

# Managed SAPs with Routed CO

---

## In This Chapter

This section provides information about Managed SAPs with Routed CO.

Topics in this section include:

- [Applicability on page 2512](#)
- [Overview on page 2513](#)
- [Configuration on page 2516](#)
- [Conclusion on page 2544](#)

## Applicability

This section is applicable to the 7750 SR7/12 with IOM2 or higher (for BRAS functionality) with Chassis mode B or higher (for Routed Central Office (CO) model) and the 7710/7750 SR-c12 and was tested on release 12.0.R1. Routed CO is supported on 7450 ESS-7 or ESS-12 in mixed-mode since 8.0.R1. The 7750 SR-c4 is supported from 8.0.R4 and higher.

This note is related only to the use of IPv4.

MSAPs are also supported with Bridged CO model and on the 7450, however, applicable configuration information is beyond the scope of this document.

## Overview

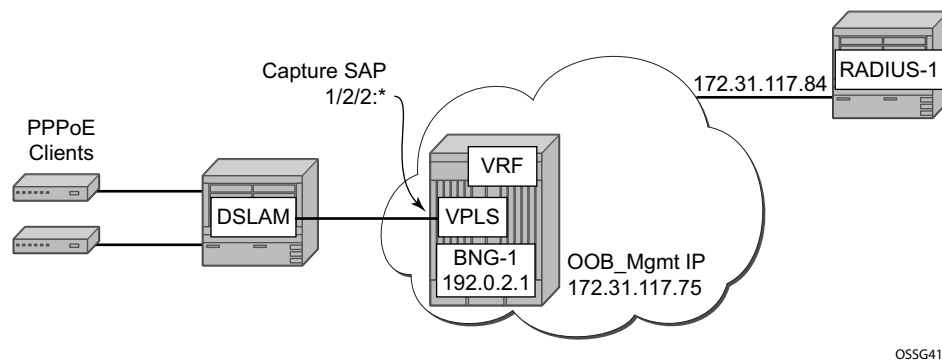
Managed Service Access Point (MSAP) allows the use of policies and a SAP template for the creation of a SAP. As part of the MSAP feature, individual SAPs are created along with the subscriber host with minimal configuration on the BRAS node. Creation of a managed SAP is triggered by a DHCP-DISCOVER and/or a PPPoE-PADI message. In this case, the authentication response message not only returns the subscriber host attributes, but also the managed SAP policy and service ID. These latter two parameters are used by the system to create the subscriber SAP with default settings as indicated in the managed SAP policy and then assigning it to the corresponding VPN service. In this model, each subscriber is defined with its own VLAN. This feature uses authentication mechanisms supported by the node to create a SAP.

When enabled, receiving a triggering packet initiates RADIUS authentication that provides a service context. The authentication, together with the service context for this request, creates a managed SAP.

The VLAN is the same as the triggering packet. This SAP behaves as a regular SAP but its configuration is not user editable and not maintained in the configuration file. The managed SAP remains active as long as the session is active.

Knowledge of Alcatel-Lucent TPSDA (Triple Play Service Delivery Architecture) and functionality is assumed throughout this document.

The network topology is displayed in [Figure 390](#). The configuration consists of one 7750 SR-12 acting as a BNG with BRAS functionality.



**Figure 390: Network Topology**

## Capture SAP

A capture SAP is used to capture triggering packets and initiate RADIUS authentication. This SAP is defined in a similar way to a default SAP but does not forward traffic.

A capture SAP and default SAP cannot be configured at the same time for a single port with the dot1q encapsulation or for a single port:topq combination with qinq encapsulation. Managed SAPs and regular SAPs can co-exist on the same port and in the same service.

The capture SAP is used if a more specific match for the Q or Q-in-Q tags is not found by the traffic classification on the IOM. If a capturing SAP is defined, triggering packets are sent to the CPM. Non-triggering packets captured by the capturing SAP are dropped.

The following are examples for supported modes:

SAP 1/2/2:\* for dot1Q

SAP 1/2/2:Q1.\* for QinQ (where Q1 > 0)

The MSAP created will have a single tag (for dot1q) or both q-tags (for qinq) that arrived in the original packet if authenticated by RADIUS.

While MSAPs are supported in both routed CO and bridged CO Triple Play Service Delivery Architecture (TPSDA) models, the triggering SAP must be created in a VPLS service.

---

## Triggering Packets

DHCP discover (or requests if re-authentication is configured) for DHCP clients. The managed SAP lifetime is defined by the lease time.

PPPoE PADI for the PPPoE client. The MSAP lifetime is defined by the session time. The MSAP is installed after the IP address is provided.

ARP packets as trigger packets within a capture SAP. ARP trigger packets can be used for static IP hosts. The managed SAP lifetime is defined by the ARP entry lifetime and is subject to the same ARP entry refresh mechanisms as other ARP entries.

All trigger types can be combined on a SAP supporting DHCP, PPPoE and ARP hosts. In this chapter, a PPPoE client is used.

## **RADIUS Authentication and Vendor Specific Attributes (VSAs) for MSAP**

An MSAP is created in the service-id context that is returned from RADIUS. The RADIUS attribute Alc-MSAP-Serv-Id refers to the service in which the MSAP is created.

In a Routed CO scenario, the MSAP is created in a group-interface context. The group-interface name is returned from RADIUS attribute Alc-MSAP-Interface and must exist in the provided service for the MSAP to be installed.

The MSAP parameters are defined in the creation policy. The policy name is returned from RADIUS in the attribute Alc-MSAP-Policy in order for the MSAP to be created.

## Configuration

---

### Configure RADIUS Authentication Policy “authentication-1”

The following output shows a RADIUS authentication policy configuration defining “authentication-1”.

```

configure subscriber-mgmt
  authentication-policy "authentication-1" create
    radius-authentication-server
      source-address 172.31.117.75
      router "management"
      server 1 address 172.31.117.84 secret ALU
    exit
  pppoe-access-method pap-chap
  include-radius-attribute
    remote-id
    nas-identifier
    mac-address
  exit
exit
exit

```

Where, management routing instance and the out-of-band and IP address 172.31.117.75 are used as a source address to communicate authentication messages between the BNG and the RADIUS server. The RADIUS server IP address is 172.31.117.84. Up to five servers can be configured. When having multiple servers two possible access algorithms can be configured to access the list of RADIUS servers, **direct** or **round-robin**.

The value of secret is ALU which is case sensitive and must be configured on Clients.conf file on the RADIUS server in advance. Up to 20 characters in length are possible.

The authentication method used in our example is PAP/CHAP, so the pap-chap value is used for the pppoe-access-method.

The user’s remote-id and mac-address are sent as well the nas-identifier into the access request message towards the RADIUS.

By default, the RADIUS authentication messages are send over port 1812 but can be overridden by adding an explicit port setting to the **server** command.

```

configure subscriber-mgmt
  authentication-policy "authentication-1" create
    radius-authentication-server
      server 1 address 172.31.117.84 secret ALU port <value>

```

## Configure a RADIUS Accounting Policy

This example configures radius-accounting-policy "accounting-1".

```
configure subscriber-mgmt
  radius-accounting-policy "accounting-1" create
  update-interval 10
  include-radius-attribute
    framed-ip-addr
    subscriber-id
    circuit-id
    remote-id
    nas-port-id
    nas-identifier
    sub-profile
    sla-profile
    user-name
  no detailed-acct-attributes
  std-acct-attributes
exit
session-id-format number
radius-accounting-server
  router "management"
  server 1 address 172.31.117.84 secret ALU
exit
exit
exit
```

Where, accounting updates are sent every 10 mins (the default update-interval is 5 minutes). The accounting session-id-format in this example is a number (40 HEX character string).

```
SESSION ID [44] 40 000000010241000000000064000000034B090B2D
```

Whereas, session-id-format <description> can be used in this case. The session-id-format is as follows:

```
<subscriber>@<sapid>@<SLA-profile>_<creation-time>
```

```
SESSION ID [44] 50 user1@1/2/2:100@sla-profile-2M_2009/11/22 11:56:25
```

Since std-acct-attributes is used, only the total number of octets/packets in ingress and egress directions are sent.

ALU VSAs are used for accounting, in such case, detailed accounting values for each queue (in case multiple queues for the subscriber can be used) and the in-profile and the out-profile values are shown. This feature can be enabled by adding **no std-acct-attribute**, which is the default.

By default, the RADIUS accounting messages are sent over port 1813 but can be overridden by adding an explicit port setting in addition to the **server** command.

## Configure a RADIUS Accounting Policy

```
configure subscriber-mgmt
  radius-accounting-policy accounting-1 create
  radius-authentication-server
    server 1 address 172.31.117.84 secret ALU port <value>
```



## Configure an QoS SAP Ingress Policy

Configure QoS SAP ingress policy where shaping and SAP egress policy performs shaping and remarking. Values for dot1p and dscp are used as examples.

```
configure qos
  sap-ingress 20 create
    description "64K_upstream"
    queue 1 create
      rate 64
    exit
  exit
  sap-ingress 30 create
    description "128K_upstream"
    queue 1 create
      rate 128
    exit
  exit
  sap-ingress 40 create
    description "256K_upstream"
    queue 1 create
      rate 256
    exit
  exit
  sap-ingress 50 create
    description "512K_upstream"
    queue 1 create
      rate 512
    exit
  exit
  sap-egress 20 create
    description "256K_downstream"
    queue 1 create
      rate 256
    exit
    fc be create
      queue 1
      dot1p 5
      dscp ef
    exit
  exit
  sap-egress 30 create
    description "512K_downstream"
    queue 1 create
      rate 512
    exit
    fc be create
      queue 1
      dot1p 4
      dscp af21
    exit
  exit
  sap-egress 40 create
    description "1M_downstream"
    queue 1 create
      rate 1024
    exit
```

## Configure an QoS SAP Ingress Policy

```
        fc be create
            queue 1
            dot1p 5
            dscp ef
        exit
    exit
    sap-egress 50 create
        description "2M_downstream"
        queue 1 create
            rate 2048
        exit
        fc be create
            queue 1
            dot1p 3
            dscp cs1
        exit
    exit
exit
```

## Configure Enhanced Subscriber Management Parameters

Four SLA profiles are configured where the downstream speed is four times the upstream speed and the SLA profile will be named with the downstream speed.

Also, a subscriber profile will be configured to initiate RADIUS accounting and doing SLA profile mapping.

```

configure subscriber-mgmt
  sla-profile "sla-profile-1M" create
    ingress
      qos 40 shared-queuing
    exit
  egress
    qos 40
  exit
  no qos-marking-from-sap
exit
sla-profile "sla-profile-256K" create
  ingress
    qos 20 shared-queuing
  exit
  egress
    qos 20
  exit
  no qos-marking-from-sap
exit
sla-profile "sla-profile-2M" create
  ingress
    qos 50 shared-queuing
  exit
  egress
    qos 50
  exit
  no qos-marking-from-sap
exit
sla-profile "sla-profile-512K" create
  ingress
    qos 30 shared-queuing
  exit
  egress
    qos 30
  exit
  no qos-marking-from-sap
exit
sub-profile "sub-profile-default" create
  radius-accounting-policy "accounting-1"
  sla-profile-map

```

## Configure Enhanced Subscriber Management Parameters

```
        use-direct-map-as-default
    exit
exit
sub-ident-policy "sub-id-default" create
    sub-profile-map
        use-direct-map-as-default
    exit
    sla-profile-map
        use-direct-map-as-default
    exit
exit
exit
```

## Configure an MSAP Policy

MSAP policies contain the configuration template (parameters) to be used for MSAP creation and the necessary information to complete the subscriber identification process.

The MSAP policy that will be used is either returned by RADIUS in the access-accept message during authentication phase if this MSAP policy is already configured under subscriber management context, or else the default MSAP policy will be used instead.

```
configure subscriber-mgmt
  msap-policy "msap-ISP1" create
    sub-sla-mgmt
      def-sub-id use-sap-id
      def-sub-profile "sub-profile-default"
      def-sla-profile "sla-profile-512K"
      sub-ident-policy "sub-id-default"
      single-sub-parameters
        profiled-traffic-only
      exit
    exit
  exit
  msap-policy "msap-default" create
    sub-sla-mgmt
      def-sub-id use-sap-id
      def-sub-profile "sub-profile-default"
      def-sla-profile "sla-profile-256K"
      sub-ident-policy "sub-id-default"
      single-sub-parameters
        profiled-traffic-only
      exit
    exit
  exit
exit
```

If managed routes are required for a certain subscriber, add the following command under msap-policy. The default anti-spoof is **ip-mac**. Managed routes are out of the scope of this document.

```
configure subscriber-mgmt
  msap-policy "msap-ISP1" create
    ies-vprn-only-sap-parameters
      anti-spoof nh-mac
    exit
  exit
```

## Configure a VPLS Service with a Capture SAP

Configure a VPLS service with capture SAP and define the triggering packet types. The **trigger-packet** and **authentication-policy** commands are mandatory within the capture SAP. Additionally, the **cpu-protection** command can be added to enable CPU protection policies

```
configure
  service
    vpls 1 customer 1 create
      description "VPLS for Capture SAPs"
      stp
        shutdown
      exit
      sap 1/2/2:* capture-sap create
        description "capture SAP for MSAP creation on port 1/2/2"
        trigger-packet arp dhcp pppoe
        msap-defaults
          policy "msap-default"
        exit
        authentication-policy "authentication-1"
      exit
      no shutdown
    exit
```

Verify the details of capture SAP:

```
A:BNB# show service id 1 sap 1/2/2:* detail
=====
Service Access Points(SAP)
=====
Service Id      : 1
SAP             : 1/2/2:*           Encap           : q-tag
Description     : capture SAP for MSAP creation on port 1/2/2
Admin State    : Up                 Oper State      : Up
Flags          : None
Multi Svc Site : None
Last Status Change : 03/20/2014 11:28:26
Last Mgmt Change  : 03/20/2014 11:28:09
Sub Type       : capture
Triggers       : arp dhcp pppoe
Dot1Q Ethertype : 0x8100           QinQ Ethertype  : 0x8100
Split Horizon Group: (Not Specified)

<snipped>

Egr MCast Grp   :
Auth Policy     : authentication-1
DHCP User Db    : None
PPP Policy      : None
PPP User Db     : None
PPPoE Policy    : default
PPPoE User Db   : None
DHCPv6 User Db  : None

<snipped>
```

```

-----
Sap Statistics
-----
Last Cleared Time      : N/A

                Packets                Octets
CPM Ingress           : 0                0

Forwarding Engine Stats
Dropped               : 0                0

DHCP Capture Stats
Received              : 0
Redirected            : 0
Dropped              : 0

<snipped>

PPP Capture Stats
Received              : 0
Redirected            : 0
Dropped              : 0

Rtr-Sol Capture Stats
Received              : 0
Redirected            : 0
Dropped              : 0
-----
Sap per Queue stats
-----
                Packets                Octets
No entries found
=====
A:BNG#

```

Note that the dropped packets are those that are non triggering packets. Also, there are no SAP queues instantiated for a capture SAP.

## Configuration Scenario — Routed CO/VLAN-Per-Subscriber (PPPOE)

The following output shows a Routed CO configuration example.

```

configure service vprn 2
  route-distinguisher 65000:2
  subscriber-interface "sub-int-1" create
  address 10.255.255.254/8
  group-interface "group-int-1" create
  description "ROUTED CO MSAP VLAN X"
  authentication-policy "authentication-1"
  pppoe
    session-limit 2000
    no shutdown
  exit
exit
exit
no shutdown
exit

```

Note that the number of PPPoE sessions can be controlled under a group interface by applying the **pppoe session-limit** command.

Initially, since no MSAPs are present, the operational state of both the subscriber interface and group interface context are down.

```

*A:BNG# show router 2 interface
=====
Interface Table (Service: 2)
=====
Interface-Name          Adm      Opr (v4/v6)  Mode      Port/SapId
  IP-Address            PfxState
-----
group-int-1             Up       Down/Down   VPRN G*   n/a
sub-int-1               Up       Down/Down   VPRN S*   subscriber
  10.255.255.254/8
                                     n/a
-----
Interfaces : 2
=====
* indicates that the corresponding row element may have been truncated.
*A:BNG#

```



To allow the subscriber interface to consider this group interface to be operationally enabled without any active SAPs, the following command can be added to the configuration (this would be useful in order to propagate the subnet interface address into a routing protocol) :

```
configure service vprn 2
    subscriber-interface "sub-int-1" create
        group-interface "group-int-1" create
            oper-up-while-empty
```

```
*A:BNG# show router 2 interface
```

```
=====
Interface Table (Service: 2)
=====
```

Interface-Name IP-Address	Adm	Opr (v4/v6)	Mode	Port/SapId PfxState
group-int-1	Up	Down/Down	VPRN G*	n/a
sub-int-1 10.255.255.254/8	Up	Up/Down	VPRN S*	subscriber n/a

```
-----
Interfaces : 2
=====
```

\* indicates that the corresponding row element may have been truncated.

```
*A:BNG#
```

Note the status of the group interface once the first MSAP is created.

## Configure RADIUS User Files

The following entry is an example of a user entry in a RADIUS users file for FreeRadius server.

```
"user1@ISP1.com"      Cleartext-Password := "user1_pass"
                      Alc-Subsc-ID-Str := "%{ADSL-Agent-Remote-Id}",
                      Alc-SLA-Prof-Str == "sla-profile-2M",
                      Alc-MSAP-Serv-ID = 2,
                      Alc-MSAP-Policy == "msap-ISP1",
                      Alc-MSAP-Interface == "group-int-1",
                      Framed-IP-Address = 10.255.0.1,
                      Alc-Primary-DNS = 67.138.54.100,
                      Alc-Secondary-DNS = 207.225.209.66
```

So when the PPPoE user sends the correct username and password, the RADIUS will accept the access message and returns the correct VPRN service id 2, the correct group interface group-int-1 the MSAP policy to use msap-ISP1.

In case there are no MSAP policy returned from RADIUS, the default MSAP policy sap-default under the capture SAP will be used instead.

In the above entry, the PPPoE user will have its IP address and DNS assigned by RADIUS as well. The DNS values are examples for public Free DNSs.

## Connect PPPoE “user1”

Connect PPPoE user1, initiate a PPPoE session on VLAN 1 and verify PPPoE session establishment.

```
*A:BNG# show service id 2 pppoe session
=====
PPPoE sessions for svc-id 2
=====
Sap Id          Mac Address      Sid   Up Time          Type
  IP/L2TP-Id/Interface-Id          MC-Stdby
-----
[1/2/2:1]      00:00:86:1c:79:a1 1     0d 00:00:29     local
  10.255.0.1
-----
Number of sessions : 1
=====
*A:BNG#
```

The PPPoE session is established successfully and the user obtained the IP and subscriber strings from the RADIUS server.

In order to differentiate between the MSAP and the normal SAP, the MSAP will be shown between square brackets [1/2/2:1] in the show commands

## Verify Subscriber Values

Verify subscriber values returned from RADIUS for user1.

```
*A:BNG# show service id 2 pppoe session ip-address 10.255.0.1 detail
=====
PPPoE sessions for svc-id 2
=====
Sap Id          Mac Address      Sid  Up Time      Type
  IP/L2TP-Id/Interface-Id          MC-Stdby
-----
[1/2/2:1]      00:00:86:1c:79:a1 1    0d 00:00:42  local
  10.255.0.1

LCP State       : Opened
IPCP State      : Opened
IPv6CP State    : Initial
PPP MTU         : 1492
PPP Auth-Protocol : CHAP
PPP User-Name   : user1@ISP1.com

Subscriber-interface : sub-int-1
Group-interface     : group-int-1

IP Origin        : radius
DNS Origin       : radius
NBNS Origin      : none

Subscriber       : "user1"
Sub-Profile-String : ""
SLA-Profile-String : "sla-profile-2M"
ANCP-String      : ""
Int-Dest-Id      : ""
App-Profile-String : ""
Category-Map-Name : ""
Acct-Session-Id  : "EA4BFF00000000532AD1CD"
Sap-Session-Index : 1

IP Address       : 10.255.0.1/32
Primary DNS      : 67.138.54.100
Secondary DNS    : 207.225.209.66
Primary NBNS     : N/A
Secondary NBNS   : N/A
Address-Pool     : N/A

IPv6 Prefix      : N/A
IPv6 Prefix Origin : none
IPv6 Prefix Pool : ""
IPv6 Del.Pfx.    : N/A
IPv6 Del.Pfx. Origin : none
IPv6 Del.Pfx. Pool : ""
IPv6 Address     : N/A
IPv6 Address Origin : none
IPv6 Address Pool : ""
Primary IPv6 DNS : N/A
Secondary IPv6 DNS : N/A
```

Circuit-Id : DSLAM1\_1/1/1/1:0.35  
Remote-Id : user1

Radius Session-TO : N/A  
Radius Class :  
Radius User-Name : user1@ISP1.com  
Logical-Line-Id :  
Service-Name :

-----  
Number of sessions : 1  
=====

\*A:BNG#

## Check the Actual Values

Check the actual values used by user1, subscriber profile, SLA profile, VPRN and group interface association, the subscriber queues statistics and others.

```
*A:ENG# show service active-subscribers subscriber "user1" detail
=====
Active Subscribers
=====
-----
Subscriber user1 (sub-profile-default)
-----
I. Sched. Policy : N/A
E. Sched. Policy : N/A
E. Agg Rate Limit: Max
I. Policer Ctrl. : N/A
E. Policer Ctrl. : N/A
Q Frame-Based Ac*: Disabled
Acct. Policy      : N/A
Collect Stats    : Disabled
Rad. Acct. Pol.  : accounting-1
Dupl. Acct. Pol. : N/A
ANCP Pol.        : N/A
HostTrk Pol.     : N/A
IGMP Policy      : N/A
MLD Policy       : N/A
Sub. MCAC Policy : N/A
NAT Policy       : N/A
Def. Encap Offset: none
Encap Offset Mode: none
Avg Frame Size   : N/A
Vol stats type   : full
Preference       : 5
Sub. ANCP-String : "user1"
Sub. Int Dest Id : ""
Icmp Rate Adj    : N/A
RADIUS Rate-Limit: N/A
Oper-Rate-Limit  : Maximum
* indicates that the corresponding row element may have been truncated.
-----
(1) SLA Profile Instance
    - sap:[1/2/2:1] (VPRN 2 - group-int-1)
    - sla:sla-profile-2M
-----
Description      : (Not Specified)
Host Limit       : No Limit
Egr Sched-Policy : N/A
Ingress Qos-Policy : 50
Egress Qos-Policy : 50
Ingress Queuing Type : Shared-queuing (Not Applicable to Policer)
Ingr IP Fltr-Id   : N/A
Egr IP Fltr-Id    : N/A
Ingr IPv6 Fltr-Id : N/A
Egr IPv6 Fltr-Id  : N/A
Ingress Report-Rate : Maximum
Egress Report-Rate : Maximum
Egress Remarking   : from SLA Profile Qos
Credit Control Pol. : N/A
Category Map       : (Not Specified)
Use ing L2TP DSCP  : false
-----
IP Address
```

```

-----
MAC Address          PPPoE-SID Origin
-----
10.255.0.1          00:00:86:1c:79:a1 1      IPCP
-----

```

-----  
SLA Profile Instance statistics  
-----

	Packets	Octets
Off. HiPrio	: 0	0
Off. LowPrio	: 0	0
Off. Uncolor	: 0	0
Off. Managed	: 0	0

Queueing Stats (Ingress QoS Policy 50)

Dro. HiPrio	: 0	0
Dro. LowPrio	: 0	0
For. InProf	: 0	0
For. OutProf	: 0	0

Queueing Stats (Egress QoS Policy 50)

Dro. InProf	: 0	0
Dro. OutProf	: 0	0
For. InProf	: 0	0
For. OutProf	: 1	64

-----  
SLA Profile Instance per Queue statistics  
-----

	Packets	Octets
Ingress Queue 1 (Unicast) (Priority)		
Off. HiPrio	: 0	0
Off. LowPrio	: 0	0
Dro. HiPrio	: 0	0
Dro. LowPrio	: 0	0
For. InProf	: 0	0
For. OutProf	: 0	0

Egress Queue 1

Dro. InProf	: 0	0
Dro. OutProf	: 0	0
For. InProf	: 0	0
For. OutProf	: 1	64

-----  
\*A:BNG#

Where, the subscriber id is **user1**, subscriber profile is sub-profile-default (note that the RADIUS did not return subscriber profile string, so the system will use the **def-sub-profile** configured under the msap-policy msap-ISP1.

Another command can also be used to show less detail in a hierarchical form.

```

*A:BNG# show service active-subscribers hierarchy subscriber "user1"
=====

```

## Check the Actual Values

```
Active Subscriber hierarchy
=====
-- user1 (sub-profile-default)
|
|-- sap:[1/2/2:1] - sla:sla-profile-2M
| |
| |-- 10.255.0.1
| |   00:00:86:1c:79:a1 - 1 (IPCP)
| |
|
=====
*A:BNG#
```



Verify that the IPv4 state of the group interface is now up.

```
*A:BNG# show router 2 interface
=====
Interface Table (Service: 2)
=====
Interface-Name      Adm      Opr (v4/v6)  Mode      Port/SapId
  IP-Address                               PfxState
-----
group-int-1         Up       Up/Down      VPRN G*   1/2/2
sub-int-1           Up       Up/Down      VPRN S*   subscriber
  10.255.255.254/8                               n/a
-----
Interfaces : 2
=====
* indicates that the corresponding row element may have been truncated.
*A:BNG#
```

Verify the capture service id (VPLS), capture SAP and the msap policy used to created user1 and the SAP sub type.

```
*A:BNG# show service id 2 sap 1/2/2:1 detail
=====
Service Access Points(SAP)
=====
Service Id          : 2
SAP                 : 1/2/2:1          Encap           : q-tag
Description         : Managed SAP - Capture Svc 1 1/2/2:*
Admin State         : Up              Oper State      : Up
Flags               : None
Multi Svc Site      : None
Last Status Change : 03/20/2014 11:28:08
Last Mgmt Change   : 03/20/2014 11:32:29
Sub Type            : managed
Capture Service Id : 1              Capture SAP     : 1/2/2:*
MSAP Policy         : msap-ISPL
Dot1Q Ethertype    : 0x8100          QinQ Ethertype  : 0x8100
Split Horizon Group: (Not Specified)

<snip>
-----
Sap per Queue stats
-----
Packets      Octets
-----
No entries found
=====
*A:BNG#
```

The sub type shows managed for MSAPs, whereas regular for normal saps ( a SAP created manually under a group-interface).

## MSAP with Redundant Configurations

MSAPs are High Availability (HA) enabled (there is no service impact following a CPM failover). In addition, the MSAPs are also stored in the subscriber management persistence file (if enabled), allowing the MSAPs to be recreated after a reboot.

MSAPs can be used in dual-homed BNG scenarios with multi-chassis LAG, multi-chassis ring and subscriber router redundancy protocol.

### MSAP QoS Notes

An MSAP is always created with default QoS policies.

```
*A:BNG# show service id 2 sap 1/2/2:1 detail
=====
Service Access Points(SAP)
=====
Service Id      : 2
SAP             : 1/2/2:1          Encap           : q-tag
Description    : Managed SAP - Capture Svc 1 1/2/2:*
Admin State    : Up              Oper State      : Up

<snip>
-----
QoS
-----
Ingress qos-policy : 1          Egress qos-policy : 1
Ingress FP QGrp   : (none)      Egress Port QGrp  : (none)
Ing FP QGrp Inst  : (none)      Egr Port QGrp Inst: (none)
Shared Q plcy    : default      Multipoint shared : Disabled
I. Sched Pol     : (Not Specified)
E. Sched Pol     : (Not Specified)
I. Policer Ctl Pol : (Not Specified)
E. Policer Ctl Pol : (Not Specified)
-----
Subscriber Management
-----
Admin State      : Up          MAC DA Hashing   : False
Def Sub-Id      : Use sap-id (1/2/2:1)
Def Sub-Profile  : sub-profile-default
Def SLA-Profile  : sla-profile-512K

<snip>
=====
*A:BNG#
```

## QoS Egress Remarking

In order to have remarking for egress traffic for MSAP taken from SLA profile, use **no qos-marking-from-sap** command.

```
configure subscriber-mgmt
...
sla-profile "sla-profile-512K" create
  ingress
    qos 30 shared-queuing
    exit
  exit
  egress
    qos 30
    exit
    no qos-marking-from-sap
  exit
exit
```

By default, the egress QoS marking for subscriber-host traffic is derived from the SAP-egress QoS policy associated with the corresponding SAP rather than the SLA profile associated with the corresponding subscriber-host. As a consequence, no egress QoS marking (for example, dot1p marking was set to 0, DSCP/PREC field is unchanged) is performed for traffic transmitted on an MSAP because per default, SAP-egress policy one (1) was attached to every MSAP.

## Queue Optimization

Shared queuing can be used to optimize queues on ingress direction.

```
configure subscriber-mgmt
...
sla-profile "sla-profile-512K" create
  ingress
    qos 30 shared-queuing
  exit
exit
```

The SAP queues will not be instantiated when using the following option in the msap-policy.

```
configure subscriber-mgmt
  msap-policy "msap-ISP1" create
    sub-sla-mgmt
      single-sub-parameters
        profiled-traffic-only
      exit
    exit
  exit
```

## Configuration Tips

The authentication policy used in the capture SAP must be the same as the policy used for the managed SAP.

The managed SAP will not be created if the group-interface name returned from RADIUS points to a different authentication policy other than the policy defined by the capture SAP.

```
configure
  service
    vpls 1
      --- snip ---
      sap 1/2/2:* capture-sap create
      --- snip ---
      authentication-policy "authentication-1"
    exit
  no shutdown
exit
```

```
configure
  service
    vprn 2
      subscriber-interface "sub-int-1" create
      --- snip ---
      group-interface "group-int-1" create
      authentication-policy "authentication-2"
      --- snip ---
    exit
  no shutdown
exit
```

This can be seen in log 99:

```
84 2014/03/20 11:35:37.80 UTC WARNING: PPPOE #2001 Base PPPoE session failure
"PPPoE session failure on SAP 1/2/2:* in service 1 - [00:00:86:1c:79:a1,1,user1@ISP1.com]
MSAP group-interface "group-int-1" RADIUS auth-policy "authentication-2" differs from cap-
ture SAP"
```

```
83 2014/03/20 11:35:37.80 UTC MINOR: SVCMMGR #2214 Base Managed SAP creation failure
"The system could not create Managed SAP:1/2/2:1, MAC:00:00:86:1c:79:a1, Capturing SAP:1/
2/2:*, Service:1. Description: MSAP group-interface "group-int-1" RADIUS auth-policy
"authentication-2" differs from capture SAP"
```

On the 7750 SR, enable debug for PPPoE and RADIUS packets to help in case there is a problem in session establishment:

```
debug
  router "management"
  radius
    packet-type authentication accounting coa
```

## Queue Optimization

```
        detail-level medium
    exit
exit
service
    id 1
        ppp
            packet
                mode egr-ingr-and-dropped
                detail-level medium
                discovery
                ppp
            exit
        exit
    exit
    id 2
        ppp
            packet
                mode egr-ingr-and-dropped
                detail-level medium
                discovery
                ppp
                dhcp-client
            exit
        exit
    exit
exit
exit
```

```
configure
log
    log-id 1
        from debug-trace
        to session
    exit
exit
exit
```

Disconnect/connect user1 then check the RADIUS access request/accept and accounting messages from the debug output.

```
14 2014/03/20 12:38:42.04 UTC MINOR: DEBUG #2001 management RADIUS
"RADIUS: Transmit
  Access-Request(1) 172.31.117.84:1812 id 26 len 184 vrid 4095 pol authenticatio
n-1
  USER NAME [1] 14 user1@ISP1.com
  NAS IP ADDRESS [4] 4 172.31.117.75
  SERVICE TYPE [6] 4 Framed(2)
  FRAMED PROTOCOL [7] 4 PPP(1)
  CHAP PASSWORD [3] 17 1 0xb54dcb79d5de3fd6cff4ad7b98ac3598
  CHAP CHALLENGE [60] 51 0xa52131167c5ff2adef841422767b7acb458de8c95c2bf2c7185
8fe09a1794f471a80dd975f50c44fd4d8f0cb54ea9719f781e2
  VSA [26] 7 DSL(3561)
    AGENT REMOTE ID [2] 5 user1
  NAS PORT TYPE [61] 4 PPPoEoVLAN(33)
  NAS PORT ID [87] 7 1/2/2:1
  NAS IDENTIFIER [32] 3 BNG
  VSA [26] 19 Alcatel(6527)
```

```

CHADDR [27] 17 00:00:86:1c:79:a1
"
15 2014/03/20 12:38:42.04 UTC MINOR: DEBUG #2001 management RADIUS
"RADIUS: Receive
  Access-Accept(2) id 26 len 133 from 172.31.117.84:1812 vrid 4095 pol authentic
ation-1
    VSA [26] 7 Alcatel(6527)
      SUBSC ID STR [11] 5 user1
    VSA [26] 16 Alcatel(6527)
      SLA PROF STR [13] 14 sla-profile-2M
    VSA [26] 6 Alcatel(6527)
      MSAP SERVICE ID [31] 4 2
    VSA [26] 11 Alcatel(6527)
      MSAP POLICY [32] 9 msap-ISP1
    VSA [26] 13 Alcatel(6527)
      MSAP INTERFACE [33] 11 group-int-1
    FRAMED IP ADDRESS [8] 4 10.255.0.1
    VSA [26] 6 Alcatel(6527)
      PRIMARY DNS [9] 4 67.138.54.100
    VSA [26] 6 Alcatel(6527)
      SECONDARY DNS [10] 4 207.225.209.66
" "

```

The 7750 sends also accounting request message to the RADIUS accounting server.

```

23 2014/03/20 12:38:42.11 UTC MINOR: DEBUG #2001 management RADIUS
"RADIUS: Transmit
  Accounting-Request(4) 172.31.117.84:1813 id 15 len 200 vrid 4095 pol accountin
g-1
    STATUS TYPE [40] 4 Start(1)
    NAS IP ADDRESS [4] 4 172.31.117.75
    USER NAME [1] 14 user1@ISP1.com
    SERVICE TYPE [6] 4 Framed(2)
    FRAMED PROTOCOL [7] 4 PPP(1)
    FRAMED IP ADDRESS [8] 4 10.255.0.1
    NAS IDENTIFIER [32] 3 BNG
    SESSION ID [44] 22 EA4BFF0000000E532AE152
    EVENT TIMESTAMP [55] 4 1395319122
    NAS PORT TYPE [61] 4 PPPoEoVLAN(33)
    NAS PORT ID [87] 7 1/2/2:1
    VSA [26] 28 DSL(3561)
      AGENT CIRCUIT ID [1] 19 DSLAM1_1/1/1/1:0.35
      AGENT REMOTE ID [2] 5 user1
    VSA [26] 44 Alcatel(6527)
      SUBSC ID STR [11] 5 user1
      SUBSC PROF STR [12] 19 sub-profile-default
      SLA PROF STR [13] 14 sla-profile-2M
"

```

After 10 mins (update interval) the 7750 sends accounting Interim updates with the same session ID including the counter values for total input and output octets/packets for user1.

```

25 2014/03/20 12:48:47.65 UTC MINOR: DEBUG #2001 management RADIUS
"RADIUS: Transmit
  Accounting-Request(4) 172.31.117.84:1813 id 16 len 230 vrid 4095 pol accountin
g-1

```

## Queue Optimization

```
STATUS TYPE [40] 4 Interim-Update(3)
NAS IP ADDRESS [4] 4 172.31.117.75
USER NAME [1] 14 user1@ISP1.com
SERVICE TYPE [6] 4 Framed(2)
FRAMED PROTOCOL [7] 4 PPP(1)
FRAMED IP ADDRESS [8] 4 10.255.0.1
NAS IDENTIFIER [32] 3 BNG
SESSION ID [44] 22 EA4BFF0000000E532AE152
SESSION TIME [46] 4 606
EVENT TIMESTAMP [55] 4 1395319727
NAS PORT TYPE [61] 4 PPPoEoVLAN(33)
NAS PORT ID [87] 7 1/2/2:1
VSA [26] 28 DSL(3561)
  AGENT CIRCUIT ID [1] 19 DSLAM1_1/1/1/1:0.35
  AGENT REMOTE ID [2] 5 user1
VSA [26] 44 Alcatel(6527)
  SUBSC ID STR [11] 5 user1
  SUBSC PROF STR [12] 19 sub-profile-default
  SLA PROF STR [13] 14 sla-profile-2M
INPUT PACKETS [47] 4 0
INPUT OCTETS [42] 4 0
OUTPUT PACKETS [48] 4 11
OUTPUT OCTETS [43] 4 704
"

26 2014/03/20 12:48:47.65 UTC MINOR: DEBUG #2001 management RADIUS
"RADIUS: Receive
  Accounting-Response(5) id 16 len 20 from 172.31.117.84:1813 vrid 4095 pol acco
unting-1
" "
```

To verify the MSAP policies and associations of MSAPs created, use the following commands:

```
*A:BNG# show subscriber-mgmt msap-policy
=====
Managed SAP Policies
=====
Name                               Num   Description
                                   MSAPs
-----
msap-ISP1                           1     (Not Specified)
msap-default                         0     (Not Specified)
-----
Number of MSAP Policies : 2
Number of MSAPs         : 1
=====
*A:BNG#

*A:BNG# show subscriber-mgmt msap-policy "msap-ISP1" association
=====
MSAP Policy Associations
=====
Service-Id : 2 (VPRN)
- SAP : [1/2/2:1]
-----
Number of associated MSAPs: 1
=====
*A:BNG#
```



To check all MSAPs created and associations to services.

```
*A:BNG# show service sap-using msap
=====
Service Access Points
=====
PortId                               SvcId      Ing. Ing.  Egr. Egr.  Adm  Opr
                               QoS  Fltr  QoS  Fltr
-----
[1/2/2:1]                             2          1   none  1   none  Up   Up
-----
Number of SAPs : 1
-----
Number of Managed SAPs : 1, indicated by [<sap-id>]
-----
=====
*A:BNG#
```

It is possible to use a **tools** command to update an existing MSAP when a specific msap-policy has changed.

```
A:BNG-1# tools perform subscriber-mgmt eval-msap ?
  - eval-msap { policy <msap-policy-name< | msap <sap-id> }

<msap-policy-name>      : [32 chars max]
<sap-id>                 : <port-id|lag-id>:qtag1
                           <port-id|lag-id>:qtag1.qtag2
```

To delete an MSAP.

```
A:BNG-1# clear service id 2 msap 1/2/2:1

166 2014/03/20 11:48:21.39 UTC INDETERMINATE: LOGGER #2010 Base Clear SVCMMGR
"Clear function clearSvcIdMsap has been run with parameters: svc-id="2" sap-id="1/2/2:1".
The completion result is: success. Additional error text, if any, is: "
```

To delete all MSAPs associated with a certain MSAP policy use the following command:

```
A:BNG-1# clear service id 2 msap-policy msap-ISPl

168 2014/03/20 11:48:32.15 UTC INDETERMINATE: LOGGER #2010 Base Clear SVCMMGR
"Clear function clearSvcIdMsapPly has been run with parameters: svc-id="2" policy-
name="msap-ISPl". The completion result is: success. Additional error text, if any, is: "
```

## Conclusion

MSAP allows dynamic creation of SAPs which results in:

- Less provisioning.
- Less possibility for introducing provisioning errors.
- Reduced configuration file.