ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

Multiprotocol Label Switching over IPv4 and IPv6

Hardik Prajapati

Assistant Professor, Dept. of E.C., Indus University, Ahmedabad, Gujarat, India

ABSTRACT: Multi-Protocol Label Switching (MPLS) is a core networking technology that operates between Layers 2 and 3 of the OSI model. Sometimes it is also referred to as a layer 2.5 technology. It is basically a framework for WAN. MPLS is a highly evolved than its predecessors Frame relay and ATM in terms of providing solution for VPN, QoS, network convergence, security, traffic engineering etc. As a result, today MPLS is widely used in supporting applications like voice, video and data on the internet. Most service providers are migrating their backbone network from traditional Frame Relay and ATMs to MPLS. This paper basically deals with the implementation of MPLS as VPN service, how it is implemented, maintained, pros and cons.

KEYWORDS: MPLS, LDP, CE1, QOS, 6PE, IPv6, VPN.

I. INTRODUCTION

MPLS stands for "Multiprotocol Label Switching" as it works with Internet Protocol (IP), Asynchronous Transport Mode (ATM) and Frame Relay network protocols [1]. MPLS is a scalable, protocol-independent transport. In an MPLS network, data packets are assigned labels. Packet-forwarding decisions are made solely on the contents of this label, without the need to examine the packet itself. This allows one to create end-to-end circuits across any type of transport medium, using any protocol [2]. The primary benefit is to eliminate dependence on a particular OSI model data link layer technology, such as Asynchronous Transfer Mode (ATM), Frame Relay or Ethernet. So it is clearly a protocol-independent transport system

MPLS operates at a layer that is generally considered to lie between traditional definitions of layer 2 (data link layer) and layer 3 (network layer), and this is often referred to as a "Layer 2.5" protocol. It was designed to provide a unified data-carrying service for both circuit-based clients and packet-switching clients which provide a datagram service model. It can be used to carry many different kinds of traffic, including IP packets, as well as native ATM, SONET and Ethernet frames. The Label Distribution Protocol (LDP) is often used to establish MPLS and handle the labels.

II. WORKING OF MPLS

In an MPLS network, incoming packets are assigned a "label" by a "label edge router (LER)". Packets are forwarded along a "label switch path (LSP)" where each "label switch router (LSR)" makes forwarding decisions based solely on the contents of the label. At each hop, the LSR removes the existing label and assigns a new label which tells the next hop how to forward the packet.[3]

Label Switch Paths (LSPs) are established by network operators for a variety of purposes, such as to guarantee a certain level of performance, to route around network congestion, or to create IP tunnels for network-based virtual private networks. In many ways, LSPs are no different than circuit-switched paths in ATM or Frame Relay networks, except that they are not dependent on a particular Layer 2 technology.

Some of the basic terminologies of MPLS are explained as follows:

(1) Label Switch Path: In MPLS networking, a Label Switched Path (LSP) is a path through an MPLS network, set up by a protocol such as LDP. The path is set up based on criteria in the forwarding equivalence class.

(2)Ingress Label Switch Router (LSR)/ Provider Edge (PE) Router: It is basically the router that is on the edge of the network. This router receives a packet from the outside world and assigns a label to it and forwards it on the link. This router is a part of provider network with which the customer router peers.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

(3)Egress Label Switch Router (LSR)/ Provider Edge (PE) Router: This router is the other end of MPLS network. It receives a labeled packet. It pops the label off and forwards it to destination. This router is a part of provider network with which the customer router peers.

(4)Intermediate Label Switch Router (LSR)/ Provider core (P) Router: These are the routers within the MPLS network. They receive a labeled packet and their operation is to only swap labels and switch the packet. These routers need not have information about the customer routes.

(5)Customer edge router (CE router): This is the edge router on customer network with which the PE router peers.

(6)Forwarding Equivalence Class (FEC): A Forwarding Equivalence Class (FEC) is a group of destination routes, services, QOS parameters or a combination of these attributes which share a common path in MPLS domain.

(7)Label Distribution Protocol (LDP): Label binding information between LSR is exchanged with the help of Label Distribution Protocol (LDP). It is basically run between adjacent LSR and is used to exchange label to FEC mapping. LSR basically establishes a session between them and form peers. After they form peers they exchange information about label assignment on label switched path.

(8)Label Information Base (LIB): The LIB stores all the labels that have been advertised by other LSRs in MPLS network. LSR can exchange the mapping of labels using LDP, MP-BGP.

(9)Label Forwarding Information Base (LFIB): The LFIB cache is used for the actual packet forwarding process. It contains information like incoming label value, outgoing label value, prefix/FEC, next hop. If a MPLS LSR needs to forward a packet it will consult this cache in order to find out on which next-hop interface must the packet be sent.

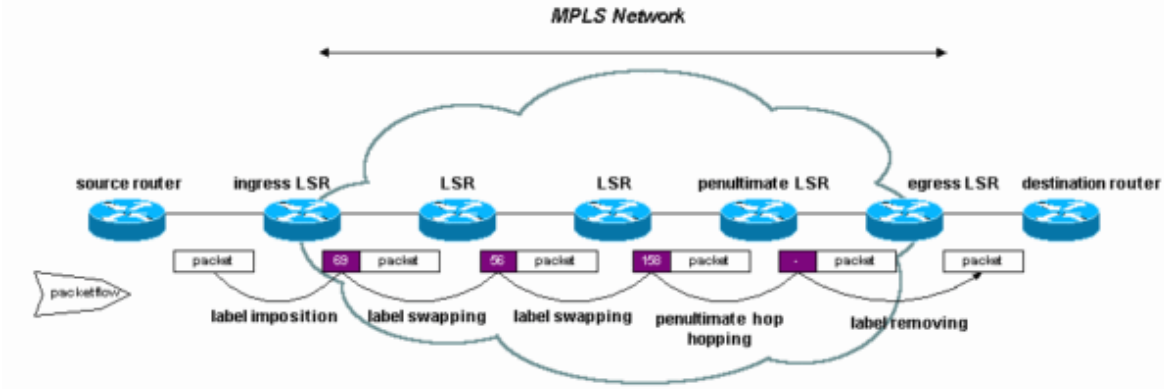

Fig. 1. MPLS Network

III. MPLS LABELS

(1) Bottom of Stack (S): This bit is set to one for the last entry in the label stack (i.e., for the bottom of the stack), and zero for all other label stack entries.

(2) Time to Live (TTL): This eight-bit field is used to encode a time-to-live value.

(3) Experimental Use (EXP): This three-bit field is used for encoding TOS values.

(4) Label Value: This 20-bit field carries the actual value of the Label. It gives information about next hop to which packet would be forwarded.

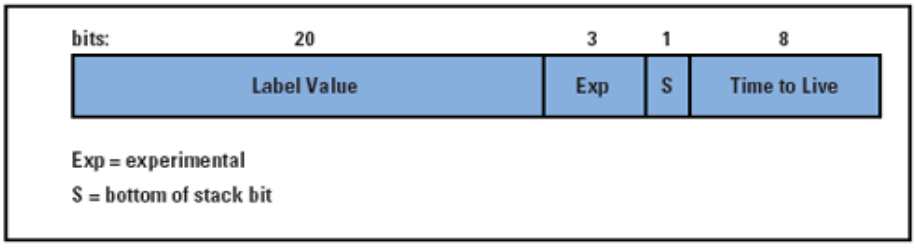

Fig. 2. MPLS Labels

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

The possible label operations that occur when a packet arrives at the LSR are swap, push, and pop. By looking at the top label of the received labelled packet and the corresponding entry in the LFIB, the LSR knows how to forward the packet[2]. The LSR determines what label operation needs to be performed—swap, push, or pop—and what the next hop is to which the packet needs to be forwarded. The swap operation means that the top label in the label stack is replaced with another, and the push operation means that the top label is replaced with another and then one or more additional labels are pushed onto the label stack. The pop operation means that the top label is removed. Untagged or No Label means the stack is removed, and the packet is forwarded unlabelled. Aggregate means the label stack is removed, and an IP lookup is done on the IP packet. Also the penultimate hop (PHP) optimizes CPU performance by reducing CPU load on edge routers. The edge LSR's advertise a pop or implicit null label (value 3) to a neighbour i.e the label is removed on the last intermediate LSR before it reaches the PE.

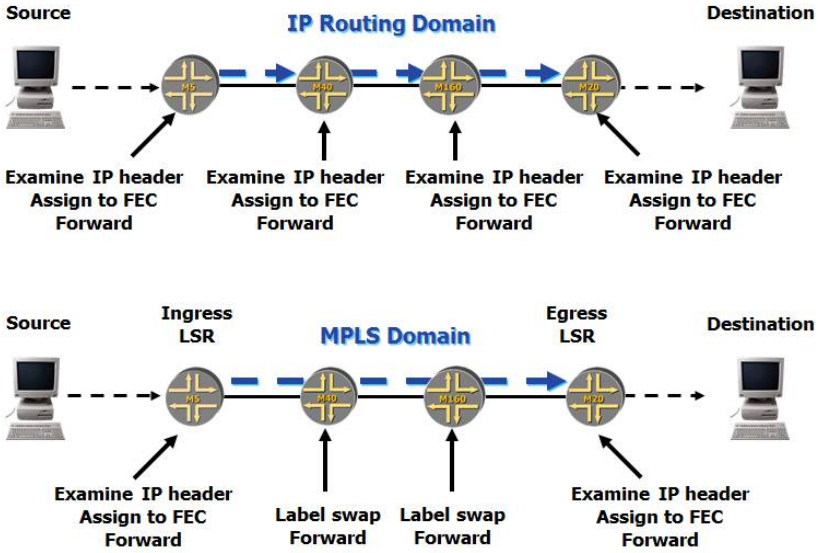

Fig. 3. MPLS Vs. IP

MPLS has two major elements:

1) Control Plane: It looks after routing information exchange and label binding information exchange. It performs Layer 3 routing or Layer 2 switching in addition to switching labelled packets.
2) Forwarding Plane: It is responsible for forwarding packets based on labels attached. It uses LFIB to forward labelled packets.

IV. MPLS ADVANTAGES

Before the inception of MPLS, the most popular WAN protocols were ATM and Frame relay. These were predominantly layer 2 technologies. The disadvantages associated with this overlay models were that Frame-relay and ATM needed virtual circuits to be established (Source-Destination path behaves much like a telephone circuit).Typical problems included: Virtual circuit set up, maintenance & teardown, packet carries virtual circuit identifier and not destination IP address, high cost, complexity of meshed configuration, network delays, remote access issues.

Each customer site peers with every other customer site. So the number of connections to be established are (n*(n-1)/2). In this case if a new site is added, it would need to peer with site 1all the other sites and configuration changes on all sites. This causes potential configuration issues if multiple (for example 10) new sites to be added. This results in increased cost, complexity of maintenance and troubleshooting.

The advantage of MPLS over this is that MPLS basically uses a peer model. There are various advantages of using a peer model:

1) Customer router peers with a Provider router and not with other customer routers
2) Customer Edge (CE1) router peers only with Provider Edge (PE1) router and not with CE2 and CE3

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

3) Adding a new site requires configuration only at the Provider edge router
4) If a new site (site 4 is added) configuration changes only on Provider Edge (PE)router
5) No configuration changes or modifications on CE1, CE2 & CE3
6) No need to establish a dedicated/virtual circuit from source to destination
7) Packet carries following information
8) Destination IP address
9) Quality of Service(QOS) and Class of Service (COS) parameters
10) Less network delays as no circuit establishment, maintenance and teardown process needed

V. MPLS-VPN NETWORK

A VPN is a generic term that describes any combination of technologies that can be used to secure a connection through an otherwise unsecured or untrusted network. A virtual private network (VPN) extends a private network across a public network, such as the Internet. It enables a computer or network-enabled device to send and receive data across shared or public networks as if it were directly connected to the private network, while benefiting from the functionality, security and management policies of the public network.[6]
The main elements of a VPN are as follows:

1.) Virtual routing and forwarding table (VRF): The advent of VRF has been a great added advantage to MPLS VPN. The VRF can be considered as separate routing and forwarding table in PE router. A PE router has a vrf instance for each attached VPN. For example if the ISP has multiple customers suppose ABC XYZ, PQR. Because the routing should be separate and private for each customer, each customer would have a separate instance of vrf in PE router so thus preventing leaking of routes from one customer to another.[3]

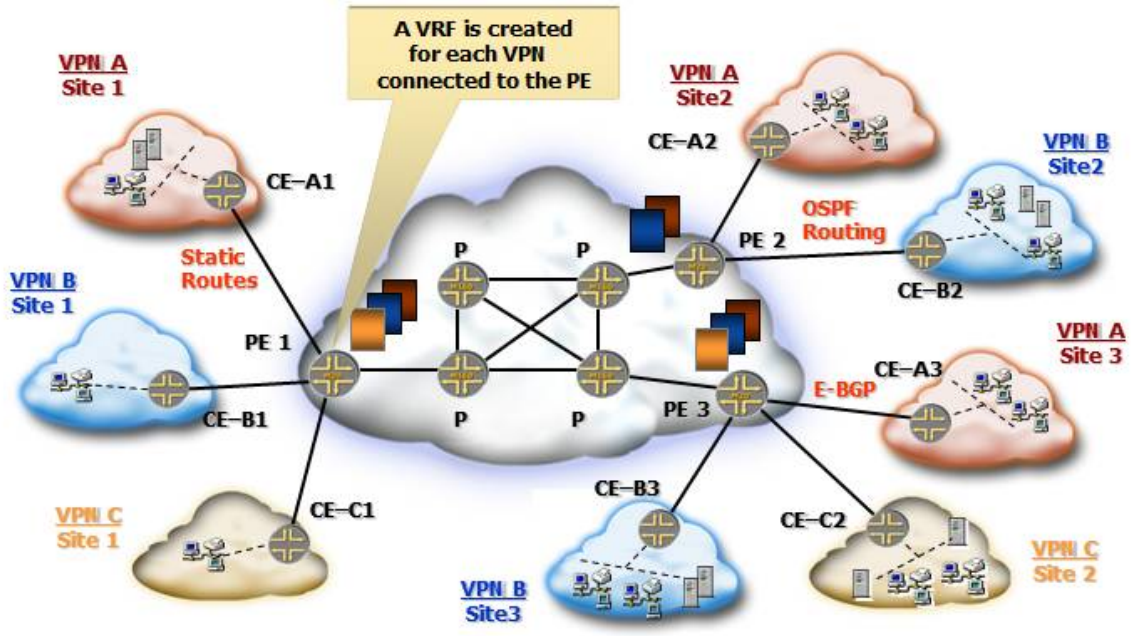

Fig.4 An MPLS-VPN Network

2.) Route Distinguisher (RD): Ipv4 address space is limited. The problem is when customer had overlapping IP addressing, the routing would be wrong. For example most companies use private addressing for their internal network to prevent use of public addresses. It can be quite possible that two companies may have same

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

internal address space 192.168.10.0/24. To prevent the customer routes from getting routed wrongly MPLS consists of 64-bit field called as Route Distinguisher. RD= 16 bit type + 48 bit value. The RD is only used to make Ipv4 address unique. Generally (ASN: IP Address) Autonomous system number is included in the RD value field to make a unique 96-bit address for each VPN. 64 bit –RD + 32 bit IP address = Unique VPN route

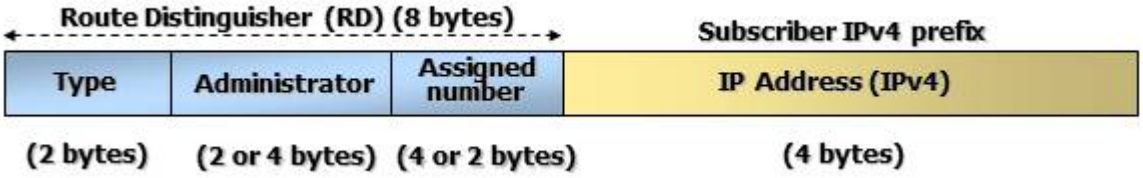

Fig.4 Route Distinguisher Format

3.) Route Target (RT): Route Targets are generally used to control the policy of who sees what routes. Typically carried as an extended BGP community. It is a 64 –bit quantity. For example, there are two companies A and B and both have sites X and Y. Sites X and Y of A can talk to each other and similarly for company B but Site X and Y of company A cannot talk to X and Y of B. If in case you need site X of A to talk to site X of B, route target comes into picture. In that case routes will be exported to remote PE and also imported from remote PE in order to make it work.

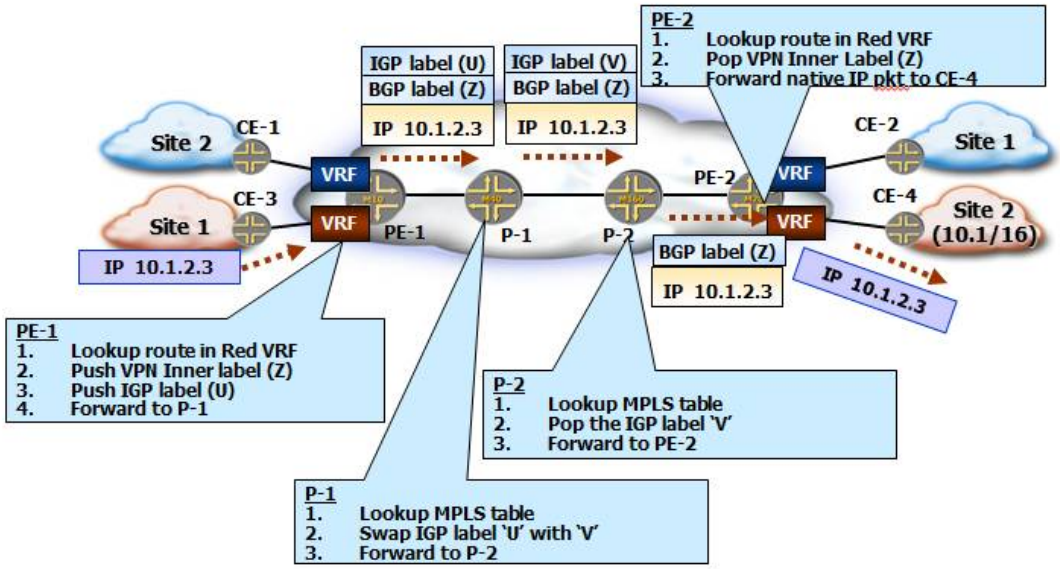

Figure 5: Packet transfer and look-ups in a MPLS-VPN network

VI. MPLS OVER IPV6

There are several approaches for providing IPv6 connectivity over an MPLS core network including (i) requiring that MPLS networks support setting up IPv6-signaled Label Switched Paths (LSPs) and establish IPv6 connectivity by using those LSPs, (ii) use configured tunneling over IPv4-signaled LSPs, or (iii) use the IPv6 Provider Edge (6PE) approach. The 6PE approach is required as an alternative to the use of standard tunnels. It provides a solution for an MPLS environment where all tunnels are established dynamically, thereby addressing environments where the effort to configure and maintain explicitly configured tunnels is not acceptable. The approach requires that the edge routers

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

connected to IPv6 islands be Dual Stack Multiprotocol-BGP-speaking routers, while the core routers are only required to run IPv4 MPLS. The approach uses MP-BGP over IPv4, relies on identification of the 6PE routers by their IPv4 address, and uses IPv4-signaled MPLS LSPs that do not require any explicit tunnel configuration.[8]

A typical example of an IPv6 island would be a customer's IPv6 site connected via its IPv6 Customer Edge (CE) router to one (or more) Dual Stack Provider Edge router(s) of a Service Provider. These IPv6 Provider Edge routers (6PE) are connected to an IPv4 MPLS core network. The interconnection method described in this document typically applies to an Internet Service Provider (ISP) that has an IPv4 MPLS network, that is familiar with BGP (possibly already offering BGP/MPLS VPN services), and that wants to offer IPv6 services to some of its customers. However, the ISP may not (yet) want to upgrade its network core to IPv6, nor use only IPv6-over-IPv4 tunneling. With the 6PE approach, the provider only has to upgrade some Provider Edge (PE) routers to Dual Stack operations so that they behave as 6PE routers while leaving the IPv4 MPLS core routers untouched. These 6PE routers provide connectivity to IPv6 islands. They may also provide other services simultaneously (IPv4 connectivity, IPv4 L3VPN services, L2VPN services, etc.). Also with the 6PE approach, no tunnels need to be explicitly configured, and no IPv4 headers need to be inserted in front of the IPv6 packets between the customer and provider edge. The ISP obtains IPv6 connectivity to its peers and upstream using means outside of the scope of this document, and its 6PE routers readvertise it over the IPv4 MPLS core with MP-BGP.

The interface between the edge router of the IPv6 island (Customer Edge (CE) router) and the 6PE router is a native IPv6 interface which can be physical or logical. A routing protocol (IGP or EGP) may run between the CE router and the 6PE router for the distribution of IPv6 reachability information. Alternatively, static routes and/or a default route may be used on the 6PE router and the CE router to control reachability. An IPv6 island may connect to the provider network over more than one interface. The 6PE approach can be used for customers that already have an IPv4 service from the network provider and additionally require an IPv6 service, as well as for customers that require only IPv6 connectivity.

VII. CONCLUSION

When non- MPLS networks is used i.e. in case of point to point leased lines each site needs to ne connected with each and every site in the network which took a lot of time, energy and money. In case of MPLS the customers need to connect each location with a single link only i.e. to a service provider MPLS network. So the cost of leased lines is saved. For organizations that are having a lot of branches or expanding with new branches, MPLS network would be very cost-effective as each branch needs one MPLS link while each branch would need n-1 links for point to point Leased Lines (n being the total number of branches). MPLS makes it easy for instantaneous addition and deletion of sites. An MPLS core network is generally designed and built to overcome individual hardware (router) faults or line disconnection. In such cases, the data is re-routed through the next optimum path with a minimum fail-over time. This we saw in the previous chapter when we failed one link and the packets travelled through an alternate route. MPLS networks can carry any type of packets – be it IP, frame relay or ATM using the same infrastructure. This is because, whatever type of packets comes in, MPLS labels would be attached to it for transmitting them over the MPLS network and these labels are protocol independent. So multiple type of packets can be transmitted. Also, MPLS is a connection-oriented network unlike connection less networks like IP, so it is more reliable.

REFERENCES

1. B. Davie, et al., “MPLS using ATM VC Switching”, IETF Internet Draft, work in progress, MPLS WG, November1998.
2. M. Behringer, Request for Comments: 4381,” Analysis of the Security of BGP/MPLS IP Virtual Private Networks (VPNs)”, Cisco Systems Inc. February 2006
3. CCNA routing and switching by Todd Lamhe
4. Multiprotocol BGP Extensions for IP Multicast Commands http://www.cisco.com/c/en/us/td/docs/ios/12_2/iproute/command/reference/fiprrp_r/1rfmbgp.html
5. Kaur .G, Kumar .D, “MPLS Technology on IP Backbone Network” , International Journal of Computer Applications (0975-8887), 2010.
6. Alo .S, Aga .A, Nou .A“A Novel Approach for Fault Tolerance in MPLS Networks”, IEEE 2006.
7. Alouneh .S, En-Nouaary .A, Agarwal .A, “A Multiple LSPs Approach to Secure Data in MPLS Networks”, Journal of Networks, Vol 2, Issue 4, pp 51-58, August 2007
8. J. De Clercq, D. Ooms, S. Prevost, Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE), RFC4798