IP Subscriber Awareness over Ethernet

This chapter provides information about how various Cisco 7600 features are being scaled to support the IP Subscriber Awareness over Ethernet feature (sometimes referred to as *IP subscriber aggregation*), which was introduced for the Cisco 7600 series router in Cisco IOS Release 12.2SRB. From Cisco IOS Release 12.2(33)SRE onwards, the ISG functionality in distributed IP and PPPoE sessions on Cisco 7600 series routers is supported on Ethernet Services Plus (ES+) access-facing line cards. From Cisco IOS Release 12.2(33)SRE8 onwards, Intelligent Services Gateway (ISG) will be disabled for ES+ Low Queue cards.

This chapter contains the following sections:

Note Effective with Cisco IOS Release 15.2(4)S, the Broadband (IP and PPPoE sessions) support is deprecated in Cisco 7600 routers.

Overview

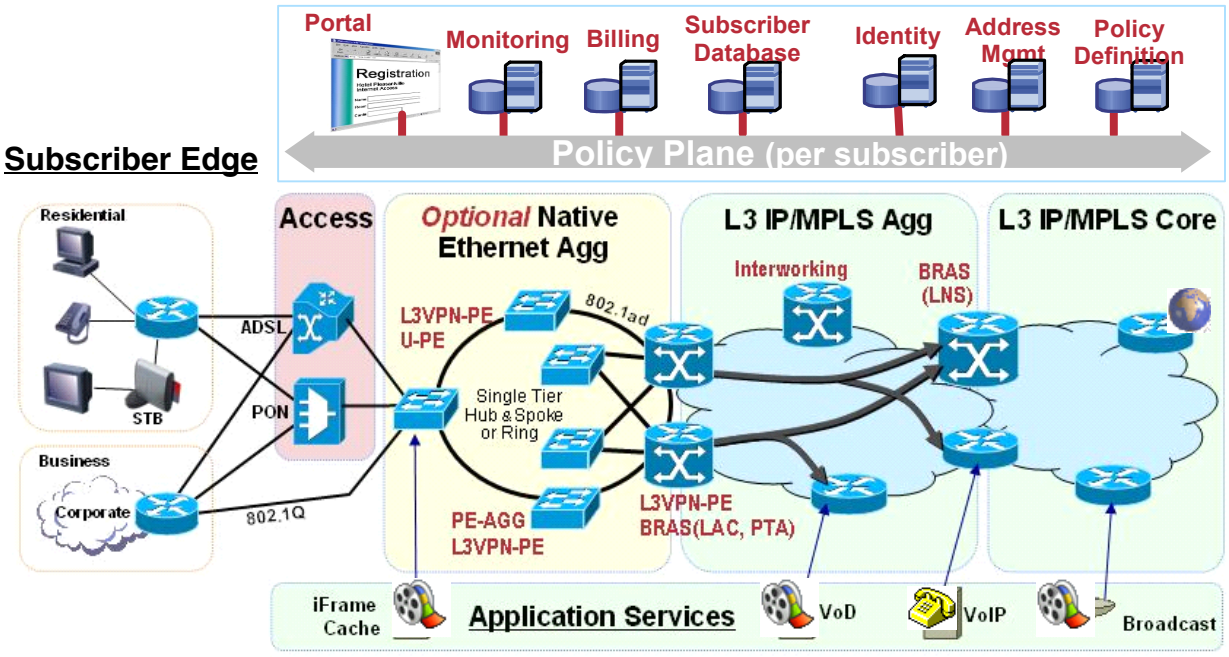
IP Subscriber Awareness over Ethernet is designed for use in an architecture in which the Cisco 7600 router is used as a DSLAM Gigabit Ethernet (GE) aggregator. In this scenario, the DSLAM is connected to the router through a physical port that can carry data for multiple VLANs.

The IP Subscriber Awareness over Ethernet feature supports two models of carrying services between the subscriber and the DSLAM:

- Per-service VLAN model—One or more ATM VCs is used to carry each type of service (video, voice, and data) between the subscriber and the VLAN.
- Per-subscriber VLAN model—A single ATM VC is used to carry all traffic (video, voice, and data) between the subscriber and the DSLAM.

Figure 24-1 shows an example of a wireline Ethernet architecture where IP Subscriber Awareness over Ethernet might be used.

Figure 24-1 Wireline Ethernet Architecture



The following sections provide more details about the IP Subscriber Awareness over Ethernet feature:

Benefits

The IP Subscriber Awareness over Ethernet feature provides the following benefits:

- IP session termination and IP session aggregation on the Cisco 7600 router.
- Support for up to 32000 IP subscribers on a router (with a maximum of 8000 subscribers on a single Cisco 7600 SIP-400).
- Interface scalability to support up to 32000 interfaces on the router.
  - Support for up to 1000 subinterfaces on each physical port.
  - Support for up to 8000 subinterfaces on each Cisco 7600 SIP-400.
- DHCP and Radius accounting for IP subscribers. Support for 256 DHCP pools, and DHCP can handle up to 150 calls per second for IP subscriber sessions.
- QoS support for individual IP subscribers (up to 32000 subscribers), including: classification (IP prec and DSCP), policing, shaping, marking, priority queues, and weighted random early detection (WRED).
- Per-subscriber statistics and accounting information.

- Support for up to 96000 ARP entries.
- RPR, RPR+, stateful switchover (SSO), and non-stop forwarding (NSF) are provided for the IP subscribers.
- Control plane protection (CoPP) protects against denial of service (DOS) and other attacks.

IP Subscriber Interfaces

Cisco IOS Release 12.2SRB introduces a new type of interface to represent IP subscribers:

- Access—A subinterface that represents an individual IP subscriber. The access subinterface can be configured for .1Q or Q-in-Q encapsulation.

  You apply traffic shaping and policing policies (including HQoS) to the access interface to define the amount of bandwidth to allocate for different types of subscriber traffic (for example, voice and data).

Note You configure the access interface as a subinterface of the physical interface that the IP subscriber is connected to.

Example

The following example shows an access subinterface on the interface :

```
interface GigabitEthernet 1/0/0.100 access
    ip vrf forwarding vrf0
    encapsulation dot1q 100
```

- On a ES+ line card, this feature is supported on the access interfaces and non-access interfaces (limited to 500 subinterfaces).

IP Subscriber Session

An IP subscriber session exists while an IP subscriber is using its shared VLAN to access the network. To begin an IP subscriber session, the router must assign an IP address to the subscriber's access subinterface. You can either assign a static IP address to the subinterface, or you can allow DHCP to assign an address. Following are some notes about both methods of assigning an IP address:

- Static IP address—If you assign a static IP address to the access subinterface, the IP subscriber session is considered to always be Up. We recommend that you do not configure many IP subscribers with static IP addresses.
- DHCP-assigned IP address—You can allow DHCP to assign an IP address for the subscriber session. An IP subscriber session begins when the router receives a DHCP discover packet for the subscriber and an IP address is assigned for the subscriber. The session is terminated when the subscriber receives a DHCP release message and its IP address is released. If the subscriber session is VRF aware (that is, if the subscriber belongs to a VRF), the VRF-aware DHCP pool must be used.

Note

- The router can be operating as a DHCP server or DHCP relay device.
- To configure an IP subscriber as part of a VRF (that is, to make the subscriber session VRF aware), configure the VRF under the access subinterface.

This feature supports the following sessions in a ES+ line card:

- IP sessions (routed and L2-connected)
- DHCP integration with IP sessions
- Static IP subnet sessions
- Source IP address and MAC address sessions (IP sessions)
- PPPoE supported in the PPP Termination and Aggregation (PTA) mode
- PPPoEoVLAN supported in the PTA mode
- PPPoEoQinQ supported in the PTA mode
- PPPoEoDot1Q supported in the PTA mode

IP Subscriber Session Features

The following features are provided for IP subscriber sessions:

- Per-subscriber control plane policing and protection (CoPP)—Provides protection against denial of service (DOS) and other attacks for individual subscribers. When an attack occurs, the router notifies the network administrator and begins policing the malicious traffic. This feature allows policing of ARP, DHCP, and ICMP traffic. For information about how CoPP operates on the Cisco 7600 SIP-400, see:

  http://www.cisco.com/en/US/products/hw/routers/ps368/module_installation_and_configuration_guides_chapter09186a0080440138.html#wp1351662

- Per-subscriber security ACL—Allows you to apply security access control lists (ACLs) to individual subscribers. For information about how this feature works on the Cisco 7600 SIP-400, see:

  http://www.cisco.com/en/US/products/hw/routers/ps368/module_installation_and_configuration_guides_chapter09186a0080440138.html#wp1351562

- Per-subscriber Radius accounting—Enables system administrators to track IP session activity for individual subscribers, and to extract subscriber accounting records periodically. Per-subscriber Radius accounting works with DHCP IP address assignment, and improves the authentication, authorization, and accounting (AAA) of broadband service delivery. For information about this feature, see its feature description at:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/ipradacc.htm

- Lawful intercept—Enables a Law Enforcement Agency (LEA) to perform electronic surveillance on a subscriber as authorized by a court order. To assist in the surveillance, the service provider intercepts the subscriber's traffic as it passes through one of their routers, and sends a copy of the intercepted traffic to the LEA without the subscriber's knowledge. For information about this feature, see the documents at the following URLs:

  http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/76licfg/index.htm

  http://www.cisco.com/en/US/products/hw/routers/ps368/module_installation_and_configuration_guides_chapter09186a0080440138.html#wp1351508

- Quality of Service—Standard QoS features are supported for individual subscribers (access subinterfaces), including classification, marking, policing, shaping, priority queuing, and weighted random early detection (WRED). For information about recommended QoS settings for IP Subscriber Awareness over Ethernet, see the following section ("QoS Recommendations"). For information about QoS features on the Cisco 7600 SIP-400, see the information about QoS features in the "Cisco 7600 SIP-400 Features" section of the document at this URL:

http://www.cisco.com/en/US/products/hw/routers/ps368/module_installation_and_configuration_guides_chapter09186a008044013b.html#wp1094663

In addition to standard QoS features, the following new Cisco 7600 SIP-400 QoS features are being introduced to support the deployment of broadband services:

- Dual-priority queues—Provide two priority queues for voice and video traffic for 4000 to 8000 subscribers. You can assign a different priority level to each traffic class to configure the router to treat both types of traffic as priority traffic but to handle them differently (for example, by giving voice traffic precedence over video traffic).
- Bandwidth-remaining ratio (BRR)—Allows service providers to prioritize subscriber traffic during periods of congestion. You can use the Distribution of Remaining Bandwidth Using Ratio feature to specify the relative weight of a subinterface or class queue with respect to other subinterfaces or queues. For information about this feature, see the "Bandwidth-Remaining Ratio Recommendations" section on page 24-21.
- Priority-rate propagation—Takes the priority level and traffic rate assigned to priority traffic in a low-level queue and applies that level and rate to priority traffic at all higher-level queues in the queue hierarchy, even if those queues are not specifically configured for minimum rates or priority. For more information, see the "Priority-Rate Propagation Recommendations" section on page 24-25.

IP Address Assignment

- DHCP Based IP address assignment: 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.
- Static IP address assignment: If a subscriber's static IP address is configured correctly for the service domain, ISG is not involved in the assignment of an IP address for the subscriber.
- IP subnet: For IP subnet sessions, the IP subnet is specified in the user profile.

IP interface: ISG is not involved in the assignment of subscriber IP addresses.

IP Subnet (IP Range) Sessions

A client subnet identifies a IP Subnet session and applies uniform edge processing to packets associated with a particular IP subnet. IP Subnet sessions are hosted for clients directly connected or over multiple hops. The following functionalities are not supported on IP Subnet Sessions, but are supported on IP Sessions:

- DHCP session initiation not supported
- No Source MAC address session support
- No Dynamic VPN selection support

IP Interface Sessions

In an IP Interface session, all the traffic received on a particular physical or logical interface is collated. However, dynamic VRF transfer is not supported in an IP interface session and, VRF transfer can only be used with static VRF configuration. Irrespective of the subsriber logged in, a session is created by default.

PPPoE and IPoE Session Support on Port Channel (1:1 Redundancy)

The 1:1 redundancy on a port channel coupled with Link Aggregation Control Protocol (LACP) dynamically handles the member links in a port channel bundle. A port channel has two members, of which one member is active and the other is in standby or redundant mode. The member ports can be across line cards, but must originate from Ethernet Services Plus (ES+) line card. At any given point of time, one link is on the physical mode.

The following sessions support 1:1 redundancy in a ES+ line card:

- IP Subnet sessions
- IP Interface sessions
- PPPoEoX sessions.

PPPoE and IPoE Session Support on QinQ Subinterfaces with IEEE 802.1AH Customer Ethertype

This feature enables you to implement PPPoE and IPoE session (ISG functions) on QinQ subinterfaces that are configured with custom ethertype. The custom ethertype implemented on the main interface is inherited by all the subinterfaces. To implement this feature, use **dot1q tunnel ethertype** command on main interface for the respective QinQ subinterfaces.

If the outer VLAN tag on a PPPoE or IPoE session packet matches the custom ethertype VLAN settings on the QinQ subinterface, the packets are accepted otherwise the packets are dropped. You can set the outer VLAN tag to the following values:

- 0x9100
- 0x9200
- ox8100
- 0x88a8

The PPPoE or IPoE session will not come up if tthere is mismatch i the ether type between ISG and the client. For example, if the outer VLAN tag on a packet is set to 0x9100 and the interface is configured using custom ethertype to accept only packets with 0x88a8 VLAN tag, the packet will be dropped in the QinQ subinterface. Figure x-x shows an ethernet frame format for QinQ (need the figure)

You can create a QinQ subinterface using the access keyword while defining an interface. The following code shows how to define an interface with access keyword, create a VLAN QinQ subinterface, and enable PPPoE session:

```
Router> enable
Router# configure terminal
Router(config)# interface gigabitethernet 1/0/0
Router(config-if)# dot1q tunneling ethertype 0x9100
Router(config-if)# interface gigabitethernet 1/0/0.100 access
Router(config-subif)# encapsulation dot1q 100 second-dot1q 200
```

```
Router(config-subif)# ip subscriber interface
```

Restictions and Usage Guidelines

Follow these restrictions and usage guidelines when you configure an IP or a PPPoE sessions on an ES+ linecard:

- IP Sessions are not supported on ambiguous VLANs.
- Radius proxy is not supported for the IP Sessions.
- IP and MAC address spoof Prevention is not supported on subinterfaces on a ES+ linecard unlike on a SIP400 line card.
- IP sessions are supported on Link Aggregation (Ether-Channel) interfaces. LAG etherchannel interfaces are supported for links on the same and across line cards.
- PPPoE sessions are supported on ambiguous VLAN interfaces and VLAN ranges.
- There are no drop counters to identify the number of packets dropped due to custom ethertype mismatch.
- VLANs, Source MAC Address, and Ports are matched against session ids to extend security for PPPoE sessions.

Follow these restrictions and usage guidelines when you configure 1:1 redundancy on a ES+ linecard:

- Subscriber redundancy is available only on a 1:1 access standby model.
- Supports access interfaces in port channels to scale the number of port channel subinterfaces to greater than 4k.
- Link Aggregation Control Protocol (LACP) allows dynamic handling of member links in a GEC bundle.
- Supports a maximum of 64 GEC bundles with 8 links.
- Member links in a single GEC bundle reside across NPs or the linecard.
- LAG is supported with members across linecards.
- Supports LAG across linecards and membership of the LAG does not change after new sessions are initiated.
- Feature supports 32000 access subinterfaces and 8K access interfaces.
- Supports per session load balancing across member links where all the traffic for a session is relayed over a single port.
- To reduce the downtime during member link addition or deletion, QOS queues are allocated for all member links belonging to the port channel. Though the ingress and egress traffic could be on different member links, the peer relays all the traffic for a session through a single member link.
- LAG supports sessions on non access subinterfaces to support coexistence of multicast streams.

Verification

This section lists the commands to display configuration information.

- Use the following commands to configure the PPPoE:

```
Router-DJ4-dfc9#sh debug
```

```
CWAN iEdge LC:
  CWAN iEdge LC session event debug debugging is on
X40G XLIF Client:
  XLIF NP events debugging is on

Router-DJ4-dfc9# sh log
Syslog logging: enabled (0 messages dropped, 4 messages rate-limited, 0 flushes, 0
overruns, xml disabled, filtering disabled)

No Active Message Discriminator.
No Inactive Message Discriminator.

    Console logging: disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging:  level debugging, 308 messages logged, xml disabled,
                    filtering disabled
    Exception Logging: size (4096 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled

Log Buffer (1000000 bytes):

Nov 19 16:08:48.247 IST: DFC9: provision_pppoe_routed_ac: switch_info 2CDEC4A4
seghandle 2CD93474 uid 40 if_number 80
Nov 19 16:08:48.247 IST: DFC9:  type 1 2 0opaque handle = 0x186DAB48
Nov 19 16:08:48.247 IST: DFC9: inserting 186DAB48 105 40
Nov 19 16:08:48.247 IST: DFC9: cwan_iedge_session_pending_timer started
Nov 19 16:08:48.247 IST: DFC9: no dbus vlan session pending on int 105
Nov 19 16:08:48.251 IST: DFC9:  cwan_iedge_update_dbus_vlan: Session 40 gets hidden
vlan 1020 through update for Virtual-Access2.1
Nov 19 16:08:50.247 IST: DFC9: cwan_iedge_common_session_notify: cfg_type 2 va_if_num
105 phy_if_num 80 uid 0action 0
Nov 19 16:08:50.247 IST: DFC9: cwan_iedge_get_session_config: sess_type 2 if_num 105
pid 0
Nov 19 16:08:50.247 IST: DFC9: cwan_iedge_get_pppoe_config: if_num 80 va_if_num 105
vlan 1020 sess-id 40 cond_debug off
Nov 19 16:08:50.247 IST: DFC9: x40g_npc_xlif_create Cfn[965F2BC] Creating Xlif:
GigabitEthernet9/5 Xid[0] Typ[4] Ch[0] Ifn[105] Xreg[0] Xidx[205352] efp[0]
Nov 19 16:08:50.247 IST: DFC9: x40g_npc_xlif_create_internal successfully created
xlif: GigabitEthernet9/5 Xid[205352] Typ[4] Ch[0] Ifn[105] Xreg[0] Xidx[205352] efp[0]
Nov 19 16:08:50.247 IST: DFC9: x40g_npc_eg_xlif_update_port Cfn[92D1658] Xlif Update
Port 4 : GigabitEthernet9/5 Xid[205352] Typ[4] Ch[0] Ifn[105] Xreg[0] Xidx[205352]
efp[0]
Nov 19 16:08:50.247 IST: DFC9: x40g_npc_xlif_update_tag_rewrite Cfn[965F334] Tag(i-0,
o-2) Dir[2]: GigabitEthernet9/5 Xid[205352] Typ[4] Ch[0] Ifn[105] Xreg[0] Xidx[205352]
efp[0]
Nov 19 16:08:50.247 IST: DFC9: x40g_npc_xlif_update_dbus_vlan Cfn[965F36C] Updatng
Dbus Vlan 1020: GigabitEthernet9/5 Xid[205352] Typ[4] Ch[0] Ifn[105] Xreg[0]
Xidx[205352] efp[0]
Nov 19 16:08:50.247 IST: DFC9: x40g_npc_xlif_update_stats_id Cfn[965D780] Updatng
StatId 599056 Dir[0]: GigabitEthernet9/5 Xid[205352] Typ[4] Ch[0] Ifn[105] Xreg[0]
Xidx[205352] efp[0]
Nov 19 16:08:50.247 IST: DFC9: x40g_npc_xlif_update_stats_id Cfn[965D8A8] Updatng
StatId 599064 Dir[1]: GigabitEthernet9/5 Xid[205352] Typ[4] Ch[0] Ifn[105] Xreg[0]
Xidx[205352] efp[0]
Nov 19 16:08:50.247 IST: DFC9: x40g_npc_xlif_fwd_feat_enable Cfn[965F3BC] Xlif Fwd
Feat 0x1 Enable 1 : GigabitEthernet9/5 Xid[205352] Typ[4] Ch[0] Ifn[105] Xreg[0]
Xidx[205352] efp[0]
Nov 19 16:08:50.247 IST: DFC9: x40g_npc_xlif_enable Cfn[965F3F0] Xlif Enable 1:
GigabitEthernet9/5 Xid[205352] Typ[4] Ch[0] Ifn[105] Xreg[0] Xidx[205352] efp[0]
Nov 19 16:08:50.247 IST: DFC9: x40g_npc_xlif_update_feat_info Cfn[965F604] Xlif update
feature Dir[0]: GigabitEthernet9/5 Xid[205352] Typ[4] Ch[0] Ifn[105] Xreg[0]
Xidx[205352] efp[0]
```

```
Nov 19 16:08:50.247 IST: DFC9: x40g_npc_xlif_update_feat_info Cfn[965F700] Xlif update
feature Dir[1]: GigabitEthernet9/5 Xid[205352] Typ[4] Ch[0] Ifn[105] Xreg[0]
Xidx[205352] efp[0]

Router-DJ4#sh debug
PPP:
  PPP protocol negotiation debugging is on
PPPoE:
  PPPoE protocol events debugging is on
  PPPoE control packets debugging is on

Router-DJ4#sh log
Syslog logging: enabled (3340 messages dropped, 2 messages rate-limited, 0 flushes, 0
overruns, xml disabled, filtering disabled)

No Active Message Discriminator.

No Inactive Message Discriminator.

    Console logging: disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging:  level debugging, 5280 messages logged, xml disabled,
                    filtering disabled
    Exception Logging: size (4096 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled

No active filter modules.

    Trap logging: level informational, 203 message lines logged

Log Buffer (1000000 bytes):

Nov 19 16:08:48.231 IST: PPPoE 0: I PADI  R:bb00.1912.0001 L:ffff.ffff.ffff 2 Gi9/5.1
contiguous pak, size 60
 FF FF FF FF FF FF BB 00 19 12 00 01 81 00 00 02
 88 63 11 09 00 00 00 04 01 01 00 00 00 0A 03 06
 B6 00 00 01 00 00 00 01 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 06 F8 00 00 9C 88
Nov 19 16:08:48.231 IST:  Service tag: NULL Tag
Nov 19 16:08:48.231 IST: PPPoE 0: O PADO, R:a110.0050.0006 L:bb00.1912.0001 1019
Gi9/5.1
Nov 19 16:08:48.231 IST:  Service tag: NULL Tag
contiguous pak, size 100
 06 02 00 10 03 FB 28 00 03 80 00 00 44 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 02 04 00 00
 BB 00 19 12 00 01 A1 10 00 50 00 06 81 00 00 02
 88 63 11 07 00 00 00 24 01 01 00 00 01 02 00 08
 52 69 61 7A 2D 44 4A 34 ...
Nov 19 16:08:48.231 IST: PPPoE 0: I PADR  R:bb00.1912.0001 L:000c.31c9.7000 2 Gi9/5.1
contiguous pak, size 60
 00 0C 31 C9 70 00 BB 00 19 12 00 01 81 00 00 02
 88 63 11 19 00 00 00 18 01 01 00 00 01 04 00 10
 E2 DB 75 8D E5 9C 95 C1 83 35 DC 91 B2 14 32 89
 63 63 65 73 73 2D 70 70 6C 63 70 30
Nov 19 16:08:48.231 IST:  Service tag: NULL Tag
Nov 19 16:08:48.231 IST: PPPoE : encap string prepared
Nov 19 16:08:48.231 IST: [40]PPPoE 40: Access IE handle allocated
Nov 19 16:08:48.231 IST: [40]PPPoE 40: AAA get retrieved attrs
Nov 19 16:08:48.231 IST: [40]PPPoE 40: AAA get nas port details
Nov 19 16:08:48.231 IST: [40]PPPoE 40: AAA get dynamic attrs
Nov 19 16:08:48.231 IST: [40]PPPoE 40: AAA unique ID allocated
Nov 19 16:08:48.231 IST: [40]PPPoE 40: No AAA accounting method list
```

```
Nov 19 16:08:48.231 IST: [40]PPPoE 40: Service request sent to SSS
Nov 19 16:08:48.231 IST: [40]PPPoE 40: Created, Service: None R:000c.31c9.7000
L:bb00.1912.0001 2 Gi9/5.1
Nov 19 16:08:48.231 IST: [40]PPPoE 40: State NAS_PORT_POLICY_INQUIRY    Event SSS MORE
KEYS
Nov 19 16:08:48.231 IST: PPP: Alloc Context [19C03860]
Nov 19 16:08:48.231 IST: ppp40 PPP: Phase is ESTABLISHING
Nov 19 16:08:48.231 IST: [40]PPPoE 40: data path set to PPP
Nov 19 16:08:48.231 IST: [40]PPPoE 40: Segment (SSS class): PROVISION
Nov 19 16:08:48.231 IST: [40]PPPoE 40: State PROVISION_PPP    Event SSM PROVISIONED
Nov 19 16:08:48.231 IST: [40]PPPoE 40: O PADS  R:bb00.1912.0001 L:000c.31c9.7000 1019
Gi9/5.1
contiguous pak, size 100
 00 02 00 10 03 FB 28 00 03 80 00 00 44 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 02 04 00 00
 BB 00 19 12 00 01 A1 10 00 50 00 06 81 00 00 02
 88 63 11 65 00 28 00 18 01 01 00 00 01 04 00 10
 E2 DB 75 8D E5 9C 95 C1 ...
Nov 19 16:08:48.231 IST: ppp40 PPP: Using vpn set call direction
Nov 19 16:08:48.231 IST: ppp40 PPP: Treating connection as a callin
Nov 19 16:08:48.231 IST: ppp40 PPP: Session handle[28] Session id[40]
Nov 19 16:08:48.231 IST: ppp40 LCP: Event[OPEN] State[Initial to Starting]
Nov 19 16:08:48.231 IST: ppp40 PPP LCP: Enter passive mode, state[Stopped]
Nov 19 16:08:48.231 IST: ppp40 LCP: I CONFREQ [Stopped] id 0 len 14
Nov 19 16:08:48.231 IST: ppp40 LCP:    MagicNumber 0xA4E30BAF (0x0506A4E30BAF)
Nov 19 16:08:48.231 IST: ppp40 LCP:    MRU 1492 (0x010405D4)
Nov 19 16:08:48.231 IST: ppp40 LCP: O CONFREQ [Stopped] id 1 len 19
Nov 19 16:08:48.231 IST: ppp40 LCP:    MRU 1492 (0x010405D4)
Nov 19 16:08:48.231 IST: ppp40 LCP:    AuthProto CHAP (0x0305C22305)
Nov 19 16:08:48.235 IST: ppp40 LCP:    MagicNumber 0x0F501712 (0x05060F501712)
Nov 19 16:08:48.235 IST: ppp40 LCP: O CONFACK [Stopped] id 0 len 14
Nov 19 16:08:48.235 IST: ppp40 LCP:    MagicNumber 0xA4E30BAF (0x0506A4E30BAF)
Nov 19 16:08:48.235 IST: ppp40 LCP:    MRU 1492 (0x010405D4)
Nov 19 16:08:48.235 IST: ppp40 LCP: Event[Receive ConfReq+] State[Stopped to ACKsent]
Nov 19 16:08:48.235 IST: ppp40 LCP: I CONFACK [ACKsent] id 1 len 19
Nov 19 16:08:48.235 IST: ppp40 LCP:    MRU 1492 (0x010405D4)
Nov 19 16:08:48.235 IST: ppp40 LCP:    AuthProto CHAP (0x0305C22305)
Nov 19 16:08:48.235 IST: ppp40 LCP:    MagicNumber 0x0F501712 (0x05060F501712)
Nov 19 16:08:48.235 IST: ppp40 LCP: Event[Receive ConfAck] State[ACKsent to Open]
Nov 19 16:08:48.243 IST: ppp40 PPP: Phase is AUTHENTICATING, by this end
Nov 19 16:08:48.243 IST: ppp40 CHAP: O CHALLENGE id 1 len 29 from "Router-DJ4"
Nov 19 16:08:48.243 IST: ppp40 LCP: State is Open
Nov 19 16:08:48.243 IST: ppp40 CHAP: I RESPONSE id 1 len 29 from "PPP_USER"
Nov 19 16:08:48.243 IST: ppp40 PPP: Phase is FORWARDING, Attempting Forward
Nov 19 16:08:48.243 IST: ppp40 PPP: Phase is AUTHENTICATING, Unauthenticated User
Nov 19 16:08:48.243 IST: ppp40 IPCP: Authorizing CP
Nov 19 16:08:48.243 IST: ppp40 IPCP: CP stalled on event[Authorize CP]
Nov 19 16:08:48.243 IST: ppp40 IPCP: CP unstall
Nov 19 16:08:48.243 IST: ppp40 PPP: Phase is FORWARDING, Attempting Forward
Nov 19 16:08:48.243 IST: [40]PPPoE 40: State LCP_NEGOTIATION    Event SSS CONNECT
LOCAL
Nov 19 16:08:48.247 IST: [40]PPPoE 40: Segment (SSS class): UPDATED
Nov 19 16:08:48.247 IST: [40]PPPoE 40: Segment (SSS class): BOUND
Nov 19 16:08:48.247 IST: [40]PPPoE 40: data path set to Virtual Acess
Nov 19 16:08:48.247 IST: [40]PPPoE 40: State LCP_NEGOTIATION    Event SSM UPDATED
Nov 19 16:08:48.247 IST: Vi2.1 PPP: Phase is AUTHENTICATING, Authenticated User
Nov 19 16:08:48.247 IST: Vi2.1 CHAP: O SUCCESS id 1 len 4
Nov 19 16:08:48.247 IST: [40]PPPoE 40: AAA get dynamic attrs
Nov 19 16:08:48.247 IST: Vi2.1 PPP: Phase is UP
Nov 19 16:08:48.247 IST: Vi2.1 IPCP: Protocol configured, start CP. state[Initial]
Nov 19 16:08:48.247 IST: Vi2.1 IPCP: Event[OPEN] State[Initial to Starting]
Nov 19 16:08:48.247 IST: Vi2.1 IPCP: O CONFREQ [Starting] id 1 len 10
Nov 19 16:08:48.247 IST: Vi2.1 IPCP:    Address 100.0.0.1 (0x030664000001)
Nov 19 16:08:48.247 IST: Vi2.1 IPCP: Event[UP] State[Starting to REQsent]
```

```
Nov 19 16:08:48.247 IST: Vi2.1 IPCP: I CONFREQ [REQsent] id 0 len 10
Nov 19 16:08:48.247 IST: Vi2.1 IPCP:    Address 0.0.0.0 (0x030600000000)
Nov 19 16:08:48.247 IST: Vi2.1 IPCP AUTHOR: Start.  Her address 0.0.0.0, we want
0.0.0.0
Nov 19 16:08:48.247 IST: Vi2.1 IPCP AUTHOR: Done.  Her address 0.0.0.0, we want
0.0.0.0
Nov 19 16:08:48.247 IST: Vi2.1 IPCP: Pool returned 182.0.0.1
Nov 19 16:08:48.247 IST: Vi2.1 IPCP: O CONFNAK [REQsent] id 0 len 10
Nov 19 16:08:48.247 IST: Vi2.1 IPCP:    Address 182.0.0.1 (0x0306B6000001)
Nov 19 16:08:48.247 IST: Vi2.1 IPCP: Event[Receive ConfReq-] State[REQsent to REQsent]
Nov 19 16:08:48.247 IST: Vi2.1 IPCP: I CONFACK [REQsent] id 1 len 10
Nov 19 16:08:48.247 IST: Vi2.1 IPCP:    Address 100.0.0.1 (0x030664000001)
Nov 19 16:08:48.247 IST: Vi2.1 IPCP: Event[Receive ConfAck] State[REQsent to ACKrcvd]
Nov 19 16:08:48.251 IST: [40]PPPoE 40: State PTA_BINDING    Event STATIC BIND RESPONSE
Nov 19 16:08:48.251 IST: [40]PPPoE 40: Connected PTA
Nov 19 16:08:48.251 IST: Vi2.1 IPCP: I CONFREQ [ACKrcvd] id 1 len 10
Nov 19 16:08:48.251 IST: Vi2.1 IPCP:    Address 182.0.0.1 (0x0306B6000001)
Nov 19 16:08:48.251 IST: Vi2.1 IPCP: O CONFACK [ACKrcvd] id 1 len 10
Nov 19 16:08:48.251 IST: Vi2.1 IPCP:    Address 182.0.0.1 (0x0306B6000001)
Nov 19 16:08:48.251 IST: Vi2.1 IPCP: Event[Receive ConfReq+] State[ACKrcvd to Open]
Nov 19 16:08:48.255 IST: Vi2.1 IPCP: Event[DOWN] State[Open to Starting]
Nov 19 16:08:48.255 IST: Vi2.1 IPCP: Event[CLOSE] State[Starting to Initial]
Nov 19 16:08:48.255 IST: Vi2.1 IPCP: Event[OPEN] State[Initial to Starting]
Nov 19 16:08:48.255 IST: Vi2.1 IPCP: O CONFREQ [Starting] id 2 len 10
Nov 19 16:08:48.255 IST: Vi2.1 IPCP:    Address 100.0.0.1 (0x030664000001)
Nov 19 16:08:48.255 IST: Vi2.1 IPCP: Event[UP] State[Starting to REQsent]
Nov 19 16:08:48.255 IST: Vi2.1 IPCP: I CONFREQ [REQsent] id 2 len 10
Nov 19 16:08:48.255 IST: Vi2.1 IPCP:    Address 182.0.0.1 (0x0306B6000001)
Nov 19 16:08:48.255 IST: Vi2.1 IPCP AUTHOR: Start.  Her address 182.0.0.1, we want
182.0.0.1
Nov 19 16:08:48.255 IST: Vi2.1 IPCP AUTHOR: Reject 182.0.0.1, using 182.0.0.1
Nov 19 16:08:48.255 IST: Vi2.1 IPCP AUTHOR: Done.  Her address 182.0.0.1, we want
182.0.0.1
Nov 19 16:08:48.255 IST: Vi2.1 IPCP: O CONFACK [REQsent] id 2 len 10
Nov 19 16:08:48.255 IST: Vi2.1 IPCP:    Address 182.0.0.1 (0x0306B6000001)
Nov 19 16:08:48.255 IST: Vi2.1 IPCP: Event[Receive ConfReq+] State[REQsent to ACKsent]
Nov 19 16:08:48.255 IST: Vi2.1 IPCP: I CONFACK [ACKsent] id 2 len 10
Nov 19 16:08:48.255 IST: Vi2.1 IPCP:    Address 100.0.0.1 (0x030664000001)
Nov 19 16:08:48.255 IST: Vi2.1 IPCP: Event[Receive ConfAck] State[ACKsent to Open]
Nov 19 16:08:48.275 IST: Vi2.1 IPCP: State is Open (Indicates that the PPPoE session
is up)
Nov 19 16:08:48.275 IST: Vi2.1 Added to neighbor route AVL tree: topoid 0, address
182.0.0.1
Nov 19 16:08:48.275 IST: Vi2.1 IPCP: Install route to 182.0.0.1
Router-DJ4#

interface GigabitEthernet9/17.1
 encapsulation dot1Q 2000
 ip address 180.0.0.1 255.255.255.0

interface GigabitEthernet9/5.1
 encapsulation dot1Q 2
 ip address 192.0.0.1 255.255.255.0
 pppoe enable group dj4_bba_group1

aaa new-model
aaa authentication login default group radius local
aaa authentication ppp default local
aaa authorization network default local
aaa authorization subscriber-service default group radius
aaa session-id common

bba-group pppoe dj4_bba_group1
 virtual-template 1
```

```
 sessions per-vc limit 16000
 sessions per-mac limit 16000
 sessions per-vlan limit 8000

interface Loopback1
 ip address 100.0.0.1 255.255.255.255

interface Virtual-Template1
 ip unnumbered Loopback1
 no logging event link-status
 peer default ip address pool PPPPool_1
 no snmp trap link-status
 keepalive 300
 ppp authentication chap
```

Use the following commands to verify the PPPoE session:

```
Router-DJ4#sh pppoe summary
    PTA  : Locally terminated sessions
    FWDED: Forwarded sessions
    TRANS: All other sessions (in transient state)

                                  TOTAL     PTA   FWDED   TRANS
TOTAL                                 1       1       0       0
GigabitEthernet9/5                    1       1       0       0
Router-DJ4#sh pppoe ses
Router-DJ4#sh pppoe session
     1 session  in LOCALLY_TERMINATED (PTA) State
     1 session  total

Uniq ID  PPPoE  RemMAC          Port                    VT  VA         State
           SID  LocMAC                                      VA-st      Type
     42     42  bb00.1912.0001  Gi9/5.1                  1  Vi2.1      PTA
                000c.31c9.7000  VLAN:   2                   UP
Router-DJ4#sh sss session uid 42 detailed
Unique Session ID: 42
Identifier: PPP_USER
SIP subscriber access type(s): PPPoE/PPP
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 00:19:04, Last Changed: 00:19:04
Interface: Virtual-Access2.1

Policy information:
  Context 137426FC: Handle 2400002A
  AAA_id 00000038: Flow_handle 0
  Authentication status: authen
  Downloaded User profile, excluding services:
    Framed-Protocol      1 [PPP]
    username             "PPP_USER"
  Downloaded User profile, including services:
    Framed-Protocol      1 [PPP]
    username             "PPP_USER"
  Config history for session (recent to oldest):
    Access-type: PPP Client: SM
     Policy event: Process Config Connecting
      Profile name: apply-config-only, 2 references
        Framed-Protocol      1 [PPP]
        username             "PPP_USER"
  Rules, actions and conditions executed:
    subscriber rule-map PPPoE-SUB
      condition always event session-start
        1 service local

Configuration sources associated with this session:
```

```
Interface: Virtual-Template1, Active Time = 00:19:04

Router-DJ4# sh pppoe session packets
Total PPPoE sessions 1


SID     Pkts-In         Pkts-Out        Bytes-In        Bytes-Out
42      12              13              184             190
Router-DJ4#

Router-DJ4#sh cef int gig 9/5.1
GigabitEthernet9/5.1 is up (if_number 80)
  Corresponding hwidb fast_if_number 80
  Corresponding hwidb firstsw->if_number 25
  Internet address is 192.0.0.1/24
  ICMP redirects are always sent
  IP unicast RPF check is disabled
  Output features: MFIB Adjacency, HW Shortcut Installation
  IP policy routing is disabled
  BGP based policy accounting on input is disabled
  BGP based policy accounting on output is disabled
  Hardware idb is GigabitEthernet9/5
  Fast switching type 28, interface type 146
  IP CEF switching enabled
  IP CEF switching turbo vector
  IP Null turbo vector
  IP prefix lookup IPv4 mtrie generic
  Input fast flags 0x40000000, Output fast flags 0x0
  ifindex 24(24)
  Slot 9/0 (9) Slot unit 5 VC -1
  IP MTU 1500
```

- Use the following commands to configure IP session:

```
aaa new-model
!
aaa session-id common
!
interface GigabitEthernet2/9
 no ip address
 load-interval 30
!
interface GigabitEthernet2/9.1 access
 encapsulation dot1Q 2 second-dot1q 2
 ip address 182.0.0.1 255.255.255.0
 ip subscriber routed
  initiator unclassified ip-address
!
interface GigabitEthernet2/10
 no ip address
 load-interval 30
!
interface GigabitEthernet2/10.1
 encapsulation dot1Q 2000 second-dot1q 2001
 ip address 180.0.0.1 255.255.255.0
!
no ip http server
no ip http secure-server
!
arp 182.0.0.2 aa00.0000.0001 ARPA
arp 180.0.0.2 0000.0000.0001 ARPA
!
```

Use the following commands to debug IP session:

```
ISG_NMB#sh deb
CWAN iEdge RP:
  CWAN iEdge RP debug debugging is on

IP Subscriber:
  all IP subscriber debugs debugging is on
ISG_NMB#
Nov 19 16:02:46.087 IST: IPSUB_DP: [Gi2/9.1:I:CEF:DFL:21.0.0.1] Packet triggers
session initiation
Nov 19 16:02:46.087 IST: IPSUB_DP: [Gi2/9.1:I:CEF:DFL:21.0.0.1] Packet classified,
results = 0x1
Nov 19 16:02:46.087 IST: IPSUB_DP: [uid:0] Insert new entry for mac 0000.1500.0001
Nov 19 16:02:46.087 IST: IPSUB_DP: [uid:0] Processing new in-band session request
Nov 19 16:02:46.087 IST: IPSUB_DP: [uid:0] Delete mac entry 0000.1500.0001
Nov 19 16:02:46.087 IST: IPSUB_DP: [uid:0] In-band session request event for session
Nov 19 16:02:46.087 IST: IPSUB_DP: [uid:0] Added upstream entry into the classifier
Nov 19 16:02:46.087 IST: IPSUB_DP: [uid:0] VRF = DFL, IP = 21.0.0.1, MASK =
255.255.255.255
Nov 19 16:02:46.087 IST: IPSUB: Try to create a new session
Nov 19 16:02:46.087 IST: IPSUB: IPSUB: Check IP DHCP session recovery: 21.0.0.1
Gi2/9.1 mac aa00.0000.0001
Nov 19 16:02:46.087 IST: IPSUB: IPSUB: No DHCP binding found
Nov 19 16:02:46.087 IST: IPSUB: [uid:0] IPSUB: Proceed to create the IP inband session
Nov 19 16:02:46.087 IST: IPSUB: [uid:0] Request to create a new session
Nov 19 16:02:46.087 IST: IPSUB: [uid:0] Session start event for session
Nov 19 16:02:46.087 IST: IPSUB: [uid:0] Event session start, state changed from idle
to requesting
Nov 19 16:02:46.087 IST: IPSUB: HA[uid:32]: Session init-notification on Active
Nov 19 16:02:46.087 IST: IPSUB: HA[uid:32]: Allocated SHDB handle (0xF1000020)
Nov 19 16:02:46.087 IST: IPSUB: HA[uid:32]: Successfully initialized for HA
Nov 19 16:02:46.087 IST: IPSUB: [uid:32] AAA unique ID allocated
Nov 19 16:02:46.087 IST: IPSUB: [uid:32] Added session 21.0.0.1 to L3 session table
Nov 19 16:02:46.087 IST: IPSUB: [uid:32] Added session to session table with access
session keys
Nov 19 16:02:46.087 IST: IPSUB: [uid:32] IP session(0x63000020) to be associated to
Gi2/9.1
Nov 19 16:02:46.087 IST: IPSUB: [uid:32] Inserted IP session(0x63000020) to
sessions-per-interface db with interface Gi2/9.1
Nov 19 16:02:46.087 IST: IPSUB_DP: [uid:0] Sent message to control plane for in-band
session creation
Nov 19 16:02:46.087 IST: IPSUB_DP: [uid:0] Event inband-session, state changed from
idle to intiated
Nov 19 16:02:46.091 IST: IPSUB: [uid:32] Recieved Message = connect local
Nov 19 16:02:46.091 IST: IPSUB: [uid:32] Connect Local event for session
Nov 19 16:02:46.091 IST: IPSUB: [uid:32] Event connect local, state changed from
requesting to waiting
Nov 19 16:02:46.091 IST: IPSUB: [uid:32] Inside processing IPSIP info
Nov 19 16:02:46.091 IST: IPSUB-ROUTE: [uid:32] Checking whether routes to be
inserted/removed
Nov 19 16:02:46.091 IST: IPSUB-ROUTE: [uid:32] Context not present, creating context
Nov 19 16:02:46.091 IST: IPSUB-ROUTE: [uid:32] Entered the sg subrte context alloc
Nov 19 16:02:46.091 IST: IPSUB-ROUTE: [uid:32] Returning the sg subrte context
0x1348DD20
Nov 19 16:02:46.091 IST: IPSUB-ROUTE: [uid:32] Added Fib Prefix [DFL]:
21.0.0.1/255.255.255.255
Nov 19 16:02:46.091 IST: IPSUB-ROUTE: [uid:32] Both IP addresses and VRF are same, no
need to add route
Nov 19 16:02:46.091 IST: IPSUB: [uid:32] Keys not changed, seg needn't be updated
Nov 19 16:02:46.091 IST: IPSUB: [uid:32] Key list to be created to update SM
Nov 19 16:02:46.091 IST: IPSUB: [uid:32] Created key list to update SM
Nov 19 16:02:46.091 IST: IPSUB: [uid:32] Session Keys Available event for session
Nov 19 16:02:46.091 IST: IPSUB: [uid:32] Event session keys available, state changed
from waiting to provisioning
```

```
Nov 19 16:02:46.091 IST: IPSUB: [uid:32] Access and service keys same, no need to add
session with service keys
Nov 19 16:02:46.091 IST: IPSUB: [uid:32] Data plane prov successful event for session
Nov 19 16:02:46.091 IST: IPSUB: [uid:32] Event dataplane prov successful, state
changed from provisioning to connected
Nov 19 16:02:46.091 IST: IPSUB: HA[uid:32]: Session up notification
Nov 19 16:02:46.091 IST: IPSUB: HA[uid:32]: Session ready to sync data (0xF1000020)
Nov 19 16:02:46.091 IST: IPSUB_DP: [uid:0] Setup event for session (session hdl
3858759691)
Nov 19 16:02:46.091 IST: IPSUB_DP: [uid:32] Added downstream entry into the classifier
Nov 19 16:02:46.091 IST: IPSUB_DP: [uid:32] VRF = DFL, IP = 21.0.0.1, MASK =
255.255.255.255
Nov 19 16:02:46.091 IST: IPSUB_DP: [uid:32] Session setup successful
Nov 19 16:02:46.091 IST: IPSUB_DP: [uid:32] Event setup-session, state changed from
intiated to established
Nov 19 16:02:46.091 IST: IPSUB_DP: [uid:32] Activate event for session
Nov 19 16:02:46.091 IST: IPSUB_DP: [uid:32] Event activate-session, state changed from
established to connected

Use the following commands to verify IP session:

ISG_NMB#sh ip sub
Displaying subscribers in the default service vrf:

Type        Subscriber Identifier    Display UID    Status
---------   ----------------------   ------------   ------
routed      21.0.0.1/32              [32]           up
ISG_NMB#
ISG_NMB#sh sss sess
Current Subscriber Information: Total sessions 1

Uniq ID Interface    State         Service      Identifier           Up-time
32      IP           unauthen      Local Term   21.0.0.1             00:02:40

ISG_NMB#sh sss sess uid 32
Unique Session ID: 32
Identifier: 21.0.0.1
SIP subscriber access type(s): IP
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 00:02:46, Last Changed: 00:02:46

Policy information:
  Authentication status: unauthen

Configuration sources associated with this session:
Interface: GigabitEthernet2/9.1, Active Time = 00:02:46

ISG_NMB#sh sss sess uid 32 de
ISG_NMB#sh sss sess uid 32 detailed
Unique Session ID: 32
Identifier: 21.0.0.1
SIP subscriber access type(s): IP
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 00:02:49, Last Changed: 00:02:49

Policy information:
  Context 133B22FC: Handle DF000020
  AAA_id 00000030: Flow_handle 0
  Authentication status: unauthen

Configuration sources associated with this session:
Interface: GigabitEthernet2/9.1, Active Time = 00:02:49
```

```
Following details is for a L2-connected DHCP session on Dot1Q interface:-
=========================================================================

Use the following commands to configure L2-connected DHCP session:

aaa new-model
!
!
aaa session-id common
!
!
!
clock timezone IST 5
ip source-route
!
!
ip dhcp excluded-address 182.0.0.11 182.0.0.15
no ip dhcp ping packets
!
ip dhcp pool pool_global1
   network 182.0.0.0 255.255.255.240
   lease 0 0 3
   update arp
!
!
!
interface Loopback10
 ip address 182.0.0.11 255.255.255.255
!
!
interface GigabitEthernet2/9
 no ip address
 load-interval 30
!
interface GigabitEthernet2/9.1 access
 encapsulation dot1Q 2
 ip unnumbered Loopback10
 ip subscriber l2-connected
  initiator dhcp class-aware
!
interface GigabitEthernet2/10
 no ip address
 load-interval 30
!
interface GigabitEthernet2/10.1
 encapsulation dot1Q 2000
 ip address 180.0.0.1 255.255.255.0
!
!
no ip http server
no ip http secure-server
ip route 7.0.0.0 255.0.0.0 7.38.0.1
ip route 202.153.0.0 255.255.0.0 7.38.0.1
!
!

Use the following commands to debug L2-connected DHCP session:

ISG_NMB#sh deb
DHCP server packet debugging is on.
DHCP server event debugging is on.

IP Subscriber:
  IP subscriber events debugging is on
```

```
  IP subscriber errors debugging is on
  IP subscriber packets debugging is on


ISG_NMB#
Nov 19 15:40:33.595 IST: IPSUB_DP: [Gi2/9.1:I:PROC:aa00.1314.0001] Packet classified,
results = 0x40
Nov 19 15:40:33.595 IST: IPSUB_DP: [Gi2/9.1:I:PROC:aa00.1314.0001] Rx driver allowing
IP routing
Nov 19 15:40:33.595 IST: DHCPD: Reload workspace interface GigabitEthernet2/9.1
tableid 0.
Nov 19 15:40:33.595 IST: DHCPD: tableid for 182.0.0.11 on GigabitEthernet2/9.1 is 0
Nov 19 15:40:33.595 IST: DHCPD: client's VPN is .
Nov 19 15:40:33.595 IST: DHCPD: Sending notification of DISCOVER:
Nov 19 15:40:33.595 IST:   DHCPD: htype 1 chaddr aa00.1314.0001
Nov 19 15:40:33.595 IST:   DHCPD: remote id 020a0000b600000b21010002
Nov 19 15:40:33.595 IST:   DHCPD: interface = GigabitEthernet2/9.1
Nov 19 15:40:33.595 IST:   DHCPD: class id 49786961
Nov 19 15:40:33.595 IST: IPSUB: Create session keys from SSS key list
Nov 19 15:40:33.595 IST: IPSUB: Mac_addr = aa00.1314.0001, Recvd Macaddr =
aa00.1314.0001
Nov 19 15:40:33.599 IST: IPSUB: Session input interface(0x13348754) =
GigabitEthernet2/9.1
Nov 19 15:40:33.599 IST: IPSUB: SHDB Handle = 5A00000B
Nov 19 15:40:33.599 IST: IPSUB: Remote_id = 020a0000b600000b21010002
Nov 19 15:40:33.599 IST: IPSUB: Vendor_Class_id = Ixia
Nov 19 15:40:33.599 IST: DHCPD: DHCPDISCOVER received from client 01aa.0013.1400.01 on
interface GigabitEthernet2/9.1.
Nov 19 15:40:33.599 IST: DHCPD: Sending notification of DISCOVER:
Nov 19 15:40:33.599 IST:   DHCPD: htype 1 chaddr aa00.1314.0001
Nov 19 15:40:33.599 IST:   DHCPD: remote id 020a0000b600000b21010002
Nov 19 15:40:33.599 IST:   DHCPD: interface = GigabitEthernet2/9.1
Nov 19 15:40:33.599 IST:   DHCPD: class id 49786961
Nov 19 15:40:33.599 IST: DHCPD: Saving workspace (ID=0x8900000B)
Nov 19 15:40:33.599 IST: DHCPD: New packet workspace 0x1333D0D8 (ID=0x2700000C)
Nov 19 15:40:33.599 IST: IPSUB: Try to create a new session
Nov 19 15:40:33.599 IST: IPSUB: [uid:0] Request to create a new session
Nov 19 15:40:33.599 IST: IPSUB: [uid:0] Session start event for session
Nov 19 15:40:33.599 IST: IPSUB: [uid:11] AAA unique ID allocated
Nov 19 15:40:33.599 IST: IPSUB: [uid:11] Added session aa00.1314.0001 to L2 session
table
Nov 19 15:40:33.599 IST: IPSUB: [uid:11] Added session to session table with access
session keys
Nov 19 15:40:33.599 IST: IPSUB: [uid:11] IP session(0xC500000B) to be associated to
Gi2/9.1
Nov 19 15:40:33.599 IST: IPSUB: [uid:11] Inserted IP session(0xC500000B) to
sessions-per-interface db with interface Gi2/9.1
Nov 19 15:40:33.599 IST: DHCPD: Callback for workspace (ID=0x8900000B)
Nov 19 15:40:33.599 IST: DHCPD: No authentication required. Continue
Nov 19 15:40:33.599 IST: DHCPD: Callback: class '' now specified for client
01aa.0013.1400.01
Nov 19 15:40:33.599 IST: DHCPD: Reprocessing saved workspace (ID=0x8900000B)
Nov 19 15:40:33.599 IST: DHCPD: Reload workspace interface GigabitEthernet2/9.1
tableid 0.
Nov 19 15:40:33.599 IST: DHCPD: tableid for 182.0.0.11 on GigabitEthernet2/9.1 is 0
Nov 19 15:40:33.599 IST: DHCPD: client's VPN is .
Nov 19 15:40:33.599 IST: DHCPD: Sending notification of DISCOVER:
Nov 19 15:40:33.599 IST:   DHCPD: htype 1 chaddr aa00.1314.0001
Nov 19 15:40:33.599 IST:   DHCPD: remote id 020a0000b600000b21010002
Nov 19 15:40:33.599 IST:   DHCPD: interface = GigabitEthernet2/9.1
Nov 19 15:40:33.599 IST:   DHCPD: class id 49786961
Nov 19 15:40:33.599 IST: DHCPD: DHCPDISCOVER received from client 01aa.0013.1400.01 on
interface GigabitEthernet2/9.1.
Nov 19 15:40:33.599 IST: DHCPD: Adding binding to radix tree (182.0.0.1)
```

```
Nov 19 15:40:33.599 IST: DHCPD: Adding binding to hash tree
Nov 19 15:40:33.599 IST: DHCPD: assigned IP address 182.0.0.1 to client
01aa.0013.1400.01. (13 1)
Nov 19 15:40:33.599 IST: DHCPD: DHCPOFFER notify setup address 182.0.0.1 mask
255.255.255.240
Nov 19 15:40:33.599 IST: IPSUB: [uid:11] IP session context 0x133D28C8 available to
authorize
Nov 19 15:40:33.599 IST: IPSUB-VRFSET: [uid:11] Entered allocate feature info
Nov 19 15:40:33.599 IST: IPSUB-VRFSET: [uid:11] Allocated sg vrfset info 0x13488EE0
Nov 19 15:40:33.599 IST: IPSUB-VRFSET: [uid:11] Freeing the sg vrfset info 0x13488EE0
Nov 19 15:40:33.599 IST: IPSUB: [uid:11] IPSIP Parsing HostIP: 182.0.0.1 SubnetMask=
255.255.255.255
Nov 19 15:40:33.599 IST: IPSUB: [uid:11] Recieved Message = connect local
Nov 19 15:40:33.599 IST: IPSUB: [uid:11] Connect Local event for session
Nov 19 15:40:33.599 IST: IPSUB: [uid:11] Inside processing IPSIP info
Nov 19 15:40:33.599 IST: IPSUB: [uid:11] Processing IPSIP info: 0x1330208C (APPLY)
Nov 19 15:40:33.599 IST: IPSUB: [uid:11] Got IP address- IP:-182.0.0.1
Nov 19 15:40:33.599 IST: IPSUB: [uid:11] Set IP address- IP:-182.0.0.1
Nov 19 15:40:33.599 IST: IPSUB-VRFSET: [uid:11] Applying SG VRFSET info
Nov 19 15:40:33.599 IST: IPSUB-VRFSET: [uid:11] DHCP Initiated session, no config,
ignore
Nov 19 15:40:33.599 IST: IPSUB-ROUTE: [uid:11] Checking whether routes to be
inserted/removed
Nov 19 15:40:33.599 IST: IPSUB-ROUTE: [uid:11] Context not present, creating context
Nov 19 15:40:33.599 IST: IPSUB-ROUTE: [uid:11] Entered the sg subrte context alloc
Nov 19 15:40:33.599 IST: IPSUB-ROUTE: [uid:11] Returning the sg subrte context
0x1348DD04
Nov 19 15:40:33.599 IST: IPSUB-ROUTE: [uid:11] Installed ARP entry [DFL]: 182.0.0.1
Nov 19 15:40:33.599 IST: IPSUB-ROUTE: [uid:11] Added Fib Prefix [DFL]:
182.0.0.1/255.255.255.255
Nov 19 15:40:33.599 IST: IPSUB-ROUTE: [uid:11] Route insert not required for DHCP
hosts with IP unnumbered config on: GigabitEthernet2/9.1
Nov 19 15:40:33.599 IST: IPSUB-ROUTE: [uid:11] Both IP addresses and VRF are same, no
need to add route
Nov 19 15:40:33.599 IST: IPSUB: [uid:11] Found that seg to be updated with new session
keys
Nov 19 15:40:33.599 IST: IPSUB: [uid:11] Key list to be created to update SM
Nov 19 15:40:33.599 IST: IPSUB: [uid:11]   Update IP-Address-VRF key: 182.0.0.1:0
Nov 19 15:40:33.599 IST: IPSUB: [uid:11] Created key list to update SM
Nov 19 15:40:33.599 IST: IPSUB: [uid:11] Found address change to be notified
Nov 19 15:40:33.599 IST: IPSUB: [uid:11] Session Keys Available event for session
Nov 19 15:40:33.603 IST: IPSUB: [uid:11] Added session 182.0.0.1 to L3 session table
Nov 19 15:40:33.603 IST: IPSUB: [uid:11] Added session to session table with service
session keys
Nov 19 15:40:33.603 IST: IPSUB: [uid:11] Recieved Message = update SIP config
Nov 19 15:40:33.603 IST: IPSUB: [uid:11] Config Update event for session
Nov 19 15:40:33.603 IST: IPSUB: [uid:11] Inside processing IPSIP info
Nov 19 15:40:33.603 IST: IPSUB-ROUTE: [uid:11] Checking whether routes to be
inserted/removed
Nov 19 15:40:33.603 IST: IPSUB-ROUTE: [uid:11] Ctx present, No config change, Nothing
to be done
Nov 19 15:40:33.603 IST: IPSUB-ROUTE: [uid:11] Both IP addresses and VRF are same, no
need to add route
Nov 19 15:40:33.603 IST: IPSUB: [uid:11] Keys not changed, seg needn't be updated
Nov 19 15:40:33.603 IST: IPSUB: [uid:11] Key list to be created to update SM
Nov 19 15:40:33.603 IST: IPSUB: [uid:11] Created key list to update SM
Nov 19 15:40:33.603 IST: IPSUB: [uid:11] Data plane prov successful event for session
Nov 19 15:40:33.603 IST: IPSUB: [uid:11] Notifying about address change: 182.0.0.1
Nov 19 15:40:33.603 IST: DHCPD: Callback for workspace (ID=0x8900000B)
Nov 19 15:40:33.603 IST: DHCPD: Callback: switching path now setup for client
01aa.0013.1400.01
Nov 19 15:40:33.603 IST: DHCPD: Reprocessing saved workspace (ID=0x8900000B)
Nov 19 15:40:33.603 IST: DHCPD: Sending notification of DISCOVER:
Nov 19 15:40:33.603 IST:   DHCPD: htype 1 chaddr aa00.1314.0001
```

```
Nov 19 15:40:33.603 IST:   DHCPD: remote id 020a0000b600000b21010002
Nov 19 15:40:33.603 IST:   DHCPD: interface = GigabitEthernet2/9.1
Nov 19 15:40:33.603 IST:   DHCPD: class id 49786961
Nov 19 15:40:33.603 IST: DHCPD: DHCPDISCOVER received from client 01aa.0013.1400.01 on
interface GigabitEthernet2/9.1.
Nov 19 15:40:33.603 IST: DHCPD: Found previous server binding
Nov 19 15:40:33.603 IST: DHCPD: Sending DHCPOFFER to client 01aa.0013.1400.01
(182.0.0.1).
Nov 19 15:40:33.603 IST: DHCPD: ARP entry exists (182.0.0.1, aa00.1314.0001).
Nov 19 15:40:33.603 IST: DHCPD: unicasting BOOTREPLY to client aa00.1314.0001
(182.0.0.1).
Nov 19 15:40:33.603 IST: DHCPD: unicast BOOTREPLY output i/f override
GigabitEthernet2/9.1
Nov 19 15:40:33.603 IST: IPSUB_DP: [Gi2/9.1:O:PROC:DFL:182.0.0.1] Packet classified,
results = 0x0
Nov 19 15:40:33.603 IST: DHCPD: removing ARP entry (182.0.0.1 vrf default).
Nov 19 15:40:33.603 IST: DHCPD: Freeing saved workspace (ID=0x8900000B)
Nov 19 15:40:33.603 IST: IPSUB_DP: [uid:0] Setup event for session (session hdl 0)
Nov 19 15:40:33.603 IST: IPSUB_DP: [uid:0] Insert new entry for mac aa00.1314.0001
Nov 19 15:40:33.603 IST: IPSUB_DP: [uid:11] Added upstream entry into the classifier
Nov 19 15:40:33.603 IST: IPSUB_DP: [uid:11] MAC = aa00.1314.0001
Nov 19 15:40:33.603 IST: IPSUB_DP: [uid:11] Added downstream entry into the classifier
Nov 19 15:40:33.603 IST: IPSUB_DP: [uid:11] VRF = DFL, IP = 182.0.0.1, MASK =
255.255.255.255
Nov 19 15:40:33.603 IST: IPSUB_DP: [uid:11] Session setup successful
Nov 19 15:40:33.603 IST: IPSUB_DP: [uid:11] Sent update msg to the control plane
Nov 19 15:40:33.603 IST: IPSUB_DP: [uid:11] Activate event for session
Nov 19 15:40:33.603 IST: IPSUB: [uid:11] Data plane prov successful event for session
Nov 19 15:40:33.603 IST: IPSUB_DP: [uid:0] Found mac entry aa00.1314.0001
Nov 19 15:40:33.603 IST: IPSUB_DP: [Gi2/9.1:I:PROC:aa00.1314.0001] Packet classified,
results = 0x40
Nov 19 15:40:33.603 IST: IPSUB_DP: [Gi2/9.1:I:PROC:aa00.1314.0001] Rx driver allowing
IP routing
Nov 19 15:40:33.603 IST: DHCPD: input i/f override GigabitEthernet2/9.1 for client
Nov 19 15:40:33.603 IST: DHCPD: Reload workspace interface GigabitEthernet2/9.1
tableid 0.
Nov 19 15:40:33.603 IST: DHCPD: tableid for 182.0.0.11 on GigabitEthernet2/9.1 is 0
Nov 19 15:40:33.603 IST: DHCPD: client's VPN is .
Nov 19 15:40:33.603 IST: DHCPD: DHCPREQUEST received from client 01aa.0013.1400.01.
Nov 19 15:40:33.603 IST: DHCPD: Sending notification of ASSIGNMENT:
Nov 19 15:40:33.603 IST:  DHCPD: address 182.0.0.1 mask 255.255.255.240
Nov 19 15:40:33.603 IST:   DHCPD: htype 1 chaddr aa00.1314.0001
Nov 19 15:40:33.603 IST:   DHCPD: lease time remaining (secs) = 180
Nov 19 15:40:33.603 IST:   DHCPD: interface = GigabitEthernet2/9.1
Nov 19 15:40:33.603 IST: DHCPD: Sending DHCPACK to client 01aa.0013.1400.01
(182.0.0.1).
Nov 19 15:40:33.603 IST:  DHCPD: lease time = 180
Nov 19 15:40:33.603 IST: DHCPD: dhcpd_lookup_route: host = 182.0.0.1
Nov 19 15:40:33.603 IST: DHCPD: dhcpd_lookup_route: index = 183
Nov 19 15:40:33.603 IST: DHCPD: dhcpd_create_and_hash_route: host = 182.0.0.1
Nov 19 15:40:33.603 IST: DHCPD: dhcpd_create_and_hash_route index = 183
Nov 19 15:40:33.603 IST: DHCPD: dhcpd_add_route: lease = 180
Nov 19 15:40:33.607 IST: DHCPD: ARP entry exists (182.0.0.1, aa00.1314.0001).
Nov 19 15:40:33.607 IST: DHCPD: Changing arp entry 182.0.0.1 to secure arp entry
Nov 19 15:40:33.607 IST: DHCPD: Failed to secure arp entry 182.0.0.1
Nov 19 15:40:33.607 IST: DHCPD: unicasting BOOTREPLY to client aa00.1314.0001
(182.0.0.1).
Nov 19 15:40:33.607 IST: DHCPD: unicast BOOTREPLY output i/f override
GigabitEthernet2/9.1
Nov 19 15:40:33.607 IST: IPSUB_DP: [Gi2/9.1:O:PROC:DFL:182.0.0.1] Packet classified,
results = 0x10
```

Use the following commands to verify L2-connected DHCP session:

```
ISG_NMB#sh ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
182.0.0.1           01aa.0013.1400.01       Nov 19 2009 03:45 PM    Automatic

ISG_NMB#sh sss session
Current Subscriber Information: Total sessions 1

Uniq ID Interface    State         Service      Identifier           Up-time
11      IP           unauthen      Local Term   aa00.1314.0001       00:00:58

ISG_NMB#sh sss session uid 11
Unique Session ID: 11
Identifier: aa00.1314.0001
SIP subscriber access type(s): IP
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 00:01:04, Last Changed: 00:01:04

Policy information:
  Authentication status: unauthen

Configuration sources associated with this session:
Interface: GigabitEthernet2/9.1, Active Time = 00:01:04

ISG_NMB#sh sss session uid 11 de
Unique Session ID: 11
Identifier: aa00.1314.0001
SIP subscriber access type(s): IP
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 00:01:07, Last Changed: 00:01:07

Policy information:
  Context 133B2154: Handle 9000000B
  AAA_id 00000017: Flow_handle 0
  Authentication status: unauthen

Configuration sources associated with this session:
Interface: GigabitEthernet2/9.1, Active Time = 00:01:07
```

QoS Recommendations

When you configure QoS features on the Cisco 7600 SIP-400 for use with the IP Subscriber Awareness over Ethernet feature, note the following configuration guidelines and recommendations:

- The Cisco 7600 SIP-400 is capable of throughput of 5.1 to 5.6 gigabits per second (Gbps). We recommend that you do not oversubscribe the card beyond 8 Gbps. Beyond this limit, the card's behavior is unpredictable. [CSCsg67629]
- Oversubscription is supported only on the 5-Port Gigabit Ethernet SPA (SPA-5X1GE-V2).

Egress Oversubscription

- High-priority traffic (typically voice and video) must have an IP precedence value of 5, 6, or 7.
- IP precedence values of 0, 1, 2, 3, or 4 will result in drops if oversubscription occurs, even if the traffic is classified as priority traffic in a QoS policy. [CSCsg67721]

Note We strongly recommend that the IP precedence value and VLAN user priority values of packets match. If ingress oversubscription occurs, priority traffic with non-matching IP precedence and VLAN user priority values might be dropped at the SPA level. [CSCsg97434]

Ingress Oversubscription

- High-priority traffic (typically voice) must have VLAN user priority values of 5, 6, or 7. Priority values of 0, 1, 2, 3, or 4 will result in drops if oversubscription occurs, even if the traffic is classified as priority traffic by a QoS policy. [CSCsg97434, CSCsg67721]

QoS Counter Updates

- To obtain statistics for an individual IP subscriber session, issue the **show policy-map interface** command two or three times. This is necessary because the counters retain their existing values the first time you issue the command.
- If you issue the **show policy-map interface** command and do not specify an interface, the router must update all of the session counters. With 32000 subscribers, this can take up to 30 minutes.

Bandwidth-Remaining Ratio Recommendations

The Bandwidth-Remaining Ratio (BRR) feature (also called Distribution of Remaining Bandwidth Using Ratio) allows service providers to prioritize subscriber traffic during periods of congestion. You can use the feature to specify the relative weight of a subinterface or class queue with respect to other subinterfaces or queues. During congestion, the router uses the bandwidth-remaining ratio to optimize the scheduling of uncommitted bandwidth on subinterfaces and class queues. Without BRR, the unassigned bandwidth on a physical interface is equally distributed among all queues. For an overview of this feature, see its feature description at:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb31/bwratio.htm

This section provides recommendations and guidelines for configuring BRR on the Cisco 7600 SIP-400 to support IP Subscriber Awareness over Ethernet. It contains the following sections:

- BRR Configuration Guidelines
- BRR Configuration Instructions

BRR Configuration Guidelines

Observe the following Cisco 7600 specific guidelines and considerations as you configure this feature:

- Supported only on the Cisco 7600 SIP-400 with 2-port and 5-port Gigabit Ethernet (GE) SPAs.
- Available only on GE interfaces (because the feature is only supported on GE SPAs).
- Requires RSP720, Sup720, or Sup32.
- If two subinterfaces have bandwidth remaining ratios that vary greatly (for example, 1000 to 1), you must configure a low queue limit (between 2 and 50) for the child default class of the subinterface with the lower ratio. Without a low queue limit, the packets that are buffered due to the default queue-limit value are allowed to pass after traffic is stopped, which affects bandwidth remaining ratios significantly. Configuring a low queue limit ensures that the ratios are maintained even after the traffic is stopped.

Note We recommend that you use BRR with priority-rate propagation. See the "Priority-Rate Propagation Recommendations" section on page 24-25 for more information.

BRR Configuration Instructions

Following is a summary of the steps required to configure configure a QoS policy that defines BRR for a subscriber (access) interface on the Cisco 7600 SIP-400. The following table provides detailed instructions.

Note The command lines include only those arguments and keywords required to configure BRR.

1. **enable**
2. **configure terminal**
3. **qos scheduler priority-rate-propagation platform sip-400** (optional but recommended)
4. **policy-map *child-policy-name***
5. **class** *class-map-name*
6. **priority level** *level* (optional but recommended)
7. **police** *bps*
8. exit
9. exit
10. **policy-map *parent-policy-name***
11. **class class-default**
12. **bandwidth remaining ratio** *ratio*
13. **shape average** *cir* [*bc*] [*be*]
14. **service-policy** *child-policy-name*
15. exit
16. exit
17. **interface** *type slot*/*module*/*port*.*subinterface* **access**
18. **service-policy output** *parent-policy-name*

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	**qos scheduler priority-rate-propagation platform sip-400** **Example:** `Router(config)# qos scheduler priority-rate-propagation platform sip-400`	Enables the priority-rate propagation feature on the Cisco 7600 SIP-400. This feature applies a priority level and traffic rate for priority traffic to all higher-level queues in the queue hierarchy, even if the queues are not specifically configured for minimum rates or priority. **Note** This step is optional; however, if you are using BRR, we recommend that you perform this step.
Step 4	**policy-map** *child-policy-name* **Example:** `Router(config)# policy-map child`	Creates or modifies a child policy map and enters policy-map configuration mode. • *child-policy-name* is the name of the child policy map.
Step 5	**class** *class-map-name* **Example:** `Router(config-pmap)# class precedence_0`	Configures the class map that you specify. Enters policy-map class configuration mode. • *class-map-name* is the name of a previously created class map.
Step 6	**priority level** *level* **Example:** `Router(config-pmap-c)# priority level 1`	Assigns a priority level to this traffic class. • *level* is the priority level to assign. Valid values are: 1 (high) and 2 (low). **Note** Do not specify the same priority level for two different classes in the same policy map.
Step 7	police *bps* **Example:** `Router(config-pmap-c)# police 200000000`	(Optional) Specifies the rate at which to police traffic belonging to this traffic class. • *bps* specifies the average rate in bits per second (bps). Valid values are from 8,000 to 2,488,320,000 bps.
Step 8	exit	Exits policy-map class configuration mode.
Step 9	exit	Exits policy-map configuration mode.
Step 10	**policy-map** *parent-policy-name* **Example:** `Router(config)# policy-map Parent`	Creates or modifies a parent policy map. Enters policy-map configuration mode. • *parent-policy-name* is the name of the parent policy map.

	Command or Action	Purpose
Step 11	**class class-default** **Example:** `Router(config-pmap)# class class-default`	Configures the class-default class. Enters policy-map class configuration mode. **Note** The router interprets any features configured under the class-default class as aggregate features on the subinterface.
Step 12	**bandwidth remaining ratio** *ratio* **Example:** `Router(config-pmap-c)# bandwidth remaining ratio 10`	Specifies the bandwidth-remaining ratio for the subinterface. The scheduler allocates the excess bandwidth relative to other subinterfaces. • *ratio* is the value that is used to determine the amount of unused bandwidth to allocate to each queue on the subinterface during periods of congestion. Valid values are 1 to 1000. The default and minimum values are 1. **Note** The CLI supports a *ratio* value of 1 to 65535 but you cannot apply a policy with a BRR value above 1000 to a Cisco 7600 SIP-400 interface.
Step 13	**shape average** *cir* [*bc*] [*be*] **Example:** `Router(config-pmap-c)# shape average 100000000`	(Optional) Shapes the average rate to the rate you specify. • **average** specifies average rate shaping. • *cir* specifies the committed information rate (CIR), in bits per second (bps). • (Optional) *bc* specifies the committed burst size, in bits. • (Optional) *be* specifies the excess burst size, in bits.
Step 14	**service-policy** *child-policy-name* **Example:** `Router(config-pmap-c)# service-policy child`	Applies the specified child policy map to the default traffic class of the parent policy. The router applies the QoS actions specified in the child policy to the traffic class. • *child-policy-name* is the name of the child policy. **Note** Do not include **input** or **output** keyword when applying a child policy to a parent policy. **Note** On a subinterface, the child policy can be applied only to the parent's default traffic class.
Step 15	`exit`	Exits policy-map class configuration mode.
Step 16	`exit`	Exits policy-map configuration mode.

	Command or Action	Purpose
Step 17	**interface** *type slot/module/port.subinterface* **access** **Example:** `Router(config)# interface GigabitEthernet 1/0/0.1 access`	Creates or modifies the access subinterface you specify. Enters subinterface configuration mode. • *type* is the interface type (for example, Gigabit Ethernet). • *slot/module/port.subinterface* identifies the subinterface (for example, 1/0/0.1). • **access** identifies this as an IP subscriber interface.
Step 18	**service-policy output** *parent-policy-name* **Example:** `Router(config-subif)# service-policy output parent`	Applies the parent policy to the subinterface. • **output** applies the service policy to outbound traffic. • *parent-policy-name* is the name of the parent policy. **Note** A policy map with BRR can be used only in the egress direction. The router shapes the subinterface traffic to the shaping rate specified in the parent class-default class and applies the QoS actions specified in the child policy to traffic matching the traffic classes. During periods of congestion, the router uses the bandwidth-remaining ratio specified in the parent policy map to allocate unused bandwidth on this subinterface relative to other subinterfaces.

Priority-Rate Propagation Recommendations

Priority-rate propagation applies (propagates) a priority level and traffic rate from a lower-level queue to all of the upper-layer queues in the queue hierarchy, even if the upper-layer queues are not specifically configured for minimum rates or priority. For example, if you configure a priority level and traffic rate for a traffic class (such as video) in a child policy, you can use priority-rate propagation to apply that rate to video traffic at all queue levels (parent queue, subinterface queue, and interface queue).

Dual-priority queues enable you to define two classes of high-priority traffic in a single policy map. You can also use the **priority level** command to assign a priority (high or low) to each priority queue. The **priority level** command specifies that a class of traffic has latency requirements with respect to other classes. Currently, the router supports two priority levels: level 1 (high) and level 2 (low). The router places traffic with a high priority level on the outbound link ahead of traffic with a low priority level. High priority packets, therefore, are not delayed behind low priority packets.

The router associates a single priority queue with each priority level and services the high level priority queues until empty before servicing the next level priority queues and non-priority queues. While the router services a queue, the service rate is as fast as possible and is constrained only by the rate of the underlying link or parent node in a hierarchy. If a rate is configured and the router determines that a traffic stream has exceeded the configured rate, the router drops the exceeding packets during periods of congestion. If the link is currently not congested, the router places the exceeding packets onto the outbound link.

If bandwidth remaining ratio (BRR) has also been configured, the router services priority traffic first. After servicing the priority traffic bandwidth, the router allocates unused bandwidth to the logical queues based on the configured bandwidth-remaining ratio. In this default case, the three-level scheduler allocates an equal share of the unused bandwidth to each logical queue.

If high priority traffic is not policed appropriately, bandwidth starvation of low priority traffic can occur. Therefore, though not required, we recommend that you use the **police** command to configure a policer for high priority traffic. If you configure the **police** command for priority queues, the traffic rate is policed to the police rate for each of the priority queues.

Priority-Rate Propagation Configuration Guidelines

As you configure priority-rate propagation for use with BRR, consider the following guidelines:

- Use the [**no**] **qos scheduler priority-rate-propagation platform sip400** command in global configuration mode to enable and disable the priority-rate propagation feature.
- The [**no**] **qos scheduler priority-rate-propagation platform sip400** command has no effect on QoS policies that are already attached to interfaces. Therefore, we recommend that you issue the command before attaching QoS policies.

Note If you issue the [**no**] **qos scheduler priority-rate-propagation platform sip400** command after attaching QoS policies to Cisco 7600 SIP-400 interfaces, you must save the configuration and reload the router for the command to take effect.

- Priority-rate propagation and BRR work together as follows:
  - When priority-rate propagation is enabled, the router services the priority bandwidth for all subinterface policies. The remaining bandwidth is then distributed according to the bandwidth remaining ratios. In this scenario, the priority rate was propagated from the child level to the interface queue.
  - When priority-rate propagation is disabled, the aggregate subinterface bandwidth (priority and best effort) is shared according to the bandwidth remaining ratios. In this scenario, the priority bandwidth is not propagated from the child queue to the interface queue.

Priority-Rate Propagation and BRR Configuration Example

Here is an example of a priority level (2) being assigned to video traffic in a child policy map and used with BRR, which is configured in the parent policy map:

```
policy-map parent
 class class-default
   bandwidth remaining ratio 1
   service-policy child

policy-map child
 class video
   priority level 2
   police 200 Mbps
```

Unsupported IP Subscriber Session Features

Due to the way that internal VLANs are allocated for sharing among IP subscribers, the following features are not available for individual subscribers:

- Policy-based routing (PBR), Network Address Translation (NAT), or unicast Reverse Path Forwarding (uRPF)
- IPv4 and IPv6 multicast

- Encoded address resolution logic (EARL) features, such as reflexive ACL, Generic Route Encapsulation (GRE) tunneling, Context-Based Access Control (CBAC), and server load balancing (SLB)

IP Subscriber Awareness over Ethernet Configuration Guidelines

Note The IP Subscriber Awareness over Ethernet feature is not available in the IP services software image (*xxx*-ipservices_wan-mz). Although the image shows the **access** keyword as being available for the **interface** command, the subscriber awareness functionality is not available.

Observe the following guidelines and limitations as you configure IP Subscriber Awareness over Ethernet on Cisco 7600 routers:

- Software and hardware requirements:
  - Cisco IOS Release 12.2SRB or later
  - RSP720 with PFC3C or PFC3CXL (other supervisor engines are not supported)
  - Cisco 7600 SIP-400 and 5-Port Gigabit Ethernet SPA (SPA-5X1GE-V2)
  - Support for ES+ linecards from 12.2(33)SRE onwards.
- Oversubscription is supported only on the 5-Port Gigabit Ethernet SPA.
- A maximum of 32000 interfaces are supported on the router. To support 32000 interfaces:
  - The RSP720 must have 2 GB of RP memory and 1 GB of SP memory.
  - The Cisco 7600 SIP-400 must have 1 GB of memory.
- The Cisco 7600 SIP-400 supports a maximum of 8000 IP subscribers.
- The 5-Port Gigabit Ethernet SPA (SPA-5X1GE-V2) supports up to 8000 VLANs.
- The access subinterface that represents an IP subscriber must be configured for .1Q or Q-in-Q encapsulation.
- The MTU of the access subinterface is 1500 and this value cannot be changed.
- You can convert a regular GE subinterface to an access interface, but you cannot convert an access interface to a regular GE subinterface. Instead, you must delete the access subinterface.
- EARL-based features are not supported. This includes Network Address Translation (NAT), Reflexive ACL, Generic Route Encapsulation (GRE) tunneling, Context-Based Access Control (CBAC), and server load balancing (SLB).
- We recommend that you do not configure Hot Standby Routing Protocol (HSRP) for link redundancy.
- See the "QoS Recommendations" section on page 24-20 for QoS guidelines.

Interaction with Other Features

The following list describes the interaction between IP Subscriber Awareness over Ethernet and other features that are configured on the router:

- Multicast traffic is not affected by the feature. The router can participate in IGMP functions and replication without being affected by IP Subscriber Awareness over Ethernet. In addition, the router supports multicast traffic without the authentication of data service. This allows basic video service to be provided without data service.

  The DSLAM (not the router) is responsible for replicating multicast traffic and delivering it to IP subscribers. Therefore, it is not necessary for the IP Subscriber Awareness over Ethernet feature to support multicast traffic on IP subscriber interfaces (access interfaces).

Configuring IP Subscriber Awareness over Ethernet

The following sections provide information about configuring the IP Subscriber Awareness over Ethernet feature on a Cisco 7600 series router:

Configuration Summary

Following is a summary of the steps required to configure IP Subscriber Awareness over Ethernet on Cisco 7600 routers. Detailed configuration instructions are provided in the next section.

Before Starting

- Determine which VPN routing and forwarding (VRF) table each IP subscriber should be part of. All of the subscribers in a VRF share a single internal VLAN for data services. Use the **ip vrf** and **rd** commands to create each of the VRF tables that you need.

  To use the same VRF, subscribers must all belong to the same network service provider (NSP), Internet service provider (ISP), or access service provider (ASP). If you do not assign a subscriber to a VRF, the subscriber is added to the default VRF, which the router creates during system bootup.

- Make sure that the router is configured as a DHCP server or a DHCP relay device in order to allow IP addresses to be dynamically assigned for IP subscriber sessions. Otherwise, you would have to assign a static IP address to each IP subscriber access subinterface (which is not recommended).

  For information about configuring DHCP, see "Configuring DHCP" in the *Cisco IOS IP Configuration Guide* at:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcprt1/1cfdhcp.htm

- Determine which physical interfaces are used by IP subscribers. For each IP subscriber, you configure an access subinterface on the physical interface that the subscriber is connected to.

Configure QoS and HQoS Policies for IP Subscribers

- Define QoS policies (class maps and policy maps) to define traffic bandwidth and shaping policies for subscriber traffic. You can use a hierarchical QoS (HQoS) policy to shape traffic at different levels. For example, the parent policy could define the total bandwidth for the subscriber, and the child policy could define the bandwidth for different types of subscriber traffic (such as video). On a subinterface, the child policy can be attached only at the default class of the parent.
- (Optional) You can create dual-priority queues to handle the subscriber's voice and video traffic.

- You can also define a class-based weighted fair queue (CBWFQ) or priority queue (PQ) for different types of subscriber traffic.

Configure Access Lists and Security ACLs

- Determine the security policies that are needed for IP subscribers. Create access lists and security ACLs to define these policies.

  Here is an example of two access lists (2 and 3) that will be applied to IP subscribers:

```
access-list 2 permit 18.18.18.18
access-list 3 permit 23.23.23.23
access-list 101 deny   ip 44.1.1.0 0.0.0.255 any
access-list 101 permit icmp any any
```

  The following example configures an input and output security ACL for the IP subscriber session that is represented by the access subinterface gig0/1/1.100:

```
interface gig0/1/1.100 access
  encapsulation dot1q 100
  ip address 10.10.10.1 255.255.255.0
  ip access-group 101 in
  ip access-group 102 out
```

Configure IP Subscriber Interfaces

- Create an access interface for each IP subscriber. Create the access interface as a subinterface of the subscriber's physical interface. For example, if the subscriber is connected to Gig1/0/0, you could configure the access interface as Gig1/0/0.100.
- Configure the access interface as follows:
  - If necessary, assign an IP address to the interface (this is a static IP address). We recommend that you do not configure many access interfaces with a static IP address. Instead, you should allow DHCP to dynamically assign IP addresses for IP subscriber sessions.
  - If the IP subscriber belongs to a particular VRF table, include the **ip vrf forwarding** *vrf-name* command in the configuration to associate the interface with the table. If you do not specify a VRF table, the subscriber is added to the default VRF.
  - Set the encapsulation type (.1Q or Q-in-Q) and specify which VLAN the interface is part of.
  - Attach QoS policies to the interface to define traffic bandwidth and shaping policies for the subscriber traffic.

  This example shows two IP subscriber access interfaces (gig1/0/0.100 and gig1/0/0.300). Since the subscribers connect through Gig1/0/0, the access interfaces are created as subinterfaces of Gig1/0/0. Notice that gig1/0/0.100 is assigned a static IP address and gig1/0/0.300 uses DHCP to obtain an IP address. In addition, notice that gig1/0/0.300 is VRF aware.

```
interface gig1/0/0.100 access
 ip address 10.10.10.10 255.255.255.255
 encapsulation dot1q 100
 service-policy input bband-in1
 service-policy output bband-out1

interface gig1/0/0.300 access
 ip vrf forwarding vrf1
 encapsulation dot1q 300
 service-policy input bband-in1
 service-policy output bband-out1
```

Verify the IP Subscriber Awareness over Ethernet Feature

Use the following commands to verify the status of each access interface that represents an IP subscriber. An access subinterface should exist for each subscriber and the interfaces should be in the Up state.

- Issue the **show running-config interface** *interface***.***subinterface* command to verify the configuration of each access subinterface (where *interface* is the physical interface and **.***subinterface* is the access subinterface). For example, **show running-config interface Gig1/0/2.1** displays the access subinterface (.1) that exists on the physical interface Gig1/0/2.

Configuration Examples

The following example shows a configuration with three subscribers (Gig3/2/0.10, Gig3/2/0.11, and Gig3/2/0.12), each receiving a different type of service: gold (30 Mbps), silver (15 Mbps), and bronze (5 Mbps). Each subscriber has per-subscriber accounting and per-subscriber ACL configured.

The QoS policy maps are configured so that video traffic is never dropped, and default traffic is shared in the ratio of 30:15:5 (which results in a bandwidth remaining ratio of 6:3:1).

```
aaa new-model
aaa accounting network defaul start group radius
radius-server key cisco
radius-server host 2.2.2.2
int loopback 1
ip address 13.0.7.254 255.255.248.0

ip dhcp pool Loopback1
  network 13.0.0.0 255.255.248.0

Class-map voip
 match ip precedence 5

Class-map video
 match ip precedence 6

policy-map data_gold_child_out
 class video
   priority level 2
   police 27000000
   set cos 5
 class class-default
   police 30000000
   set cos 3

policy-map data_gold_parent_out
 class class-default
   shape average 29900000
   bandwidth remaining ratio 6
   service-policy data_gold_child_out

policy-map data_silver_child_out
 class video
   priority level 2
   police 27000000
   set cos 5
 class class-default
   police 15000000
   set cos 2

policy-map data_silver_parent_out
 class class-default
```

```
   shape average 29900000
   bandwidth remaining ratio 3
   service-policy data_silver_child_out

policy-map data_bronze_child_out
 class video
   priority level 2
   police 27000000
   set cos 5
 class class-default
   police 5000000
   set cos 1

access-list 102 permit ip any any precedence 5
access-list 102 permit ip any any precedence 2
access-list 102 permit ip any any precedence 0

policy-map data_bronze_parent_out
 class class-default
   shape average 29900000
   bandwidth remaining ratio 1
   service-policy data_bronze_child_out

policy-map data_gold_in
  class class-default
    police 5000000
policy-map data_silver_in
  class class-default
    police 2000000
policy-map data_bronze_in
  class class-default
    police 2000000


interface gig 3/2/0.10 access
    ip unnumbered Loopback 1
    encapsulation dot1q 10
    service-policy output data_gold_parent_out
    service-policy input data_gold_in
    accounting dhcp source-ip aaa list default
    ip access-group 103 in

interface gig 3/2/0.11 access
    ip unnumbered Loopback 1
    encapsulation dot1q 11
    service-policy output data_silver_parent_out
    service-policy input data_silver_in
    accounting dhcp source-ip aaa list default
    ip access-group 103 in

interface gig 3/2/0.12 access
    ip unnumbered Loopback 1
    encapsulation dot1q 12
    service-policy output data_bronze_parent_out
    service-policy input data_bronze_in
    accounting dhcp source-ip aaa list default
    ip access-group 103 in
```

Command Reference

This section describes the new commands for IP Subscriber Awareness over Ethernet. The following new command is being introduced as part of this feature:

- interface access

interface access

To create an access interface for an IP subscriber, use the **interface access** command in global configuration mode. Use the **no** form of the command to delete an IP subscriber access interface.

interface *interface***.***subinterface* **access**

no interface *interface***.***subinterface* **access**

Syntax Description

interface	Identifies the physical interface that this IP subscriber is connected to.
.*subinterface*	A subinterface number to assign to the access interface.

Defaults

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SRB	This command was introduced.

Usage Guidelines

This command creates an access interface for an IP subscriber. Create the access interface as a subinterface of the physical interface that the subscriber is connected to. For example, if the subscriber is connected to Gig1/0/0, you could configure the access interface as Gig1/0/0.1, Gig1/0/0.2, Gig1/0/0.3, and so on.

Include the **ip vrf forwarding** *vrf-name* command in the configuration to associate the IP subscriber with the specified VRF table. If you do not specify a VRF table, the subscriber is added to the default VRF table (which is created during router bootup).

Examples

The following command example creates an access interface for an IP subscriber and assigns the subscriber to the VRF table named vrf1. The access interface is created as subinterface .300 on the physical interface Gig2/0/1. You would issue additional commands to complete the configuration (for example, to specify encapsulation type, and to assign QoS policies).

```
Router(config)# interface Gig2/0/1.300 access
Router(config-if)# ip vrf forwarding vrf1
Router(config-if)#
```