **statistics** {**arp** | **dangling**}]] **Example:** `Device# show ip subscriber ip 10.10.10.10`	(Optional) Displays information about ISG IP subscriber sessions.
Step 3	**clear ip subscriber** [**interface** *interface-name* | **mac** *mac-address* | **slot** *slot-number* **no-hardware** | [**vrf** *vrf-name*] [**dangling** *seconds* | **ip** *ip-address* | **statistics**]] **Example:** `Device# clear ip subscriber ip 10.10.10.10`	Clears ISG IP subscriber sessions.

Troubleshooting Tips

Use the following commands to troubleshoot ISG IP subscriber sessions:

- **debug ip subscriber**
- **debug condition**

Managing ISG Subscriber IP Addresses Using DHCP

The tasks in this section assume that you have configured DHCP support in your network.

Configuring an ISG Interface for Dynamic DHCP Class Association

Perform this task to enable ISG to influence the assignment of IP addresses to subscribers on the interface by providing the local DHCP component with a class name. The class name refers to a class configured using the**ip dhcp pool** command and can reference a pool of addresses or a relay destination.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Do one of the following:
   - **interface** *type number*
   - or
   - **interface** *type number* **access**
4. **ip address** *ip-address mask* [**secondary**]
5. **ip subscriber** {**l2-connected** | **routed**}
6. **initiator dhcp class-aware**
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

Command or Action	Purpose

Step 3 Do one of the following:
• **interface** *type number*
• or
• **interface** *type number* **access**
 	
Example:
`Router(config)# interface GigabitEthernet 1/0/0`
 	
Example:
 	
Example:
`Router(config)# interface GigabitEthernet 1/0/0.100 access`
	Specifies an interface for configuration, and enters interface configuration mode.
	• **access** --Specifies a subinterface.

Step 4 **ip address** *ip-address mask* [**secondary**] **Example:** `Router(config-if)# ip address 209.165.200.225 255.255.0.0`	Sets a primary or secondary IP address for an interface.
Step 5 **ip subscriber** {**l2-connected** | **routed**} **Example:** `Router(config-if)# ip subscriber l2-connected`	Enables ISG IP subscriber configuration mode.
Step 6 **initiator dhcp class-aware** **Example:** `Router(config-subscriber) initiator dhcp class-aware`	Configures ISG to create IP sessions upon receipt of DHCP DISCOVER packets. • **class-aware** --Allows ISG to influence the IP address assigned by DHCP by providing DHCP with a class name.
Step 7 **end** **Example:** `Router(config-subscriber)# end`	(Optional) Returns to privileged EXEC mode.

Configuring DHCP Server User Authentication

Perform this task to authenticate the DHCP clients on the server.

You need to use the ISG framework to enable DHCP server user authentication.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication login** *list-name* **local**
5. **ip dhcp pool** *pool-name*
6. **network** *network-number mask*
7. **exit**
8. **interface** *type number*
9. **ip subscriber l2-connected**
10. **initiator dhcp class-aware**
11. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Device(config)# aaa new model`	Enables authentication, authorization, and accounting (AAA).
Step 4	**aaa authentication login** *list-name* **local** **Example:** `Device(config)# aaa authentication login mylist local`	Sets the AAA authentication at login.

	Command or Action	Purpose
Step 5	**ip dhcp pool** *pool-name* **Example:** `Device(config)# ip dhcp pool testpool`	Creates a name for the DHCP server address pool and enters DHCP pool configuration mode.
Step 6	**network** *network-number mask* **Example:** `Device(dhcp-config)# network 172.16.0.0 255.240.0.0`	Configures the network number and mask for a DHCP address pool primary or secondary subnet on a Cisco DHCP server.
Step 7	**exit** **Example:** `Device(dhcp-config)# exit`	Exits DHCP pool configuration mode and returns to global configuration mode.
Step 8	**interface** *type number* **Example:** `Device(config)# interface GigabitEthernet 0/0`	Enters interface configuration mode.
Step 9	**ip subscriber l2-connected** **Example:** `Device(config-if)# ip subscriber l2-connected`	Configures a Layer 2-connected IP session on the interface and enters IP subscriber configuration mode.
Step 10	**initiator dhcp class-aware** **Example:** `Device(config-subscriber)# initiator dhcp class-aware`	Initiates a class for DHCP for an IP session initiated by DHCP.
Step 11	**end** **Example:** `Device(config-subscriber)# end`	Returns to privileged EXEC mode.

- Troubleshooting Tips, page 36

Troubleshooting Tips

You can determine the DHCP authentication by using the **debug ip dhcp server events**, **debug ip dhcp server packet**,and**debug subscriber policy dpm event** commands. The following is sample output from the **debug subscriber policy dpm event** command:

```
*Apr 20 20:20:03.510: SG-DPM: DHCP Discover notification from client, mac_address = 001a.
7014.c03e
*Apr 20 20:20:03.510: SG-DPM: getting the context for mac_address = 001a.7014.c03e
*Apr 20 20:20:03.510: SG-DPM: Could not find a dhcp_context for 001a.7014.c03e:
*Apr 20 20:20:03.510: SG-DPM: Sending an ID manager request with key as 001a.7014.c03e
*Apr 20 20:20:03.510: SG-DPM: Received reply from Id manager
*Apr 20 20:20:03.510: SG-DPM: Session Initiation notification on Active
*Apr 20 20:20:03.510: SG-DPM: Allocated SHDB Handle (0xB6000252) for Mac address 001a.
7014.c03e
*Apr 20 20:20:03.510: SG-DPM: Client is able to perform DHCP Authentication.Setting the
SSS_INFOTYPE_DHCP_AUTH_KEY
*Apr 20 20:20:03.510: SG-DPM: Sending Session start to PM, mac_address = 001a.7014.c03e
*Apr 20 20:20:03.514: SG-DPM: Request for Classname from client, mac_address = 001a.
7014.c03e
*Apr 20 20:20:03.514: SG-DPM: getting the context for mac_address = 001a.7014.c03e
*Apr 20 20:20:03.514: SG-DPM: Sending an ID manager request with key as 001a.7014.c03e
*Apr 20 20:20:03.514: SG-DPM: Received reply from Id manager
*Apr 20 20:20:03.514: SG-DPM: No session found in ID manager
*Apr 20 20:20:03.514: SG-DPM: Processing sg_dpm_get_more_keys from SSS hdl 56000E52
*Apr 20 20:20:03.514: SG-DPM: DPM is providing Auth-User
```

You can also use the **show subscriber session detailed** and **show ip dhcp binding**commands to display subscriber information and DHCP pool information. The following is sample output from the **show ip dhcp binding** command:

```
Router# show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
10.0.0.1            0100.1a70.1530.38       Nov 18 2008 03:43 PM    Automatic
```

Configuring a DHCP Class in a Service Policy Map

Perform this task to assign a DHCP class to a service policy map. Subscribers for which this service policy map is activated will be assigned IP addresses from the DHCP pool or the remote server that is associated with the class.

Before configuring a DHCP class in a service policy map, you must configure a DHCP pool and the classes configured within the DHCP pool must match the DHCP classes configured in the service policy map.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-name*
4. **classname** *class-name*
5. **end**
6. **show policy-map type service**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type service** *policy-name* **Example:** `Device(config)# policy-map type service service1`	Creates a service policy map or specifies an existing service policy map for configuration, and enters service policy-map configuration mode.
Step 4	**classname** *class-name* **Example:** `Device(config-service-policymap)# classname class1`	Associates a DHCP pool with a service policy map.
Step 5	**end** **Example:** `Device(config-service-policymap)# end`	(Optional) Returns to privileged EXEC mode.
Step 6	**show policy-map type service** **Example:** `Device# show policy-map type service`	(Optional) Displays the contents of all service policy maps. • Use this command to verify that the DHCP class is associated with the service policy map.

- What to Do Next, page 37

What to Do Next

Once you have configured the DHCP address pool class in a service policy map, you may want to configure a method of activating the service policy map; for example, control policies can be used to activate services. For more information about methods of service activation, see the module "Configuring ISG Subscriber Services".

Configuring a DHCP Class in a Service Profile or User Profile

Perform this task to add the vendor-specific attribute (VSA) for a DHCP class to a user profile or service profile. Subscribers for whom the user or service profile is activated will be assigned IP addresses from the DHCP pool or the remote server that is associated with the class.

- Prerequisites, page 38
- What to Do Next, page 38

Prerequisites

A DHCP address pool must be configured. Classes configured within the DHCP address pool must match the DHCP address pool classes configured in the service or user profile.

SUMMARY STEPS

1. Add the DHCP Class attribute to the user or service profile.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Add the DHCP Class attribute to the user or service profile. **Example:** `26,9,1 = "subscriber:classname=class-name"`	Associates a DHCP address pool with a service or specific subscriber.

What to Do Next

You may want to configure a method of activating the service policy map or service profile; for example, control policies can be used to activate services. For more information about methods of service activation, see the module "Configuring ISG Subscriber Services."

Configuring a DHCP Server IP Address

Perform this task to either specify which DHCP servers to use on your network or to configure the IP address of one or more DHCP servers available on the network, and to specify the DHCP Lease Query for routed IP sessions.

Note The DHCP server IP address needs to be configured for routed IP sessions if the DHCP Lease Query is performed.

The following prerequisites apply for this task:

- The DHCP server must support the DHCP lease protocol.
- The IP address of the phone must be assigned by DHCP address assignments.
- The traffic must be classified as Layer 3.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp-server** {*ip-address* | **query lease** {**retries** *max-retransmissions* | **timeout** *timeout-query-seconds*}}
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip dhcp-server** {*ip-address* | **query lease** {**retries** *max-retransmissions* | **timeout** *timeout-query-seconds*}} **Example:** `Device(config)# ip dhcp-server query lease retries 3`	Configures the IP address of one or more DHCP servers available on the network, and specifies the DHCP Lease Query for routed IP sessions.
Step 4	**end** **Example:** `Device(config)# end`	Exits global configuration mode.

Configuring ISG Dynamic VPN Selection

Configuring a Multiservice Interface

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface multiservice** *interface-number*
4. **ip vrf forwarding** *vrf-name*
5. **ip address** *ip-address mask*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface multiservice** *interface-number* **Example:** `Device(config)# interface multiservice 1`	Creates a multiservice interface, which enables dynamic VPN selection, and enters interface configuration mode.
Step 4	**ip vrf forwarding** *vrf-name* **Example:** `Device(config-if)# ip vrf forwarding vrf1`	Associates a VPN VRF with an interface or subinterface.
Step 5	**ip address** *ip-address mask* **Example:** `Device(config-if)# ip address 172.16.0.0 255.255.255.0`	Sets the primary IP address for an interface. • Specifies the IP address of the VPN.

	Command or Action	Purpose
Step 6	**end** **Example:** `Device(config-if)# end`	(Optional) Returns to privileged EXEC mode.

Specifying a VRF in a Service Policy Map

VPN routing and forwarding (VRF) transfer occurs when a new primary service is activated for a session, causing the session to transfer from one VRF to another. Services can be configured in service profiles on an external authentication, authorization, and accounting (AAA) server or they can be configured on the ISG device in service policy maps. Perform this task to configure a VRF in a service policy map on the ISG device.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-map-name*
4. **ip vrf forwarding** *name-of-vrf*
5. **sg-service-type primary**
6. **sg-service-group** *service-group-name*
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Command or Action	Purpose
Step 3 **policy-map type service** *policy-map-name* **Example:** `Device(config)# policy-map type service service1`	Creates or modifies a service policy map, which is used to define an ISG service, and enters service policy-map configuration mode.
Step 4 **ip vrf forwarding** *name-of-vrf* **Example:** `Device(config-service-policymap)# ip vrf forwarding vrf1`	Associates the service with a VRF.
Step 5 **sg-service-type primary** **Example:** `Device(config-service-policymap)# sg-service-type primary`	Defines the service as a primary service. • A primary service contains a network-forwarding policy. A service must be defined as a primary service by using the **sg-service-type primary** command. Any service that is not a primary service is defined as a secondary service by default.
Step 6 **sg-service-group** *service-group-name* **Example:** `Device(config-service-policymap)# sg-service-group group1`	(Optional) Associates an ISG service with a service group. • A service group is a group of services that may be active simultaneously for a given session. Typically, a service group includes one primary service and one or more secondary services.
Step 7 **end** **Example:** `Device(config-service-policymap)# end`	(Optional) Returns to privileged EXEC mode.

Verifying VRF Transfer for IP Sessions

Perform the following task as needed to verify VRF transfer for IP sessions. You can use the **show** commands in this task in any order.

SUMMARY STEPS

1. **enable**
2. **show subscriber session uid** *session-identifier* **detail**
3. **show ip subscriber** [**dangling** *seconds* | **detail** | **ip** *ip-address* | **mac** *mac-address* | **vrf** *vrf-name* [**dangling** *seconds* | **detail** | **ip** *ip-address*]]
4. **show idmgr** {**memory** [**detailed** [**component** [*substring*]]] | **service key session-handle** *session-handle-string* **service-key** *key-value* | **session key** {**aaa-unique-id** *aaa-unique-id-string* | **domainip-vrf ip-address** *ip-address* **vrf-id** *vrf-id* | **nativeip-vrf ip-address** *ip-address* **vrf-id** *vrf-id* | **portbundle ip** *ip-address* **bundle** *bundle-number* | **session-guid** *session-guid* | **session-handle** *session-handle-string* | **session-id** *session-id-string*} | **statistics**}
5. **show ip route** [**vrf** *vrf-name*]
6. **show ip dhcp binding** [**ip-address**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show subscriber session uid** *session-identifier* **detail** **Example:** `Device# show subscriber session uid 4 detail`	Displays information about ISG subscriber sessions with a specific session identifier.
Step 3	**show ip subscriber** [**dangling** *seconds*	**detail**	**ip** *ip-address*	**mac** *mac-address*	**vrf** *vrf-name* [**dangling** *seconds*	**detail**	**ip** *ip-address*]] **Example:** `Device# show ip subscriber vrf vrf1`	Displays information about ISG IP subscriber sessions.
Step 4	**show idmgr** {**memory** [**detailed** [**component** [*substring*]]]	**service key session-handle** *session-handle-string* **service-key** *key-value*	**session key** {**aaa-unique-id** *aaa-unique-id-string*	**domainip-vrf ip-address** *ip-address* **vrf-id** *vrf-id*	**nativeip-vrf ip-address** *ip-address* **vrf-id** *vrf-id*	**portbundle ip** *ip-address* **bundle** *bundle-number*	**session-guid** *session-guid*	**session-handle** *session-handle-string*	**session-id** *session-id-string*}	**statistics**} **Example:** `Device# show idmgr session key nativeip-vrf ip-address 209.165.200.225`	Displays information related to ISG session and service identity.

	Command or Action	Purpose
Step 5	**show ip route** [**vrf** *vrf-name*] **Example:** `Device# show ip route`	Displays the current state of the routing table.
Step 6	**show ip dhcp binding** [**ip-address**] **Example:** `Device# show ip dhcp binding`	Displays address bindings on the Cisco IOS DHCP server.

Troubleshooting VRF Transfer for IP Sessions

The commands in this task can be used to troubleshoot VRF transfer of IP sessions. The **debug** commands can be entered in any order.

SUMMARY STEPS

1. **enable**
2. **debug subscriber** {**event** | **error** | **packet** | **policy** | **service**}
3. **debug ip subscriber** {**event** | **error** | **packet** | **fsm** | **all**}
4. **debug subscriber policy dpm** {**error** | **event**}
5. **debug ip dhcp server** {**events** | **packets** | **linkage** | **class**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug subscriber** {**event**	**error**	**packet**	**policy**	**service**} **Example:** `Device# debug subscriber service`	Displays debugging messages pertaining to subscriber policies, policy server events, and changes to service.
Step 3	**debug ip subscriber** {**event**	**error**	**packet**	**fsm**	**all**} **Example:** `Device# debug ip subscriber error`	Displays debugging messages pertaining to an IP session created on the service gateway.

	Command or Action	Purpose
Step 4	**debug subscriber policy dpm** {**error** | **event**} **Example:** `Device# debug subscriber policy dpm event`	Displays diagnostic information about policy execution that is related to DHCP events.
Step 5	**debug ip dhcp server** {**events** | **packets** | **linkage** | **class**} **Example:** `Device# debug dhcp ip dhcp server events`	Enables Cisco IOS DHCP server debugging.

What to Do Next

After you have configured the ISG to bring up Layer 3 sessions, you may want to configure policies for subscriber identification and authorization, such as the Port-Bundle Host Key feature, redirection of unauthenticated subscriber traffic, or automatic subscriber logon. Instructions on how to configure these policies can be found in the following modules:

- Configuring ISG Port-Bundle Host Key
- Redirecting Subscriber Traffic Using ISG Layer 4 Redirect
- Configuring ISG Policies for Automatic Subscriber Logon

Configuration Examples for ISG Access for IP Subscriber Sessions

Example: Creating ISG IP Interface Sessions

The following example shows how to configure an IP interface session on GigabitEthernet interface 0/0/1.401:

```
interface GigabitEthernet 0/0/1.401
 ip subscriber interface
```

Example: Configuring ISG Routed IP Subscriber

The following example shows how to configure ISG to create IP sessions for subscribers who connect to ISG on GigabitEthernet interface 0/0/1.401 through a routed access network. ISG will create IP sessions upon receipt of DHCP DISCOVER packets, incoming valid IP packets, and RADIUS Access-Request packets.

```
interface GigabitEthernet 0/0/1.401
 ip subscriber routed
  initiator dhcp class-aware
  initiator unclassified ip-address
  initiator radius-proxy
```

Example: Creating IP Subscriber Sessions for Layer 2-Connected ISG Subscribers

The following example shows how to configure ISG to create IP sessions for subscribers who connect to ISG on GigabitEthernet interface0/0/1.401 through a Layer 2-connected access network. ISG will create IP sessions upon receipt of any frame with a valid source MAC address.

```
interface GigabitEthernet0/0/1.401
 ip subscriber l2-connected
  initiator unclassified mac-address
```

Example: Creating ISG Static Sessions

The following example shows how to create an ISG static session for server 209.165.200.225 for subscribers who connect to ISG on GigabitEthernet interface 0/4 through a Layer 2-connected access network. ISG will create a static session upon receipt of valid source IP address.

```
ip subscriber list mylist
 ip source 209.165.200.225 mac 0.7.f
interface GigabitEthernet 0/4
 ip subscriber l2-connected
  initiator static ip subscriber list mylist
```

Example: Configuring IP Session Recovery for DHCP-Initiated IP Session

The following example shows how to configure an ISG policy that applies a service called “FIRST-SERVICE” upon session restart for subscribers belonging to the VRF “FIRST”:

```
class-map type control TEST
 match vrf FIRST
policy-map type control GLOBAL
 class type control TEST event session-restart
  1 service-policy type service name FIRST-SERVICE
```

Example: Configuring an ISG Interface for Dynamic DHCP Class Association

In the following example, GigabitEthernet interface 1/0/0.400 is configured with DHCP class-aware functionality, which enables ISG to influence DHCP IP address assignment. If the service SERVICE-DHCP is activated, the DHCP pool DHCP-POOL2 is used for address assignment. Otherwise, the default pool DHCP-POOL1 is used.

```
interface GigabitEthernet1/0/0.400
```

```
 encapsulation dot1Q 400
 ip address 10.1.15.1 255.255.255.0 secondary
 ip address 10.1.10.1 255.255.255.0
 no snmp trap link-status
 service-policy type control RULE_406a
 ip subscriber l2-connected
  initiator dhcp class-aware
!
ip dhcp excluded-address 10.1.10.1
!
ip dhcp pool DHCP-POOL1
   network 10.1.10.0 255.255.255.0
   default-router 10.1.10.1
   lease 0 0 30
   class default
!
ip dhcp class default
!
ip dhcp pool DHCP-POOL2
   network 10.1.15.0 255.255.255.0
   default-router 10.1.15.1
   lease 0 0 30
   class DHCP_CLASS2
!
ip dhcp class DHCP-CLASS2
!
policy-map type service SERVICE-DHCP
 classname DHCP-CLASS2
!
```

Example: Configuring DHCP Address Pool Classes and Relay Actions for ISG

This section contains examples of DHCP address pool configuration and relay actions for ISG.

DHCP Server Coresident with ISG Configuration

In the following configuration example, the ISPs are ISP1 and ISP2 companies. The ISP1 company has its addresses assigned from an address pool that is dynamically allocated using on-demand address pools (ODAP). The ISP2 company has its customer addresses assigned from the address pool 10.100.0.0/16. Customers not associated with any ISP will have an address allocated from the address pool 10.1.0.0/16, and the lease time is set to 10 minutes.

```
!Address pool for ISP1 customers
ip dhcp pool isp1-pool
 origin dhcp
 class isp1
!
!Address pool for ISP2 customers
!
ip dhcp pool isp2-pool
 network 10.100.0.0 255.255.0.0
 class isp2
!
!Address pool for customers without an ISP
!
ip dhcp pool temp
 network 10.1.0.0 255.255.0.0
 lease 0 0 10
 class default
```

DHCP Relay Agent Coresident with ISG Configuration

In the following configuration example, there are two ISPs, “poolA” and “poolB”. The “poolA” ISP and its customers are allowed to have addresses in the ranges 10.1.0.0/16 and 10.3.0.0/16 and are relayed to the

DHCP server at 10.55.10.1. The “poolB” ISP and its customers are allowed to have addresses in the range 10.2.0.0/16 and 10.4.0.0/16, and are relayed to the DHCP server at 10.10.2.1.

```
!Address ranges:
interface gigabitethernet1/0/0
 ip address 10.1.0.0 255.255.0.0
 ip address 10.2.0.0 255.255.0.0 secondary
interface gigabitethernet2/0/0
 ip address 10.3.0.2 255.255.0.0
 ip address 10.4.0.2 255.255.0.0
!Address pools for poolA1 and poolB2:
 ip dhcp pool poolA1
 relay source 10.1.0.2 255.255.0.0
 class poolA1
 relay target 10.55.10.1
!Address pool for poolA2:
ip dhcp pool poolA2
 relay source 10.3.0.2 255.255.0.0
 class poolA2
 relay target 10.55.10.1
!Address pools for poolB1 and poolB2:
ip dhcp pool poolB1
 relay source 10.2.0.2 255.255.0.0
 class poolB1
 relay target 10.10.2.1
ip dhcp pool poolB2
 relay source 10.4.0.0 255.255.0.0
 class poolB2
  relay target 10.10.2.1
```

Configuration of secure ARP for the relay uses the same configuration command as secure ARP uses on a DHCP server. It uses the **update arp** command in address-pool configuration mode. If the system allocates an address from this address pool, secure ARP is added to it. If the system relays a packet using this address pool, secure ARP is also added to it.

Example: Configuring ISG Dynamic VPN Selection

The following example shows a configuration in which subscribers are initially assigned an IP address from the DHCP global pool DHCP-POOL1. After a subscriber accesses the web portal and selects the Corporate VPN service, ISG performs a VRF transfer and the subscriber is assigned a new IP address from the DHCP pool, VPN-POOL1. In this case, a single multiservice interface is required.

```
!
ip vrf VPN_406_1001
rd 406:1001
route-target export 406:1001
route-target import 406:1001
!
interface GigabitEthernet 1/0/0.400
 encapsulation dot1Q 400
 ip address 10.1.10.1 255.255.255.0
 no snmp trap link-status
 service-policy type control RULE-406a
 ip subscriber l2-connected
  initiator dhcp class-aware
!
ip dhcp relay information trust-all
ip dhcp use vrf connected
!
!!!! Default Global DHCP Pool
!
ip dhcp excluded-address 10.1.10.1
!
ip dhcp pool DHCP-POOL1
 network 10.1.10.0 255.255.255.0
 default-router 10.1.10.1
 lease 0 0 30
```

```
 class default
!
ip dhcp class default
!
!
!!! DHCP Pool for CorporateVPN
!
ip dhcp excluded-address 10.1.11.1
!
ip dhcp pool VPN-POOL1
 vrf VPN-406-1001
 network 10.1.11.0 255.255.255.0
 default-router 10.1.11.1
 lease 0 0 30
class DHCP-CLASS-VPN-406-1001
!
interface multiservice 1
 ip vrf forwarding VPN_406_1001
 ip address 10.1.11.1 255.255.255.0
 no keepalive
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	*Cisco IOS Master Commands List, All Releases*
ISG commands	*Cisco IOS Intelligent Services Gateway Command Reference*
DHCP configuration	*IP Addressing: DHCP Configuration Guide*
Configuring ISG control policies	"Configuring ISG Control Policies" module in the *Intelligent Services Gateway Configuration* Guide.

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for ISG Access for IP Subscriber Sessions

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 4 Feature Information for ISG Access for IP Subscriber Sessions

Feature Name	Releases	Feature Information
DHCP Server User Authentication	12.2(33)SRE 15.0(1)S	The DHCP Server User Authentication feature is used to authenticate the DHCP clients. In Cisco IOS Release 12.2(33)SRE, support was added for the Cisco 7600 router.
IP Session Recovery for DHCP-Initiated IP Sessions	12.2(31)SB 12.2(33)SRC2	ISG provides a default policy and the ability to configure a policy that determines the actions ISG will take upon session restart following the recovery of a DHCP-initiated IP session. In Cisco IOS Release 12.2(33)SRC, support was added for the Cisco 7600 router. The following commands were introduced or modified by this feature: **class type control**, **match vrf**.

Feature Name	Releases	Feature Information
IP Subscriber Session CLI Updates	12.2(31)SB2 12.2(33)SRC	Some of the commands that are used to configure ISG IP subscriber sessions were modified or replaced. In Cisco IOS Release 12.2(33)SRC, support was added for the Cisco 7600 router. The following commands were introduced or modified by this feature: **clear ip subscriber**, **debug ip subscriber**, **identifier interface**, **identifier ip src-addr**, **initiator**, **interface multiservice**, **ip subscriber interface, ip subscriber**, **show ip subscriber**.
ISG: Instrumentation: DHCP Lease Query Support	12.2(33)SRE 12.2(33)XNE	The DHCP Lease Query transaction is a DHCP transaction with special message types that enable, among other things, clients to query DHCP servers regarding the owner and the lease expiration time of an IP address. In Cisco IOS Release 12.2(33)XNE, support was added for the Cisco 10000 series routers.
ISG: Session: Creation: Interface IP Session: L2	12.2(28)SB 12.2(33)SRC 12.2SRE	ISG IP interface sessions include all IP traffic received on a specific physical or virtual interface. IP interface sessions are provisioned through the CLI; that is, a session is created when the IP interface session commands are entered. In Cisco IOS Release 12.2(33)SRC, support was added for the Cisco 7600 router.

Feature Name	Releases	Feature Information
ISG: Session: Creation: Interface IP Session: L3	12.2(28)SB 12.2(33)SRC 12.2SRE	ISG IP interface sessions include all IP traffic received on a specific physical or virtual interface. IP interface sessions are provisioned through the CLI; that is, a session is created when the IP interface session commands are entered. In Cisco IOS Release 12.2(33)SRC, support was added for the Cisco 7600 router. The following sections provide information about this feature:
ISG: Session: Creation: IP Session: Protocol Event (DHCP)	12.2(28)SB 12.2(33)SRC	Most ISG sessions are created upon detection of a data flow that cannot be affiliated with an already active session. An ISG can be configured to create an IP session upon receipt of the first DHCP DISCOVER packet received from a subscriber. In Cisco IOS Release 12.2(33)SRC, support was added for the Cisco 7600 router.
ISG: Session: Creation: IP Session: Subnet and Source IP: L2	12.2(28)SB 12.2(33)SRC	The ISG session is the primary component used for associating services and policies across specific data flows. An IP subnet session is an ISG session that includes any IP traffic from a single IP subnet. A source-IP-based session includes traffic from a single source IP address. In Cisco IOS Release 12.2(33)SRC, support was added for the Cisco 7600 router.

Feature Name	Releases	Feature Information
ISG: Session: Creation: IP Session: Subnet and Source IP: L3	12.2(28)SB 12.2(33)SRC	The ISG session is the primary component used for associating services and policies across specific data flows. An IP subnet session is an ISG session that includes any IP traffic from a single IP subnet. A source-IP-based session includes traffic from a single source IP address. In Cisco IOS Release 12.2(33)SRC, support was added for the Cisco 7600 router.
ISG: Session: Multicast: Coexistence	12.2(33)SRE	The ISG Session Multicast Coexistence feature introduces the ability to host all the subscribers and services (data and multicast) on the same VLAN by enabling multicast and IP sessions to coexist on the same subinterface for Cisco 7600 series routers. In Cisco IOS Release 12.2(33)SRE, support was added for the Cisco 7600 router.
ISG: Session: VRF Transfer:	12.2(28)SB 12.2(33)SRC	The ISG session is the primary component used for associating services and policies with specific data flows. ISG sessions are associated with virtual routing and forwarding instances when routing is required for the network service. ISG VRF transfer provides a means to dynamically switch an active session between virtual routing domains. In Cisco IOS Release 12.2(33)SRC, support was added for the Cisco 7600 router.

Feature Name	Releases	Feature Information
ISG: Static Session Creation	12.2(33)SRE 12.2(33)XNE	The ISG Static Session Creation feature enables administrator-initiated static IP sessions. In Cisco IOS Release 12.2(33)SRE, support was added for the Cisco 7600 router. In Cisco IOS Release 12.2(33)XNE, support was added for the Cisco 10000 series routers. The following commands were introduced or modified by this feature: **initiator static subscriber list**,**ip source**,**ip subscriber list**,**show ip subscriber static list**.
VRF-Aware Support for CoA Clients	12.2(31)SB12	Allows one CoA client to support ISG subscribers in different VRFs.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned 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. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2012 Cisco Systems, Inc. All rights reserved.