A

Capstone Project Report

On

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

April 14, 2014

Brijesh Shingadia

Supervised By: - Mr. Pete Nanda, Sr. Engineer, TELUS Technology Strategy

Abstract

Today's subscribers are driven by the freedom and flexibility of on-demand, video services and wide range of consumer electronics choices. They want a more flexible and personalized broadband experience in which they can consume any content or application on any device, anytime, anywhere. To achieve these enriched service offerings, service providers must first overcome the limitations of the centralized Broadband Remote Access Server (BRAS) architectures that are in place today. Service providers require a distributed architecture deployed closer to the subscriber.

Network and Services Convergence aims to deliver bundled residential voice, video and Internet data services as an integrated package, leveraging a converged IP-based infrastructure. To provide these services subscriber management is critical, because it provides the means to manage subscriber accounts and associated service profiles to specify the services each subscriber is entitled to use. It provides authentication, authorization and accounting (AAA) capabilities which enables registered subscribers and associated end-user equipment with network access to use eligible services and quantify service usage.

Dynamic subscriber management solutions address the issue of subscriber management by enabling fully dynamic provisioning of access, quality of service (QoS) and security aspects for residential subscribers without the need of intervention of network operator.

Contents

Chapter 1

Introduction

1.1 Introduction and Motivation

Subscriber management allows the network to recognize who is attempting to use network resources and dictate the services which the subscriber has access to. Managing the subscriber can be broken into two basic components, which together constitute the "policy" assigned to each subscriber:

- Determining which resources (services) the subscriber can use. The services may be optional (for example, IPTV) or automatically enabled (for example, Internet Access).
- Determining the priority of each subscriber's traffic (for each service) as it traverses the network. QoS policies can be defined to allow the amount of bandwidth the subscriber has subscribed for.

More recently, Dynamic Host Configuration Protocol (DHCP)-based IP over Ethernet (IPoE) support has been implemented in the service provider networks. Initial subscriber management implementations were static and required manual configuration of subscriber entities. This caused a substantial amount of configuration overhead on the network operator. With the increase in number of subscribers, the manual subscriber management became almost impossible. A Dynamic Provisioning solution had to be implemented to dynamically provision subscriber entities.

1.2 Problem Statement

Managing subscriber profiles continues to become increasingly challenging for service providers. The fundamental requirement for high availability remains as the number of subscribers and subscriber data continue to grow. Many service providers now operate multiple systems for authentication, authorization, and accounting (AAA), potentially on a distributed basis, further complicating seamless service delivery. Due to all these factors, subscriber management in service provider networks becomes very essential. Numerous new subscribers must be provisioned on a daily basis, while existing subscribers may make changes to their service subscriptions as well. This may amount to a significant amount of subscriber management activities on a daily basis. A dynamic subscriber management solution is required to reduce the overhead of manually provisioning the subscribers and the applicable parameters.

1.3 Objectives

The objective of this project was to design and implement a dynamic subscriber management solution to provision the subscribers on Alcatel-Lucent IP edge devices. The specific goals of this project are as follows:-

- Design and implement an Open Source based RADIUS authentication solution for authenticating and dynamically provisioning subscribers on ALU IP Edge devices.
- Configure ALU IP Edge devices with IP/MPLS configuration to simulate service provider core network.
- Configure DHCP Relay Agent to add DHCP Option 82 to outgoing DHCP requests.

Chapter 2

Solution

In this chapter, solution and analysis to the problem statement described earlier are discussed in detail. The various aspects of the subscriber management are studied and a step by step procedure followed to resolve the problem is describer briefly. The results derived from the lab testing are analyzed and their implications in problem resolution are discussed.

2.1 Challenges to DHCP based Dynamic Subscriber Management

Due to its general simplicity and scalability, along with the increased usage of Ethernet in access networks, DHCP deployments in broadband networks have increased. Understanding the challenges to providing a policy to each subscriber requires an understanding of how connections are created and packets are forwarded in a broadband network. There is one critical function that must be created using DHCP to identify the subscriber.

- RADIUS Name: - Standard DHCP does not provide any mechanism to uniquely and consistently identify a subscriber. A mechanism has to be implemented to uniquely and consistently identify the subscribers.

In DHCP networks, there are several potential ways to uniquely construct a RADIUS name. These include:

- The Media Access Control (MAC) address of the client. A network administrator would need to provision the MAC address before the subscriber could use the network. Re-provisioning would be required if the device gets replaced. As a result, this is not an acceptable method.

- The IP address of the client. In a DHCP environment, the IP address is likely to change over time. Thus, the subscriber cannot be uniquely identified in the RADIUS database based on the assigned IP address.

- A name forwarded by a downstream device such as a digital subscriber line access multiplexer (DSLAM). The DSLAM dynamically creates the identifier and inserts the name into the DHCP stream. DHCP option 82 allows a downstream device such as a DSLAM to insert a unique identifier, called a circuit identifier, during DHCP session establishment. This name is typically created dynamically by the DSLAM based upon a unique DSLAM name and physical port to which the subscriber is connected. Hence this name is unique for each subscriber.

In the service provider network, usually the subscribers are connected to a DSLAM which is then connected to a BSA or BSR. The DHCP requests from the subscribers will be intercepted by the DSLAM which will then insert the circuit-id information based on the port where it is connected to and send it to the BSA or BSR. The BSA or BSR will then trigger an authentication process to authenticate the subscriber. Once the subscriber is authenticated, the DHCP request will be forwarded to the DHCP server which will assign IP address to the client. During the process described above several policies are applied to the subscriber and several entities are created on the BSA to manage the subscriber and enforce QoS and other parameters on the subscriber.

2.2 Solution

As mentioned in figure 2.1, in a service provider environment using DHCP, during boot-up the client device sends a DHCP Discover message to get an IP address from the DHCP Server. The message contains:

- Destination MAC address — broadcast
- Source MAC address — MAC of client device
- Client hardware address — MAC of client device

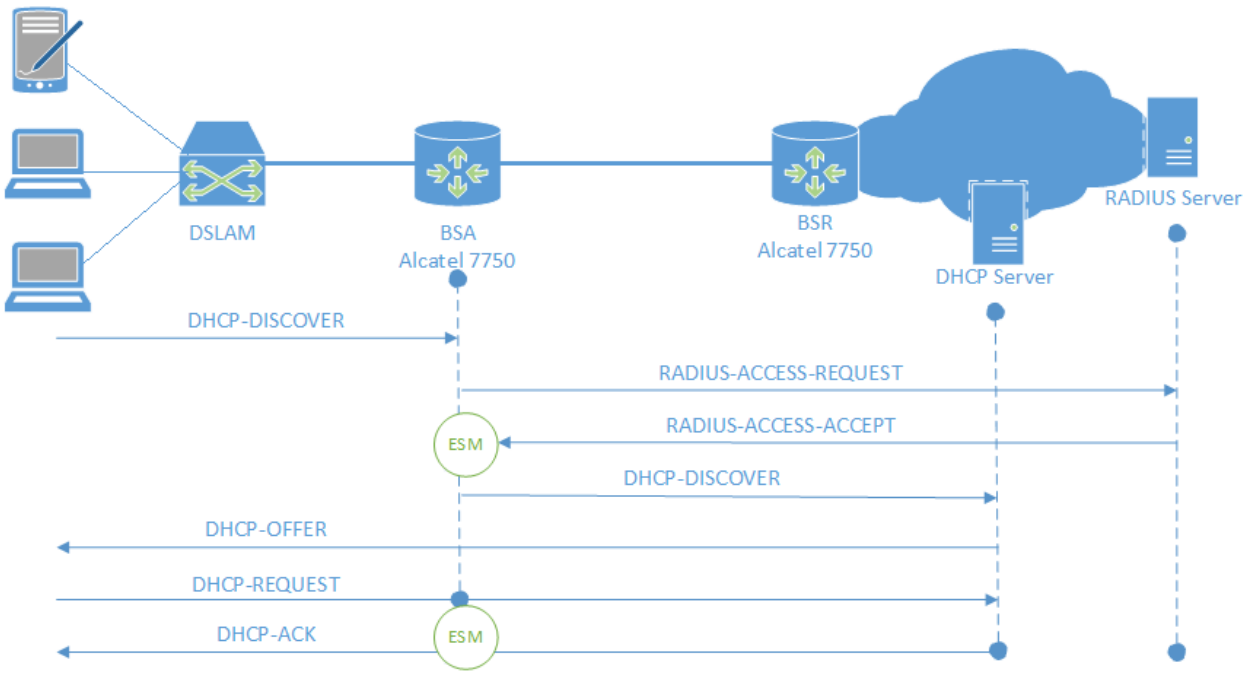

Figure 2.1: Dynamic Subscriber Management using DHCP

If this message passes through a DSLAM or other access node, typically the Relay information option (Option 82) field is added, indicating slot, port, VPI, VCI etc. to identify the subscriber. DHCP relay is enabled on the first IP interface in the upstream direction. Depending on the scenario, the DSLAM, BSA or the BSR will relay the Discover message as a unicast packet towards the configured DHCP server. DHCP relay is configured to insert the giaddr in order to indicate to the DHCP server in which subnet an address should be allocated.

When this DHCP Discover message reaches the BSA, it holds the incoming DHCP request and triggers the RADIUS authentication mechanism and sends a RADIUS Request to the RADIUS server with the circuit-id information as the RADIUS name. The RADIUS server identifies the subscriber information based on the circuit-id information, authenticates the request and sends the RADIUS Accept message back to the router. The RADIUS Accept message also contains the information about the managed SAP policy and other parameters that apply to the subscriber which are then used to create a dynamic SAP entity for the subscriber. The router on receiving the RADIUS Accept message creates the SAP for the subscriber and forwards the DHCP request to the DHCP server.

The DHCP server will look up the client MAC address and Option 82 information in its database. If the client is recognized and authorized to access the network, an IP address will be assigned and a DHCP offer message is returned back to the router. The router which can be BSA or BSR will relay this offer message back to the client device. The client selects one of the offered IP addresses and confirms it wants to use this in a DHCP request message, sent as unicast to the DHCP server that offered it.

The DHCP server confirms that the IP address is still available, updates its database to indicate it is now in use, and replies with a DHCP ACK message back to the router. The DHCP ACK message from the server also contains the subscriber identification string and the SLA and subscriber profiles applicable to the subscriber. The router intercepts the DHCP ACK message and retrieves the subscriber profiles and SLA profiles applicable to the subscriber using a Python or Perl script.

Thus using the Enhanced Subscriber Management (ESM) process described as above, helps in enabling fully dynamic provisioning of access, quality of service (QoS) and security aspects for residential subscribers without the need for manual operator intervention. It also supports a universal approach for

managing subscriber entities, subscriber profiles, and Service Level Agreement (SLA) policies across a range of deployment models.

2.2.1 Solution Setup

We followed a three phase approach to arrive to a dynamic subscribing solution. For the first two phases which were completed in the University Of Alberta lab, FreeRADIUS server acted as RADIUS and DHCP server whereas a Cisco router acted as a DHCP Relay Agent. The FreeRADIUS server and Cisco router were replaced by Alcatel DSC server and DSLAM to act as RADIUS/DHCP server and DHCP relay agent respectively.

Phase-1:- The goal of phase-1 was to get familiar with the basic authentication and DHCP relay agent mechanism. In phase-1, a PC was configured to be a DHCP/RADIUS client which was to be authenticated by a FreeRADIUS server. A Cisco router was connected between the PC and the FreeRADIUS server to act as DHCP relay agent and add the relay agent information. The server will authenticate the client based on the circuit-id field added by the DHCP relay agent and allocate IP address to the client.

Phase-2:- Once phase-1 was completed successfully, in phase-2 the Alcatel 7750 router was introduced in the setup between the DHCP relay agent and the RADIUS server to implement the subscriber and service entities. In the beginning of phase-2, only one Alcatel 7750 was introduced and the entire configuration was done on the single router with FreeRADIUS server directly connected to the network interface of the Alcatel 7750 router. IES and VPLS services were configured on the Alcatel 7750 for subscriber management. An authentication policy had to be created to initiate the authentication and send RADIUS request to the RADIUS server. A capture SAP was created on the VPLS service which would trigger the RADIUS authentication mechanism on receiving the DHCP Discover message from the client. The RADIUS request is

sent to the FreeRADIUS server which authenticates the client based on the circuit-id. Once the client is authenticated the server sends a bunch of parameters such as Managed-SAP ID, MSAP-Policy and MSAP-Interface in the RADIUS Access-Accept message. On receiving the Access-Accept message, a managed SAP is created on the group interface configured in the IES service. On successful creation of managed SAP, the DHCP Discover message is forwarded to the DHCP server which then allocates IP address to the client. The Alcatel 7750 snoops the DHCP ACK message from the server to retrieve the subscriber information and creates an active-subscriber entry in the subscriber table.

Once the provisioning worked as expected, a second Alcatel 7750 was added to the setup and MPLS, ISIS was configured between two Alcatel routers to emulate the IP/MPLS core of the service provider network.

Phase-3:- The purpose of phase-3 was to replicate the actual real world dynamic subscribing scenario which is used by TELUS in their dynamic subscribing solution.

2.3 Test Procedure

The test procedure again followed the three phased approach as discussed earlier. The first task in the phase-1 was to install the FreeRADIUS server, configure and test it to make sure it is configured properly. Once the FreeRADIUS server was installed properly, the next task was to create a test user and make sure that the RADIUS authentication worked properly. A test user was created in the users.conf file in the FreeRADIUS server along with the required parameters for authentication. The testing of the RADIUS authentication involved two steps. In step one; I tried testing the authentication locally by using the radtest command to test the authentication. Once the authentication worked locally, I modified the clients.conf file to add the IP

address of the RADIUS client and tried to send a RADIUS request from a remote client. The test results were normal as expected without any problems. Once the authentication was working fine, a DHCP Relay Agent had to be configured. A Cisco router was configured in the setup to act as a DHCP relay agent. The IP address of the DHCP server was configured as ip-helper address on the Cisco router to redirect the incoming DHCP requests to the DHCP server along with adding the circuit-id in the option 82 field in the DHCP request. The router then converts the broadcast DHCP Discover message and sends it to the DHCP server as a unicast message with the interface of the router as source IP and the DHCP server IP as destination IP address. The users.conf file in the FreeRADIUS server acts as the user database for authentication. On receiving an incoming RADIUS Request the FreeRADIUS server looks into the users.conf file to authenticate the user. The users.conf file had to be modified to add the information about the subscriber and authenticate the request based on the circuit-id information added by the DHCP relay agent. The authentication worked fine, once the required configuration was done.

Phase-2 required in depth configuration of several services and other subscriber management parameters on the Alcatel 7750 router. The first step in the configuration of Alcatel 7750 was to configure a customer which is the basic entity in the dynamic provisioning. The next step was to create the subscriber profiles and SLA profiles to be applied to the customer. The subscriber profile is a template which contains those hierarchical QoS (HQoS) and accounting settings which are applicable to all hosts belonging to the same subscriber. For the purpose of supporting multiple service types for a single subscriber, the hosts associated with a subscriber can be subdivided into multiple SLA profiles. The SLA profile contains those QoS and security settings which are applicable to individual hosts. The subscriber profile maps to the SLA profile which in turn decides the QoS settings to be applied to the customer. During the initial stages I tried to emulate the basic subscriber management by manually configuring a service access point (SAP) on the IES

service to verify the connectivity between the client and the server. A SAP is configured on the customer facing side and acts as an entry point for the traffic to enter the IP/MPLS core. An IES service is a layer-3 connectivity service which is configured to allow the customers to connect to the Internet. DHCP relay agent parameters were configured on the server to add the giaddr and remote-id to the DHCP request. In the later stages, a capture SAP was configured which would then trigger the RADIUS authentication and receive the MSAP parameters from the RADIUS server and create managed SAP on the IES service dynamically. After giving a static route from the IES IP interface to the server and configuring a default gateway on the FreeRADIUS server, I was able to ping from the client to the server and client was receiving IP address from the DHCP server.

After the basic connectivity was established, it was time to configure the enhanced subscriber management parameters on the Alcatel 7750. We have implemented a Routed-CO model in this subscribing solution which provides layer-3 services to the subscribers. This model is a combination of two key technologies, subscriber interfaces and group interfaces. Each IES service concentrates a number of subscriber-interfaces. Each subscriber interface will define at least one IP subnet. A group-interface is to be provisioned within the subscriber interface. All group interfaces created under the subscriber interface will share the same subnet. Group interfaces are configured as unnumbered and are associated with the subscriber interface under which they are configured. SAPs can be configured under the group-interface. In a VLAN-per-DSLAM model only, one SAP per group-interface is needed, while in the VLAN-per-subscriber model, a subscriber of the DSLAM will require its own SAP. All SAPs on a group-interface must be on the same physical port.

A VPLS service had to be configured on which, a capture SAP was created. 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. The capture SAP intercepts the DHCP Discover messages

from the client and initiates the RADIUS authentication. The server authenticates the client based on the circuit-in information again and returns the parameters for creation of a 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 with minimal configuration on the Alcatel 7750 router. Creation of a managed SAP is triggered by a DHCP Discover message. The authentication response message returns the subscriber host attributes with the managed SAP policy and service ID. These two parameters are used by the system to create the subscriber SAP with the settings indicated in the managed SAP policy and then assigns it to the corresponding IES service. Once the MSAP is created, the router will forward the intercepted DHCP Discover message to the DHCP server. The 7750 snoops through the DHCP ACK message from the server and retrieves the subscriber information from the message. A subscriber identification policy had to be configured to provide the python script to snoop the DHCP ACK message and retrieve the subscriber id and subscriber profile and SLA-profile values from the circuit-id and remote-id option in the DHCP ACK message.

2.4 Issues and Challenges

There were several minor to major issues and challenges faced during the completion of this project. The problems faced during the project proved to be a valuable learning experience for me and strengthened my understanding about some of the fundamental networking concepts.

One of the major challenge of this project was to develop in depth understanding about some of the fundamental concepts of service provider terminology and understand how exactly subscriber provisioning works. Developing understanding about the actual flow of traffic during the dynamic

provisioning was very important to complete this project. The configuration guides of Alcatel 7750 proved to be very handy in developing understanding about those key concepts. Though the information provided in the guide was sometimes over-whelming and was more detailed than what was required, it was very helpful in understanding the basic service provider terminologies such as SAP, Service, etc. The guides also proved to be very helpful in the configuration and troubleshooting during the entire project.

The configuration of the DHCP relay agent and FreeRADIUS server during the initial stages was very thought-provoking as well. Initially, the client was supposed to insert the option 82 information in the DHCP Discover message itself. However, after extensive research we found out that it was not possible to add the option 82 information on the client itself as the relay agent information is usually added by the first layer-3 interface en route to the DHCP Server. Hence, it was decided to make the Cisco switch as a DHCP relay agent to add the option 82 information. Once the FreeRADIUS server and DHCP relay agent information was installed and configured, authenticating based on the circuit-id information was extremely strenuous. The central issue was that the circuit-id information sent by the Cisco router was using ascii values whereas the FreeRADIUS server understands it in the GELT format. After trying out several tweaks and work around finally the issue was resolved successfully.

The configuration of the profiles and services on the Alcatel 7750 wasn't a big problem once I had developed the understanding about the concepts. The subscriber profiles, SLA profiles, IES service and SAP's were configured very easily without any major glitches. However, one major problem occurred while testing the authentication from the Alcatel 7750 using the capture SAP. It was seen in the logs that the capture SAP was dropping the DHCP Discover messages instead of triggering the RADIUS authentication mechanism. The configuration of the capture SAP looked fine. The authentication policy was also configured correctly with IP Address of the FreeRADIUS server. It seemed to me in the beginning that it was a routing issue on the Alcatel 7750 router as

I was not able to ping from the subscriber interface of the Alcatel 7750 to the FreeRADIUS server. However, after collecting the debug captures on the Alcatel 7750 and TCP dump on the FreeRADIUS server, I found out that the Gateway IP address was missing on the FreeRADIUS server because of which it was not able to route the packets for subscriber interface. Once the IP address of the Alcatel 7750 was configured as the Default Gateway, the authentication worked fine.

Once the RADIUS authentication worked as intended, the router was forwarding the intercepted DHCP Discover message to the DHCP server. However, the client was not receiving the IP address from the DHCP server. In the debug logs, I could see that the DHCP Boot Request was being forwarded to the server. However, it was unsure whether the server was replying back or not. After, collecting TCP dumps on the DHCP server it was clear that the server was replying back as well. The connectivity didn't seem like a problem as the RADIUS authentication worked fine. After collecting several other debug logs on the Alcatel 7750, I saw an error message stating "Dropped DHCP DISCOVER packet on group interface g1. Problem: 10.3.31.249. No route to destination found from the interface." It seemed like a routing issue again from the message. The Alcatel router was not able to find a route to the IP Address 10.3.31.249 from the group interface which was odd because the IP Address was of the network interface of the same router. The status of the subscriber interface was staying down because the group interface configured on the subscriber interface was down as well. I thought this could be the problem because of which the DHCP request was getting dropped. Hence, I executed the command oper-up-when-empty to make the subscriber interface stay up. However, still this did not resolve the issue. The next step I tried was to make the network interface connected to the FreeRADIUS server as an IES interface, but still the problem remain unresolved. After doing some research, I found out that I had given an attribute called Framed-IP-Address in the FreeRADIUS configuration which is the IP address that is given to the client. However, along

with the Framed-IP-Address it is also essential to provide the Framed-Route attribute which provides the route to the client. However, the entire attribute configuration was unnecessary as the IP address to the client is to be given from the DHCP server. Once I removed that attribute from the FreeRADIUS configuration everything worked fine. The Alcatel 7750 was initiating the RADIUS authentication on receiving the incoming DHCP Discover message and after successful authentication the client was getting IP address from the DHCP server as desired.

There were several minor and major obstructions in the project completion as mentioned above. However, these issues made the project more challenging and helped me develop a thorough understanding of the concepts.

2.5 Results Analysis

The results of the dynamic provisioning show that by using Enhanced Subscriber Management it is possible to enable fully dynamic provisioning of access, quality of service (QoS) and security aspects for residential subscribers without any manual intervention. The RADIUS authentication process to authenticate subscriber on incoming DHCP request was verified by collecting the debug logs on the BSA and on the FreeRADIUS server. The output of the RADIUS authentication logs is as shown below:-

```
*A:NS133380112# show log log-id 5
===============================================================
Event Log 5
===============================================================
Description : (Not Specified)
Memory Log contents  [size=500   next event=17  (not wrapped)]

16 2000/01/01 01:31:01.97 UTC MINOR: DEBUG #2001 Base PIP
"PIP: DHCP instance 1 (Base), interface index 5 (g1),transmitted DHCP Boot
Reply to Interface g1 (1/1/1:10) Port 68
```

```
   H/W Type: Ethernet(10Mb)  H/W Address Length: 6
   ciaddr: 0.0.0.0           yiaddr: 192.168.1.2
   siaddr: 10.3.31.40        giaddr: 192.168.1.1
   chaddr: c8:9c:1d:32:e0:80    xid: 0xd79

   DHCP options:
   [82] Relay agent information: len = 14
      [1] Circuit-id: (hex) 00 00 00 05
   [53] Message type: Ack
   [1] Subnet mask: 255.255.255.0
   [3] Router: 192.168.1.1
   [51] Lease time: 7200
   [54] DHCP server addr: 10.3.31.40
   [57] Max msg size: 1200
   [255] End
"

15 2000/01/01 01:31:01.97 UTC MINOR: DEBUG #2001 Base Python Result
"Python Result: script1.py
sub_ident: 1/1/1:10
sub_profile_string: subsla1
sla_profile_string: subscprofile1
"

13 2000/01/01 01:31:01.96 UTC MINOR: DEBUG #2001 Base PIP
"PIP: DHCP instance 1 (Base), interface index 2 (to_RADIUS), received DHCP
Boot Reply on Interface to_RADIUS (1/1/2) Port 67

   H/W Type: Ethernet(10Mb)  H/W Address Length: 6
   ciaddr: 0.0.0.0           yiaddr: 192.168.1.2
   siaddr: 10.3.31.40        giaddr: 192.168.1.1
   chaddr: c8:9c:1d:32:e0:80    xid: 0xd79

   DHCP options:
   [82] Relay agent information: len = 30
      [1] Circuit-id: (hex) 00 00 00 05
      [2] Remote-id: sla1-subscprofile1
   [53] Message type: Ack
   [1] Subnet mask: 255.255.255.0
   [3] Router: 192.168.1.1
   [51] Lease time: 7200
   [54] DHCP server addr: 10.3.31.40
   [57] Max msg size: 1200
   [255] End
"
```

12 2000/01/01 01:31:01.94 UTC MINOR: DEBUG #2001 Base PIP
"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: 192.168.1.1
chaddr: c8:9c:1d:32:e0:80 xid: 0xd79

DHCP options:
[82] Relay agent information: len = 14
[1] Circuit-id: (hex) 00 00 00 05
[53] Message type: Request
[57] Max msg size: 1200
[61] Client id: (hex) 00 63 69 73 63 6f 2d 63 38 39 63 2e 31 64 33 32 2e 65 30 38 30 2d 47 69 30 2f 30
[54] DHCP server addr: 10.3.31.40
[50] Requested IP addr: 192.168.1.2
[12] Host name: Router
[55] Param request list: len = 8
1 Subnet mask
6 Domain name server
15 Domain name
44 NETBIOS name server
3 Router
33 Static route
150 Unknown option
43 Vendor specific
[60] Class id: dslforum.org
[255] End
"
10 2000/01/01 01:31:01.94 UTC MINOR: DEBUG #2001 Base PIP
"PIP: DHCP instance 1 (Base), interface index 5 (g1), transmitted DHCP Boot Reply to Interface g1 (1/1/1:10) Port 68

H/W Type: Ethernet(10Mb) H/W Address Length: 6
ciaddr: 0.0.0.0 yiaddr: 192.168.1.2
siaddr: 10.3.31.40 giaddr: 192.168.1.1
chaddr: c8:9c:1d:32:e0:80 xid: 0xd79

DHCP options:
[82] Relay agent information: len = 14
[1] Circuit-id: (hex) 00 00 00 05
[53] Message type: Offer
[1] Subnet mask: 255.255.255.0
[3] Router: 192.168.1.1

```
   [51] Lease time: 7200
   [54] DHCP server addr: 10.3.31.40
   [57] Max msg size: 1200
   [255] End
"

9 2000/01/01 01:31:01.94 UTC MINOR: DEBUG #2001 Base RADIUS
"RADIUS: Receive
  Access-Accept(2) id 30 len 78 from 10.3.31.40:1812 vrid 1 pol acctpol1
    VSA [26] 10 Alcatel(6527)
      SUBSC ID STR [11] 8 1/1/1:10
    VSA [26] 6 Alcatel(6527)
      MSAP SERVICE ID [31] 4 1
    VSA [26] 14 Alcatel(6527)
      MSAP POLICY [32] 12 msap-default
    VSA [26] 4 Alcatel(6527)
      MSAP INTERFACE [33] 2 g1
"

8 2000/01/01 01:31:01.93 UTC MINOR: DEBUG #2001 Base RADIUS
"RADIUS: Transmit
  Access-Request(1) 10.3.31.40:1812 id 30 len 79 vrid 1 pol acctpol1
    USER NAME [1] 17 00 00 00 05
    PASSWORD [2] 16 FWa7dO.80zXEd9R8hBEp6E
    NAS IP ADDRESS [4] 4 10.1.2.1
    NAS PORT TYPE [61] 4 Ethernet(15)
    NAS PORT ID [87] 8 1/1/1:10

3 2000/01/01 01:31:01.90 UTC MINOR: DEBUG #2001 Base PIP
"PIP: DHCP instance 1 (Base), interface index 5 (g1), received DHCP Boot
Request on Interface g1 (1/1/1:10) 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: c8:9c:1d:32:e0:80    xid: 0xd79

   DHCP options:
   [82] Relay agent information: len = 14
     [1] Circuit-id: (hex) 00 00 00 05
   [53] Message type: Discover
   [57] Max msg size: 1200
   [61] Client id: (hex) 00 63 69 73 63 6f 2d 63 38 39 63 2e 31 64 33 32 2e
   65 30 38 30 2d 47 69 30 2f 30
   [12] Host name: Router
   [55] Param request list: len = 8
```

```
        1  Subnet mask
        6  Domain name server
       15  Domain name
       44  NETBIOS name server
        3  Router
       33  Static route
      150  Unknown option
       43  Vendor specific
[60] Class id: dslforum.org
[255] End
```

As shown in the logs, the RADIUS Access-Request message is sent to the RADIUS server on receiving the DHCP message. The Access-Request message contains the circuit-id as the user name for the authentication. As seen in Figures 3.1 and 3.2, the RADIUS server authenticates the subscriber and sends the Access-Accept message which has the information about the MSAP policy and the service id and the group interface on which the MSAP is to be configured.

```
rad_recv: Access-Request packet from host 10.1.2.1 port 64384, id=36, length=79
        User-Name = " 312f312f313a3130"
        User-Password = "password123"
        NAS-IP-Address = 10.1.2.1
        NAS-Port-Type = Ethernet
        NAS-Port-Id = "1/1/1:10"
```

Figure 3.1: RADIUS Access-Request Message received at FreeRADIUS server

```
Sending Access-Accept of id 36 to 10.1.2.1 port 64384
        Alc-Subsc-ID-Str = "1/1/1:10"
        Alc-MSAP-Serv-Id = 1
        Alc-MSAP-Policy == "msap-default"
        Alc-MSAP-Interface == "g1"
```

Figure 3.2: RADIUS Access-Accept Message received at FreeRADIUS server

Once the MSAP is created the DHCP request is relayed to the DHCP server to the DHCP server as visible in Figure 3.3.

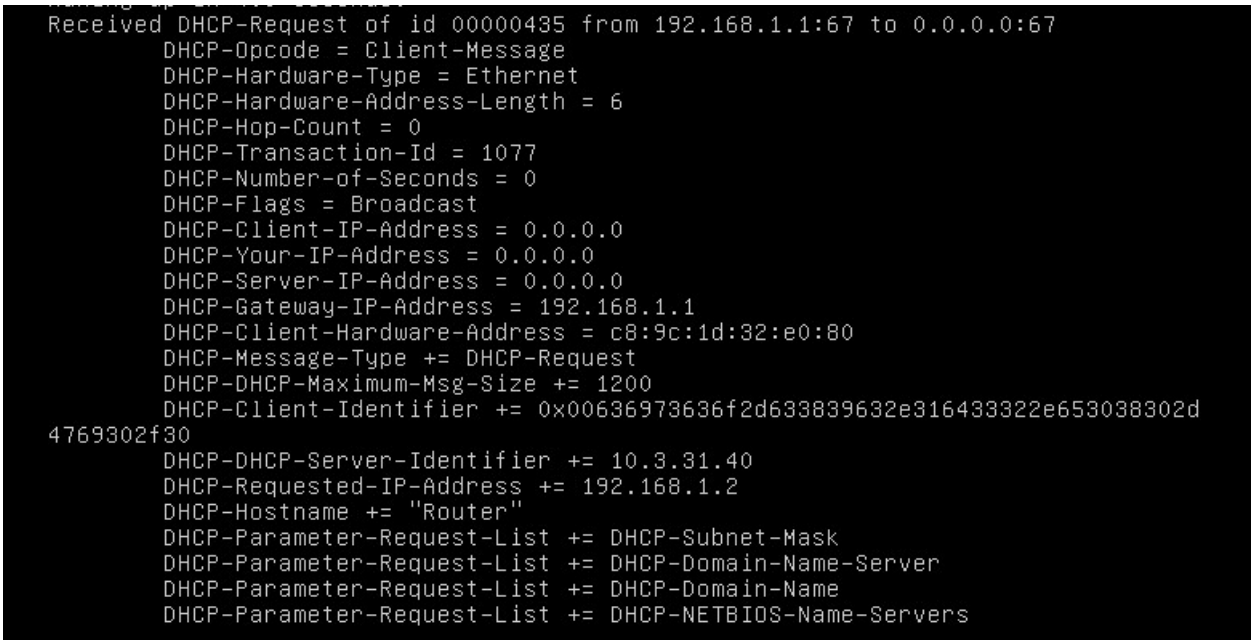

Figure 3.3: DHCP Request message at DHCP Server

The DHCP Reply message sent by the DHCP server has the information about the IP address assigned to the client. The message also contains the circuit-id and remote-id information from which the BSA will retrieve the subscriber identification string and the SLA and subscriber profiles applicable to the subscriber using a Python script. The BSA identifies the subscriber and manages the subscriber information using the subscriber identification string. The SLA profile will determine the QoS and the security setting s applied to the subscriber. The main focus of this project was on the Dynamic Provisioning; hence SLA and Subscriber profiles have been kept to a basic level. However, several SLA profiles could be created and applied to the subscriber for bandwidth allocation and other QoS aspects.

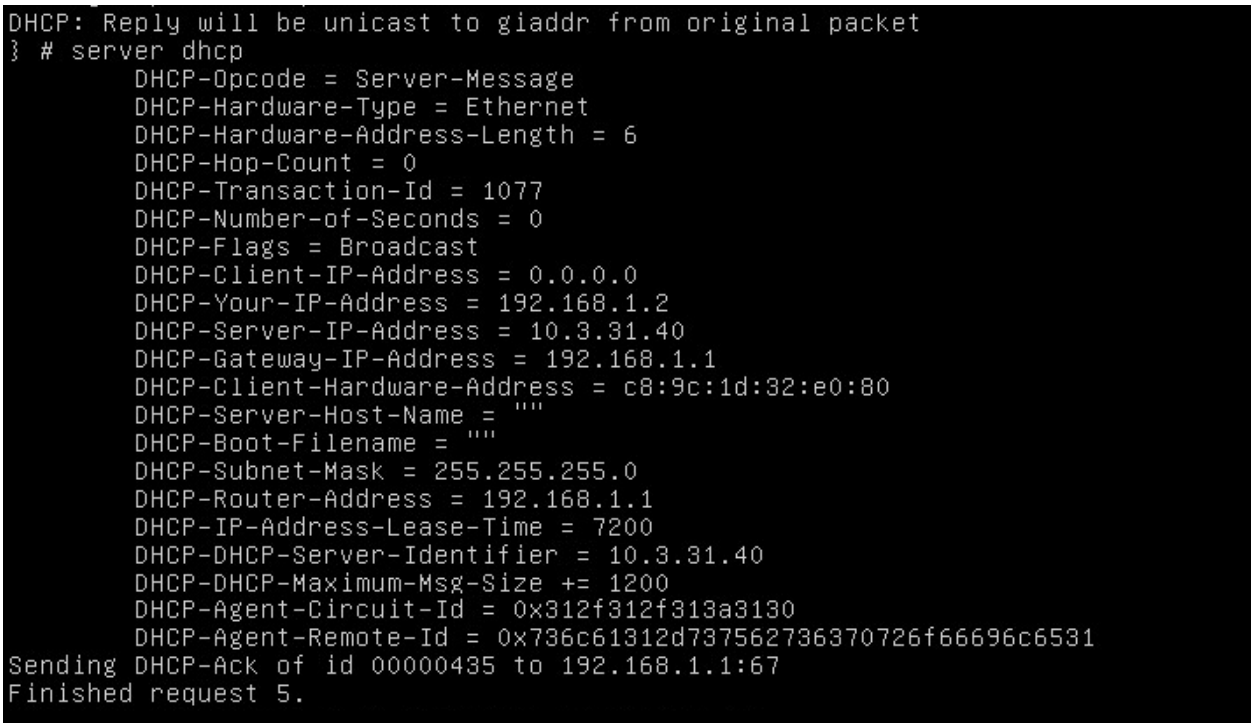

Figure 3.3: DHCP ACK message from the DHCP server

Figure 3.3 shows the DHCP ACK message sent by the DHCP server with the client IP address and the circuit-id and remote id information.

When ESM is enabled on a SAP, the system expands the information it stores about the subscriber host which allows SLA enforcement and accounting features to be applied on per SAP basis. The additional information can be retrieved by snooping the DHCP ACK message using a Python or a Perl script that assists in the subscriber host identification process. A subscriber host is identified using a subscriber identification string which is derived by manipulating the Option 82 information in the DHCP ACK message. A subscriber identification policy must be used to process the dynamic host DHCP events to manage the lease state information stored per subscriber host. The script is configured as a part of the subscriber identification policy to retrieve the subscriber information. The script also derives the appropriate

subscriber and SLA profiles used to define the hierarchical QoS and unique queuing and filtering required for each subscriber host. The system performs SLA enforcement functions on a per subscriber SLA profile instance basis. SLA enforcement functions include QoS, security, and accounting which are applicable to the subscriber. The subscriber and SLA profiles derived from the DHCP ACK message and applied to the subscriber can be verified using the command show service active subscribers hierarchy as shown below:-

```
*A:NS133380112#  show service active-subscribers hierarchy
===============================================================
Active Subscriber hierarchy
===============================================================
-- 1/1/1:10 (subscprofile1)
   |
   |-- sap:[1/1/1:10] -sla:sla1
   |    |
   |    |-- 192.168.1.2
   |    |   c8:9c:1d:32:e0:80  - N/A (DHCP)
   |    |

===============================================================
*A:NS133380112
```

The subscriber identification string 1/1/1:10 is derived from the option 82 information. Once the subscriber is identified, the subscriber and SLA profiles are also derived and applied to the active subscriber host as shown above. The host's IP address + MAC address are populated in the subscriber host table on the appropriate SAP to allow packets matching the IP address and MAC address access to the provider's network. The subscriber host table can be verified using the command show service active-subscribers.

```
*A:NS133380112# show service active-subscribers
===============================================================
Active Subscribers
===============================================================
-------------------------------------------------------------------------------------------------------
Subscriber 1/1/1:10 (subscprofile1)
-------------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------------
(1) SLA Profile Instance sap:[1/1/1:10] - SLA:SLA1
-------------------------------------------------------------------------------------------------------
IP Address
                MAC Address       PPPoE-SID Origin
-------------------------------------------------------------------------------------------------------
192.168.1.2
                c8:9c:1d:32:e0:80  N/A       DHCP

-------------------------------------------------------------------------------------------------------
Number of active subscribers : 1
-------------------------------------------------------------------------------------------------------
*A:NS133380112#
```

Chapter 3

Conclusions

In this project, a dynamic subscriber management solution was designed and implemented to dynamically provision subscriber entities and enforce applicable profiles and QoS policies on them. The project was accomplished in a multivendor environment to demonstrate interoperability in service provider network designs. The use of Enhanced Subscriber Management (ESM) provides a subscriber management model that can be used with both DHCP and RADIUS based authentication to facilitate the integration in existing environments. It helps to maintain consistent and universal subscriber IDs, subscriber profiles and SLA profiles in the form of user friendly labels that are independent from the network-level resource implementation details. The complexity of the policy configuration tasks is significantly reduced, because high-level subscriber and service-oriented policies can be conveyed and track-down to the network level. Dynamic policy auto configuration for subscriber hosts during the DHCP process further improves subscriber management scalability by making changes of subscriber hosts as and when required. It minimizes the amount of state information and resources being used in the network, because policies are automatically created and removed as required. It significantly limits the proliferation of static policy information in the network. ESM supports ultimate flexibility for subscriber connectivity and service aggregation models in any mode of operation, and optimizes the operational deployment of the Triple Play Service Delivery Architecture for customer-specific deployment scenarios. Through the introduction of subscriber identification scripts and DHCP, a flexible subscriber-management solution is obtained without any constraints. It overcomes implementation-specific differences when using broadband access equipment of different technologies, makes and models by using powerful scripting capabilities.

Although in this project, the dynamic subscriber solution was implemented on ALU 7750 devices, a similar solution can be implemented using IP Edge network elements from other IP networking equipment vendors.

3.1 Future Work

The main focus of this project was to implement Dynamic Subscriber Management for subscribers using an Open Source based RADIUS authentication. However, this is just the first step in managing the subscribers. A significant amount of configuration is still required to track the data usage and implement bandwidth and other restrictions on the subscribers as required. The future work may include replacing the open source FreeRADIUS servers with ALU DSC server for ease of configuration and management. A more real world scenario could be implemented by using DSLAM to act as a DHCP relay agent in the setup. The future work would also include configuration of QoS policies to enforce bandwidth restrictions on subscribers depending on the plan they have subscribed for. IP filtering policies could also be configured on ingress and egress interfaces to screen subscribers based on IP or MAC addresses. RADIUS accounting can be configured to track the data usage for billing purposes.

Appendices

Appendix A: Customers and Subscribers

The terms customers and subscribers are often used synonymously in service provider networks. A customer or a subscriber is an individual device or a collection of devices that are enforced with similar set of policies. The most basic required entity is the customer ID value which is assigned when the customer account is created. To provision a service, a customer ID must be associated with the service at the time of service creation.

A host is a device identified by a unique combination of IP address and MAC address. A host can be any type of end-user device such as PC, VoIP phone, set-top box or a Residential Gateway. Each subscriber host must be either statically provisioned or dynamically learned by the system.

Appendix B: Service

A service is a globally unique entity that refers to a type of connectivity service for either Internet or VPN connectivity. Each service is uniquely identified by a service ID within a service area. The 7750 SR service model uses logical service entities to construct a service. In the service model, logical service entities are provide a uniform, service-centric configuration, management, and billing model for service provisioning. Services can provide Layer 2/bridged service or Layer3/IP routed connectivity between a service access point (SAP) on one router and another service access point (a SAP is where traffic enters and exits the service) on the same (local) or another router (distributed). A distributed service spans more than one router.

Appendix C: Service Access Point (SAP)

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 router. The SAP configuration requires that slot, XMA/MDA, and port information be specified. The slot, MCM/XMA/MDA, and port/channel parameters must be configured prior to provisioning a service.

Managed SAP with Routed CO

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

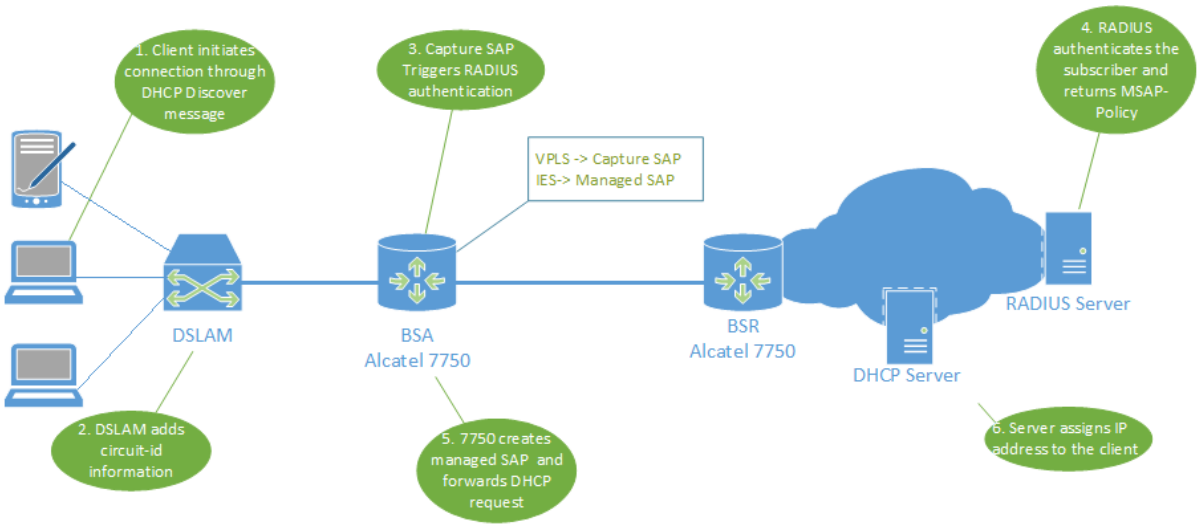

Figure a: Managed SAP with Routed CO model

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.

Appendix D: BSR Configuration

```
*A:NS133380112# 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 SAT JAN 01 20:39:31 2000 UTC

exit all
configure
#--------------------------------------------------------------------------------------------
echo "System Configuration"
#--------------------------------------------------------------------------------------------
    system
        snmp
            shutdown
        exit
        time
            sntp
                shutdown
            exit
            zone UTC
        exit
        thresholds
            rmon
            exit
        exit
    exit
#--------------------------------------------------------------------------------------------
echo "System Security Configuration"
#--------------------------------------------------------------------------------------------
     system
        security
            ftp-server
            profile "ftp-profile"
            exit
            user "admin"
                password "kMOqdD4PN1LZ6JSpuT6Ehk" hash2
                access console ftp
                console
                    member "administrative"
                exit
            exit
```

```
            per-peer-queuing
        exit
    exit
#--------------------------------------------------------------------------------------------------
echo "Log Configuration"
#--------------------------------------------------------------------------------------------------
    log
        log-id 5
            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
        ethernet
            mode access
            encap-type dot1q
        exit
        no shutdown
    exit
    port 1/1/2
```

```
        ethernet
            mtu 1518
        exit
        no shutdown
    exit
    port 1/1/3
        ethernet
        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 "Management Router Configuration"
#--------------------------------------------------------------------------------------------
    router management
    exit

#--------------------------------------------------------------------------------------------
echo "Router (Network Side) Configuration"
#--------------------------------------------------------------------------------------------
    router
        interface "system"
            address 10.1.2.1/32
            no shutdown
        exit
        interface "to_RADIUS"
            address 192.168.3.1/24
            port 1/1/2
```

```
            no shutdown
        exit
        interface "to_ftp"
            address 192.168.2.64/24
            port 1/1/3
            no shutdown
        exit
#--------------------------------------------------------------------------------------------------
echo "ISIS Configuration"
#--------------------------------------------------------------------------------------------------
        isis
            area-id 49.0001.0001
            interface "system"
                no shutdown
            exit
            interface "to_RADIUS"
                no shutdown
            exit
            no shutdown
        exit
#--------------------------------------------------------------------------------------------------
echo "MPLS Configuration"
#--------------------------------------------------------------------------------------------------
        mpls
            admin-group "to_alcatel" 10
            interface "system"
                admin-group "to_alcatel"
                no shutdown
            exit
            interface "to_RADIUS"
                admin-group "to_alcatel"
                no shutdown
            exit
        exit
#--------------------------------------------------------------------------------------------------
echo "RSVP Configuration"
#--------------------------------------------------------------------------------------------------
        rsvp
            interface "system"
                no shutdown
            exit
            interface "to_RADIUS"
                no shutdown
            exit
            no shutdown
        exit
```

```
#--------------------------------------------------------------------------------------------
echo "MPLS LSP Configuration"
#--------------------------------------------------------------------------------------------
        mpls
            path "to_alcatel"
                shutdown
                hop 1 192.168.3.2 loose
            exit
            lsp "to_alcatel"
                to 192.168.3.2
                from 192.168.3.1
                include "to_alcatel"
                primary "to_alcatel"
                exit
                no shutdown
            exit
            no shutdown
        exit
#--------------------------------------------------------------------------------------------
echo "LDP Configuration"
#--------------------------------------------------------------------------------------------
         ldp
            interface-parameters
                interface "to_RADIUS"
                exit
            exit
            targeted-session
                peer 192.168.3.2
                    tunneling
                        lsp "to_alcatel"
                    exit
                exit
            exit
            no shutdown
        exit
#--------------------------------------------------------------------------------------------
echo "Web Portal Protocol Configuration"
#--------------------------------------------------------------------------------------------
    exit

#--------------------------------------------------------------------------------------------
echo "Subscriber-mgmt Configuration"
#--------------------------------------------------------------------------------------------
    subscriber-mgmt
        authentication-policy "acctpol1" create
            password "vioHpykZnpg05KPEpK4.62FjEOoDteks7eGP7HzePeA" hash2
```

```
            radius-authentication-server
                source-address 192.168.1.1
            exit
            user-name-format circuit-id
        exit
        SLA-profile "SLA1" create
        exit
        sub-profile "subscprofile1" create
            SLA-profile-map
                entry key "SLA1" SLA-profile "SLA1"
            exit
        exit
        sub-ident-policy "identificationpolicy1" create
        exit
        sub-ident-policy "subident" create
            SLA-profile-map
                entry key "SLA1" SLA-profile "SLA1"
            exit
            primary
                script-url "cf3:\script1.py"
                no shutdown
            exit
        exit
        sub-ident-policy "subident1" create
        exit
        msap-policy "msap1" create
            sub-SLA-mgmt
                def-sub-id use-sap-id
            exit
        exit
        msap-policy "msap-default" create
            sub-SLA-mgmt
                def-sub-id use-sap-id
                def-sub-profile "subscprofile1"
                def-SLA-profile "SLA1"
                sub-ident-policy "subident"
            exit
        exit
    exit
#--------------------------------------------------------------------------------------------
echo "Service Configuration"
#--------------------------------------------------------------------------------------------
    service
        customer 1 create
            description "Brijesh"
        exit
```

```
customer 2 create
    description "abc"
exit
ies 1 customer 1 create
    subscriber-interface "to_DSLAM" create
        group-interface "g1" create
        exit
    exit
exit
ies 1 customer 1 create
    subscriber-interface "to_DSLAM" create
        address 192.168.1.1/24
        group-interface "g1" create
            arp-populate
            dhcp
                proxy-server
                    emulated-server 192.168.1.1
                    no shutdown
                exit
                option
                    action keep
                    no remote-id
                exit
                server 10.3.31.40
                trusted
                lease-populate 8000
                relay-unicast-msg release-update-src-ip
                gi-address 192.168.1.1 src-ip-addr
                no shutdown
            exit
            authentication-policy "acctpol1"
            oper-up-while-empty
        exit
    exit
    no shutdown
exit
vpls 10 customer 1 create
    stp
        shutdown
    exit
    sap 1/1/1:* capture-sap create
        trigger-packet arp dhcp dhcp6 pppoe
        msap-defaults
            group-interface "g1"
            policy "msap-default"
            service 1
```

```
            exit
            authentication-policy "acctpol1"
         exit
         no shutdown
      exit
   exit
#--------------------------------------------------------------------------------------------------
echo "Router (Service Side) Configuration"
#--------------------------------------------------------------------------------------------------
   router
#--------------------------------------------------------------------------------------------------
echo "ISIS Configuration"
#--------------------------------------------------------------------------------------------------
      isis
         interface "to_DSLAM"
            passive
            no shutdown
         exit
         no shutdown
      exit
#--------------------------------------------------------------------------------------------------
echo "RADIUS Server Configuration"
#--------------------------------------------------------------------------------------------------
      radius-server
         server "1" address 10.3.31.40 secret
"ICqVF3w1MsTsnbDibh8rr5sy2UmTBfy3" hash2 create
         exit
      exit
   exit

#--------------------------------------------------------------------------------------------------
echo "Source IP Address Configuration"
#--------------------------------------------------------------------------------------------------
   system
      security
         source-address
            application ftp "to_FTP"
         exit
      exit
   exit
#--------------------------------------------------------------------------------------------------
echo "Subscriber-mgmt (Service Side) Configuration"
#--------------------------------------------------------------------------------------------------
   subscriber-mgmt
      authentication-policy "acctpol1"
         radius-authentication-server
```

```
        server 1 address 10.3.31.40 secret
        "Kw1aR4QXVzxKwnc47zY0G5gqq.jfTH3I" hash2
          exit
      exit
      user-name-format circuit-id
    exit

exit all

# Finished SAT JAN 01 20:39:34 2000 UTC
*A:NS133380112#
```

Appendix E: BSR Configuration

```
*A:NS133380116# 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 SUN JAN 02 01:39:23 2000 UTC

exit all
configure
#--------------------------------------------------------------------------------------------------
echo "System Configuration"
#--------------------------------------------------------------------------------------------------
    system
        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 5
            from debug-trace
```

```
            to memory 500
        exit
    exit
#--------------------------------------------------------------------------------------------
echo "System Security Cpm Hw Filters and PKI Configuration"
#--------------------------------------------------------------------------------------------
    system
        security
        exit
    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
            mtu 1518
        exit
        no shutdown
    exit
    port 1/1/2
        ethernet
            mtu 1518
        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 10.1.3.1/32
            no shutdown
        exit
        interface "to_RADIUS"
            address 10.3.31.150/24
            port 1/1/2
            no shutdown
        exit
        interface "to_alcatel1"
            address 192.168.3.2/24
            port 1/1/1
            no shutdown
        exit
#--------------------------------------------------------------------------------------------------
echo "ISIS Configuration"
#--------------------------------------------------------------------------------------------------
        isis
            area-id 49.0001.0001
            interface "system"
                no shutdown
            exit
```

```
            interface "to_RADIUS"
                no shutdown
            exit
            interface "to_alcatel1"
                no shutdown
            exit
            no shutdown
        exit
#--------------------------------------------------------------------------------------------------
echo "MPLS Configuration"
#--------------------------------------------------------------------------------------------------
        mpls
            admin-group "to_alcatel" 10
            interface "system"
                no shutdown
            exit
            interface "to_alcatel1"
                no shutdown
            exit
        exit
#--------------------------------------------------------------------------------------------------
echo "RSVP Configuration"
#--------------------------------------------------------------------------------------------------
        rsvp
            interface "system"
                no shutdown
            exit
            interface "to_alcatel1"
                no shutdown
            exit
            no shutdown
        exit
#--------------------------------------------------------------------------------------------------
echo "MPLS LSP Configuration"
#--------------------------------------------------------------------------------------------------
        mpls
            path "to_alcatel"
                hop 1 192.168.3.1 loose
                no shutdown
            exit
            lsp "to_alcatel"
                to 192.168.3.1
                from 192.168.3.2
                include "to_alcatel"
                primary "to_alcatel"
                exit
```

```
            no shutdown
         exit
         no shutdown
      exit
#------------------------------------------------------------------------------------------------
echo "LDP Configuration"
#------------------------------------------------------------------------------------------------
       ldp
         interface-parameters
            interface "to_alcatel1"
            exit
         exit
         targeted-session
            peer 192.168.3.1
               tunneling
                  lsp "to_alcatel"
               exit
            exit
         exit
         no shutdown
      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

# Finished SUN JAN 02 01:39:25 2000 UTC
*A:NS133380116
```

References

1) Alcatel-Lucent, “Alcatel-Lucent 7750 SR OS Triple Play Configuration Guide”, pp. 29-47, 571-655, October 2013.
2) Alcatel-Lucent, “Alcatel-Lucent 7750 SR OS Advanced Configuration Guide”, pp. 337-368, October 2013.
3) Alcatel-Lucent, “Alcatel-Lucent 7750 SR OS Services Guide”, pp. 37-44, October 2013.
4) Alcatel-Lucent, “Alcatel-Lucent 7750 SR for Residential Broadband”, pp 1-3, April, 2012.
5) Alcatel-Lucent, “Residential Services Delivery”, 2014.