

DYNAMIC PROVISIONING OF SUBSCRIBERS ON ALCATEL-LUCENT PLATFORM IP EDGE DEVICES BASED ON AUTHENTICATION SOLUTION USING OPEN SOURCE RADIUS IMPLEMENTATION

MINT 709 CAPSTONE PROJECT REPORT

APRIL 2015

BIKRAMJEET SHARMA

MSc Internetworking

Supervisor: Pete Nanda

Abstract

The solution implemented in this project focuses on fast and reliable provisioning of subscriber hosts using Circuit-ID sub-option of DHCP. This project works on the principles of DHCP relay. Triple Play for enhanced subscriber management knowledge is required to understand the working of this project.

This solution reduces the burden of provisioning subscribers manually. Service Level Agreement profiles can be shared by more than one hosts at a time. Different quality of Service policies can be configured according to the subscriber needs using this project.

TABLE OF CONTENTS

Abstract	2
1 Project Problem Description	6
2 Solution	6
3 Solution Setup	8
3.1 Network Topology	8
3.2 Network Devices and Software	9
3.2.1 Subscriber End	9
3.2.2 Service Provider End	9
4 Test Procedure	10
4.1 Network Diagram with Protocol flow	10
4.2 Network Testing Scenario	11
STEP 1	11
STEP 2	12
STEP 3	14
STEP 4	16
STEP 5	20
STEP 6	21
STEP 7	22
5 Issues and challenges	25
6 Result Analysis	26

7 Conclusion.....	30
8 Appendices and References	31
Appendix A – Technologies used in the project	32
8.1 DHCP Snooping	32
8.1.1 DHCP Snooping option-82 insertion	32
8.1.2 Sub-option Circuit-ID	32
8.2 SLA Profile	32
8.3 Managed Service Access Point.....	33
8.4 Capture SAP	34
8.5 Internet Enhanced Service	35
8.6 MPLS	35
8.6.1 Label Edge Router	35
8.6.2 Label Distribution Protocol	36
8.7 IS-IS	36
8.8 DHCP Relay Agent	38
8.9 RADIUS	38
8.9.1 Radius Based Authorization and Authentication	38
8.9.2 Radius Based Accounting	39
Appendix B – Configuration of Network Devices	40

LIST OF FIGURES

Figure 1: DHCP Discover, DHCP offer & Access-Request	6
Figure 2: DHCP Request and ACK	7
Figure 3: Network Diagram	8
Figure 4: Network Diagram with protocol flow	10
Figure 5: Sub-option Circuit-ID	32
Figure 6: SLA profile determining	33
Figure 7: Capture SAP	34
Figure 8: Internet Enhanced Service	35
Figure 9: IS-IS routing domain example	36
Figure 10: IS-IS functionality	37
Figure 11: Radius Authentication and Authorization flow	38

1 Project Problem Description

The larger goal of this project is to achieve dynamic provisioning of subscribers. Which will include authentication of subscribers using circuit-id sub-option of DHCP option-82 as the user identification parameter. RADIUS (Remote Authentication and Dial in User Service) protocol principles should be followed for authenticating the subscriber and after authentication the subscriber should get assigned with a Managed - Subscriber SAP (Service Access Point), QoS policies and SLAs (Service Level Agreements).

2 Solution

DHCP Snooping is enabled on the subscriber side which adds OPTION 82 sub-options (Circuit-ID) on the DHCP Discover packet. When the DHCP discover packet reaches at the Provider Edge where radius authentication is enabled. The Provider Edge router holds the DHCP discover message and sends an Access-Request to Freeradius Server, after looking at authentication policy created on router. When the request reaches at freeradius server, MYSQL database is checked and the subscriber is authenticated looking at the Circuit-ID sub-option. After authentication Access-Accept message is forwarded to the Provider Edge router.

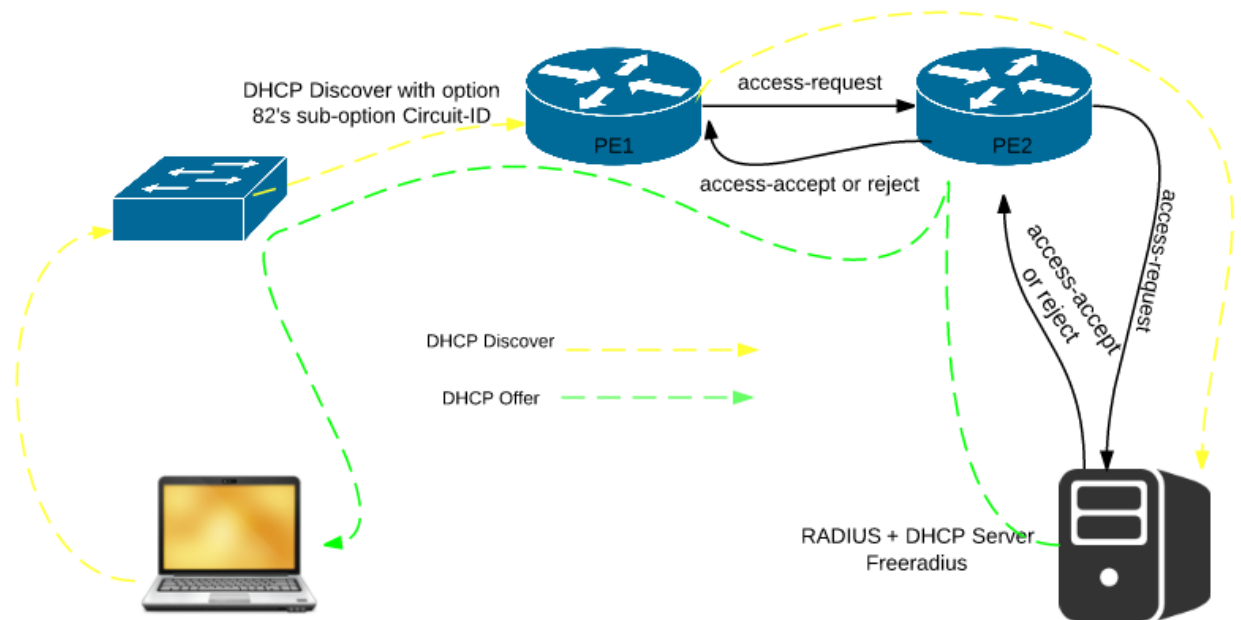


Figure 1: DHCP Discover, DHCP offer & Access-Request

When the subscriber gets authenticated, then authentication along with service context of this request creates a Managed-Service Access Point. Subscriber is then assigned QoS policies and SLA profiles.

PE router now forwards the DHCP Discover message to the DHCP server. DHCP Server looks at the DHCP Discover message and sends the DHCP offer message with an IP address to the subscriber. Subscriber looks at the DHCP offer and sends a unicast DHCP request message to the DHCP server. The DHCP server then confirms that the IP address is still available and replies to the client with DHCP ACK message.

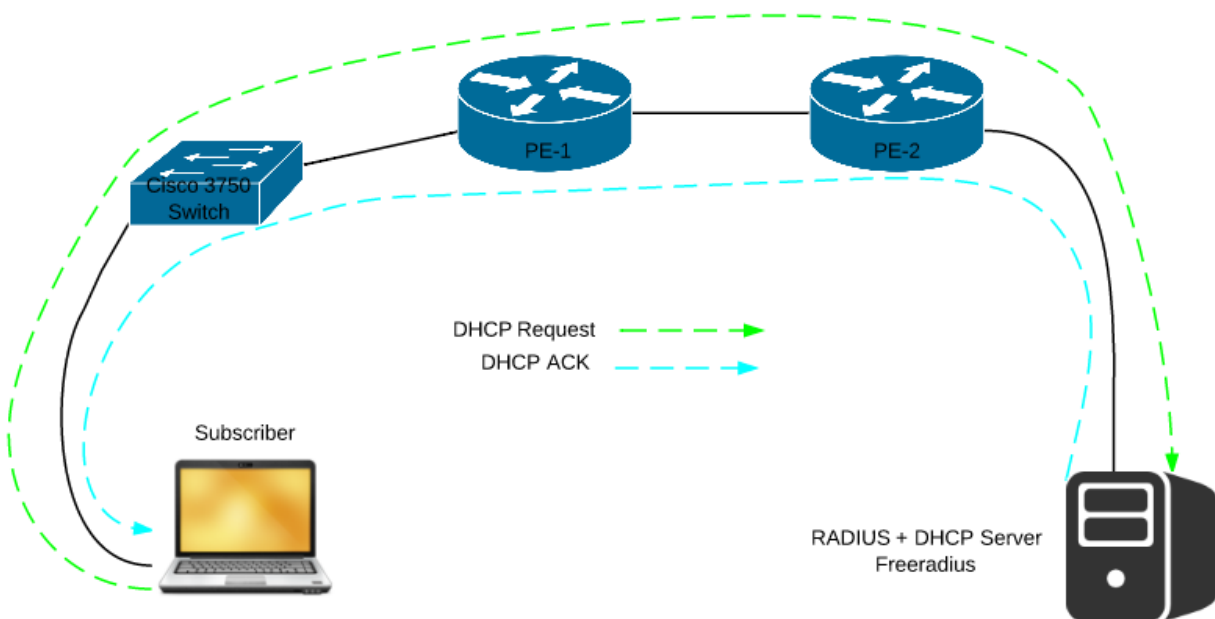


Figure 2: DHCP Request and ACK

This project is basically running with the DHCP relay principle. A DHCP relay agent intercepts broadcast requests and forwards them as a unicast message to the DHCP Server. DHCP relay is practical only in Layer 3 environment, therefore only IES (Internet Enhanced Service) and VPRN (Virtual Private Routed Network) services are supported. This project is implemented using IES service. ISP side is running MPLS/LDP and interior gateway protocol IS-IS along with Radius (Remote Authentication Dial in User Service) Server which supports authentication, authorization

and accounting features for subscribers to connect to a network service. In this network scenario open source RADIUS server Freeradius is used along with DHCP server.

3 SOLUTION SETUP

3.1 Network Topology

The LAB setup for testing and configuration was done in MINT Lab. The network scenario for this project is configured keeping in mind the DHCP relay principles Triple Play network for Enhanced Subscriber Management (ESM). There is one subscriber which can be any of the home devices, e.g. Laptop, Personal Computer, iPhone, Router etc. In this test scenario Laptop is used. Below is the network scenario showing different devices used for this project. A cisco 3750 switch is used on the subscriber side to enable DHCP snooping. Two Alcatel routers are used named as PE-1 and PE-2. PE-1 acts as Broadband Network Gateway (BNG).

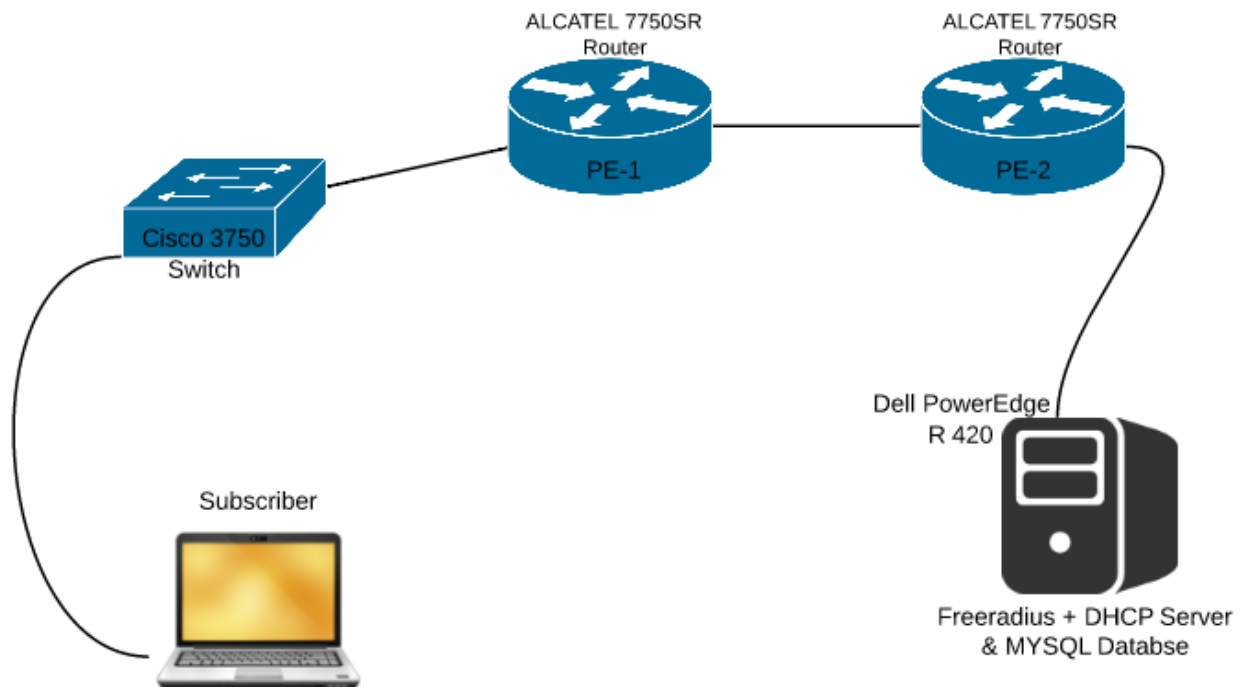


Figure 3: Network Diagram

3.2 Network Devices and Software

Different devices according to their functionality are used on both subscriber and provider end.

3.2.1 Subscriber End

Laptop: laptop is used as a subscriber device for sending DHCP requests.

Cisco 3750 Switch: The switch is used for enabling DHCP snooping. When switch receives DHCP discover message from subscriber device it appends option 82 parameters. Sub-option Circuit-ID in particular for this scenario. This switch was used because it supports DHCP snooping and doesn't have any bugs in its IOS.

3.2.2 Service Provider End

AICATEL 7750SR ROUTERS: Alcatel-Lucent 7750 Service Routers (SR) support enhanced subscriber management features which are required for accomplishment of this project. One of the main features is IES (Internet Enhanced Service). We can run MPLS and interior gateway protocols on these routers, such as IS-IS in this scenario.

Dell PowerEdge 420 Server: This server is being used for installation of VMware esxi 5.5.

VMware esxi 5.5 and vSphere Client: These software were installed for remote access to UBUNTU Server.

UBUNTU Server 14.04.2 LTS: Latest UBUNTU server was used for further installation of open source RADIUS server (Freeradius) and DHCP server.

FreeRADIUS: FreeRADIUS is an open source RADIUS server which is most widely deployed RADIUS server in the world. It supplies the AAA needs of many Fortune-500 and Tier 1 ISPs. It is also widely used in the academic community, including eduroam. The server is fast, modular and scalable.

MySQL: MySQL is the world's second most popular relational database management system and it uses Structured Query Language (SQL). SQL is the language used for adding, accessing and updating contents in the database. SQL is very flexible and reliable with quick processing speed.

The stable release FreeRADIUS version 2.2.6 is installed and configured with DHCP. This version also supports DHCP and can serve DHCP queries form SQL database. It can also act as DHCP relay.

FreeRADIUS is downloaded using the following command

```
wget ftp://ftp.freeradius.org/pub/freeradius/freeradius-server-2.2.0.tar.gz
```

unpacked using the following commands

```
tar -xvzf freeradius-server-2.2.6.tar.gz
```

cd freeradius-server-2.2.6

and configured with DHCP using ./configure --with-dhcp command in the directory.

4 TEST PROCEDURE

4.1 Network Diagram with Protocol flow

The figure clearly depicts the protocol flow with different protocols running on different networking devices according to the network scenario.

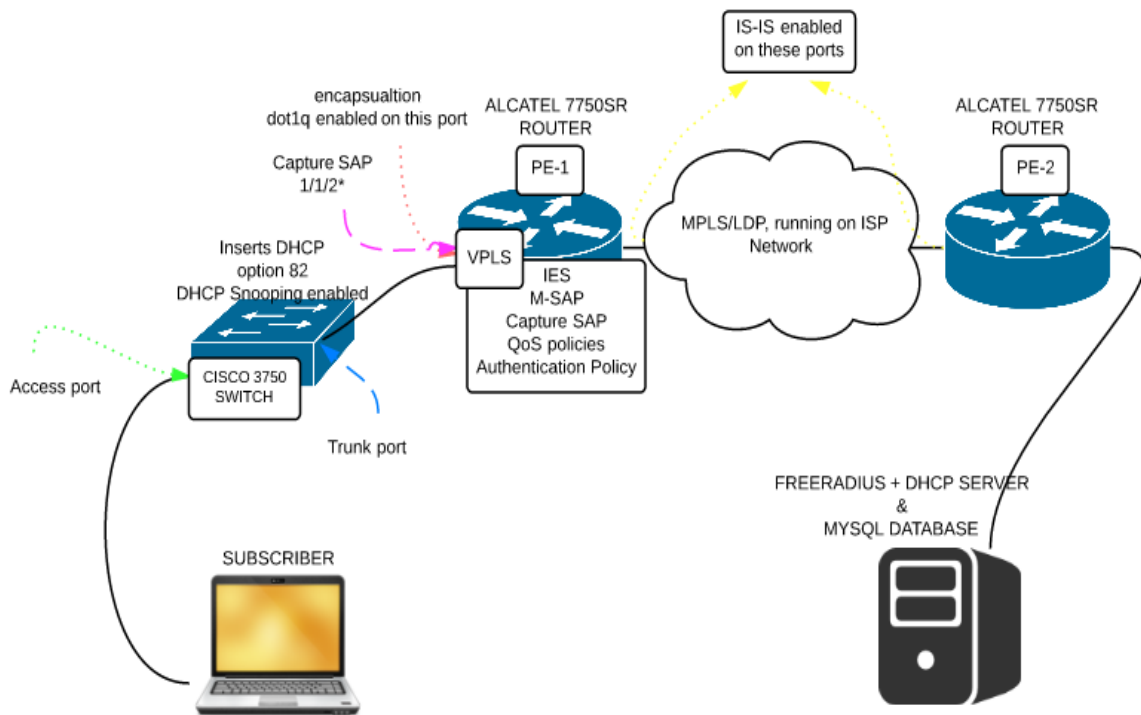


Figure 4: Network Diagram with protocol flow

4.2 Network Testing Scenario

STEP 1

Subscriber host, in this scenario Laptop generates a DHCP Discover message. When it reaches the Cisco 3750 Switch through access port which is inside VLAN 20. Switch appends DHCP option-82 sub-options. IP DHCP Snooping is enabled on the VLAN 20. After this DHCP discover with other packets is forwarded to the Alcatel Provider Edge router through trunk port with dot1q encapsulation enabled.

Here is the output from switch showing DHCP discover message and appending of option-82.

Switch#debug ip dhcp server events

DHCP server event debugging is on.

Switch#

```
*Mar 6 21:53:42.927: DHCPD: checking for expired leases.
*Mar 6 21:53:49.428: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/2, changed state to up
*Mar 6 21:53:49.428: DHCPD: interface GigabitEthernet1/0/2 coming up
*Mar 6 21:53:49.437: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet1/0/2, changed state to up
*Mar 6 21:54:21.297: DHCP Snooping(hl_fm_set_if_input): Setting if_input to Gi1/0/2 for pak. Was
VI20
*Mar 6 21:54:21.297: DHCP Snooping(hl_fm_set_if_input): Setting if_input to VI20 for pak. Was
Gi1/0/2
*Mar 6 21:54:21.297: DHCP Snooping(hl_fm_set_if_input): Setting if_input to Gi1/0/2 for pak. Was
VI20
*Mar 6 21:54:21.297: DHCP_SNOOPING: received new DHCP packet from input interface
(GigabitEthernet1/0/2)
*Mar 6 21:54:21.305: DHCP_SNOOPING: process new DHCP packet, message type:
DHCPDISCOVER, input interface: Gi1/0/2, MAC da: ffff.ffff.ffff, MAC sa: 74d0.2b23.5ff2, IP da:
255.255.255.255, IP sa: 0.0.0.0, DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 0.0.0.0, DHCP siaddr: 0.0.0.0,
DHCP giaddr: 0.0.0.0, DHCP chaddr: 74d0.2b23.5ff2
*Mar 6 21:54:21.305: DHCP_SNOOPING: add relay information option.
*Mar 6 21:54:21.305: DHCP_SNOOPING_SW: Encoding opt82 CID in string format
```

*Mar 6 21:54:21.305: DHCP_SNOOPING_SW: Encoding opt82 RID in MAC address format

*Mar 6 21:54:21.305: DHCP_SNOOPING: binary dump of relay info option, length: 27 data:
0x52 0x19 0x1 0xD 0x1 0xB 0x30 0x30 0x30 0x30 0x66 0x66 0x30 0x30 0x30 0x30 0x30 0x2 0x8
0x0 0x6 0x0 0x18 0x18 0x6E 0x9B 0x0

*Mar 6 21:54:21.305: DHCP_SNOOPING_SW: bridge packet send packet to cpu port: Vlan20.

*Mar 6 21:54:21.305: DHCPD: Sending notification of **DISCOVER**:

*Mar 6 21:54:21.305: DHCPD: htype 1 chaddr 74d0.2b23.5ff2

*Mar 6 21:54:21.305: DHCPD: remote id 00060018186e9b00

*Mar 6 21:54:21.305: **DHCPD: circuit id 010b3030303066663030303030**

*Mar 6 21:54:21.305: DHCPD: interface = Vlan20

*Mar 6 21:54:21.305: DHCPD: class id 4d53465420352e30

*Mar 6 21:54:53.140: DHCP_SNOOP(hlfm_set_if_input): Setting if_input to Gi1/0/2 for pak. Was VI20

*Mar 6 21:54:53.140: DHCP_SNOOP(hlfm_set_if_input): Setting if_input to VI20 for pak. Was Gi1/0/2

*Mar 6 21:54:53.140: DHCP_SNOOP(hlfm_set_if_input): Setting if_input to Gi1/0/2 for pak. Was VI20

*Mar 6 21:54:53.140: DHCP_SNOOPING: received new DHCP packet from input interface (GigabitEthernet1/0/2)

*Mar 6 21:54:53.140: DHCP_SNOOPING: process new DHCP packet, message type: DHCPDISCOVER, input interface: Gi1/0/2, MAC da: ffff.ffff.ffff, MAC sa: 74d0.2b23.5ff2, IP da: 255.255.255.255, IP sa: 0.0.0.0, DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 0.0.0.0,

STEP 2

First of all, to make ALCATEL routers fully functional we need to configure Cards. There can be as many as 12 cards on the largest router of same Alcatel family. In this scenario using Alcatel 7750 SR router we only need to configure one Card. After configuring the card next step is to configure MDA slots. The main purpose of an MDA is to incorporate all circuitry that is particular to a layer 2 connection. At last now ports and interfaces are configured on Alcatel 7750 SR routers. Following are some outputs showing the up status of CARD, MDA and Interfaces.

Sub interfaces are configured in service context of IES. Sub interfaces are a combination of a couple of technologies, subscriber interfaces and group interfaces. Sub interfaces allow sharing of subnets among one or many group interfaces. Whereas, Group interfaces aggregate multiple SAPs on single port.

Following are some outputs showing the up status of card, MDAs, interfaces and sub-interfaces on PE-1 router.

A:PE1# show card

```

=====
=
Card Summary
=====
=
Slot  Provisioned Type          Admin Operational  Comments
      Equipped Type (if different)  State State
-----
1     iom-xp                    up   up
A     cfm-xp                    up   up/active
B     cfm-xp                    up   down/standby
      (not equipped)
=====
=

```

A:PE1# show mda

```

=====
=
MDA Summary
=====
=
Slot Mda  Provisioned Type          Admin  Operational
      Equipped Type (if different)  State  State

```

```
-----  
1 1 c5-1gb-xp-sfp up up  
=====
```

A:PE1# show router interface

```
=====
```

Interface Table (Router: Base)

```
=====
```

Interface-Name	Adm	Opr(v4/v6)	Mode	Port/SapId
group-int-1	Up	Up/Down	IES Grp	n/a
sub-int-1	Up	Up/Down	IES Sub	subscriber
10.1.0.254/24			n/a	
system	Up	Up/Down	Network	system
192.168.2.1/32			n/a	
toPE2	Up	Up/Down	Network	1/1/1
192.168.1.1/30			n/a	

```
-----
```

Interfaces : 4

```
=====
```

STEP 3

The Alcatel PE-1 router, the router that is connected to subscriber switch has dot1q encapsulation enabled on the port facing subscriber end and this port has been configured as access port for allowing access to subscribers to use the SAP associated with this port. Now

Capture SAP (Service Access point) is configured on the PE1 router under the VPLS service context. Capture SAP does not forward the traffic but it triggers RADIUS authentication. A SAP template for the creation of SAPs use of policies is allowed by Managed Service Access Point (MSAP). MSAP policies are configured on PE-1 router along with Service Level Agreements (SLAs). SLAs are created to fulfill different needs of subscribers. QoS policies are configured inside SLAs along with Subscriber Profile, Subscriber Identification Policy and MSAP policy.

Following are some outputs showing encapsulation type on port connected to subscriber and others showing MSAP is up and running after user gets authenticated from RADIUS server and association of Capture sap with MSAP is also shown in the outputs.

A:PE1# show port

```
=====
=
```

Ports on Slot 1

```
=====
=
```

Port Id	Admin State	Link State	Port State	Cfg MTU	Oper MTU	LAG/ Bndl Mode	Port Encp	Port Type	C/QS/S/XFP/ MDIMDX
---------	-------------	------------	------------	---------	----------	----------------	-----------	-----------	--------------------

```
-----
```

1/1/1	Up	Yes	Up	9212	9212	- netw	null	xcme	MDI GIGE-T
1/1/2	Up	Yes	Up	1518	1518	- accs dotq	xcme	MDI	GIGE-T
1/1/3	Up	No	Down	1500	1500	- netw	null	xcme	GIGE-T
1/1/4	Down	No	Down	9212	9212	- netw	null	xcme	GIGE-T
1/1/5	Down	No	Down	9212	9212	- netw	null	xcme	GIGE-T

A:PE1# show subscriber-mgmt msap-policy

```
=====
=
```

Managed SAP Policies

```
=====
=
```

Name Num Description

MSAPs

```
-----  
msap-1          1  (Not Specified)  
msap-default    0  (Not Specified)  
-----
```

Number of MSAP Policies : 2

Number of MSAPs : 1

=====
A:PE1# show subscriber-mgmt msap-policy "msap-1" association

=====
=

MSAP Policy Associations

=====

Service-Id : 2 (IES)

- SAP : [1/1/2:1]

Number of associated MSAPs:1

=====

STEP 4

IES (Internet Enhanced Service) is configured on this Provider Edge (PE1) router for providing access to the subscribers through the router IP interface for sending and receiving traffic over the provider network. Interior Gateway protocol IS-IS is configured to route the traffic along with Multiprotocol Label Switching Protocol (MPLS) on both PE1 and PE2 routers. MPLS makes the packet forwarding a lot simpler by just looking at the packet label which is assigned by the label distribution protocol (LDP).

This project could have been done using static-routes on provider edge also. But to make it more realistic, considering that there are hundreds of routers in real life telecommunication companies

IS-IS and LDP were enabled on the system interfaces and the interfaces between both PE1 and PE2 routers.

Following are some outputs showing that technologies discussed above are working properly.

A:PE1# show router route-table

```
=====
=
```

Route Table (Router: Base)

```
=====
=
```

Dest Prefix[Flags]	Type	Proto	Age	Pref
Next Hop[Interface Name]				Metric
10.1.0.0/24	Local	Local	02d17h17m	0
sub-int-1				0
10.3.31.0/24	Remote	ISIS	02d17h17m	15
192.168.1.2				10
192.168.1.0/30	Local	Local	02d17h17m	0
toPE2				0
192.168.2.1/32	Local	Local	02d17h17m	0
system				0
192.168.3.1/32	Remote	ISIS	02d17h17m	15
192.168.1.2				10

```
-----
```

No. of Routes: 5

Flags: L = LFA nexthop available B = BGP backup route available

n = Number of times nexthop is repeated

```
=====
```

A:PE1# show router isis routes

=====
=

Route Table

=====
=

Prefix[Flags]	Metric	Lvl/Typ	Ver.	SysID/Hostname
NextHop		MT		AdminTag

10.1.0.0/24	20	2/Int.	3	PE2
192.168.1.2		0	0	
10.3.31.0/24	10	1/Int.	3	PE2
192.168.1.2		0	0	
192.168.1.0/30	10	1/Int.	3	PE1
0.0.0.0		0	0	
192.168.2.1/32	0	1/Int.	1	PE1
0.0.0.0		0	0	
192.168.3.1/32	10	1/Int.	3	PE2
192.168.1.2		0	0	

No. of Routes: 5

Flags: L = LFA nexthop available

=====

A:PE1# show router ldp bindings

=====
=

LDP LSR ID: 192.168.2.1

=====
=

Legend: U - Label In Use, N - Label Not In Use, W - Label Withdrawn

S - Status Signaled Up, D - Status Signaled Down

E - Epipe Service, V - VPLS Service, M - Mirror Service

A - Apipe Service, F - Fpipe Service, I - IES Service, R - VPRN service

P - Ipipe Service, WP - Label Withdraw Pending, C - Cpipe Service

BU - Alternate For Fast Re-Route, TLV - (Type, Length: Value)

=====
=

LDP Prefix Bindings

=====
=

Prefix	IngLbl	EgrLbl	EgrIntf/	EgrNextHop
Peer	LspId			
192.168.2.1/32	131071U	--	--	--
192.168.3.1				
192.168.3.1/32	--	131071	1/1/1	192.168.1.2
192.168.3.1				

No. of Prefix Bindings: 2

A:PE1# show router ldp session

```
=====
LDP Sessions
=====
Peer LDP Id    Adj Type  State      Msg Sent  Msg Recv  Up Time
-----
192.168.3.1:0 Link     Established 88134    88138    2d 17:22:23
-----
No. of Sessions: 1
=====
```

A:PE1# show router ldp interface

```
=====
=
LDP Interfaces
=====
=
Interface          Adm Opr  Hello  Hold  KA   KA   Transport
                   Factor Time Factor Timeout Address
-----
toPE2             Up Up 3   15 3   30   System
-----
No. of Interfaces: 1
=====
```

STEP 5

Now we create a layer 3 DHCP relay agent on PE1 in the group-interface where dhcp host will instantiate. DHCP server address is also defined in this group interface. We should make sure that

the DHCP server is in the same routing instance as where subscriber interface is designed. The gateway-IP interface address is defined in here which is usually the subscriber interface ip address. [7]

Here is a configuration of DHCP layer 3 relay agent under IES service context on PE1 router.

```
ies 2 customer 1 create
  subscriber-interface "sub-int-1" create
    description "Routed CO"
    address 10.1.0.254/24
    group-interface "group-int-1" create
      description "Routed CO MSAP"
      dhcp
        server 10.3.31.16
        trusted
        lease-populate 11
        gi-address 10.1.0.254
        no shutdown
      exit
      authentication-policy "authenticate-1"
    exit
  exit
no shutdown
exit
```

STEP 6

Two types of policies are created on the PE1 routers. i.e. RADIUS authentication policy and RADIUS accounting policy. In these policies the address of RADIUS server is defined with a secret. Authentication is done at port 1812 and Accounting in radius is performed at port

number 1813. Both of these ports are defined under authorization and accounting policy on PE1 router respectively. Here is the configuration of both policies.

```
#-----  
echo "Subscriber-mgmt (Service Side) Configuration"  
#-----  
subscriber-mgmt  
    authentication-policy "authenticate-1"  
        radius-authentication-server  
            server 1 address 10.3.31.16 secret "o7NOqMIY6j4gF25OixH4/r3AWJy0yEwo" hash2  
        exit  
    exit  
    radius-accounting-policy "accounting-1"  
        radius-accounting-server  
            server 1 address 10.3.31.16 secret "o7NOqMIY6j4gF25OixH4/r3AWJy0yEwo" hash2  
        exit  
    exit  
    exit  
exit all
```

STEP 7

This step explains about the RADIUS Server configuration and debugging. Radius server is connected with PE2 router as shown in figure 3. The open source version of RADIUS, FreeRADIUS is in scenario as discussed earlier. FreeRADIUS is then configured with DHCP so that it supports all the DHCP features to assign IP address to the host on the subscriber end. At last MYSQL database is configured with Circuit-ID as user name.

Interface eth0 is configured manually by editing the /etc/network/interfaces file.

```
# The loopback interface.
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address 10.3.31.16
gateway 10.3.31.1
netmask 255.255.255.0
network 10.3.31.0
broadcast 10.3.31.255
```

Here is a screenshot of login access to MYSQL database after enabling it through freeradius and defining user as root and group as root.

```
bikram@ubuntu10:~$ sudo bash
root@ubuntu10:~# sudo mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 69
Server version: 5.5.41-0ubuntu0.14.04.1 (Ubuntu)

Copyright (c) 2000, 2014, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> _
```

Path to all the files edited while configuring and setting up FreeRADIUS, DHCP and MYSQL are listed below.

`/etc/network/interfaces`

`/usr/local/etc/raddb/radius.conf`

`/usr/local/etc/raddb/sql.conf`

`/usr/local/etc/raddb/dictionary`

`/usr/local/etc/raddb/sql/mysql/dialup.conf`

`/usr/local/etc/raddb/sql/mysql/schema.sql`

`/usr/local/etc/raddb/sql/mysql/clients.conf`

`/usr/local/etc/raddb/sites-enabled/default`

`/usr/local/etc/raddb/sites-enabled/dhcp_static`

`/usr/local/etc/raddb/sites-available/dhcp`

5 Issues and Challenges

One of the main challenges was to select the right set of protocols on provider and subscriber end. During the initial stages project was built using Virtual Private Routed Network (VPRN), multi-protocol Border Gateway Protocol (mp-BGP) and Open Shortest Path First (OSPF) concepts, which was making the project a lot more complex. But later discussing with Pete Sir, the final changes were made and project was developed using a much simpler approach using Internet Enhanced Service and IS-IS concepts.

Installation of RADIUS server was the most challenging part, during installation a lot of other features were added by doing proper debugging and online help from freeradius and other websites sited in references. One main problem was that the OpenSSL version that comes with Ubuntu had to be removed because it wasn't supported during FreeRADIUS installation. The latest version openssl-1.0.2a was installed which resolved that problem. There were several other problems faced during the installation and configuration which can be resolved with online help.

Another main challenge was using the application of Programmable Subscriber Configuration Policies (PSCP). Python scripts were used for assignment of subscriber and SLA profiles using PSCP. With proper understanding of Python and Enhanced subscriber management principles some of the problems faced during this phase of the project were resolved but not completely.

6 Results Analysis

This section illustrates the results achieved from the real life scenario implemented in the MINT (MSc in Internetworking) Lab.

The main requirement of the network is to authorize the users using Circuit-ID sub-option of Option-82. Which was achieved using the following approach. After the Circuit-ID lookup is done then user is authorized by FreeRADIUS using MYSQL database lookup and then IP address is assigned to the user and according to the different requirements from the user Service Level Agreements and Quality of Service policies can be assigned to the user.

Circuit-ID is lookup is done by debugging the switch using the following command.

Switch# debug ip dhcp server events

```
*Mar 6 21:54:21.305: DHCPD: Sending notification of DISCOVER:
*Mar 6 21:54:21.305: DHCPD: htype 1 chaddr 74d0.2b23.5ff2
*Mar 6 21:54:21.305: DHCPD: remote id 00060018186e9b00
*Mar 6 21:54:21.305: DHCPD: circuit id 010b3030303066663030303030
*Mar 6 21:54:21.305: DHCPD: interface = Vlan20
*Mar 6 21:54:21.305: DHCPD: class id 4d53465420352e30
```

Alcatel router PE1 forwards the Circuit-ID as username, using its own IP address as the source IP address.

Circuit-ID id lookup on the server side can be done by using the following command.

```
bikram@ubuntu10@:~$ sudo tcpdump -vv
```

```
16:28:02.102151 IP (tos 0xc0, ttl 63, id 16625, offset 0, flags [none], proto UDP (17), length 103)
192.168.2.1.64390 > 10.3.31.16.radius: Iudp sum oh] RADIUS, length: 75
Access Request (1), id: 0x37, Authenticator: 59756ca10a3b71462c441ef670fc4c91
Username Attribute (1), length: 15, Value: .0000ff000000
0x0000: 010b 3030 3030 6666 3030 3030 30
Password Attribute (2), length: 18, Value:
0x0000: e8a2 36eb 6e61 fela 6268 f575 5a5c 2b8a
NAS IP Address Attribute (4), length: 6, Value: 192.168.2.1
0x0000: c0a8 0201
NAS Port Type Attribute (61), length: 6, Value: Ethernet
0x0000: 0000 000f
NAS Port ID Attribute (87), length: 10, Value: 1/1/2:20
0x0000: 312f 312f 323a 3230
```

0000ff0000 output in front of the username attribute is the Circuit-ID string Value configured manually using the following command on the access interface where subscriber host is connected.

```
ip dhcp snooping vlan 20 information option format-type circuit-id string 0000ff00000
```

Now, MYSQL database looks up the Circuit-ID and if it matches with the values in its table then user is authenticated and assigned with an IP address further with DHCP.

Following Screenshots show the sql startup to accept queries for authorization and authentication.

```
Module: Linked to module rlm_sql
Module: Instantiating module "sql" from file /usr/local/etc/raddb/sql.conf
sql {
    driver = "rlm_sql_mysql"
    server = "localhost"
    port = ""
    login = "root"
    password = "bikram91"
    radius_db = "radius"
    read_groups = yes
    sqltrace = no
    sqltracefile = "/usr/local/var/log/radius/sqltrace.sql"
    readclients = no
    deletestalesessions = yes
    num_sql_socks = 32
    lifetime = 0
    max_queries = 0
    sql_user_name = "%{User-Name}"
    default_user_profile = ""
    nas_query = "SELECT id, nasname, shortname, type, secret, server FROM nas"
    authorize_check_query = "SELECT id, username, attribute, value, op FROM radcheck"
    authorize_reply_query = "SELECT id, username, attribute, value, op FROM radreply"
    authorize_group_check_query = "SELECT id, groupname, attribute, Value, op
```

User gets authenticated using MYSQL database, gets IP address and further will get assigned MSAP, Service Level Agreements and Quality of Service Polices. These policies are assigned according to the subscriber's requirements.

```
++[preprocess] = ok
++[chap] = noop
++[mschap] = noop
++[digest] = noop
[suffix] No '@' in User-Name = "??0000ff000000", looking up realm NULL
[suffix] No such realm "NULL"
++[suffix] = noop
[eap] No EAP-Message, not doing EAP
++[eap] = noop
[sql] expand: %{User-Name} -> \001\0130000ff000000
[sql] sql_set_user escaped user --> '\001\0130000ff000000'
rlm_sql (sql): Reserving sql socket id: 3
      expand: SELECT id, username, attribute, value, op          FROM radcheck          WHERE
username = '%{SQL-User-Name}'          ORDER BY id -> SELECT id, username, attribute, value, op
FROM radcheck          WHERE username = '\001\0130000ff000000'          ORDER BY id
[sql] User found in radcheck table
      expand: SELECT id, username, attribute, value, op          FROM radreply          WHERE
username = '%{SQL-User-Name}'          ORDER BY id -> SELECT id, username, attribute, value, op
FROM radreply          WHERE username = '\001\0130000ff000000'          ORDER BY id
      expand: SELECT groupname          FROM radusergroup          WHERE username =
'%{SQL-User-Name}'          ORDER BY priority -> SELECT groupname          FROM radusergroup
WHERE username = '\001\0130000ff000000'          ORDER BY priority
rlm_sql (sql): Released sql socket id: 3
++[sql] = ok
++[expiration] = noop
++[logintime] = noop
[pap] Normalizing MD5-Password from hex encoding
++[pap] = updated
Found Auth-Type = PAP
+- entering group PAP {...}
[pap] login attempt with password ""
[pap] Using MD5 encryption.
[pap] User authenticated successfully
++[pap] = ok
```

Switch#dehug ip dhcp server packet

```
*Mar 12 12:11:03.224: DHCP_SNOOPING: process new DHCP packet, message type: DHCPDISCOVER, input interface: Gi1/0/2, MAC da: ffff.ffff.ffff,
ciaddr: 0.0.0.0, DHCP yiaddr: 0.0.0.0, DHCP siaddr: 0.0.0.0, DHCP giaddr: 0.0.0.0, DHCP chaddr: 74d0.2b23.5ff2
*Mar 12 12:11:03.224: DHCP_SNOOPING_SW: bridge packet get invalid mat entry: FFFF.FFFF.FFFF, packet is flooded to ingress VLAN: (20)
*Mar 12 12:11:03.224: DHCP_SNOOP(hlfm_set_if_input): Setting if_input to Gi1/0/1 for pak. Was V120
*Mar 12 12:11:03.224: DHCP_SNOOP(hlfm_set_if_input): Clearing if_input for pak. Was Gi1/0/1
*Mar 12 12:11:03.224: DHCP_SNOOP(hlfm_set_if_input): Setting if_input to Gi1/0/1 for pak. Was V120
*Mar 12 12:11:03.224: DHCP_SNOOPING: received new DHCP packet from input interface (GigabitEthernet1/0/1)
*Mar 12 12:11:03.224: DHCP_SNOOPING: process new DHCP packet, message type: DHCPOFFER, input interface: Gi1/0/1, MAC da: ffff.ffff.ffff, MAC
ciaddr: 0.0.0.0, DHCP yiaddr: 10.1.0.10, DHCP siaddr: 0.0.0.0, DHCP giaddr: 10.1.0.254, DHCP chaddr: 74d0.2b23.5ff2
*Mar 12 12:11:03.224: DHCP_SNOOPING: direct forward dhcp reply to output port: GigabitEthernet1/0/2.
*Mar 12 12:11:03.224: DHCP_SNOOP(hlfm_set_if_input): Setting if_input to Gi1/0/2 for pak. Was V120
*Mar 12 12:11:03.224: DHCP_SNOOP(hlfm_set_if_input): Clearing if_input for pak. Was Gi1/0/2
*Mar 12 12:11:03.224: DHCP_SNOOP(hlfm_set_if_input): Setting if_input to Gi1/0/2 for pak. Was V120
*Mar 12 12:11:03.224: DHCP_SNOOPING: received new DHCP packet from input interface (GigabitEthernet1/0/2)
*Mar 12 12:11:03.224: DHCP_SNOOPING: process new DHCP packet, message type: DHCPREQUEST, input interface: Gi1/0/2, MAC da: ffff.ffff.ffff, MA
ciaddr: 0.0.0.0, DHCP yiaddr: 0.0.0.0, DHCP siaddr: 0.0.0.0, DHCP giaddr: 0.0.0.0, DHCP chaddr: 74d0.2b23.5ff2
*Mar 12 12:11:03.224: DHCP_SNOOPING_SW: bridge packet get invalid mat entry: FFFF.FFFF.FFFF, packet is flooded to ingress VLAN: (20)
*Mar 12 12:11:03.232: DHCP_SNOOP(hlfm_set_if_input): Setting if_input to Gi1/0/1 for pak. Was V120
*Mar 12 12:11:03.232: DHCP_SNOOP(hlfm_set_if_input): Clearing if_input for pak. Was Gi1/0/1
*Mar 12 12:11:03.232: DHCP_SNOOP(hlfm_set_if_input): Setting if_input to Gi1/0/1 for pak. Was V120
*Mar 12 12:11:03.232: DHCP_SNOOPING: received new DHCP packet from input interface (GigabitEthernet1/0/1)
*Mar 12 12:11:03.232: DHCP_SNOOPING: process new DHCP packet, message type: DHCPACK, input interface: Gi1/0/1, MAC da: ffff.ffff.ffff, MAC sa
0.0.0.0, DHCP yiaddr: 10.1.0.10, DHCP siaddr: 0.0.0.0, DHCP giaddr: 10.1.0.254, DHCP chaddr: 74d0.2b23.5ff2
*Mar 12 12:11:03.232: DHCP_SNOOPING: add binding on port GigabitEthernet1/0/2.
*Mar 12 12:11:03.232: DHCP_SNOOPING: added entry to table (index 119)
*Mar 12 12:11:03.232: DHCP_SNOOPING: dump binding entry: Mac=74:D0:2B:23:5F:F2 Ip=10.1.0.10 Lease=86400 Type=dhcp-snooping Vlan=20 If=Gi
*Mar 12 12:11:03.232: DHCP_SNOOPING_SW no entry found for 74d0.2b23.5ff2 0.0.0.20 GigabitEthernet1/0/2
*Mar 12 12:11:03.232: DHCP_SNOOPING_SW host tracking not found for update add dynamic (10.1.0.10, 0.0.0.0, 74d0.2b23.5ff2) vlan 20
*Mar 12 12:11:03.232: DHCP_SNOOPING: direct forward dhcp reply to output port: GigabitEthernet1/0/2.
```

7 Conclusion

This project covered provisioning of home subscribers using open source RADIUS Server, DHCP Server and Alcatel and Cisco technologies. Therefore, it was very important to choose the right devices and right protocols for the implementation of this project. This is a multi-vendor product. As Cisco, Alcatel technologies were used along with Dell PowerEdge 420 Server.

A lot of research was done on understanding ALCATEL 7750 SR routers, because they are very different to configure as compared to Cisco Devices. Understanding of triple play concepts with enhanced subscriber management was very crucial to understand the overall working of the project.

Subscriber host was authenticated from RADIUS server by checking the MYSQL database. After the authentication IP address gets assigned to the subscriber host and host was assigned with a Quality of Service Policy and Service Level agreements.

This project is very lively project based on the services those telecommunication companies are providing to the home users. E.g. Internet services, Home TV services and Voice services. These all services can be provided with the use of different SLAs and Quality of Service features according to the user needs.

This scenario is a very real life implementation scenario. As we know that there are millions of subscribers out there in different countries. This project helps to provision subscribers dynamically which reduces a large amount of work that had to be done if every subscriber had to be assigned statically.

Future research can be done on this project using different technologies. As this project was done on one subscriber host. Virtual Private Routed Network concept can be implemented for authorizing more than one subscribers at a same time. More than one DHCP servers can be allocated. More work can be done on dynamic provisioning of subscriber and SLA profiles using the python scripting language.

Appendices and References

[1] http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/release/12-2_52_se/configuration/guide/3750scg/swdhcp82.html

[2] <https://www.ietf.org/rfc/rfc3046.txt>

[3] https://infoproducts.alcatel-lucent.com/html/0_add-h-f/93-0076-10-01/7750_SR_OS_Services_Guide/services_con_ies.html

[4] https://infoproducts.alcatel-lucent.com/html/0_add-h-f/93-0098-09-01/7750_SR_OS_Triple_Play_Guide/TriplePlay-con-subscr_mgmt.html#446447

[5] en.wikipedia.org/wiki/RADIUS

[6] https://infoproducts.alcatel-lucent.com/html/0_add-h-f/93-0098-09-01/7750_SR_OS_Triple_Play_Guide/concepts_dhcp.html

[7] https://infoproducts.alcatel-lucent.com/html/0_add-h-f/93-0267-HTML/7X50_Advanced_Configuration_Guide/dhcp-hosts.html

[8] https://infoproducts.alcatel-lucent.com/html/0_add-h-f/93-0074-10-01/7750_SR_OS_Routing_Protocols_Guide/ISIS.html

[9] https://infoproducts.alcatel-lucent.com/html/0_add-h-f/93-0267-HTML/7X50_Advanced_Configuration_Guide/MSAP-PPPoE.html#425040

[10] <http://wiki.freeradius.org/guide/SQL-HOWTO>

[11] http://en.wikipedia.org/wiki/Multiprotocol_Label_Switching

[12] <https://www.digitalocean.com/community/tutorials/a-basic-mysql-tutorial>

[13] 7750 SR OS Triple Play Guide – Alcatel Lucent

APPENDIX A – Technologies Used In The Project

DHCP Snooping and its features are described below

8.1 DHCP Snooping

DHCP snooping is basically a security feature that acts like a firewall between untrusted hosts and trusted servers. DHCP snooping feature perform the following activities.

- Validates DHCP messages received from untrusted sources and filters out invalid messages.
- Builds and maintains the DHCP snooping binding database and utilizes binding database to validate subsequent requests from untrusted hosts. [1]

8.1.1 DHCP Snooping option-82 insertion

In residential networks Ethernet-access environments DHCP can centrally manage the IP address assignment for a large number of subscribers. When we enable DHCP snooping, option-82 feature is enabled on the switch, a subscriber device usually is identified by the switch port through which it connects to the network. Multiple hosts on subscriber LAN can be connected to the same port on the access switch and are uniquely identified. [1]

8.1.2 Sub-option Circuit-ID

In our scenario sub-option Circuit-ID is used for subscriber identification which will be inserted on switch. On provider edge user-name format is changed to Circuit-ID and is forwarded to radius server for authentication. Circuit id should be qualified with giaddr value that identifies the relay agent. Circuit ID field can take the sap-id, ifindex, ascii-tuple, vlan-ascii-tuple values.

SubOpt	Len	Circuit ID							
1	n	c1	c2	c3	c4	c5	c6	...	

Figure 5: Sub-option Circuit-ID [2]

8.2 SLA Profile

To provide mobility to the hosts of a single subscriber over the SLA profile at the same time different hosts are subdivided into multiple SLA profiles. . By doing this we ensure that one SLA profile is accessible to all the hosts of a subscriber at the same time. The basic purpose of

subdividing the SLA profile is to provide multiple services like video on demand, broadcast TV, Internet and voice for a particular subscriber. While configuring SLA profiles following settings should be kept in mind.

- Egress and ingress QoS settings
- Egress and ingress IP filters
- Host limit

The figure below shows how SLA profile is derived based on the subscriber identification string:

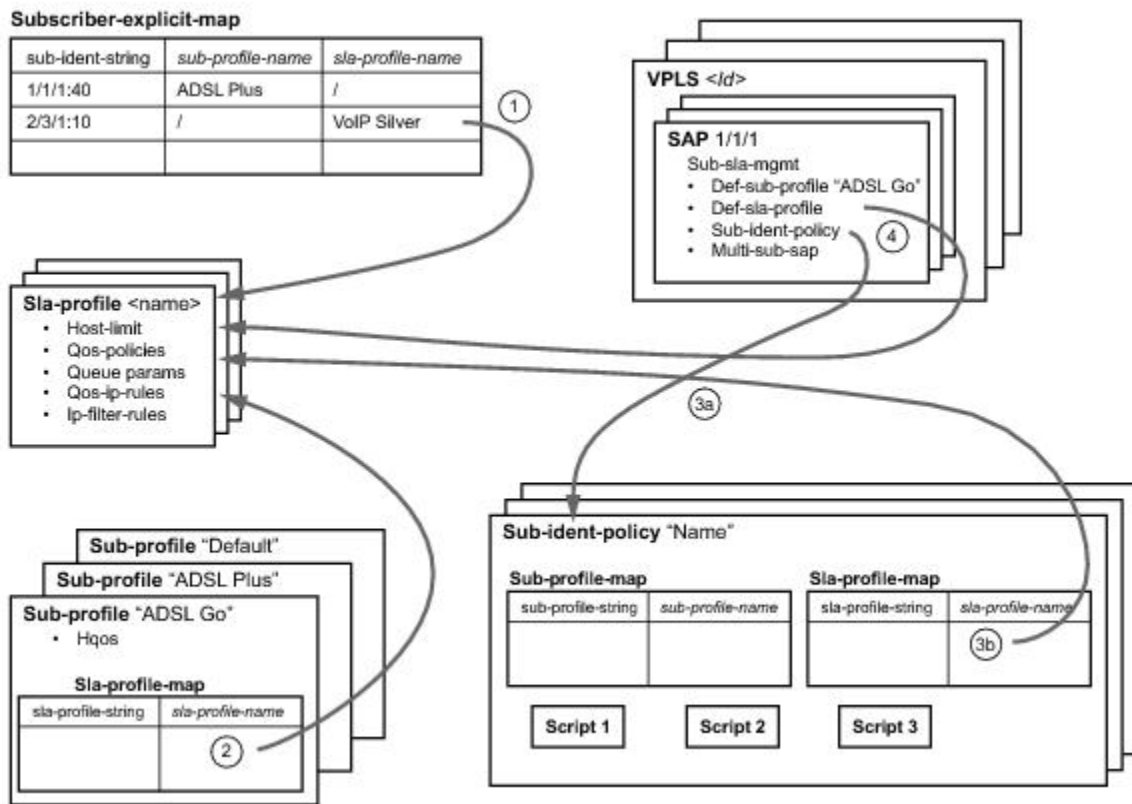


Figure 6: SLA profile determining [4]

8.3 Managed Service Access Point (MSAP)

SAP's creation is triggered when DHCP discover message arrives at the Provider Edge. Managed SAP policy and service ID are the two parameters that contribute toward the creation of a subscriber SAP using default settings those are indicated in Managed SAP. These two parameters

along with host attributes are returned when the host is authenticated. Policy use is allowed by the Managed SAP and it also provides a SAP template for creation of a SAP. [9]

8.4 Capture SAP

A managed SAP and Capture SAP can both co-exist in the same service and on the same port.

A Capture SAP is defined in a very similar way as a default SAP is defined. But traffic forwarding does not occur in case of Capture SAP. The configuration of Capture SAP is not possible on the same port where default SAP is configured. Basic feature of Capture SAP is that it captures the triggering packets and initiate RADIUS authentication. [9]

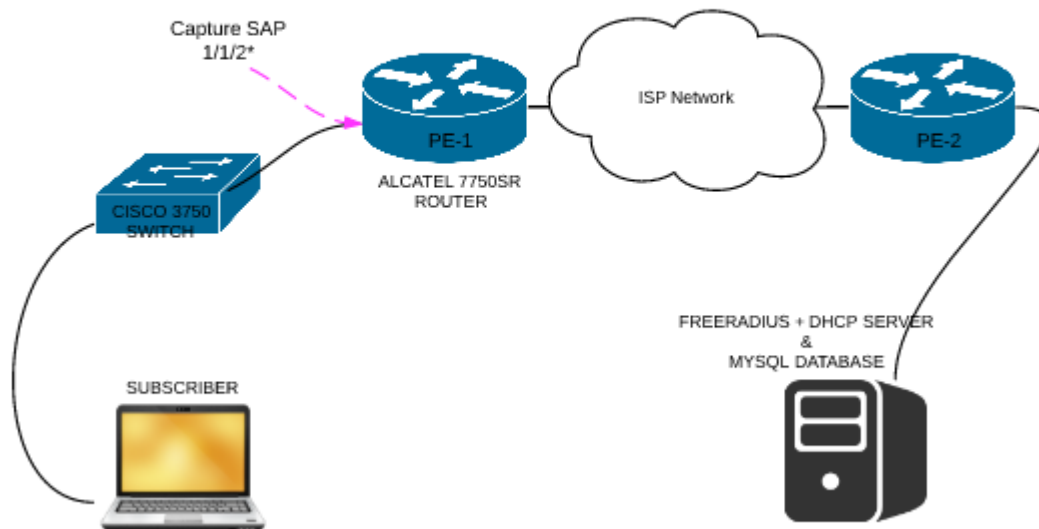


Figure 7: Capture SAP

Capture SAP can be created using any of the following modes.

SAP 1/2/2:* for dot1Q -> This mode is being used in configuration of this scenario.

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

MSAP will have a single tag for dot1q or both q-tags for qinq which arrives in the original packet authenticated by RADIUS. [9]

8.5 Internet Enhanced Service (IES)

IES is a routed connectivity service that is used by the subscriber to communicate with IP router interface to send and receive internet traffic. An IES can have one or more logical IP interfaces each with a SAP which acts as the access point to the subscriber's network. IES service allows the subscriber facing interfaces to participate in the same routing instance used for service network core routing connectivity.

In this scenario IES is configured with subscriber and group interfaces. Subscriber interface acts as the gateway interface IP address and is associated with SAP connected to the subscriber end. Through this SAP IES provides access to the provider edge network to subscriber. In this scenario it provides access to RADIUS and DHCP servers. [3]

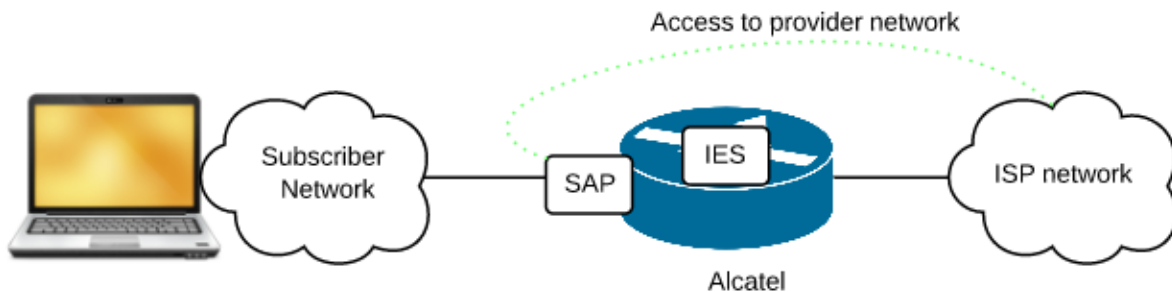


Figure 8: Internet Enhanced Service

8.6 MPLS (MultiProtocol Label Switching)

MPLS is the mechanism which directs data from one network node to another path labels rather than using long network addresses from the complex routing tables. Labels identify path between nodes rather than end-points. [11]

8.6.1 Label Edge Router (LER)

Label Edge router is any router that operates at the edge of an MPLS network. This router is the entry and exit point for the subscribers. PE-1 is the LER in our network scenario. LERs push label on an incoming packet and pop the label from the outgoing packets. [11]

8.6.2 Label Distribution Protocol (LDP)

LDP is the protocol that is used to build and maintain LSP databases that are used to forward traffic through MPLS network. Two routers with an established session are called LDP peers. In our scenario both Alcatel routers (PE-1 & PE-2) are LDP peers. LDP relies on the underlying routing information provided by IGP routing protocol. In this case IS-IS. [11]

8.7 Intermediate-system-to-intermediate-system (IS-IS)

IS-IS is a link-state interior gateway protocol. It uses the Shortest Path First (SPF) algorithm to determine routes and makes routing decisions based on the link-state information. In IS-IS, a network is a routing domain with end systems and intermediate systems. Link-state updates are sent periodically in IS-IS throughout the network.

In IS-IS a large autonomous system can be administratively divided in to smaller and more manageable areas. Level 1 routing is performed within the area and Level 2 routing is performed between different areas. We can configure the routers as Level 1, Level 2 or both Level 1/2.

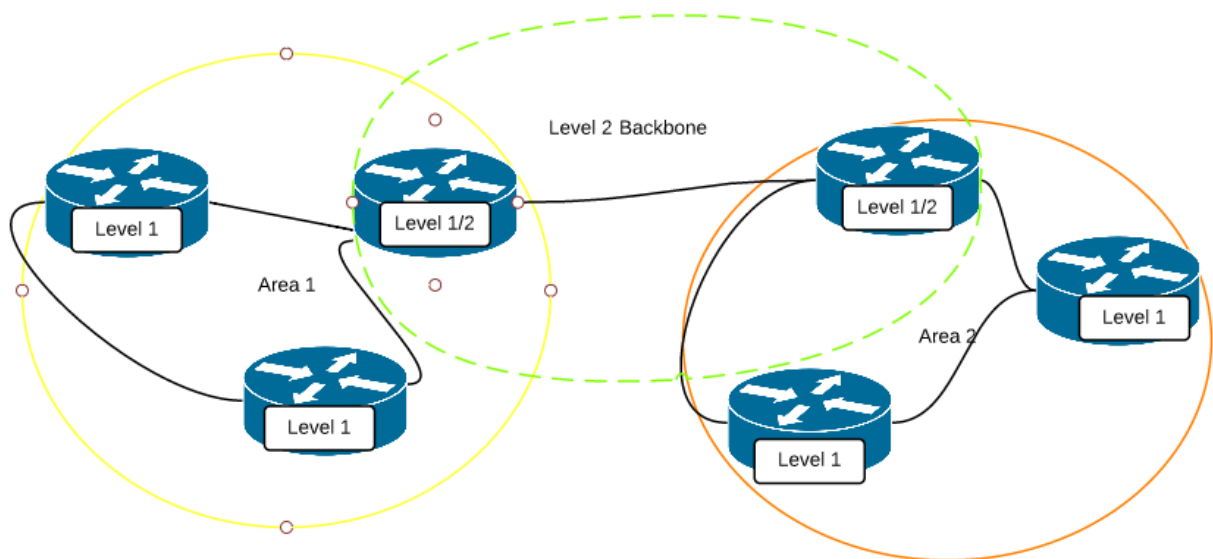


Figure 9: IS-IS routing domain example

In IS-IS level 2 routers know the topology only in their area and are also aware of the Level 2 routers. Level 1 routers forward the traffic with destinations outside of their area to Level 2 routers.

Level 2 routers are not required to know about the topology of level 1 routers. However, they can act both as level 1 and level 2 if configured according to that.

Routing is performed in IS-IS according to the following principles:

- Hello PDUs are sent on IS-IS enabled interfaces to form adjacencies and neighbor relationships are only built if the hello PDUs contain information that meets the criteria for forming an adjacency.
- Every neighbor builds a Shortest Path Tree (SPT) and routing table is built from this SPT.
- SRs flood LSPs to adjacent neighbors except from the neighbors from which they already received the same LSP. Link state database is constructed for these LSPs.

In our network topology IS-IS is enabled in between both service routers (SRs) as shown in the following diagram and both routers are running default IS-IS capability that is Level 1/2. [8]

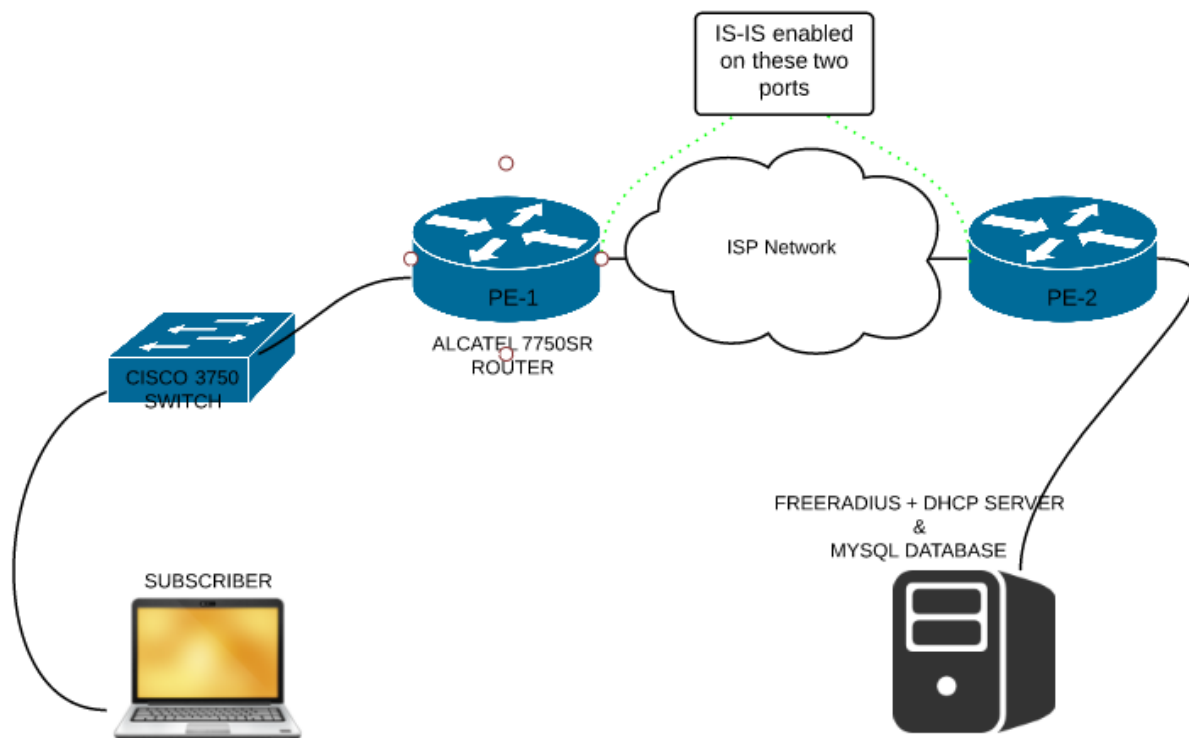


Figure 10: IS-IS functionality

8.8 DHCP Relay Agent

DHCP requests are broadcast packets that normally will not propagate outside of their IP subnet, a DHCP relay agent intercepts such requests and forwards them as a unicast message to configured DHCP server. When forwarding the DHCP message, relay agent also sets the gateway IP address in packet to the IP address of its ingress interface which allows DHCP clients to use DHCP server on a remote network. PE-1 router is acting as layer-3 relay agent in this scenario.

RADIUS and its features are described below in detail

8.9 Remote Authentication Dial in User Service (RADIUS)

RADIUS is a networking protocol that provides centralized authentication, authorization and accounting (AAA) services to subscribers who connect to ISP network. It is a client/server protocol and runs in application layer using User Datagram Protocol (UDP) as transport.

8.9.1 RADIUS Based Authorization and Authentication

In authorization and authentication process Access-Request, Access-Accept or Access-Reject messages are exchanged between a Radius Client and a Radius Server.

In our scenario Radius is used to check subscriber credentials with the help of MYSQL database. PE-1 router is configured with the destination address of the radius server.

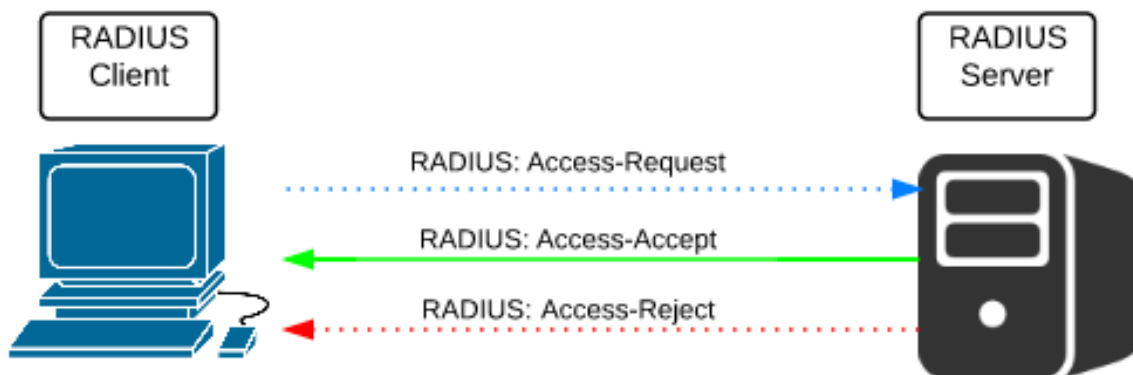


Figure 11: Radius Authentication and Authorization flow

In compliance with RFC 4679, agent-circuit-id and agent-remote-id attributes are included in authentication request message. In addition, standard RADIUS attributes are included in authentication request messages.

- NAS-identifier
- NAS-port-id
- NAS-port-type
- MAC-address
- dhcp-vendor-class-id
- calling-station-id

These will only be included in access-request if they are configured.

Both DHCP Discover and DHCP request trigger RADIUS authentication.

8.9.2 Radius based accounting

When a subscriber host is created, accounting-start packet is generated and is sent to the radius accounting server. When the session with subscriber gets terminated, an accounting-stop message including accounting statistics for a given host is generated. We can configure the router to send interim accounting messages to provide updates for a subscriber host.

The supported accounting messages are as follows:

- framed-ip-address
- framed-ip-netmask
- agent-circuit-id (as defined by subscriber on switch in this case)
- agent-remote-id
- calling-station-id
- alc-subscriber-id-string
- alc-subscriber-profile-string
- alc-sla-profile-string
- user-name
- NAS-identifier
- NAS-port-id
- NAS-port-type
- MAC-address

APPENDIX B – Configuration of Network Devices

Configuration of PE-1 Alcatel 7750 SR Router

```
A:PE-1# admin display-config
# TiMOS-B-11.0.R4 both/hops ALCATEL SR 7750 Copyright (c) 2000-2013 Alcatel-Lucent.
# All rights reserved. All use subject to applicable license agreements.
# Built on Tue Jul 23 12:48:12 PDT 2013 by builder in /rel11.0/b1/R4/panos/main
# Generated FRI JAN 07 15:38:19 2000 UTC

exit all

configure

#-----

echo "System Configuration"

#-----

system
  name "PE"
  snmp
    shutdown
  exit
  time
    sntp
    shutdown
  exit
  zone UTC
exit
thresholds
  rmon
  exit
```



```
    exit
exit
#-----
echo "System Security Configuration"
#-----

system
    security
        per-peer-queuing
    exit
exit
#-----

echo "Log Configuration"
#-----

log
exit
#-----

echo "System Security Cpm Hw Filters and PKI Configuration"
#-----

system
    security
    exit
exit
#-----

echo "QoS Policy Configuration"
#-----

qos
exit
```

```
#-----
```

```
echo "Card Configuration"
```

```
#-----
```

```
card 1
```

```
card-type iom-xp
```

```
mda 1
```

```
mda-type c5-1gb-xp-sfp
```

```
no shutdown
```

```
exit
```

```
no shutdown
```

```
exit
```

```
#-----
```

```
echo "Port Configuration"
```

```
#-----
```

```
port 1/1/1
```

```
ethernet
```

```
exit
```

```
no shutdown
```

```
exit
```

```
port 1/1/2
```

```
ethernet
```

```
mode access
```

```
encap-type dot1q
```

```
exit
```

```
no shutdown
```

```
exit
```

```
port 1/1/3
```

```
    ethernet
      mtu 1500
    exit
  no shutdown
exit
port 1/1/4
  shutdown
  ethernet
  exit
exit
port 1/1/5
  shutdown
  ethernet
  exit
exit
#-----
echo "System Sync-If-Timing Configuration"
#-----
system
  sync-if-timing
  begin
  commit
  exit
exit
#-----
echo "QoS Policy Configuration"
#-----
```

qos

```
sap-ingress 11 create
  description "256K_upstream"
  queue 1 create
    rate 256
  exit
  queue 11 multipoint create
  exit
```

exit

```
sap-ingress 22 create
  description "512K_upstream"
  queue 1 create
    rate 512
  exit
  queue 11 multipoint create
  exit
```

exit

```
sap-egress 11 create
  description "1M_downstream"
  queue 1 create
    rate 1024
  exit
```

fc be create

```
  queue 1
  dot1p 5
  dscp ef
```

exit

```
exit
sap-egress 22 create
  description "2M_downstream"
  queue 1 create
    rate 2048
  exit
fc be create
  queue 1
  dot1p 3
  dscp cs1
  exit
exit
exit
exit
#-----
echo "Management Router Configuration"
#-----
router management
exit
#-----
echo "Router (Network Side) Configuration"
#-----
router
  interface "system"
    address 192.168.2.1/32
    no shutdown
  exit
  interface "toPE2"
```

```
        address 192.168.1.1/30
        port 1/1/1
        no shutdown
    exit
#-----
echo "ISIS Configuration"
#-----

    isis
        area-id 10.0001
        export "redistribute"
        interface "system"
            no shutdown
        exit
        interface "toPE2"
            no shutdown
        exit
        no shutdown
    exit
#-----
echo "Web Portal Protocol Configuration"
#-----
    exit
#-----
echo "Subscriber-mgmt Configuration"
#-----
    subscriber-mgmt
        authentication-policy "authenticate-1" create
```

```
description "RADIUS policy for DHCP user Authentication"
radius-authentication-server
    timeout 10
exit
re-authentication
user-name-format circuit-id
exit
radius-accounting-policy "accounting-1" create
    update-interval 60
    include-radius-attribute
        circuit-id
        framed-ip-addr
        nas-identifier
        nas-port-id
        sla-profile
        sub-profile
        subscriber-id
        user-name
    exit
    session-id-format number
    use-std-acct-attributes
exit
sla-profile "sla-1M" create
    ingress
        qos 11 shared-queuing
    exit
exit
```

```
    egress
      qos 11
      exit
      no qos-marking-from-sap
    exit
  exit
  sla-profile "sla-2M" create
    ingress
      qos 22 shared-queuing
      exit
    exit
    egress
      qos 22
      exit
      no qos-marking-from-sap
    exit
  exit
  sub-profile "sub-profile-default" create
    radius-accounting-policy "accounting-1"
    sla-profile-map
      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
msap-policy "msap-1" create
  sub-sla-mgmt
    def-sub-id use-sap-id
    def-sub-profile "sub-profile-default"
    def-sla-profile "sla-2M"
    sub-ident-policy "sub-id-default"
    single-sub-parameters
      profiled-traffic-only
    exit
  exit
  ies-vprn-only-sap-parameters
    anti-spoof nh-mac
  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-1M"
    sub-ident-policy "sub-id-default"
    single-sub-parameters
      profiled-traffic-only
    exit
```

```
        exit
    exit
exit
#-----
echo "Service Configuration"
#-----

service
    customer 1 create
        description "Default customer"
    exit
    ies 2 customer 1 create
        subscriber-interface "sub-int-1" create
            group-interface "group-int-1" create
            exit
        exit
    exit
vpls 1 customer 1 create
    stp
        shutdown
    exit
    sap 1/1/2:* capture-sap create
        description "cap SAP for MSAP creation on port 1/1/2"
        trigger-packet arp dhcp pppoe
        msap-defaults
            policy "msap-1"
        exit
        authentication-policy "authenticate-1"
```

```
    exit
    no shutdown
exit
ies 2 customer 1 create
    subscriber-interface "sub-int-1" create
        description "Routed CO"
        address 10.1.0.254/24
    group-interface "group-int-1" create
        description "Routed CO MSAP"
        dhcp
            server 10.3.31.16
            trusted
            lease-populate 11
            gi-address 10.1.0.254
            no shutdown
        exit
        authentication-policy "authenticate-1"
    exit
exit
    no shutdown
exit
exit
#-----
echo "Router (Service Side) Configuration"
#-----
    router
#-----
```

```
echo "ISIS Configuration"
#-----
    isis
        no shutdown
    exit
#-----
echo "Policy Configuration"
#-----
    policy-options
        begin
        policy-statement "redistribute"
            entry 1
                from
                    protocol direct
            exit
            action accept
            exit
        exit
    exit
    commit
    exit
exit

#-----
echo "Subscriber-mgmt (Service Side) Configuration"
#-----
    subscriber-mgmt
```

```
authentication-policy "authenticate-1"
  radius-authentication-server
    server 1 address 10.3.31.16 secret "o7NOqMIY6j4gF25OixH4/r3AWJy0yEwo" hash2
  exit
exit
radius-accounting-policy "accounting-1"
  radius-accounting-server
    server 1 address 10.3.31.16 secret "o7NOqMIY6j4gF25OixH4/r3AWJy0yEwo" hash2
  exit
exit
exit
exit all
```

Configuration of PE-2 Alcatel 7750SR Router

```
A:PE2# admin display-config
# TiMOS-B-11.0.R4 both/hops ALCATEL SR 7750 Copyright (c) 2000-2013 Alcatel-Lucent.
# All rights reserved. All use subject to applicable license agreements.
# Built on Tue Jul 23 12:48:12 PDT 2013 by builder in /rel11.0/b1/R4/panos/main

# Generated FRI JAN 07 15:39:13 2000 UTC

exit all
configure
#-----
echo "System Configuration"
#-----
system
```

```
name "PE2"
snmp
  shutdown
exit
time
  snmp
    shutdown
  exit
  zone UTC
exit
thresholds
  rmon
  exit
exit
exit
#-----
echo "System Security Configuration"
#-----
system
  security
    per-peer-queuing
  exit
exit
#-----
echo "Log Configuration"
#-----
log
```

```
exit
#-----
echo "System Security Cpm Hw Filters and PKI Configuration"
#-----
system
  security
  exit
exit
#-----
echo "QoS Policy Configuration"
#-----
qos
exit
#-----
echo "Card Configuration"
#-----
card 1
  card-type iom-xp
  mda 1
    mda-type c5-1gb-xp-sfp
    no shutdown
  exit
  no shutdown
exit
#-----
echo "Port Configuration"
#-----
```

```
port 1/1/1
  ethernet
  exit
  no shutdown
exit
port 1/1/2
  ethernet
  exit
  no shutdown
exit
port 1/1/3
  shutdown
  ethernet
  exit
exit
port 1/1/4
  shutdown
  ethernet
  exit
exit
port 1/1/5
  shutdown
  ethernet
  exit
exit
#-----
echo "System Sync-If-Timing Configuration"
```



```
#-----  
system  
  sync-if-timing  
  begin  
  commit  
  exit  
exit  
#-----  
echo "Management Router Configuration"  
#-----  
router management  
exit  
#-----  
echo "Router (Network Side) Configuration"  
#-----  
router  
  interface "system"  
    address 192.168.3.1/32  
    no shutdown  
  exit  
  interface "toPE1"  
    address 192.168.1.2/30  
    port 1/1/1  
    no shutdown  
  exit  
  interface "toServer"
```

```
        address 10.3.31.1/24
        port 1/1/2
        no shutdown
    exit
#-----
echo "ISIS Configuration"
#-----

    isis
        area-id 10.0001
        export "redistribute"
        interface "system"
            no shutdown
        exit
        interface "toPE1"
            no shutdown
        exit
        no shutdown
    exit
#-----
echo "Web Portal Protocol Configuration"
#-----
    exit
#-----
echo "Service Configuration"
#-----
    service
        customer 1 create
```

```
        description "Default customer"
    exit
exit
#-----
echo "Router (Service Side) Configuration"
#-----
    router
#-----
echo "ISIS Configuration"
#-----
    isis
        no shutdown
    exit
#-----
echo "Policy Configuration"
#-----
    policy-options
        begin
        policy-statement "redistribute"
            entry 1
                from
                    protocol direct
            exit
            action accept
        exit
    exit
exit
```

```
commit
exit
exit
exit all
```

Configuration of SWITCH on Subscriber End

```
Switch#show run
Building configuration...
Current configuration : 2033 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Switch
!
boot-start-marker
boot-end-marker
!
no aaa new-model
switch 1 provision ws-c3750g-24ps
system mtu routing 1500
ip subnet-zero
!
ip dhcp snooping vlan 20
```

```
ip dhcp snooping
!
spanning-tree mode pvst
spanning-tree etherchannel guard misconfig
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface GigabitEthernet1/0/1
  switchport trunk encapsulation dot1q
  switchport mode trunk
  ip dhcp snooping trust
  ip dhcp snooping information option allow-untrusted
!
interface GigabitEthernet1/0/2
  switchport access vlan 20
  switchport mode access
  ip dhcp snooping information option allow-untrusted
  ip dhcp snooping vlan 20 information option format-type circuit-id string 0000ff000000
!
interface Vlan1
  no ip address
  no ip route-cache
!
interface Vlan20
  ip address 10.1.0.1 255.255.255.0
  no ip route-cache
```

```
!  
ip default-gateway 10.1.0.254  
ip classless  
ip http server  
!  
control-plane  
!  
!  
line con 0  
line vty 0 4  
  login  
line vty 5 15  
  login  
!  
end
```