Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 2 – No.2, June 2015 – www.caeaccess.org

Prototype Cloud-based Services on MPLS Service Provider in Iraq

Shahad H. Zwayen
College of Information Engineering
Al-Nahrain University
Iraq, Baghdad

Mustapha B. Ibrahim
College of Information Engineering
Al-Nahrain University
Iraq, Baghdad

ABSTRACT

Multiprotocol Label Switching (MPLS) is a technique for data transmission that works on wide area networks (WAN), it is used by most service providers to improve the functionality of the ISPs networks, ISPs and suppliers of Internet services use this technique to take advantage of their ability to engineering data traffic in the network traffic. Guaranteed QoS in an MPLS network requires backup paths to be preset in the network. As the world is moving to virtualization techniques Cloud computing has become an important feature for service providers. Windows Server 2012 R2 will be our tool to provide customers with the services. A business paradigm with flexible and powerful computational architecture will be shown to offer universal services to users via Internet or local network. Three main services provided by the cloud are (IaaS, SaaS and PaaS).

Keywords

Multiprotocol Label Switching (MPLS) , Frame-Relay (FR), Cloud-Computing, Graphical Network Simulator (GNS3), Virtual Private Network (VPN), Virtual Routing and Forwarding (VRF), Traffic Engineering (TE), Adaptive Security Appliance (ASA), Generic Routing Encapsulation (GRE), Internet Protocol (IP), Voice Over IP (VOIP), Open Shortest Path First (OSPF), Border Gateway Protocol (BGP).

1. INTRODUCTION

Service providers around the world can use techniques like ATM, Frame-Relay, MPLS and others to deliver services to their customers. Globally Frame-Relay was widely used but since the technology is growing so fast the world starts to migrate to a newest technology (e.g. MPLS), Frame-Relay has start to be discontinued by major Internet service providers. Our goal was to make Iraq keep pace with the world. MPLS is a private networking technology similar to the concept of Frame Relay that delivers data in the “cloud” which leads service providers in Iraq to move to virtualization world [1]. This service provider provides clients with internet, remote application access and a full access and control on the virtual machine with a full Email system. The customer can query any application, a username and password would be given to login and access the application they requested [2]. Multicast was chosen as a part of the services may be offered, based on the requirements of services that would be provided to customers like TV services that is very important and widely used In Iraq today.

2. SERVICE PROVIDER DESIGN

The proposed Visio design shown in figure 1-2 describes how the infrastructures were allocated to cover most of Iraq's provinces.

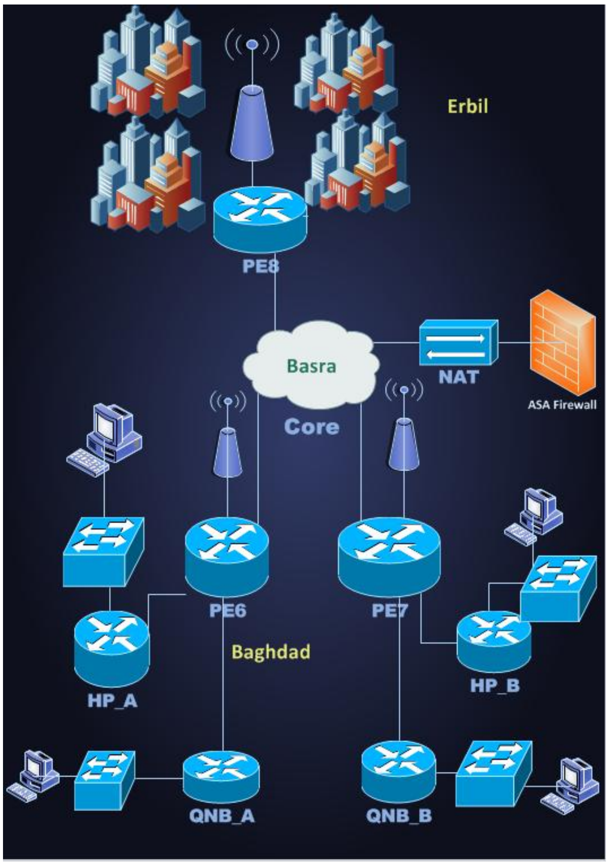

Figure 1-1: Service provider design

3. COMPETITIVE TECHNIQUES

In Iraq, service providers still work with legacy technologies like Frame-Relay. FR doesn’t support VPN's or QoS or Traffic Engineering It's based on an oversubscription model where frames get switched around in a Frame relay cloud. MPLS is a layer2.5 technology that switches data packets below layer3; it handles data much faster without the overhead of L3 protocols. We hoped to change the existing used technology with MPLS which is highly recommended by the world most popular service providers. A comparative analysis was made between existing techniques using OPNET modeler 14.5 simulator.

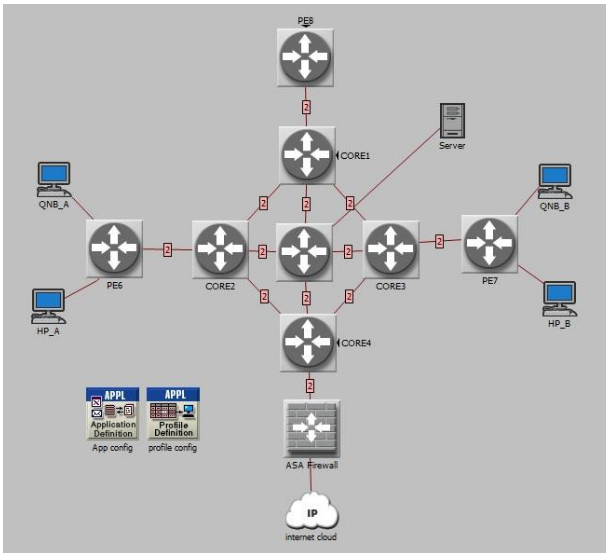

Figure 1-2: Frame relay topology

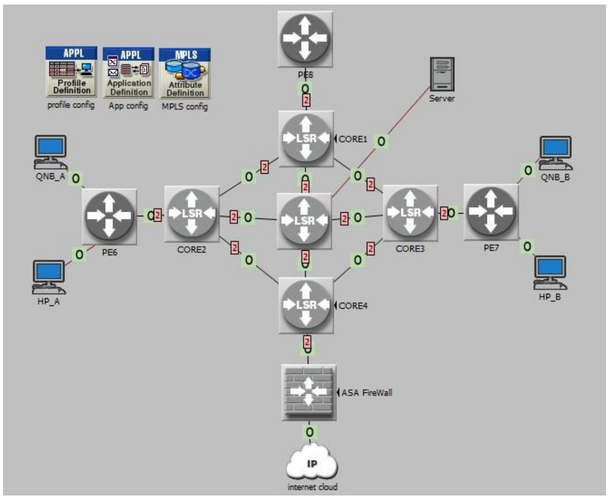

Figure 1-3: MPLS topology

The two above scenarios where simulated using OPNET modeler 14.5, using video conference as a traffic load in both scenarios the results are shown in the figures below.

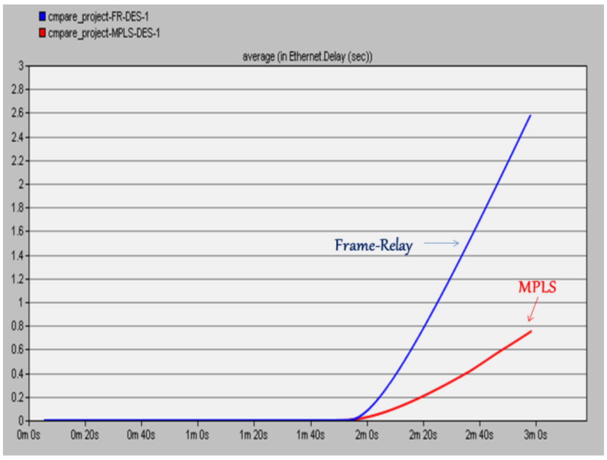

Figure 1-4: Delay result

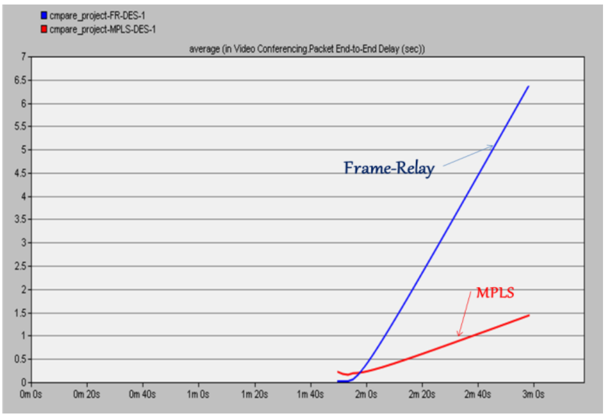

Figure 1-5: Latency result

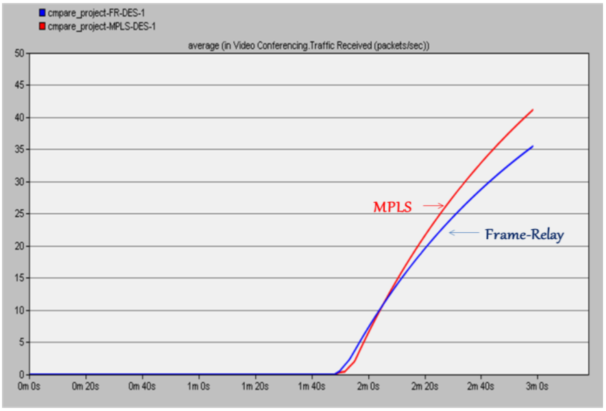

Figure 1-6: Traffic received result

the improvement in delay and latency is refer to the use of labels in MPLS which speeds up forwarding procedure by looking into the label table without the need to examine layer 3 and layer 4 information [5].

4. MPLS OVERVIEW

MPLS is a technology can be used to facilitate the service creation process for both service provider and enterprise organizations. It is working in 2.5 layers in OSI seven layers. In MPLS networks packets are forwarded based on label. These labels might correspond to IP destination addresses per router and near local significance to router generating them. An MPLS label is a 20 bit number that is assigned to destination prefix on a router that defines the properties of the prefix as well as forwarding mechanisms that will be performed for a packets destined for the prefix. Figure 1-1 shows how the packet is forwarding based on labels [3].

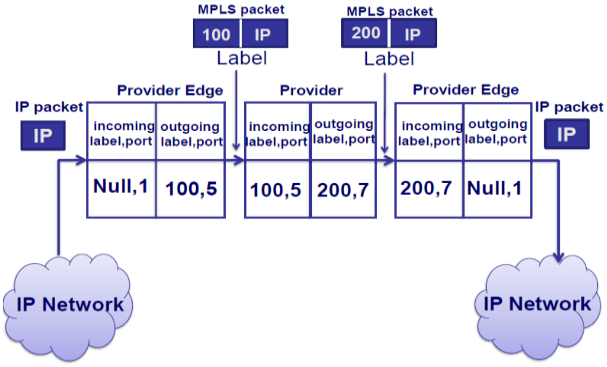

Figure 1-7: forwarding in MPLS domain

MPLS technology offers businesses the performance of traditional VPNs but is far more cost effective. As the intelligence resides in the MPLS network core, there is no need for any expensive VPN appliances to be located on the customer premises. MPLS allows service providers to create new virtual private networks without having to install new hardware; it significantly reduces the cost of implementation, which in turn reduces the overall cost of VPNs. MPLS has many benefits from the customer perspective and service provider perspective because it connect different sites on a private tunnel through the cloud and also, MPLS is interface independence hence it can bridge all sites to become connected together (connect any type of connection the service provider support)[4]. MPLS provides QoS because it tags (ToS or DSCP) the packet and the service provider get the tags and translates them to MPLS label as the packet comes to the cloud and the label tells where exactly where it's going. It's really efficient to send data to the cloud without have to open the packet to look at layer 3 and layer 4 data [5].

5. SERVICE PROVIDER CONFIGURATION PROCESS

5.1 Route protocol

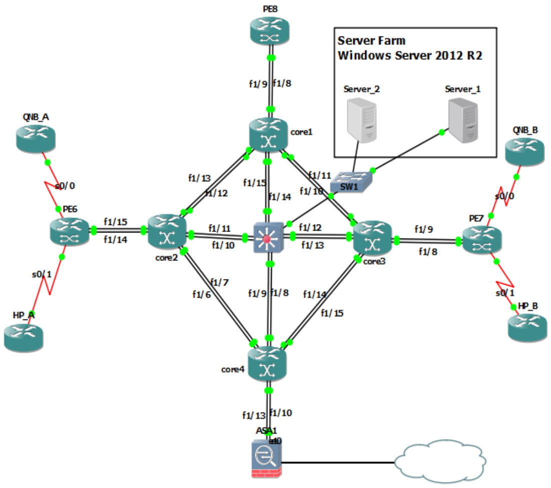

Figure 1-8: Basic routing configuration topology

1- Make basic IP addresses configuration on the whole infrastructure.

```
#interface [pick the interface]
#ip address [ip] [subnetmask]
```

2- Make basic configuration of OSPF and MPLS at the core and PE nodes.

```
#router ospf [pro ID]
#network [net ID] [WID] area [ID]
#interface [pick the interface]
#mpls label protocol ldp
#mpls ip
```

5.2 MPLS L3VPN

Configure L3VPN instance route allocation control, RT, Export Target and Import Target, route convergence, route restriction and alarm at PEs.

5.2.1 *MP-IBGP*

Configure MP-IBGP neighbor relationship between PEs and enable VPNV4 functions.

```
#router bgp [AS]
#no synchronization
#bgp log-neighbor-changes
#[IP of the neighbor loopback] remote-as [AS neighbor]
#neighbor [IP of the neighbor loopback] update-source [ID loopback]
#no auto-summary
#address-family vpnv4
#neighbor [IP of the neighbor loopback] activate
#neighbor [IP of the neighbor loopback] send-community both
#exit-address-family
#address-family ipv4 vrf [name of VRF]
#redistribute connected
#redistribute static
```

5.2.2 *VRF*

Configure VRF instance and relative RD for each VPN at PEs.

```
#ip vrf A
#rd [rd number]
#route-target [RT]
```

5.2.3 *GRE tunnel*

Establish side to side tunneling and this is under control of service provider.

```
#interface Tunnel [pick a number]
#ip address [] []
#tunnel source [exit ip address of local router or exit interface of it]
#tunnel destination [destination ip]
#tunnel mode gre
```

5.3 Traffic engineering

a- configure the nodes that require TE feature.

```
#mpls traffic-eng tunnels
#router ospf [pro id]
#mpls traffic-eng area
#mpls traffic router-id loopback [pick a number]
#int [pick interface work in mpls domain]
#ip rsvp band [bandwidth in Kbps]
#mpls traffic-eng tunnels
```

b- Configuration for PE routers to get beneficent of TE.

```
#interface Tunnel [pick a number]
#ip unnumbered Loopback [pick number]
#mpls ip
#tunnel mode mpls traffic-eng
#tunnel destination [loopback IP of the other PE]
#tunnel mpls traffic-eng autoroute announce
#tunnel mpls traffic-eng priority [0-7] [0-7]
#tunnel mpls traffic-eng bandwidth [Kbps]
#tunnel mpls traffic-eng path-option 1 [explicit | dynamic]
```

5.4 Multicast

a- configure sparse mode as a routing protocol

```
#Interface [pick interface]
#ip pim spares-mode
```

b- join a multicast group

```
#ip igmp join-group [multicast ip address]
```

5.5 VOIP

a- configure IP SLA on the core routers

```
#ip sla [pick number]
#udp-jitter [ip address][udp port number] codec [codec type]
advantage-factor [factor]
#frequency [pick number]
```

b- configure the other side with responder

```
#ip sla responder udp-echo ipaddress [ip address] port [port
number]
```

6. Security concerns

6.1 MPLS security

Configure MPLS labels security on the core nodes to provide protection for customers data transfer.

```
#mpls ldp neighbor [neighbor ip] password [select password]
```

6.2 OSPF security

Configure OSPF security to prevent any internal or external attacks.

```
#ip ospf message-digest-key [key chain number] md5
[password]
```

6.3 ACLs

Configure the following access-lists on interfaces connected to the internet.

```
# Access-list 1xx deny icmp any any echo-request
# Access-list 1xx deny icmp any any echo-reply
# Access-list 1xx permit icmp any any packet-too-big
#Access-list 1xx deny icmp any any host-unreachable
#Access-list 1xx deny ip 10.0.0.0 0.255.255.255 any class A
#Access-list 1xx deny ip 172.16.0.0 15.0.255.255 any class B
#Access-list 1xx deny ip 192.168.0.0 0.0.255.255 any class C
#Access-list 1xx deny ip 224.0.0.0 15.255.255.255 any class
D Multicast
#Access-list 1xx deny ip 255.255.255.255 0.0.0.0 any
BROADCAST.
# Access-list 1xx deny ip 127.0.0.0 0.255.255.255 any
LOOPBACK
# Access-list 1xx deny ip 169.254.0.0 0.0.255.255 any Link
Local Network
```

6.4 ASA firewall

Make basic Cisco ASA (Adaptive Security Appliance) configuration to provide proactive threat defense that stop attacks before they spread through the network.

```
#class-map inspection_default
#match default-inspection-traffic
#policy-map type inspect dns preset_dns_map
#message-length maximum 512
#policy-map global_policy
#class inspection_default
#inspect dns preset_dns_map
#inspect ftp
#inspect h323 h225
#inspect h323 ras
#inspect rsh
#inspect rtsp
#inspect sqlnet
#inspect skinny
#inspect sunrpc
#inspect xdmcp
#inspect sip
#inspect netbios
#inspect tftp
#inspect pptp
#service-policy global_policy global
```

7. SERVER PLACEMENT

Compute environments are designed with high availability to ensure a predictable degree of operational continuity during production hours. It is imperative that the uptime of business-critical applications not be compromised by unplanned equipment downtime [6]. At the core of any enterprise data center is some amount of critical data. The servers, operating systems, and infrastructure components are in place to facilitate user access to this data. Today's data center compute environments require a highly available and scalable architecture to support the mission-critical applications of the enterprise. To meets these needs by providing a solution with a simplified, scalable architecture designed with high-availability components throughout the solution. Starting with the server and extending to both storage and Ethernet networks. Network isolation is often recommended as a best practice in the data center. In a Cloud Suite environment, you might have several key VLANs, spanning two or more physical clusters. The network must be designed to meet the diverse needs of many different entities in an organization. These entities include applications, services, storage, administrators, and users. The network design should improve availability. Availability is typically achieved by providing network redundancy [7]. The network design should provide an acceptable level of security. Security can be achieved through controlled access where required and isolation where necessary. Simplify the network architecture by using a leaf and spine design. Configure common port group names across hosts to support virtual machine migration and failover. Separate the network for key services from one another to achieve greater security and better performance.

8. ACKNOWLEDGMENTS

Our thanks to the experts Jeremy Cioara and Keith Barker, whose videos and tutorials helped us contributing towards development of this paper.

9. CONCLUSION

MPLS is emerging as a widely acceptable technology today. It is important to note that MPLS is not a replacement for IP. The IP Control Plane is a fundamental component of MPLS. The ability to add the ATM, Frame-Relay and other Forwarding Plane makes it extremely attractive to both Service Providers and Enterprises. Service Providers can reduce their time to profitability by deploying MPLS VPNs, MPLS QoS and MPLS TE, rather than only providing the vanilla connectivity of VPNs. Cloud computing is possible implementation for a large-sized enterprise. IT technicians are spearheading the challenge. Several groups have recently been formed, such as the Cloud Security Alliance or the Open Cloud Consortium, with the goal of exploring the possibilities offered by cloud computing and to establish a common language among different providers. In this boiling pot, cloud computing is facing several issues in gaining recognition for its merits. Its security deficiencies and benefits need to be carefully weighed before making a decision to implement it. However, the future looks less cloudy as far as more people being attracted by the topic and pursuing research to improve on its drawbacks.

10. REFERENCES

[1] Pultz, Richard., 2004., Analysis of MPLS-Based IP VPN Security: Comparison to Traditional L2VPNs such as ATM and Frame Relay, and Deployment Guidelines

[2] Rick Gallaher's MPLS Training Guide: Building Multi Protocol Label Switching Networks Paperback – November 20, 2003, Syngress , Rick Gallaher

[3] Ghein, Luc De., 2007., MPLS Fundamentals.

[4] “Advanced MPLS Design and Implementation”,Vivek Alwayn, Published by: Cisco Press 201 West 103rd Street Indianapolis, IN 46290 USA

[5] International Journal of Computer Applications” Evaluating the Performance of MPLS and Frame-Relay using OPNET Modeler**”** Mustapha B. Ibrahim, Shahad H. Zwayen - December 2014 .

[6] Daugherty B.; Metz C.,” Multiprotocol label Switching and IP, Part1: MPLS VPNs over IP Tunnels”. IEEE Internet Computing

[7] “Installing and Configuring Windows Server 2012”, lan McLean , Microsoft prePress