

# **CAPSTONE PROJECT REPORT**

Dynamic provisioning of subscribers on Alcatel-Lucent  
Platform IP Edge devices using open source subscriber  
management solutions

Submission: April, 2014

Submitted by: Mahima Kumar

Master of Science in Internetworking

Supervisor: Mr. Pete Nanda

## **ACKNOWLEDGEMENT**

I would like to express my profound gratitude and deep regards to my supervisor Mr. Pete Nanda for his exemplary guidance, monitoring and constant encouragement throughout the project.

I would also like to thank Prof. Mike MacGregor, MINT Director and Mr. Shahnawaz Mir, MINT Coordinator for their immense support and for providing me with the golden opportunity to do this industry related project.

## **ABSTRACT**

This project aims at a general industrial multi-vendor approach enabling subscriber authentication based on DHCP Option 82 circuit-ID and dynamic provisioning of subscribers by designing and implementing an open source RADIUS authentication solution and DHCP environment. This project accomplishes the access, IP edge and RADIUS server aspects. The project involves the RADIUS and DHCP infrastructure assets using the Programmable Subscriber Configuration Policies (PSCP) as an identification mechanism using the Python scripting language to provide a unified and a full flexible framework. It also outlines the details relevant to subscriber management and provides information about the technology, network topology and the configuration to support an enhanced, scalable and integrated solution.

# TABLE OF CONTENTS

<b>CHAPTER 1 INTRODUCTION.....</b>	<b>7</b>
1.1    Problem Statement- Need for Dynamic Provisioning .....	7
1.2    Solution/Scope Statement.....	7
<b>CHAPTER 2 - SOLUTION LAB SETUP.....</b>	<b>8</b>
2.1    LAB EQUIPMENTS .....	8
2.1.1    DHCP Client (2900 CISCO Router) .....	8
2.1.2    3750 CISCO Switch (Layer 2 DHCP Relay Agent) .....	8
2.1.2.1    Option-82 Circuit-ID.....	8
2.1.2.2    DHCP Snooping.....	9
2.1.3    7750 Alcatel Service Router (SR) .....	9
2.1.3.1    Services and Service Entities.....	9
2.1.3.2    DHCP Relay Agent.....	10
2.1.3.3    Subscriber Management.....	10
2.1.4    RADIUS Server (LINUX Based FreeRADIUS) .....	10
2.1.4.1    RADIUS Authentication of Subscribers.....	11
2.1.4.2    RADIUS Attributes.....	11
2.1.5    DHCP Server (LINUX Based) .....	11
2.1.6    Python Script.....	12
2.2    DEPLOYING AND PROVISIONING SERVICES.....	12
2.3    HIGH LEVEL CONFIGURATION STEPS.....	13
2.3.1    7750 Alcatel SR-1.....	13
2.3.2    3750 Layer 2 Relay Agent.....	17
2.3.3    RADIUS Server.....	17
<b>CHAPTER 3 – TRANSACTION, LOGS AND TROUBLESHOOTING.....</b>	<b>18</b>
3.1    SUCCESSFUL RADIUS AND DHCP TRANSACTION.....	19
3.1.1    During Initial Binding Process.....	19
3.1.2    During DHCP Lease Renew and Re-authentication.....	20

3.1.3	During DHCP- RELEASE.....	20
3.1.4	RADIUS Authentication Failure.....	20
3.2	LOGS SHOWING RADIUS AND DHCP TRANSACTION.....	21
3.3	ISSUES AND TROUBLESHOOTING.....	27
<b>CHAPTER 4 - RESULTS AND ANALYSIS.....</b>		<b>28</b>
4.1	RESULT OUTPUTS .....	28
4.2	RESULT ANALYSIS.....	32
4.3	RECOMMENDATIONS FOR THE DESIGN.....	33
<b>CHAPTER 5 – CONCLUSION AND FUTURE WORK .....</b>		<b>34</b>
<b>REFERENCES.....</b>		<b>35</b>
<b>ABBREVIATIONS.....</b>		<b>38</b>
<b>APPENDIX – I ALCATEL-LUCENT TERMINOLOGY.....</b>		<b>39</b>
<b>APPENDIX - II SOLUTION CONFIGURATIONS.....</b>		<b>42</b>

## LIST OF FIGURES

Figure 1: Lab Setup.....	8
Figure 2: Subscriber Management.....	14
Figure 3: MSAP Policy.....	14
Figure 4: VPLS service.....	15
Figure 5: IES Service.....	16
Figure 6: Subscriber-management (Service side) .....	16
Figure 7: DHCP Snooping.....	17
Figure 8: DHCP Relay for Circuit-ID insertion.....	17
Figure 9: Users File on RADIUS.....	17
Figure 10: Successful RADIUS and DHCP Transaction.....	18
Figure 11: DHCP DISCOVER on L2 Relay Agent.....	21
Figure 12: Option 82 insertion .....	21
Figure 13: DHCP DISCOVER on SR-1.....	21
Figure 14: ACCESS-REQUEST .....	22
Figure 15: ACCESS-ACCEPT.....	22
Figure 16: DHCP DISCOVER forwarded by SR-1.....	23
Figure 17: DHCP OFFER received on SR-1.....	23
Figure 18: DHCP OFFER received on L2 Relay Agent.....	24
Figure 19: DHCP REQUEST on L2 Relay Agent.....	24
Figure 20: DHCP REQUEST on SR-1 .....	24
Figure 21: DHCP ACK on SR-1.....	25
Figure 22: DHCP ACK on L2 Relay Agent.....	25
Figure 23: DHCP Client allocated IP address.....	25
Figure 24: Python Script on SR-1.....	26

Figure 25: Issue.....	27
Figure 26: Active Subscribers on SR-1.....	28
Figure 27: Subscriber-Host on SR-1.....	28
Figure 28: Managed SAP on SR-1.....	29
Figure 29: MSAP Log.....	29
Figure 30: Service Access Points.....	29
Figure 31: Subscriber-Identification-Policy.....	30
Figure 32: DHCP Summary on SR-1.....	31
Figure 33: DHCP Statistics on SR-1.....	31

## **CHAPTER 1- INTRODUCTION**

This section describes the need for dynamic provisioning in the residential broadband network architectures along with a general multi-vendor solution depicting the scope of the project.

### **1.1 PROBLEM STATEMENT- Need for Dynamic Provisioning**

Typically in residential broadband networks, numerous new subscribers must be provisioned on a daily basis. Also, existing subscribers may make various changes to their subscriptions as well. All of this may lead to a significant amount of subscriber management activities on a regular basis. Manual provisioning of subscribers and managing traffic as well as requests to access the network can be an overwhelming task. It involves various Operational Support Systems (OSS) providing the service of provisioning the customers. Traditionally, provisioning was a manual process that required the assistance of several people in several roles involving multiple steps. It could take days to move a request from the submission phase through the actual activation of service. Subscribers may constantly move and add or make changes to their service subscriptions which places resource requirements on manual provisioning directly increasing the operational expenses.

Hence, there is a need for dynamic provisioning of subscribers without requiring human intervention to provide a more efficient and rapid response to the requests and cut service activation or change time. The service providers need to make the best use of available resources while supporting both existing and future users.

### **1.2 SOLUTION / SCOPE STATEMENT**

This project focusses on designing and implementing an open source RADIUS authentication solution for authenticating and dynamic provisioning of subscribers on Alcatel Lucent IP Edge devices and to cater to the needs of the subscribers and allowing them to access the network, by assigning IP addresses using a DHCP server. RADIUS server delivers authenticating capabilities by using the authentication parameter as DHCP Option 82 (Circuit-ID).

Subscriber Management is implemented and Programmable Subscriber Configuration Policy (PSCP) is used as an identification criterion that uses Python scripting language on Alcatel Lucent IP Edge devices to process DHCP messages dynamically and identify the subscribers based on the defined parameters. The solution aims at achieving the Access (Cisco Switch), IP Edge (ALU 7750) and RADIUS Server aspects for the project.



## CHAPTER 2 – SOLUTION LAB SETUP

This section describes the lab setup involving a multi-vendor approach by using Cisco, Alcatel-Lucent and Linux based equipment in order to depict a general industrial solution.

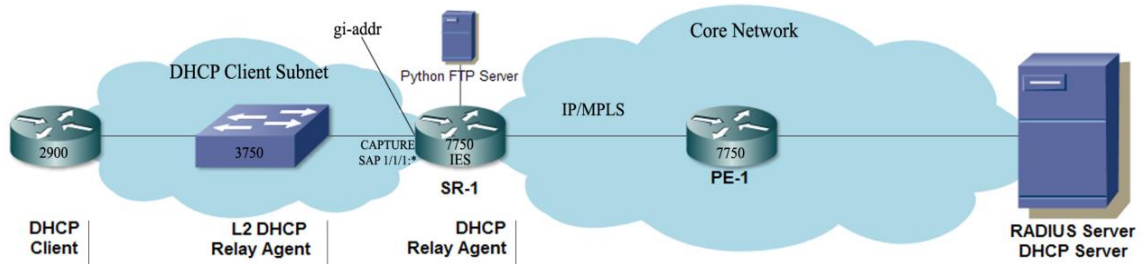


Figure 1: Lab Setup

### 2.1 LAB EQUIPMENTS

This section describes the different components used in the solution setup.

#### 2.1.1 DHCP CLIENT (2900 CISCO Router):

In this scenario a 2900 Cisco Router has been used as a DHCP client that is defined by a unique Circuit – id and Remote – id combination and broadcasts the requests to access the network for High Speed Internet (HSI) and other eligible services. Usually, a DHCP Client is a dynamic subscriber-host end-user device e.g., PC, set-top-box, VoIP phone, etc.

#### 2.1.2 3750 CISCO SWITCH (LAYER 2 DHCP RELAY AGENT):

In this scenario, the DSLAM is replaced by a 3750 Catalyst Switch acting as a DHCP Relay Agent to forward the DHCP messages between the client and server when both of them are not on the same network and for Option-82 Relay Information Agent (Circuit-ID) insertion.

##### 2.1.2.1 Option-82 Circuit-ID:

Option-82 Circuit-ID, which is the port through which the client connects to the network (Port 1/0/1 here), is the authentication parameter used here. The client broadcasts the DHCP Discover; the switch receives and adds Option-82 information i.e., Circuit-ID and then forwards the message. The RADIUS server will authenticate on the basis of this Circuit-ID and the DHCP server will assign the IP address to the client. MAC-based authentication is not as secure as agent access authentication. MAC addresses are not generally guarded as secrets, so an attacker can

spoof a MAC address and impersonate a device to gain network access. To reduce risk of an exploit, create a special VLAN for each device type.

#### 2.1.2.2 DHCP Snooping:

DHCP Snooping is a security feature for filtering the untrusted messages typically sourced from the client and the trusted server side messages. When DHCP snooping is enabled on a Vlan and the switch receives a packet on an untrusted interface belonging to that Vlan (Vlan 100 in this scenario), then the switch compares the source Mac address and the Client Hardware address (chaddr), and then forwards the packet.

#### 2.1.3 7750 ALCATEL SERVICE ROUTER (SR):

Dynamic provisioning of subscribers on Alcatel-Lucent IP edge devices platform along with subscriber management results in lowering the operational costs; rapid response to the subscriber requests; automated provisioning of access interfaces (MSAP) and flexible deployment to maximize the return on network infrastructure for access and authentication. It also protects the customers from security threats by using anti-spoofing filters which prevent certain packets gaining unauthorized network access. In this scenario, two 7750 Alcatel Service Routers are being used as:

- 7750 ALC1: Subscriber Management (known as ESM on ALU platform), Relay Agent (SR)
- 7750 ALC2: Provider Edge (PE)

#### 2.1.3.1 Services and Service Entities:

Once a subscriber is dynamically provisioned, any service can be provided to that subscriber. A service refers to the connectivity service for the Internet connectivity which is identified by a unique Service ID. Services can be provisioned on 7750 ALC1 SR and transported across an IP/MPLS provider core network in encapsulation tunnels created using MPLS Label Switched Paths (LSPs). ISIS is used as the routing protocol here.

Virtual Private LAN Service (VPLS) is a transparent and protocol independent service used to connect two or more Service Access Points (SAPs), which are the access points for the subscriber's network, on one or more 7750 SR's. A Capture SAP (1/1/1 :\*) defined under VPLS is used to trigger the authentication process using the DHCP triggering packets and also provides a context for the SAP template.

A routed connectivity service (Internet Enhanced Service (IES)) is configured where the subscriber communicates with an IP router interface to send and receive Internet traffic. SAPs are associated with the service, the subscriber interfaces define the subscriber's subnet and the group interfaces aggregates multiple SAPs on a single port.

Managed SAP (MSAP) allows the use of the SAP template and the policies for the creation of a SAP. Here the subscriber per SAP model is used where each subscriber is defined by its own VLAN (vlan id for capture and managed SAP must be the same). When MSAP is enabled, the trigger packet initiates a RADIUS authentication; the Access-Accept Radius message provides the service context i.e., the Service Id, Interface Id and the MSAP Policy name, which creates the MSAP.

#### 2.1.3.2 DHCP Relay Agent:

The DHCP Relay is only practical in a Layer 3 environment and thus it is only supported in IES Services, under subscriber interface's group interface. The Layer 2 DHCP Relay Agent (3750 Switch) adds Option 82 Circuit-ID, the 7750 ALC1 SR acting as a Relay Agent can either Keep, Replace or Drop the existing relay information. As configured here, the default behavior is Keep and authentication is based on this information. DHCP Snooping is performed both in the upstream and downstream direction for subscriber management.

#### 2.1.3.3 Subscriber Management:

A Subscriber is a customer which is created in the network element which maps into a VLAN, SAP, a MAC or an IP address or a physical port and is identified by a unique Subscriber-ID. A subscriber profile can be applied to a subscriber. The network element processes DHCP- ACK messages to determine the appropriate policies and profiles (Subscriber- Identification Policies, Subscriber Profile and Sla Profile) to apply for a given subscriber and associated host devices. The strings used for subscriber management are returned by the python script when the DHCP-ACK message is snooped and processed, and hence a host is instantiated.

### 2.1.4 RADIUS SERVER (LINUX BASED FreeRADIUS):

Remote Authentication Dial-In User Service (RADIUS) is a protocol which carries AAA (Authentication, Authorization and Accounting) information between the Network Access Server (NAS) which sends the authentication request for its client and the Radius Server, which is used by the Internet Service Providers (ISP's) to prevent any un-authorized access to the network. It supports PAP, CHAP or EAP protocols to authenticate users.

In the scope of this project, the RADIUS Server which is being used is FreeRADIUS; the NAS IP which requests the authentication is the 7750 ALC1 SR system ip address (configured) and the authentication parameter used is Option 82 Circuit-ID (inserted by L2 Relay Agent). The DHCP packets are the triggers.

#### 2.1.4.1 RADIUS Authentication of Subscribers:

The DHCP Discover message sent by the client triggers the authentication request. The 7750 Alcatel Service Router temporarily holds the DHCP-Discover; the configured system IP address which is the NAS IP in this case sends an authentication ACCESS-REQUEST to the Radius Server. Upon successful authentication based on Circuit-ID, RADIUS Server sends ACCESS-ACCEPT along with various RADIUS attributes so that the DHCP transaction can take place. If the authentication fails, RADIUS Server sends ACCESS-REJECT as a reply and the DHCP Discover packet is discarded by 7750 Alcatel Service Router.

#### 2.1.4.2 RADIUS Attributes:

Apart from granting the authentication, the RADIUS server includes several Standards and Vendor-Specific RADIUS attributes which are used for provisioning elements to the client. It describes various AAA elements in the user profile stored in the RADIUS database (raddb>users). RADIUS messages contain RADIUS attributes to communicate information between network elements running a client and server.

As configured, Access-Request to the server contains the following attributes:

- User-name: Relay Agent inserted Circuit-ID.
- Password: Encrypted password configured on 7750 ALC1 SR.
- NAS IP Address: System IP address of ALC1 where authentication request originated.
- Agent Circuit-ID: Inserted by L2 Relay Agent determining the port where the client is connected.
- NAS Port ID: Port from where the authentication request originates.
- NAS Port Type: Ethernet for DHCP Hosts

As configured, Access-Accept from the server contain the following attributes:

- MSAP Service ID: As configured on ALC1 SR i.e., *200*
- MSAP Policy: As configured on ALC1 SR i.e., *msap-1*
- MSAP Interface: AS configured on ALC1 SR i.e., *group-Subscriber-1*

#### 2.1.5 DHCP SERVER (LINUX BASED):

The DHCP server assigns IP addresses to the DHCP Clients from specified address pools. When a DHCP Client boots, a DHCP-DISCOVER message is broadcasted on the local subnet (destination ip address = 255.255.255.255). A DHCP server in the local subnet responds with a unicast DHCP-OFFER message containing the “*DHCP-Your-IP-Address*”(yiaddr) field as well as other configuration parameters in the option fields such as subnet mask, default gateway, DNS server IP addresses, DHCP Lease time, etc.

### **2.1.6 PYTHON SCRIPT:**

Python scripts can be run by Alcatel 7750 and can be written and stored centrally on a server (FTP Server) which is accessible to the 7750 SR-1. When SR-1 boots-up the Python script gets loaded inside it which can be used to derive the subscriber-identity-string from the Circuit-Id and the subscriber and service-level-agreement (Sla) profile form the Remote-Id option returned in the DHCP-ACK message from the DHCP Sever.

Here, a Python script's URL is configured in subscriber-identification-policy to return following attributes: sub-identification-string, subscriber-profile-string, Sla-profile-string. SR-1 will run the python script configured in sub-identification-policy against received DHCP-ACK message which is snooped and processed by the script, the default values for the strings is the Option 82 circuit-id and remote-id.

The circuit-ID is accessed as `alc.dhcp.options [82][1]` and remote-id as `alc.dhcp.options [82][2]`. These strings are used for a lookup in one or more maps to find the names of the sub-profile and Sla-profile to use. If none of the maps contained an entry for these strings, the names will be determined based on a set of defaults which are defined in the MSAP policy. Only when the names for both the sub-profile and Sla-profile are known, the subscriber host can be instantiated. If even no default is found for either profile, the DHCP ACK is dropped and the host will not gain network access. There are several different scripts that can be used according to the operator needs.

A subscriber identification string parses DHCP Option 82 field to extract subscriber identification for a host and optional profile identification strings. If configured, the subscriber profile names the existing ingress and egress scheduler policies and an accounting policy for use by all hosts of a subscriber. If configured, Sla profile names existing QoS policies to define the traffic shaping and also the existing ACL policies to filter the ingress and egress traffic. Here a host limit parameter is set under the Sla profile. A subscriber identification script derives the mandatory subscriber ID string and optional profile ID strings, from the DHCP option information returned in DHCP ACK message.

## **2.2 DEPLOYING AND PROVISIONING SERVICES:**

This section describes the step by step approach for deploying and dynamically provisioning services with the main phases:

### **Phase 1 Core Network Construction**

Before the services provisioning, the following steps should be configured properly:

#### **Step1.1 Build the IP or IP/MPLS core network**

Step 1.2 Configure the IS-IS Routing Protocols

Step 1.3 Configure MPLS LSPs

## **Phase 2 Service Administration**

Step 2.1 Configure user and group access privileges

Step 2.2 Create templates for QoS, filter, scheduling or accounting policies if required.

## **Phase 3 Service Provisioning**

Step 3.1 Core Tasks

Step 3.1.1 Provision customer account information.

Step 3.1.2 Create templates for QoS, filter, scheduling or accounting policies if required.

Step 3.2 Subscriber services

Step 3.2.1 Create VPLS and IES services

Step 3.2.2 Configure interfaces and SAPs and bind policies to the SAPs

Step 3.2.3 Create exclusive policies if required

## **2.3 HIGH LEVEL CONFIGURATION STEPS:**

The main configuration steps and configuration figures are shown below:

### **2.3.1 7750 ALCATEL SR-1**

#### **Step 1 Configure Subscriber Management**

**Step 1.1** Configure Sla profiles

**Step 1.2** Configure subscriber profiles

**Step 1.3** Configure subscriber identification policies

**Step 1.4** Configure authentication policies

```

#-----
echo "Subscriber-mgmt Configuration"
#-----

subscriber-mgmt
  authentication-policy "auth-pol-1" create
    description "Radius-Authentication-Policy"
    password ".IwUKPLThUa4qqE4cEPC8K8MuF/QW.IXSQD1Qbe3A36" hash2
    user-name-format ascii-converted-circuit-id
    include-radius-attribute
      circuit-id
    exit
  exit
  sla-profile "sla-1" create
    description "Service-Level-Agreement"
    host-limit 100
  exit
  sub-profile "sub-1" create
    description "Subscriber-Profile"
    sla-profile-map
      entry key "sla-1" sla-profile "sla-1"
    exit
  exit
  sub-ident-policy "ident-1" create
    description "Subscriber-Identification-Policy"
    sub-profile-map
      entry key "sub-1" sub-profile "sub-1"
    exit
    sla-profile-map
      entry key "sla-1" sla-profile "sla-1"
    exit
    primary
      script-url "ftp://mahima@192.168.254.250/mahima-script.py"
      no shutdown
    exit
  exit
exit

```

Figure 2: Subscriber Management

### Step 1.5 Configure MSAP policies

```

  msap-policy "msap-1" create
    description "ManagedSap-Policy"
    sub-sla-mgmt
      def-sub-id use-sap-id
      def-sub-profile "sub-1"
      def-sla-profile "sla-1"
      sub-ident-policy "ident-1"
    exit
  exit
exit
#-----

```

Figure 3: MSAP Policy

## **Step 2** Configure VPLS service

### **Step 2.1** Configure Capture SAP

#### **Step 2.1.1** Apply authentication policy

### **Step 2.2** Configure anti-spoofing filters (ip-mac by default)

```
vpls 100 customer 1 create
description "vpls "
stp
shutdown
exit
sap 1/1/1:* capture-sap create
trigger-packet dhcp dhcp6
msap-defaults
group-interface "group-Subscriber-1"
policy "msap-1"
service 200
exit
authentication-policy "auth-pol-1"
exit
no shutdown
```

Figure 4: VPLS service

## **Step 3** Configure IES Service

### **Step 3.1** Configure IP interfaces

#### **Step 3.1.1** Configure DHCP Relay agent

#### **Step 3.1.2** Configure DHCP snooping

### **Step 3.2** Apply authentication policies



```

ies 200 customer 1 create
description "Internet-Enhanced-Service"
subscriber-interface "to-Subscriber-1" create
address 192.168.20.1/24
group-interface "group-Subscriber-1" create
arp-populate
dhcp
    description "Dhcp-Relay-Agent"
    proxy-server
        emulated-server 192.168.20.1
        no shutdown
    exit
    server 10.3.31.40
    trusted
    lease-populate 10000
    gi-address 192.168.20.1 src-ip-addr
    no shutdown
    exit
    authentication-policy "auth-pol-1"
    oper-up-while-empty
    exit
    exit
    no shutdown
    exit
    exit
#-----

```

Figure 5: IES Service

#### Step 4 Configure Subscriber-management (Service side)

##### Step 4.1 Bind RADIUS server to the authentication policy

```

#-----
echo "Subscriber-mgmt (Service Side) Configuration"
#-----
subscriber-mgmt
    authentication-policy "auth-pol-1"
    radius-authentication-server
        server 1 address 10.3.31.40 secret "debsJaUwyaSqMO08yJZciODhuxHenils" hash2
    exit
    exit
    exit
#-----

```

Figure 6: Subscriber-management (Service side)

### 2.3.2 3750 LAYER 2 RELAY AGENT:

#### Step 1 Configure DHCP Snooping

Snooping is done for security reasons and has to be configured globally as well as on the vlan.

```
!  
ip dhcp snooping vlan 100  
ip dhcp snooping  
!  
!
```

Figure 7: DHCP Snooping

#### Step 2 Configure DHCP Relay for Circuit-ID insertion

The circuit-id is the port through which the client connects the network, which is 1/0/1 here.

```
interface GigabitEthernet1/0/1  
  switchport access vlan 100  
  switchport mode access  
  ip dhcp snooping vlan 100 information option format-type circuit-id string 1/0/1  
!
```

Figure 8: DHCP Relay for Circuit-ID insertion

### 2.3.3 RADIUS SERVER:

The RADIUS and DHCP Server have a lot of configuration parameters as they are on a Linux platform. There are numerous packages, libraries and databases installed and configured.

The main users file which maintains users profiles, resides in the RADIUS database is shown in the figure. The client's hardware address (chaddr) is used as a username here. There are several parameters for username like dhcp vendor specific options, circuit-id, ASCII converted circuit-id, ascii-tuple, etc. Password is preconfigured in SR-1 for matching. The Alc-MSAP parameters mentioned here are returned in the Access-Request message for further DHCP transaction processing. The RADIUS protocol does not transmit passwords in clear-text between the NAS IP (SR-1) and RADIUS server. A shared identical secret is used between the SR-1 and Server along with the MD5 hashing algorithm to obfuscate passwords. This is done to maintain security.

```
"312f302f31" Cleartext-Password := "password-1"  
Auth-Type := Accept,  
Alc-MSAP-Serv-Id = 200,  
Alc-MSAP-Policy == "msap-1",  
Alc-MSAP-Interface == "group-Subscriber-1"
```

Figure 9: Users File on RADIUS

## CHAPTER 3 – TRANSACTION, LOGS AND TROUBLESHOOTING

This section describes the network topology with the RADIUS and DHCP Transaction Phases used in a Lab setup depicting various aspects of the solution.

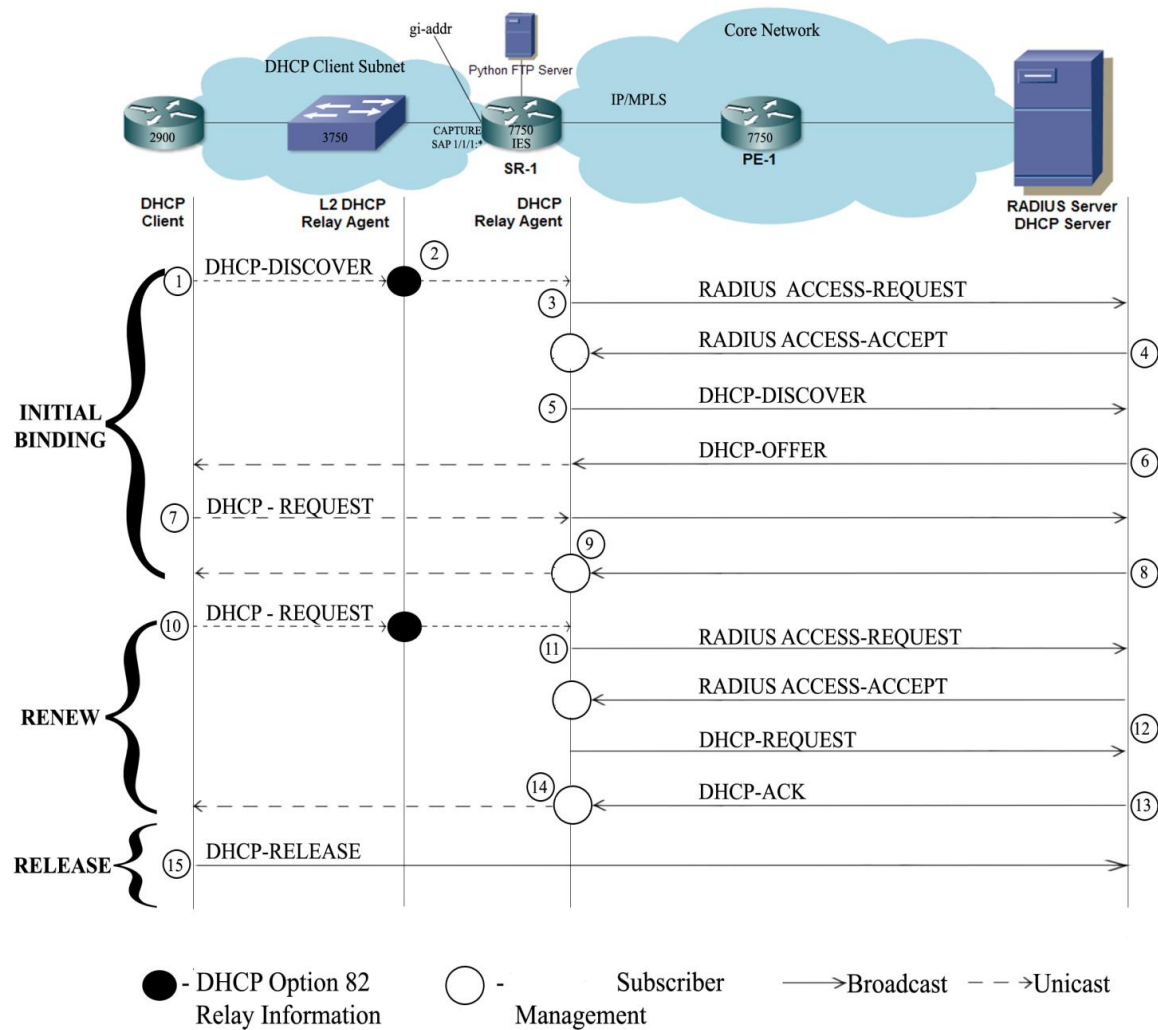


Figure10: Successful RADIUS and DHCP Transaction

### **3.1 SUCCESSFUL RADIUS AND DHCP TRANSACTION:**

The steps below explain the Figure 1 above depicting all the steps of a successful RADIUS and DHCP transaction:

#### **3.1.1 During INITIAL BINDING PROCESS:**

1. DHCP CLIENT boots-up and broadcasts a DHCP-DISCOVER message to get an IP address from the DHCP SERVER in order to access the network.
2. DHCP-DISCOVER message reaches 3750 SWITCH (L2 RELAY AGENT) which inserts DHCP Option 82 Circuit-ID and forwards DHCP-DISCOVER to 7750 SR-1.
3. DHCP-DISCOVER trigger an authentication on SR-1(DHCP RELAY AGENT). SR-1 temporarily holds the DHCP-DISCOVER and transmits an ACCESS-REQUEST to the RADIUS SERVER containing the CIRCUIT-ID (insertion by L2 RELAY AGENT).
4. Upon successful authentication, RADIUS SERVER sends the ACCESS-ACCEPT message to SR-1 containing the MSAP attributes.
5. SR-1 adds the gateway IP address (gi-addr) field and unicasts the DHCP-DISCOVER to the DHCP SERVER.
6. DHCP SERVER unicasts DHCP-OFFER containing the allocated IP address along with other IP configuration parameters to SR-1. SR-1 broadcasts the DHCP-OFFER back to the DHCP CLIENT via the L2 RELAY AGENT which removes the Option 82 information.
7. On receiving the DHCP-OFFER, the DHCP CLIENT broadcasts a DHCP-REQUEST requesting for the offered IP address. SR-1 adds the gateway address and unicasts it to the DHCP SERVER.
8. DHCP SERVER confirms that the IP address is still available and unicasts the DHCP-ACK message containing the DHCP Lease Time as an acknowledgement with other IP configuration to SR-1.
9. DHCP-ACK message is snooped and processed by a subscriber identification python script which is loaded in SR-1 using a python ftp-server. The default value for the string is the content of the Option 82 Circuit-ID and Remote-ID fields. It is used to derive the subscriber identification string, subscriber profile string and the Sla profile string. SR-1 broadcasts the DHCP-ACK to the DHCP CLIENT via L2 RELAY AGENT. DHCP

CLIENT is then bounded and can use the allocated IP address to access the network and use the eligible services.

### 3.1.2 During DHCP LEASE RENEW AND RE-AUTHENTICATION:

- 10 When half of the lease time has expired, DHCP CLIENT unicasts a DHCP-REQUEST for DHCP Lease Renewal. The L2 RELAY AGENT inserts Option 82 Circuit-ID and forwards the request to SR-1.
- 11 SR-1 temporarily holds the DHCP-REQUEST and transmits an ACCESS-REQUEST to the RADIUS SERVER containing the CIRCUIT-ID (insertion by L2 RELAY AGENT).
- 12 Upon successful authentication, RADIUS SERVER sends the ACCESS-ACCEPT message to SR-1 and the DHCP CLIENT is re-authenticated. SR-1 forwards the DHCP-REQUEST to the DHCP SERVER for DHCP Lease Renewal.
- 13 DHCP SERVER confirms that the IP address is still available and unicasts the DHCP-ACK containing the renewed DHCP Lease Time as an acknowledgement.
- 14 SR-1 unicasts the DHCP-ACK to the DHCP CLIENT and the client uses the IP address for the renewed time duration.

### 3.1.3 During DHCP- RELEASE:

Before disconnecting from the local subnet, a DHCP CLIENT may return its lease by unicasting a DHCP-RELEASE message to the DHCP SERVER. The IP address is free to be used by any other client. DHCP CLIENT is not bounded anymore.

### 3.1.4 RADIUS AUTHENTICATION FAILURE:

If the RADIUS authentication ACCESS-REQUEST is denied, the DHCP CLIENT authentication fails and the DHCP DISCOVER message is dropped. DHCP CLIENT is not allocated any IP address to access the network.

## 3.2 LOGS SHOWING RADIUS AND DHCP TRANSACTION:

DHCP DISCOVER broadcast message first reaches the SR-1 via L2 Relay Agent which adds the Option 82 Information added to it. The circuit id here is a hex string of 1/0/1 and remote id is hex string of mac address added by the Relay.

```
*Mar  5 19:04:49.496: DHCP_SNOOPING: received new DHCP packet from input interface (GigabitEthernet1/0/1)
*Mar  5 19:04:49.496: DHCP_SNOOPING: process new DHCP packet, message type: DHCP DISCOVER, input interface: Gi1/0/1, MAC da: ffff.ffff.ffff, MAC sa: c464.13dd.2410, 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: c464.13dd.2410
*Mar  5 19:04:49.496: DHCP_SNOOPING: add relay information option.
*Mar  5 19:04:49.505: DHCP_SNOOPING_SW: Encoding opt82 CID in string format
*Mar  5 19:04:49.505: DHCP_SNOOPING_SW: Encoding opt82 RID in MAC address format
```

Figure 11: DHCP DISCOVER on L2 Relay Agent

```
*Mar  5 19:04:49.505: DHCPD: Reload workspace interface Vlan100 tableid 0.
*Mar  5 19:04:49.505: DHCPD: tableid for 192.168.1.1 on Vlan100 is 0
*Mar  5 19:04:49.505: DHCPD: client's VPN is .
*Mar  5 19:04:49.505: DHCPD: using received relay info.
*Mar  5 19:04:49.505: DHCPD: Sending notification of DISCOVER:
*Mar  5 19:04:49.505:   DHCPD: htype 1 chaddr c464.13dd.2410
*Mar  5 19:04:49.505:   DHCPD: remote id 00060018186e9b00
*Mar  5 19:04:49.505:   DHCPD: circuit id 0105312f302f31
*Mar  5 19:04:49.505:   DHCPD: interface = Vlan100
*Mar  5 19:04:49.505:   DHCPD: class id 64736c666f72756d2e6f7267
```

Figure 12: Option 82 insertion

SR-1 temporarily holds the Discover message and triggers the RADIUS authentication. It is seen all the address fields are 0.0.0.0 which shows it's a broadcast message.

```
"PIP: DHCP
instance 1 (Base), interface index 5 (group-Subscriber-1),
received DHCP Boot Request on Interface group-Subscriber-1 (1/1/1:100) Port 67

H/W Type: Ethernet(10Mb)  H/W Address Length: 6
ciaddr: 0.0.0.0           yiaddr: 0.0.0.0
siaddr: 0.0.0.0           giaddr: 0.0.0.0
chaddr: c4:64:13:dd:24:10  xid: 0x1083

DHCP options:
[82] Relay agent information: len = 19
    [1] Circuit-id: (hex) 01 05 31 2f 30 2f 31
    [2] Remote-id: (hex) 00 06 00 18 18 6e 9b 00
[53] Message type: Discover
[57] Max msg size: 1200
[61] Client id: (hex) 00 63 69 73 63 6f 2d 63 34 36 34 2e 31 33 64 64 2e
32 34 31 30 2d 47 69 30 2f 30
[12] Host name: John
```

Figure 13: DHCP DISCOVER on SR-1

**RADIUS AUTHENTICATION:** When a capture SAP is configured, DHCP triggering packets initiate RADIUS authentication, which provides a service context. The authentication and the service context for this request create an MSAP. An MSAP behaves the same as a regular SAP, but the MSAP configuration is not editable.

**RADIUS Access-Request:** It is forwarded by the SR-1 before the DHCP Transaction takes place. The authentication parameter used here is Circuit-ID which is inserted by the L2 Relay Agent. DHCP DISCOVER triggers this authentication phase. The NAS attributes are sent in the Access-Request by default as the request is coming through a NAS Port.

```
"RADIUS: Transmit
Access-Request(1) 10.3.31.40:1812 id 3 len 86 vrid 1 pol auth-pol-1
  USER NAME [1] 10 312f302f31
  PASSWORD [2] 16 20fLQcdvHZqNULRmnkPGWU
  NAS IP ADDRESS [4] 4 192.168.10.1
  VSA [26] 7 DSL(3561)
    AGENT CIRCUIT ID [1] 5 1/0/1
  NAS PORT TYPE [61] 4 Ethernet(15)
  NAS PORT ID [87] 9 1/1/1:100
"
```

Figure 14: ACCESS-REQUEST

**RADIUS Access-Accept:** It is sent by the RADIUS Server upon successful authentication of the client. Along with approval, there are various service context parameters sent which are needed to provision the services to the client. MSAP parameters are required for that. These are vendor specific parameters and may change under different vendor environment.

```
"RADIUS: Receive
Access-Accept(2) id 3 len 72 from 10.3.31.40:1812 vrid 1 pol auth-pol-1
  VSA [26] 6 Alcatel(6527)
    MSAP SERVICE ID [31] 4 200
  VSA [26] 8 Alcatel(6527)
    MSAP POLICY [32] 6 msap-1
  VSA [26] 20 Alcatel(6527)
    MSAP INTERFACE [33] 18 group-Subscriber-1
"
```

Figure 15: ACCESS-ACCEPT

DHCP DISCOVER: SR-1 adds a gateway-address (gi-addr) field and unicasts it to the DHCP Server. The gateway address is the subscriber interface ip address which is pre-configured. The DHCP Server also unicasts its reply to this gi-addr which relays messages back and forth between the Client and the Server.

```
"PIP: DHCP
instance 1 (Base), interface index -1 (unknown),
  transmitted DHCP Boot Request to 10.3.31.40 Port 67

H/W Type: Ethernet(10Mb)  H/W Address Length: 6
ciaddr: 0.0.0.0           yiaddr: 0.0.0.0
siaddr: 0.0.0.0           giaddr: 192.168.20.1
chaddr: c4:64:13:dd:24:10  xid: 0x1083

DHCP options:
[82] Relay agent information: len = 19
    [1] Circuit-id: (hex) 01 05 31 2f 30 2f 31
    [2] Remote-id: (hex) 00 06 00 18 18 6e 9b 00
[53] Message type: Discover
[57] Max msg size: 1200
[61] Client id: (hex) 00 63 69 73 63 6f 2d 63 34 36 34 2e 31 33 64 64 2e
32 34 31 30 2d 47 69 30 2f 30
[12] Host name: John
```

Figure 16: DHCP DISCOVER forwarded by SR-1

DHCP OFFER DHCP server sends an available IP address in the offer message which is unicasted to the SR-1, which is your-ip-address (yiaddr) field. The source address (siaddr) is the DHCP Server IP address. There are other IP configuration parameters like the subnet mask and lease time.

```
"PIP: DHCP
instance 1 (Base), interface index 5 (group-Subscriber-1),
  transmitted DHCP Boot Reply to Interface group-Subscriber-1 (1/1/1:100) Port 68

H/W Type: Ethernet(10Mb)  H/W Address Length: 6
ciaddr: 0.0.0.0           yiaddr: 192.168.20.5
siaddr: 10.3.31.40        giaddr: 192.168.20.1
chaddr: c4:64:13:dd:24:10  xid: 0x1083

DHCP options:
[82] Relay agent information: len = 20
    [1] Circuit-id: 1/0/1
    [2] Remote-id: sla-1-sub-1
[53] Message type: Offer
[1] Subnet mask: 255.255.255.0
[3] Router: 192.168.20.1
[51] Lease time: 7200
[54] DHCP server addr: 10.3.31.40
[57] Max msg size: 1200
[255] End
```

Figure 17: DHCP OFFER received on SR-1



L2 Relay Agent receives DHCP OFFER and broadcasts it to the client. The option 82 relay information option is echoed back in the offer message and snooped by the L2 Relay Agent.

```
*Mar 5 19:04:49.564: DHCP_SNOOPING: process new DHCP packet, message type: DHCP
OFFER, input interface: Gi1/0/2, MAC da: ffff.ffff.ffff, MAC sa: 00d0.f682.08d3,
IP da: 255.255.255.255, IP sa: 192.168.20.1, DHCP ciaddr: 0.0.0.0, DHCP yiaddr:
192.168.20.5, DHCP siaddr: 10.3.31.40, DHCP giaddr: 192.168.20.1, DHCP chaddr:
c464.13dd.2410
```

Figure 18: DHCP OFFER received on L2 Relay Agent

DHCP REQUEST: Client upon receiving the offer broadcasts the DHCP REQUEST requesting the offered IP address to be allocated to it. Request reached SR-1 via L2 Relay Agent. SR-1 forwards it to the DHCP Server and adds gi-addr again.

```
*Mar 5 19:04:49.564: DHCP_SNOOPING: process new DHCP packet, message type: DHCP
REQUEST, input interface: Gi1/0/1, MAC da: ffff.ffff.ffff, MAC sa: c464.13dd.241
0, 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: c464.13dd.2410
*Mar 5 19:04:49.564: DHCP_SNOOPING: add relay information option.
```

Figure 19: DHCP REQUEST on L2 Relay Agent

```
"PIP: DHCP
instance 1 (Base), interface index -1 (unknown),
transmitted DHCP Boot Request to 10.3.31.40 Port 67

H/W Type: Ethernet(10Mb) H/W Address Length: 6
ciaddr: 0.0.0.0 yiaddr: 0.0.0.0
siaddr: 0.0.0.0 giaddr: 192.168.20.1
chaddr: c4:64:13:dd:24:10 xid: 0x1083

DHCP options:
[82] Relay agent information: len = 19
[1] Circuit-id: (hex) 01 05 31 2f 30 2f 31
[2] Remote-id: (hex) 00 06 00 18 18 6e 9b 00
[53] Message type: Request
[57] Max msg size: 1200
[61] Client id: (hex) 00 63 69 73 63 6f 2d 63 34 36 34 2e 31 33 64 64 2e
32 34 31 30 2d 47 69 30 2f 30
[54] DHCP server addr: 10.3.31.40
[50] Requested IP addr: 192.168.20.5
[12] Host name: John
```

Figure 20: DHCP REQUEST on SR-1

DHCP ACK: DHCP server responds back with the DHCP ACK message which contains the allocated IP address and other IP parameters. It contains the DHCP Lease state information with option 82 information present.

```
"PIP: DHCP
instance 1 (Base), interface index 5 (group-Subscriber-1),
transmitted DHCP Boot Reply to Interface group-Subscriber-1 (1/1/1:100) Port 68

H/W Type: Ethernet(10Mb) H/W Address Length: 6
ciaddr: 0.0.0.0 yiaddr: 192.168.20.5
siaddr: 10.3.31.40 giaddr: 192.168.20.1
chaddr: c4:64:13:dd:24:10 xid: 0x1083

DHCP options:
[82] Relay agent information: len = 20
    [1] Circuit-id: 1/0/1
    [2] Remote-id: sla-1-sub-1
[53] Message type: Ack
[1] Subnet mask: 255.255.255.0
[3] Router: 192.168.20.1
[51] Lease time: 7200
[54] DHCP server addr: 10.3.31.40
[57] Max msg size: 1200
[255] End
```

Figure 21: DHCP ACK on SR-1

L2 Relay forwards this DHCP ACK message to the Client and the Client gets an IP address.

```
*Mar 5 19:04:49.597: DHCP_SNOOPING: process new DHCP packet, message type: DHCP
ACK, input interface: Gi1/0/2, MAC da: ffff.ffff.ffff, MAC sa: 00d0.f682.08d3, I
P da: 255.255.255.255, IP sa: 192.168.20.1, DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 1
92.168.20.5, DHCP siaddr: 10.3.31.40, DHCP giaddr: 192.168.20.1, DHCP chaddr: c4
64.13dd.2410
```

Figure 22: DHCP ACK on L2 Relay Agent

DHCP CLIENT receives an IP address from the DHCP Server to access the network and use eligible services and there is end-to-end connectivity.

```
Apr 23 01:56:51.012: %DHCP-6-ADDRESS_ASSIGN: Interface GigabitEthernet0/0 assign
ed DHCP address 192.168.20.5, mask 255.255.255.0, hostname John
```

Figure 23: DHCP Client allocated IP address

PYHTON SCRIPT: Python script is defined under the subscriber-identification-policy to provide programmable flexibility.

DHCP ACK message is snooped and processed and the information inside it is the input for the Python script which is running on SR-1 for subscriber management. The operator can edit the Ack message information which is used to assign the subscriber-profile-string, service-level-agreement-string and subscriber-identification string according the python script loaded in SR-1.

```
*A:SR-1# show subscriber-mgmt sub-ident-policy "ident-1" script primary

=====
Subscriber Identification Policy ident-1
=====

-----
Primary Script
-----

URL           : ftp://*@192.168.254.250/mahima-script.py
Admin State  : Up                               Oper State : Up

-----
Source (dumped from memory)
-----

1 import re
2 import alc
3 # option 82 formatted as follows:
4 # "<subscriber Profile>-<sla-profile>"
5 ident = str(alc.dhcp.options[82][1])
6 alc.dhcp.sub_ident = ident
7 tmp = re.match("(?P<sub>.+)-(?P<sla>.+)", str(alc.dhcp.options[82][2]))
8 alc.dhcp.sub_profile_string = tmp.group("sub")
9 alc.dhcp.sla_profile_string = tmp.group("sla")

-----
=====

*A:SR-1#
```

Figure 24: Python Script on SR-1

According to this script, value from the circuit-id sub option received in DHCP ACK i.e., `alc.dhc.option[82][1]` will be the subscriber-identification-string and the value from the remote-id sub option received i.e., `alc.dhcp.option[82][2]`, the first value before “-” will be the subscriber-profile-string and after “-” will be the Sla-profile-string.

### 3.3 ISSUES AND TROUBLESHOOTING

During the phases of carrying out this project and implementing this solution there were few issues and challenges which aroused. One of the main issues was:

- **Issue:** Dropped DHCP Boot Request on the Group interface, 10.3.31.150 cannot be routed via the subscriber interface. - During earlier phases of the project, the subscriber interface ip address was 192.168.20.1. The framed ip address was 10.3.31.150 (manually configured on server). After authentication; client was not able to get the framed ip address. After seeing the logs and packet captures done by port mirroring and Tcpcdumps, it was evident that the client ip address should be from the same subnet as that of the subscriber interface and hence the group interface was dropping the request as the framed ip address could not be routed via the subscriber interface. Hence the framed ip address was changed to 192.168.20.5 which was routed via the subscriber interface being from the same subnet and the client got IP.

```
18 2000/01/02 02:20:45.16 UTC MINOR: DEBUG #2001 Base PIP
"PIP: DHCP
instance 1 (Base), interface index 4 (group-Mahima),
DROPPED DHCP Boot Request on Interface group-Mahima (1/1/1:100) Port 67
Problem: 10.3.31.150 cannot be routed via interface to-Mahima

H/W Type: Ethernet(10Mb)  H/W Address Length: 6
ciaddr: 0.0.0.0           yiaddr: 0.0.0.0
siaddr: 0.0.0.0           giaddr: 192.168.20.1
chaddr: c4:64:13:dd:25:00  xid: 0x1a04
```

Figure 25: Issue

To mitigate those issues and for easy troubleshooting of problems:

- **Port mirroring** was done on the 7750 Alcatel Service and Provider Edge Routers in order to capture the packet flow from one or more source ports in the network and using a sniffer like Wireshark that is attached to the destination port. The mirrored packets can be viewed and it became easier to troubleshoot the problems associated with the customer packet delivery and content.
- **VMware Platform** was used to configure a Linux based RADIUS and DHCP Server which allowed taking snapshots of the current configuration and reverting back to it in future. It became possible to go back and forth between our configurations at any point of time and also contributed to making it a Multivendor environment. Hypervisor ESXi 5.5 Vshpere Client was used for this.
- **Tcpcdumps** were captured and analyzed on the Server in order for a better understanding and figuring out the problem areas.

## CHAPTER 4 - RESULTS AND ANALYSIS

### 4.1 RESULT OUTPUTS

DHCP Client receives IP address from the DHCP Server and is eligible to access the network. Client is now bounded and is an active subscriber on SR-1 which has a subscriber profile associated with it. The subscriber has a subscriber identification string (which is configured to be the circuit id here), a subscriber profile (sub-1) and Sla profile (sla-1) associated with it. These are determined after MSAP has been created.

```
*A:SR-1# show service active-subscribers

=====
Active Subscribers
=====
Subscriber 0105312f302f31 (sub-1)
=====
(1) SLA Profile Instance sap:[1/1/1:100] - sla:sla-1
=====
IP Address
MAC Address      PPPoE-SID Origin
-----
192.168.20.5
c4:64:13:dd:24:10 N/A      DHCP
=====
Number of active subscribers : 1
=====
*A:SR-1#
```

Figure 26: Active Subscribers on SR-1

The subscriber-host in context with the IES can be seen here with the details of the host i.e. sap and its type (msap), Ip address assigned to the client, mac address of the client along with the subscriber-identification string configured to be the circuit id.

```
*A:SR-1# show service id 200 subscriber-hosts

=====
Subscriber Host table
=====
Sap
IP Address      Subscriber
MAC Address      PPPoE-SID Origin      Fwding State
-----
[1/1/1:100]      0105312f302f31
192.168.20.5
c4:64:13:dd:24:10 N/A      DHCP      Fwding
=====
Number of subscriber hosts : 1
=====
```

Figure 27: Subscriber-Host on SR-1

Managed SAP has been created for a fast and reliable support through on-demand service solutions which in turn reduces costs. An MSAP remains active as long as there is at least one subscriber host on the MSAP.

```
*A:SR-1# show service id 200 sap

=====
SAP(Summary), Service 200
=====
PortId                SvcId      Ing.  Ing.  Egr.  Egr.  Adm  Opr
                   QoS    Fltr  QoS   Fltr
-----
[1/1/1:100]          200        1    none  1     none  Up   Up
-----
Number of SAPs : 1
-----
Number of Managed SAPs : 1, indicated by [<sap-id>]
=====
```

Figure 28: Managed SAP on SR-1

```
90 2000/01/01 00:51:24.77 UTC WARNING: SVCMGR #2500 Base Subscriber created
"Subscriber 1/1/1:100 has been created in the system"

89 2000/01/01 00:51:24.77 UTC MINOR: SVCMGR #2213 Base MSAP create capture 1/1/1:*
"Managed SAP, 1/1/1:100 in service 200, has been created."

88 2000/01/01 00:51:24.70 UTC MINOR: SVCMGR #2505 Base
"Subscriber Authentication RADIUS server 10.3.31.40 operational status changed to inService."
```

Figure 29: MSAP Log

Service access points along with the service context that have been used in this configuration can be seen here.

```
-----
Service Access Points
-----

SAP 1/1/1:100
-----
Service Id      : 200
SAP             : 1/1/1:100          Encap             : q-tag
Description     : Managed SAP - Capture Svc 100 1/1/1:*
Admin State    : Up                  Oper State         : Up
Flags          : None
Multi Svc Site : None
Last Status Change : 01/01/2000 00:00:15
Last Mgmt Change  : 01/01/2000 01:56:41
Sub Type       : managed
Capture Service Id : 100              Capture SAP        : 1/1/1:*
MSAP Policy     : msap-1
```

Figure 30: Service Access Points

The subscriber identification policy associates a dynamic host with a subscriber. It can be seen in the figure below along with the subscriber-profile and service-level-agreements (Sla) mappings. Also the primary script which is loaded into SR-1 is operationally and administratively up and running. DHCP ACK message is snooped and processed in order to determine the subscriber and strings associated with a particular subscriber. If there are no mappings found, the default profile is considered to be used which is mentioned in the MSAP policy.

```
*A:SR-1# show subscriber-mgmt sub-ident-policy "ident-1"

=====
Subscriber Identification Policy ident-1
=====
Description          : Subscriber-Identification-Policy
Strings-From-Option : No

-----
Sub Profile Map
-----
Key                  Sub profile
-----
sub-1                sub-1

-----
SLA Profile Map
-----
Key                  SLA profile
-----
sla-1                sla-1

-----
App Profile Map
-----
Key                  App profile
-----
No mappings configured.

-----
Python Scripts
-----
#      Admin Oper  Script
      State State Name
-----
Primary  Up    Up    mahima-script.py
Secondary Down  Down  N/A
```

Figure 31: Subscriber-Identification-Policy

The dhcp summary shows the group-interface along which has been used for configuring dhcp relay agent on SR-1 along with the Managed SAP created.

```
*A:SR-1# show router dhcp summary

=====
DHCP Summary (Router: Base)
=====
Interface Name      Arp      Used/      Info      Admin
SapId/Sdp           Populate Provided      Option    State
-----
group-Subscriber-1  Yes      1/10000
sap:[1/1/1:100]    1/10000
-----
Interfaces: 1
=====
*A:SR-1#
```

Figure 32: DHCP Summary on SR-1

Here in the figure below it can be seen the number of DHCP packets which were received and transmitted by SR-1. We can see there no packet loss. The client and server packets are also relayed by SR-1 which can be seen below.

```
*A:SR-1# show router dhcp statistics

=====
DHCP Global Statistics (Router: Base)
=====
Rx Packets          : 33
Tx Packets          : 33
Rx Malformed Packets : 0
Rx Untrusted Packets : 0
Client Packets Discarded : 0
Client Packets Relayed : 18
Client Packets Snooped : 3
Client Packets Proxied (RADIUS) : 0
Client Packets Proxied (User-Db) : 0
Client Packets Proxied (Lease-Split) : 0
Server Packets Discarded : 2
Server Packets Relayed : 10
Server Packets Snooped : 0
DHCP RELEASEs Spoofed : 2
DHCP FORCERENEWs Spoofed : 0
=====
```

Figure 33: DHCP Statistics on SR-1



## 4.2 RESULT ANALYSIS

This project covers the Access (Cisco Switch), IP Edge (7750 SR-1 and PE-1) and RADIUS Server aspects of dynamic provisioning. The subscriber management feature performed the process of subscriber identification and host instantiation. This implementation provides a complete end-to-end solution across multiple vendors. The results indicates that this solution is deployable in the industry and can be scaled to provide services to multiple active subscribers at a time.

The subscriber management implemented here provides numerous key benefits out of which some of them are listed here:

- It has become easier to maintain consistent as well as universal subscriber attributes parameters like subscriber-Id, subscriber-profile and Sla profile.
- It has become easier to configure and troubleshoot tasks as the subscriber information is easily correlated with the network-related objects. Therefore, the chances of human error configurations have been reduced to a greater extent.
- With the usage of programmable subscriber configuration policy involving the python scripts and a DHCP environment, a scalable and flexible subscriber management solution is obtained.
- Multivendor access technologies and equipment makes it more powerful a general solution which can be incorporated in any vendor environment.
- This solution has enabled fully dynamic provisioning of residential subscribers without the need for manual operations.
- This solution protects the customers from security threats and provides denial of service for any unauthorized network access.

## 4.3 RECOMMENDATIONS FOR THE DESIGN

Below are listed some recommendations for this design which can be implemented in order to achieve a better solution and to broaden the horizon of this project.

- Scripting can be done locally on a 7750 Service Router instead of using an external Python Ftp Server which can be a point of failure in bigger scenarios. To avoid this point of failure, script can be loaded from SR-1 flash itself.
- Various different scripts can be used in combination with this scenario as per operator needs. Secondary and tertiary scripts can be used as well.
- Apart from using only Circuit-ID as an authentication parameter, other parameters like Remote-ID and MAC address can be used in combination with the Circuit-ID.
- An issue can arise to verify whether a subscriber host is still able to connect to the network. So keep-alive messages need to be sent periodically in order verify subscriber host connectivity. Subscriber Host Connectivity Verification (SHCV) mechanism can be implemented and integrated in this solution which periodically scans all the known hosts from their DHCP states and then can trigger an alarm whenever a subscriber host loses connectivity.
- Additional properties can be configured for bandwidth provisioning, QoS, security filtering, accounting/billing, access control lists, scheduler and accounting policies to enhance this solution.

## **CHAPTER 5 – CONCLUSION AND FUTURE WORK**

This project delivers a general industrial solution for dynamic provisioning of subscribers and provides a subscriber management model that can be used with DHCP and RADIUS based authentication environments. This solution provides a flexible architecture for less provisioning, less possibility for introducing provisioning errors and reduced configuration file. Due to the ever increasing subscriber needs, the time has come to transform the networks to realize profitable delivery of blended data, voice and video services and also providing a superior experience — anytime, anywhere.

Several technologies and cases were researched for carrying out this project including the triple play services and service delivery architecture, the DHCP and RADIUS transaction phases, the 7750 Alcatel Lucent platform, the 3750 Cisco Catalyst switch platform, the programmable subscriber configuration policies, migrating Legacy HSI Subscriber Management to TPSDA with Enhanced Subscriber Management, Alcatel-Lucent TPSDA Performance Verification Testing done by ISOCORE Internetworking Lab.

Dynamic provisioning along with subscriber management is the need of the hour. It is highly significant in the residential broadband networks where numerous subscribers are provisioned on a daily basis and manually taking care of a large number of subscribers becomes impossible. This project scenario and solution can be integrated and implemented in future and extensions can be made according to the need. This project can be implemented in wireless environments where access-points can be used instead of DHCP Client.

## REFERENCES

- 1) RFC 2865 Remote Authentication Dial In User Service (RADIUS)  
<https://tools.ietf.org/html/rfc2865>
- 2) RFC 4679 DSL Forum Vendor-Specific RADIUS Attributes  
<http://freeradius.org/rfc/rfc4679.txt>
- 3) RFC 2131 Dynamic Host Configuration Protocol  
<http://www.ietf.org/rfc/rfc2131.txt>
- 4) Alcatel-Lucent 7750 SR OS Triple Play Guide Software Version:7750 SR OS 11.0.R4 v2, September 2013, Document Part Number: 93-0098-09-04  
[https://infoproducts.alcatel-lucent.com/cgi-bin/dbaccessfilename.cgi/9300731004\\_V1\\_7750%20SR%20OS%20Router%20Configuration%20Guide%2011.0R4v2.pdf](https://infoproducts.alcatel-lucent.com/cgi-bin/dbaccessfilename.cgi/9300731004_V1_7750%20SR%20OS%20Router%20Configuration%20Guide%2011.0R4v2.pdf)
- 5) Cisco Catalyst 3750 Switch Software Configuration Guide- Configuring DHCP Features and IP Source Guard  
[http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/software/release/12-2\\_25\\_sec/configuration/guide/scg/swdhcp82.pdf](http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/software/release/12-2_25_sec/configuration/guide/scg/swdhcp82.pdf)
- 6) Alcatel-Lucent Next Generation Internet with Enhanced Subscriber Management- Wisely Ng  
[http://www.hkngis.hk/events-and-activities/presentation\\_20120309/Alcatel-Lucent.pdf](http://www.hkngis.hk/events-and-activities/presentation_20120309/Alcatel-Lucent.pdf)
- 7) Application Note - Enhanced Subscriber Management for Triple Play- Applying Programmable Subscriber Configuration Policies  
[http://www.ascend.com/wps/DocumentStreamerServlet?LMSG\\_CABINET=Docs\\_and\\_Resource\\_Ctr&LMSG\\_CONTENT\\_FILE=Brochures/EnSubMan\\_an.pdf](http://www.ascend.com/wps/DocumentStreamerServlet?LMSG_CABINET=Docs_and_Resource_Ctr&LMSG_CONTENT_FILE=Brochures/EnSubMan_an.pdf)
- 8) Alcatel-Lucent 7750 Service Router and 7450 Ethernet Service Switch- Multiservice Integrated Service Adapter Release 10  
[https://www.google.ca/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CCoQFjAA&url=http%3A%2F%2Fwww3.alcatel-lucent.com%2Fwps%2FDocumentStreamerServlet%3FLMSG\\_CABINET%3DDocs\\_and\\_Resource\\_Ctr%26LMSG\\_CONTENT\\_FILE%3DData\\_Sheets%2FMS-ISA\\_R10\\_EN\\_Datasheet.pdf&ei=TVRXU\\_XVB5e0yASag4GYDw&usg=AFQjCNGrhYomRI92esAAYDS68y6lpUmquQ&bvm=bv.65177938,d.aWw](https://www.google.ca/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CCoQFjAA&url=http%3A%2F%2Fwww3.alcatel-lucent.com%2Fwps%2FDocumentStreamerServlet%3FLMSG_CABINET%3DDocs_and_Resource_Ctr%26LMSG_CONTENT_FILE%3DData_Sheets%2FMS-ISA_R10_EN_Datasheet.pdf&ei=TVRXU_XVB5e0yASag4GYDw&usg=AFQjCNGrhYomRI92esAAYDS68y6lpUmquQ&bvm=bv.65177938,d.aWw)

- 9) F5- Subscriber Management in Service Provider Networks with BIG-IP Devices <https://www.f5.com/it-management/solution-profiles/subscriber-management>
- 10) Transforming the Network for Triple Play, Alcatel-Lucent's Triple Play Service Delivery Architecture (TPSDA)- By L. Ciangiulli, R. Mestric [http://www3.alcatel-lucent.com/enrich/v1i12007/pdf/Transforming\\_the\\_Network\\_en.pdf](http://www3.alcatel-lucent.com/enrich/v1i12007/pdf/Transforming_the_Network_en.pdf)
- 11) Alcatel- Lucent TELUS ESM Update December 2008
- 12) Alcatel-Lucent 7750 SR OS MPLS Guide, Software Version: 7750 SR OS 11.0.R4, July 2013, Document Part Number: 93-0075-10-03 [https://infoproducts.alcatel-lucent.com/cgi-bin/dbaccessfilename.cgi/9300751003A\\_V1\\_7750](https://infoproducts.alcatel-lucent.com/cgi-bin/dbaccessfilename.cgi/9300751003A_V1_7750)
- 13) Alcatel-Lucent 7750 SR OS Routing Protocols Guide, Software Version: 7750 SR OS 11.0.R4v2, September 2013, Document Part Number: 93-0074-10-04 [https://infoproducts.alcatel-lucent.com/cgi-bin/dbaccessfilename.cgi/9300741004\\_V1\\_7750%20SR%20OS%20Routing%20Protocols%20Guide%2011.0.R4.pdf](https://infoproducts.alcatel-lucent.com/cgi-bin/dbaccessfilename.cgi/9300741004_V1_7750%20SR%20OS%20Routing%20Protocols%20Guide%2011.0.R4.pdf)
- 14) Alcatel-Lucent 7750 SR OS Router Configuration Guide, Software Version: 7750 SR OS 11.0 R4, July 2013, Document Part Number: 93-0073-10-03 [https://infoproducts.alcatel-lucent.com/cgi-bin/dbaccessfilename.cgi/9300731003\\_V1\\_7750%20SR%20OS%20Router%20Configuration%20Guide%2011.0R4.pdf](https://infoproducts.alcatel-lucent.com/cgi-bin/dbaccessfilename.cgi/9300731003_V1_7750%20SR%20OS%20Router%20Configuration%20Guide%2011.0R4.pdf)
- 15) Alcatel-Lucent 7750 SR OS Basic System Configuration Guide, Software Version: 7750 SR OS 11.0 R4, July 2013, Document Part Number: 93-0070-10-03 [https://infoproducts.alcatel-lucent.com/cgi-bin/dbaccessfilename.cgi/9300701003\\_V1\\_7750%20SR%20OS%20Basic%20System%20Configuration%20Guide%2011.0R4.pdf](https://infoproducts.alcatel-lucent.com/cgi-bin/dbaccessfilename.cgi/9300701003_V1_7750%20SR%20OS%20Basic%20System%20Configuration%20Guide%2011.0R4.pdf)
- 16) Alcatel-Lucent 7750 SR OS Interface Configuration Guide, Software Version: 7750 SR OS 11.0 r4, July 2013, Document Part Number: 93-0072-10-03 [https://infoproducts.alcatel-lucent.com/cgi-bin/dbaccessfilename.cgi/9300721003\\_V1\\_7750%20SR%20OS%20Interface%20Configuration%20Guide%2011.0R4.pdf](https://infoproducts.alcatel-lucent.com/cgi-bin/dbaccessfilename.cgi/9300721003_V1_7750%20SR%20OS%20Interface%20Configuration%20Guide%2011.0R4.pdf)
- 17) Alcatel-Lucent 7750 SR-OS RADIUS Attributes Reference Guide, Software Version: SR OS R11.0 R4, July 2013, Document Part Number: 93-0472-01-03

[https://infoproducts.alcatel-lucent.com/cgi-bin/dbaccessfilename.cgi/9304720103REV.2\\_V1\\_7750%20SR-OS%20RADIUS%20Attributes%20Reference%20Guide%2011.0R4%20Rev.%202.pdf](https://infoproducts.alcatel-lucent.com/cgi-bin/dbaccessfilename.cgi/9304720103REV.2_V1_7750%20SR-OS%20RADIUS%20Attributes%20Reference%20Guide%2011.0R4%20Rev.%202.pdf)

- 18) Alcatel- Lucent User Guide Service Management, 5620 SAM Release 11.0 R2 [https://infoproducts.alcatel-lucent.com/cgi-bin/dbaccessfilename.cgi/3HE08041AAABTQZZA01\\_V1\\_5620%20SAM%20RELEASE%2011.0%20R2%20U.pdf](https://infoproducts.alcatel-lucent.com/cgi-bin/dbaccessfilename.cgi/3HE08041AAABTQZZA01_V1_5620%20SAM%20RELEASE%2011.0%20R2%20U.pdf)
- 19) Alcatel-Lucent 7750 SR OS Services Guide Software Version: 7750 SR OS 8.0 r4, July 2010, Document Part Number: 93-0076-07-02 [https://infoproducts.alcatel-lucent.com/cgi-bin/dbaccessfilename.cgi/9300760702\\_V1\\_7750%20SR%20OS%20Services%20Guide%208.0r4.pdf](https://infoproducts.alcatel-lucent.com/cgi-bin/dbaccessfilename.cgi/9300760702_V1_7750%20SR%20OS%20Services%20Guide%208.0r4.pdf)

## **ABBREVIATIONS**

AAA authentication, authorization and accounting  
DHCP dynamic host configuration protocol  
ESM enhanced subscriber management  
FTP file transfer protocol  
HSI high-speed Internet  
IES internet enhanced service  
IPTV internet protocol television  
ISIS intermediate system to intermediate system  
ISP internet service provider  
L2 layer 2  
MSAP managed service access point  
NAS network access server  
PE provider edge  
PSCP programmable subscriber configuration policy  
QoS quality of service  
RADIUS remote authentication dial-in user service  
SAP service access point  
SHCV subscriber host connectivity verification  
SLA service level agreement  
SR service router  
TPSDA triple play service delivery architecture  
VLAN virtual local area network  
VoIP voice over IP  
VPLS virtual private LAN service

## **APPENDIX – I**

### **ALCATEL-LUCENT TERMINOLOGY**

1. ESM Enhanced Subscriber Management - In residential broadband networks numerous subscribers can be provisioned that can require significant changes on a daily basis. Manually configuring the applicable parameters for each subscriber would be prohibitive. The Alcatel-Lucent 7750 SR has been designed to support fully dynamic provisioning of access, QoS and security aspects for residential subscribers using DHCP to obtain an IP address. Enabling Enhanced Subscriber Management drastically reduces the configuration burden. Enhanced Subscriber Management in the 7750 SR supports many vendor's access nodes and network aggregation models, including VLAN per customer, per service or per access node. When enabled on a SAP, the system expands the information it stores per subscriber host, allowing SLA enforcement and accounting features on a per subscriber basis. The operator can create a subscriber identification policy that will include a URL to a user-space script that assists with the subscriber host identification process.

A subscriber host is identified by a subscriber identification string instead of the limited Option 82 values (although, the identification string is normally derived from string manipulation of the Option 82 fields). A subscriber identification policy is used to process the dynamic host DHCP events to manage the lease state information stored per subscriber host. Further processing by the subscriber identification policy derives the appropriate subscriber and SLA profiles used to define the hierarchical virtual schedulers for each subscriber and the unique queuing and filtering required for the hosts associated with each subscriber. The SLA profile information is used to identify which QoS policies and which queues will be used for each subscriber host (dynamic or static). The system performs SLA enforcement functions on a per subscriber SLA profile instance basis.

**Subscriber- Identification Policies:** A subscriber-identification policy is created to process the dynamic host DHCP transactions to manage the DHCP lease state information which is stored per-subscriber host and also to derive the appropriate subscriber and SLA profiles for each subscriber.

**Subscriber Profile:** It is a template which contains the QoS and accounting settings for the subscriber-hosts.

**Sla Profile:** It is used for the purpose of supporting multiple service types for subscriber-hosts and set host-limit which defines the maximum number of dynamic subscriber hosts per subscriber for this Sla-profile.

[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#448002](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#448002)



2. **SAP Service Access Point** - Each subscriber service type is configured with at least one service access point (SAP). A SAP identifies the customer interface point for a service on an Alcatel-Lucent 7750 SR router. The SAP configuration requires that slot, MDA, and port/channel information be specified. The slot, MDA, and port/channel parameters must be configured prior to provisioning a service. Depending on the encapsulation, a physical port or channel can have more than one SAP associated with it. SAPs can only be created on ports or channels designated as “access” in the physical port configuration. SAPs cannot be created on ports designated as core-facing “network” ports as these ports have a different set of features enabled in software. A SAP is a local entity and only locally unique to a given device. The same SAP ID value can be used on another 7750 SR. There are no default SAPs. All SAPs must be created.  
[https://infoproducts.alcatel-lucent.com/html/0\\_add-h-f/93-0076-HTML/7750\\_SR\\_OS\\_Services\\_Guide/services.html](https://infoproducts.alcatel-lucent.com/html/0_add-h-f/93-0076-HTML/7750_SR_OS_Services_Guide/services.html)
3. **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. 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 forwarded. Non-triggering packets captured by the capturing SAP are dropped.  
[https://infoproducts.alcatel-lucent.com/html/0\\_add-h-f/93-0267-HTML/7X50\\_Advanced\\_Configuration\\_Guide/MSAP-PPPoE.html#425040](https://infoproducts.alcatel-lucent.com/html/0_add-h-f/93-0267-HTML/7X50_Advanced_Configuration_Guide/MSAP-PPPoE.html#425040)
4. **MSAP Managed SAP** - 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. Creation of a managed SAP is triggered by a DHCP-DISCOVER 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 service. 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.  
[https://infoproducts.alcatel-lucent.com/html/0\\_add-h-f/93-0267-HTML/7X50\\_Advanced\\_Configuration\\_Guide/MSAP-PPPoE.html](https://infoproducts.alcatel-lucent.com/html/0_add-h-f/93-0267-HTML/7X50_Advanced_Configuration_Guide/MSAP-PPPoE.html)
5. **IES Internet Enhanced Service** - Internet Enhanced Service (IES) is a routed connectivity service where the subscriber communicates with an IP router interface to send and receive Internet traffic. An IES has one or more logical IP routing interfaces each with a SAP which acts as the access point to the subscriber’s network. IES allows customer-

facing IP interfaces to participate in the same routing instance used for service network core routing connectivity. IES services require that the IP addressing scheme used by the subscriber be unique between other provider addressing schemes and potentially the entire Internet. IP interfaces defined within the context of an IES service must have a SAP associated as the uplink access point to the subscriber network. Multiple IES services are created to segregate subscriber owned IP interfaces.

[https://infoproducts.alcatel-lucent.com/html/0\\_add-h-f/93-0076-HTML/7750\\_SR\\_OS\\_Services\\_Guide/services\\_con\\_ies.pdf](https://infoproducts.alcatel-lucent.com/html/0_add-h-f/93-0076-HTML/7750_SR_OS_Services_Guide/services_con_ies.pdf)

## APPENDIX – II

### SOLUTION CONFIGURATIONS

#### 3750 SWITCH (LAYER2 RELAY AGENT)

L2-Relay-Agent#

L2-Relay-Agent#sh run

Building configuration...

Current configuration : 1935 bytes

version 12.2

no service pad

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

hostname L2-Relay-Agent

boot-start-marker

boot-end-marker

no aaa new-model

switch 1 provision ws-c3750g-24ps

system mtu routing 1600

ip subnet-zero

ip routing

!

ip dhcp snooping vlan 100

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 access vlan 100

switchport mode access

ip dhcp snooping vlan 100 information option format-type circuit-id string 1/0/1
!

interface GigabitEthernet1/0/2

switchport trunk encapsulation dot1q

switchport mode trunk

ip dhcp snooping trust

ip dhcp snooping information option allow-untrusted
!

interface Vlan1

no ip address
!

interface Vlan100

ip address 192.168.1.1 255.255.255.0

ip helper-address 10.3.31.40
!

ip classless

ip http server

control-plane

line con 0

line vty 5 15
!

end
```

## 7750 ALCATEL LUCENT SERVICE ROUTER (SR-1)

A:SR-1#

A:SR-1# admin display-config

exit all

configure

#-----

echo "System Configuration"

#-----

system

name "SR-1"

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

    log-id 50

    description "checking-the-logs"

    from debug-trace

    to memory 500

exit

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

    description "facing-customer"

    ethernet

        mode access

        encap-type dot1q

    exit

    no shutdown

exit

port 1/1/2

    description "facing-ftp-server"

    ethernet

    exit

    no shutdown

exit

port 1/1/3

    shutdown

    ethernet

    exit

exit

port 1/1/4

    description "for-port-mirroring"
```

```
    ethernet
        mode access
    exit
    no shutdown
exit
port 1/1/5
    description "facing-PE-1"
    ethernet
        mtu 1518
    exit
    no shutdown
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 "facing-PE-1"

    address 172.16.10.2/30

    port 1/1/5

    no shutdown

exit

interface "facing-ftp-server"

    address 192.168.254.251/24

    port 1/1/2

    no shutdown

exit

interface "system"

    address 192.168.10.1/32

    description "NAS-IP-Address"

    no shutdown

exit

#-----

echo "ISIS Configuration"

#-----

isis

    area-id 49.0000.1111

    interface "system"

        no shutdown

    exit

    interface "facing-PE-1"

        no shutdown

    exit

    no shutdown

exit

#-----

```

```
echo "MPLS Configuration"
```

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

```
mpls
```

```
admin-group "CAPSTONE" 1
```

```
interface "system"
```

```
admin-group "CAPSTONE"
```

```
no shutdown
```

```
exit
```

```
interface "facing-PE-1"
```

```
admin-group "CAPSTONE"
```

```
no shutdown
```

```
exit
```

```
exit
```

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

```
echo "RSVP Configuration"
```

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

```
rsvp
```

```
interface "system"
```

```
no shutdown
```

```
exit
```

```
interface "facing-PE-1"
```

```
no shutdown
```

```
exit
```

```
no shutdown
```

```
exit
```

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

```
echo "MPLS LSP Configuration"
```

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

```
mpls
```

```
path "unique"
```

```
hop 1 172.16.10.1 strict

no shutdown

exit

lsp "server"

to 172.16.10.1

from 172.16.10.2

include "CAPSTONE"

primary "unique"

exit

no shutdown

exit

no shutdown

exit

#-----

echo "LDP Configuration"

#-----

ldp

interface-parameters

interface "facing-PE-1"

exit

exit

targeted-session

exit

no shutdown

exit

#-----

echo "Web Portal Protocol Configuration"

#-----

exit
```

```

#-----
echo "Subscriber-mgmt Configuration"
#-----

subscriber-mgmt

  authentication-policy "auth-pol-1" create

    description "Radius-Authentication-Policy"

    password ".IwUKPLThUa4qqE4cEPC8K8MuF/QW.IXSQD1Qbe3A36" hash2

    user-name-format ascii-converted-circuit-id

    include-radius-attribute

      circuit-id

    exit

  exit

  sla-profile "sla-1" create

    description "Service-Level-Agreement"

    host-limit 100

  exit

  sub-profile "sub-1" create

    description "Subscriber-Profile"

    sla-profile-map

      entry key "sla-1" sla-profile "sla-1"

    exit

  exit

  sub-ident-policy "ident-1" create

    description "Subscriber-Identification-Policy"

    sub-profile-map

      entry key "sub-1" sub-profile "sub-1"

    exit

    sla-profile-map

      entry key "sla-1" sla-profile "sla-1"

    exit

```

```

primary

    script-url "ftp://mahima@192.168.254.250/mahima-script.py"

    no shutdown

exit

exit

msap-policy "msap-1" create

    description "ManagedSap-Policy"

sub-sla-mgmt

    def-sub-id use-sap-id

    def-sub-profile "sub-1"

    def-sla-profile "sla-1"

    sub-ident-policy "ident-1"

exit

exit

exit

#-----
echo "Service Configuration"
#-----

service

    customer 1 create

        description "Default customer"

    exit

    ies 200 customer 1 create

        subscriber-interface "to-Subscriber-1" create

            group-interface "group-Subscriber-1" create

        exit

    exit

exit

vpls 100 customer 1 create

    description "vpls "

```

```
stp
    shutdown
exit
sap 1/1/1:* capture-sap create
    trigger-packet dhcp dhcp6
    msap-defaults
        group-interface "group-Subscriber-1"
        policy "msap-1"
        service 200
    exit
    authentication-policy "auth-pol-1"
exit
no shutdown
exit
ies 200 customer 1 create
    description "Internet-Enhanced-Service"
    subscriber-interface "to-Subscriber-1" create
        address 192.168.20.1/24
        group-interface "group-Subscriber-1" create
            arp-populate
            dhcp
                description "Dhcp-Relay-Agent"
                proxy-server
                    emulated-server 192.168.20.1
                no shutdown
            exit
            server 10.3.31.40
            trusted
            lease-populate 10000
            gi-address 192.168.20.1 src-ip-addr
```

```

        no shutdown

    exit

    authentication-policy "auth-pol-1"

    oper-up-while-empty

    exit

    exit

    no shutdown

    exit

    exit

#-----
echo "Router (Service Side) Configuration"
#-----

    router

#-----

echo "ISIS Configuration"
#-----

    isis

        interface "to-Subscriber-1"

            passive

            no shutdown

        exit

        no shutdown

    exit

    exit

#-----

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

    subscriber-mgmt

        authentication-policy "auth-pol-1"

```

```
radius-authentication-server

server 1 address 10.3.31.40 secret "debsJaUwyaSqMOO8yJZciODhuxHenils" hash2

exit

exit

exit

#-----

echo "Mirror Configuration"

#-----

mirror

mirror-dest 1 create

sap 1/1/4 create

exit

no shutdown

exit

exit

exit all

A:SR-1#
```



## 7750 ALCATEL LUCENT PROVIDER EDGE (PE-1)

A:PE-1#

exit all

configure

#-----

echo "System Configuration"

#-----

system

name "PE-1"

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
    description "facing-server"
    ethernet
    exit
    no shutdown
exit
port 1/1/2
    shutdown
    ethernet
    exit
exit
port 1/1/3
    shutdown
    ethernet
    exit
exit
port 1/1/4
    shutdown
    ethernet
    exit
exit
port 1/1/5
    description "facing-SR-1"
    ethernet
    mtu 1518
    exit
```

```

        no shutdown

    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 "facing-SR-1"

        address 172.16.10.1/30

        port 1/1/5

        no shutdown

    exit

    interface "facing-server"

        address 10.3.31.10/24

        port 1/1/1

        no shutdown

```

```

exit

interface "system"

    address 192.168.10.2/32

    no shutdown

exit

#-----

echo "ISIS Configuration"

#-----

isis

    area-id 49.0000.1111

    interface "system"

        no shutdown

    exit

    interface "facing-SR-1"

        no shutdown

    exit

    interface "facing-server"

        no shutdown

    exit

    no shutdown

exit

#-----

echo "MPLS Configuration"

#-----

mpls

    admin-group "CAPSTONE" 1

    interface "system"

        admin-group "CAPSTONE"

        no shutdown

    exit

```

```

interface "facing-SR-1"

    admin-group "CAPSTONE"

    no shutdown

exit

exit

#-----

echo "RSVP Configuration"

#-----

rsvp

    interface "system"

        no shutdown

    exit

    interface "facing-SR-1"

        no shutdown

    exit

    no shutdown

exit

#-----

echo "MPLS LSP Configuration"

#-----

mpls

    path "unique"

        hop 1 172.16.10.2 strict

        no shutdown

    exit

    lsp "server"

        to 172.16.10.2

        from 172.16.10.1

        include "CAPSTONE"

        primary "unique"

```

```
        exit

        no shutdown

    exit

    no shutdown

exit

#-----

echo "LDP Configuration"

#-----

    ldp

        interface-parameters

            interface "facing-SR-1"

                exit

            exit

        targeted-session

            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  
exit  
exit all  
A:PE-1#
```