SEAMLESS MPLS BUSINESS DRIVERS, TECHNICAL ANALYSIS AND USE CASES

PROJECT REPORT

Submitted By:

Iftekhar Uddin Rahid

In partial fulfillment for the award of the degree 0f

Master of Science in Internetworking

UNIVERSITY OF ALBERTA

Edmonton, Cañada T6G 2E8

December 8th, 2014

UNIVERSITY OF ALBERTA

BONAFIDE CERTIFICATE

This is to certify that the project report entitled "**SEAMLESS MPLS BUSINESS DRIVERS, TECHNICAL ANALYSIS AND USE CASES"** submitted by **IFTEKHAR UDDIN RAHID** in partial fulfillment of the requirements for the award of the **MASTER OF SCIENCE IN INTERNETWORKING** in the **FACULTY OF SCIENCE and FACULTY OF ENGINEERING** is a bonafide record of the work carried out under my guidance and supervision at the **UNIVERISITY OF ALBERTA,** Edmonton.

Project Supervisor:

_____

Juned Noonari,

Fujitsu Network Communications

Project Co-Supervisor:

_____

Shanawaz Mir,

University of Alberta

Program Chairperson: M.H. (Mike) MacGregor _____

Contents

1. Business Drivers

MPLS (Multi-Protocol Label Switching) has been embraced in the network industries for more than a decade now and it has slowly become a standard part of the communication networks. There is perhaps innumerable number of reasons why MPLS has gained success over other technology, among which one clearly stands out; its ability to simplify integration with other protocols. It's coaction with IP which is universally deployed already and its versatility has definitely proven to be another reason.

Network operators need to reduce capital and operational cost thereby limiting their resources to use them more optimally and efficiently. Keeping these goals in mind, many operators have converged their separate service networks in to a single converged service based on IP MPLS network. Furthermore, applications like IP MPLS mobile backhaul driven by the evolution to LTE, lot of business and residential services has begun to extend the role of MPLS closer to the end user. As a result of which we are able to see large MPLS networks from access to the core. MPLS currently do support features that are needed for end to end services; however, these features do not completely address the need in terms of scalability, flexibility, resiliency and manageability that is needed. Hence, to fulfill the demands the 'Seamless MPLS' is the next evolution to this technology.

So what is Seamless MPLS? Currently MPLS exist mainly in the Core to Aggregation Layer of the network and its extension to the access layer making a single MPLS domain is the prime idea, thus the word Seamless MPLS. Seamless MPLS effectively has no boundaries allowing a greater flexibility in Service delivery i.e. the time from when a packet enters the network until it leaves the Network, it is based on MPLS.

2. Executive Summary

Seamless MPLS effectively has no boundaries allowing a greater flexibility in Service delivery i.e. the time from when a packet enters the network until it leaves the Network, it is based on MPLS. Not only it reduces the gap between network layers to implement to end to end MPLS networking; its excellent scalability supporting up to 100,000 MPLS nodes approximately shows the capability of its application in the networks today. Its applications these days are greatly seen in backbone networks, MAN and Mobile Backhaul. The design and implementation of these applications have begun to move closer to the End user thus extending the services of MPLS. This end to end MPLS support features of higher scalability, greater flexibility and much better manageability than the routine MPLS. The vital benefits of this technology lie within the improvised purpose in traffic engineering and Quality of Service (QoS).

In this project I have analysed and compared Seamless MPLS to several other evolving technologies out there like the MPLS Transport Profile (MPLS-TP) and Provider Backbone Bridging- Traffic Engineering (PBB-TE). All these technologies promise to support end to end connectivity. In this Project we will see through Business Drivers of this Seamless MPLS services, Technical Analysis, Scaling Benefits and Issues (Pros and Cons) with it. I will also have shown how business drives and needs, influence the usage of all these technologies and their implementation in the networking world.

Furthermore, this project includes the expansion of traditional MPLS architectures to Seamless MPLS architectures making an end to end connection. The result of this is compared with other technologies mentioned above.

3. MPLS Architectures and Options for Access Network

Let us first consider a simple basic architecture of an MPLS network.

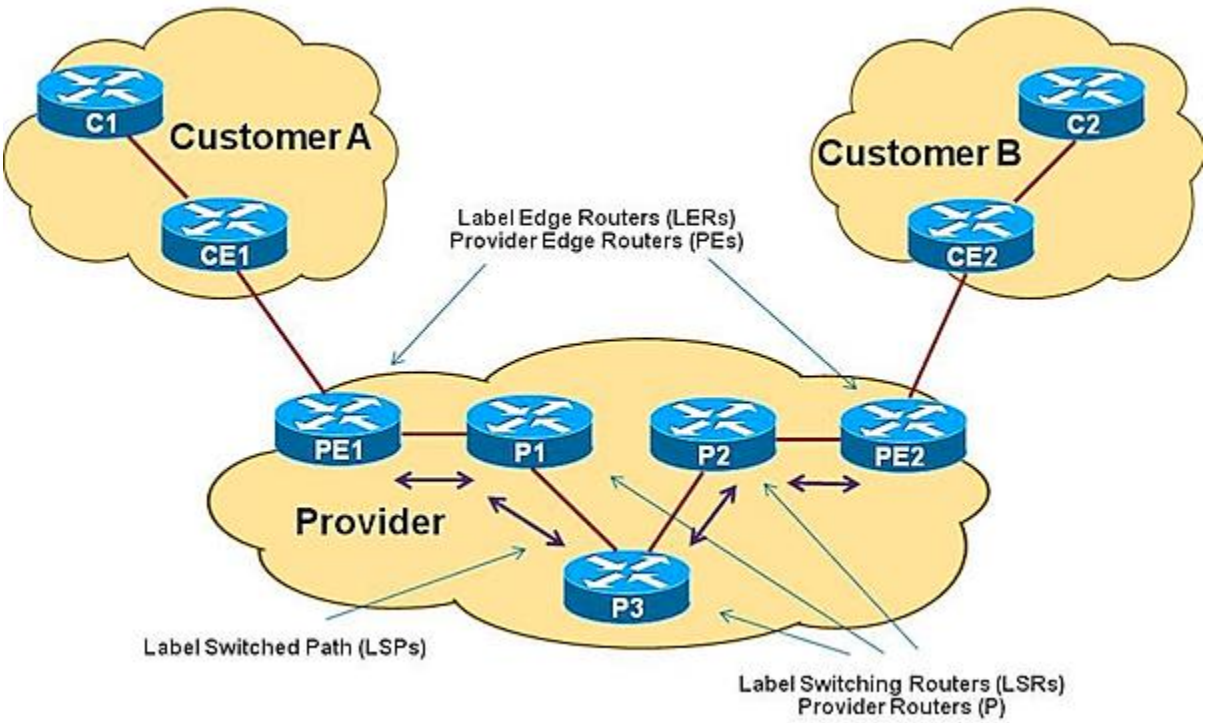

Figure 1 *A simple Architecture of Traditional MPLS*

Ref: http://blog.ine.com/2010/06/28/mpls-components-part-2/#more-3968

The Edge routers are known as Label Edge Routers (LERs) or Provider Edge Routers (PEs). Routers in the core of the provider network are called Label Switching Routers (LSRs) or Provider (P) routers. Label Switched Paths (LSPs) represent the path traffic takes through the provider MPLS network. All of the traffic that is to be forwarded using the same path is known as the Forwarding Equivalence Class (FEC). The service provider can add more customers and introduce many more network prefixes into its infrastructure, but these prefixes only need to exist on Label (Provider) Edge Routers (LERs/PERs). These edge devices are the "workhorses" of the provider network. It is their responsibility to identify the Label Switched Path (LSP) that the packet is destined for. Customer networks consist of Customer Edge routers (CEs) and

Customer (C) routers. These devices need no knowledge whatsoever about MPLS. They can be completely oblivious to the fact they are interacting with a structure that uses MPLS as its basis for forwarding traffic.

MPLS separates the control plane and the Data plane/ Forwarding plane.

3.1.Control Plane:

- The control plane focuses on how each router interact with its neighbors with state exchange.
- The route controller exchanges topology information with other routers and constructs a routing information base (RIB) and Label information base (LIB) are made here.
- Control plane packets are destined to or logically originated by router itself.
- The RIB and LIB is processed in the software to populate Forwarding information Base (FIB) and Label forwarding base (LFIB)
- Since the control functions are not performed each arriving individual packet, they do not have a strict speed constraint and are less time-critical.

Basically, a control plane feeds the Data plane/ forwarding plane with what it needs to create a forwarding table and updates topology changes as they occur. A list of functions performed in traditional routing engines/route processors are the following:

- Allocates resources to the forwarding plane.
- Maintains Routing state.
- ARP handling is always processed in the general purpose processor located in the routing engine.
- Security functions to secure the control plane.

- Establishes and maintains management sessions.

3.2.Data Plane/ Forwarding Plane

- Forwards traffic to the next hop along the path to the selected destination network according to control plane logic using the FIB and LFIB.
- Data plane packets go through the router.
- The routers/switches use what the control plane built to dispose of incoming and outgoing frames and packets.
- The data plane is the workhorse of the switching elements in our networks.
- It manages QOS, filtering, encapsulations, Queuing, Policing.
- The data/forwarding plane must do those operations in the "Fast Path" to keep up with performance needs in data centers and core networks.

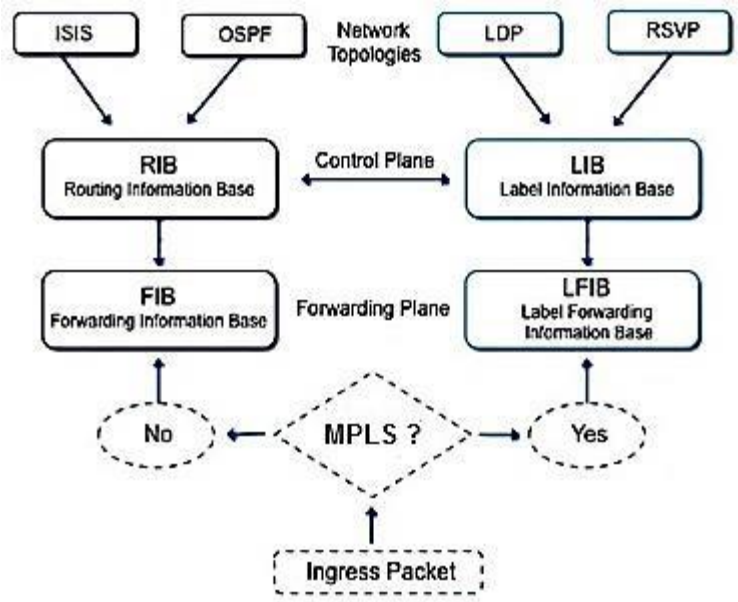

Figure 2 ***Control plane and Data/ Forwarding Plane***

Ref: http://networkstatic.net/the-control-plane-data-plane-and-forwarding-plane-in-networks/

So far, we have seen the control and data plane. To get further in to the working of Seamless MPLS, we must first discuss the working of the traditional MPLS. Figure1 shows a traditional

MPLS architecture. When PE1 receives a packet from CE1, it will engage in what we call a Push operation. PE1 is considered the ingress PE router and engages in label push operation. The P routers in the scenario will move the packets by simply swapping labels. Labels used in the Label Switch Path (LSP) learned by all the routers by Label Distribution Protocol, or other existing protocols (Tag Distribution Protocol (TDP), BGP, and RSVP). At the egress PE2 device we have label pop operation. If the second to last device in the path removes the label for us, this is termed Penultimate Hop Popping (PHP). For the assignment of labels through the Label Switch Path (LSP) Label Distribution Protocol (LDP) rely upon the underlying IGP for intra network and BGP for Inter network to build the best path for the LSP through the network. In the case of our Layer 3 MPLS VPNs, the outer label (or transport label), is used to move the packet through the LSP, while the inner label is used to identify the VPN site. This is often called the VPN label.

When a packet enters an MPLS network, it enters through a Label Edge Router and is affixed with a label stack that assigns it a forwarding equivalence class (FEC) that tells each router where to forward the packet without having to dissect its header. Each label has four main components: a 20-bit label value; a 3-bit traffic class field that designates quality of service, priority and Explicit Congestion Notification; and 8-bit time to live field indicating the maximum number of routers a packet should be sent through before it gets killed off; a 1-bit bottom of stack flag indicating that it is the last label of the stack.

Not only does this labeling technique simplify the process of forwarding packets, but it also gives networks the ability to simply handle traffic from many different kinds of networks. Because MPLS is protocol-agnostic, it can handle packets from ATM, Frame Relay, and SONET

or Ethernet networks. In other words, an MPLS network takes packets from several kinds of networks, slaps label stacks on them and forwards them to their destinations regardless of the type of network they came from.

4. Future of IP MPLS

Multiprotocol Label Switching (MPLS) has been in existence for more than a decade now and it is hard to overstate the impact of its use in our networks these days. One of the major growths of its own can be seen in our Wide Area Network (WAN) and metro Area Network (MAN) networks up to the service provider end. One of the key features of MPLS is the ability to do traffic engineering. Of more immediate interest is the potential to integrate MPLS with Long term Evolution (LTE) technology and use it for mobile backhaul because LTE is based on IP based mobile data technology which is just a perfect fit. Hence MPLS has become a Legacy of the network technology.

Increasing demand for video content, mobile broadband and cloud services are pushing the limits of service provider networks. Service providers need to add network capacity at the lowest cost per bit and reduce their network operations cost. The increased adoption of MPLS within operator networks calls for highly flexible, scalable, resilient and manageable network architectures. Many service providers are implementing fixed and mobile network convergence (FMC) to optimize network utilization and to reduce network capital and operational expenditures. When offering services over a single or converged services network, the end-to-end network must be scalable, flexible to meet evolving service needs and support simple, rapid service provisioning. Multiprotocol label switching (MPLS) is the preferred choice for implementing end-to-end networks.

Seamless MPLS offers a superior alternative for implementing end-to-end MPLS networks by integrating access, aggregation and core networks into a single MPLS domain.

5. Evolution to Seamless MPLS

Seamless MPLS makes deploying services faster and more flexible. Existing MPLS networks are typically implemented and operated as separate networks (i.e. Core, aggregation or access). MPLS Services on the other may have end points within a metro network or need to cross from one metro network to the other. Creating Services across metro networks requires provisioning of multiple segments and end points which requires co-ordination at the network boundaries. Seamless MPLS removes domain boundaries and extends the topology into a single MPLS domain, so service can be deployed faster and between any two points (Seamless) in the end-to-end MPLS network.

Seamless MPLS is not a new protocol suite. It is based on existing protocols (like BGP and LDP) and therefore provides a logical and easy evolution path. We have already understood why end to end connection is vital to us. Typically, each region is operated independently. Depending on the service deployed, the service end-points may be within the same metro region or across different regions. Deploying end to end connectivity across several metro networks require provisioning at intermediate nodes making it more complex. Hence, a preferred approach would be deploying a single convergence end to end service with minimal coordination between regions.

Seamless MPLS allows services to be provisioned wherever they are needed, no matter how the underlying transport is laid out. This is achieved by implementing a three-layer hierarchy as shown in figure 3 below consisting of a transport layer and a service layer.

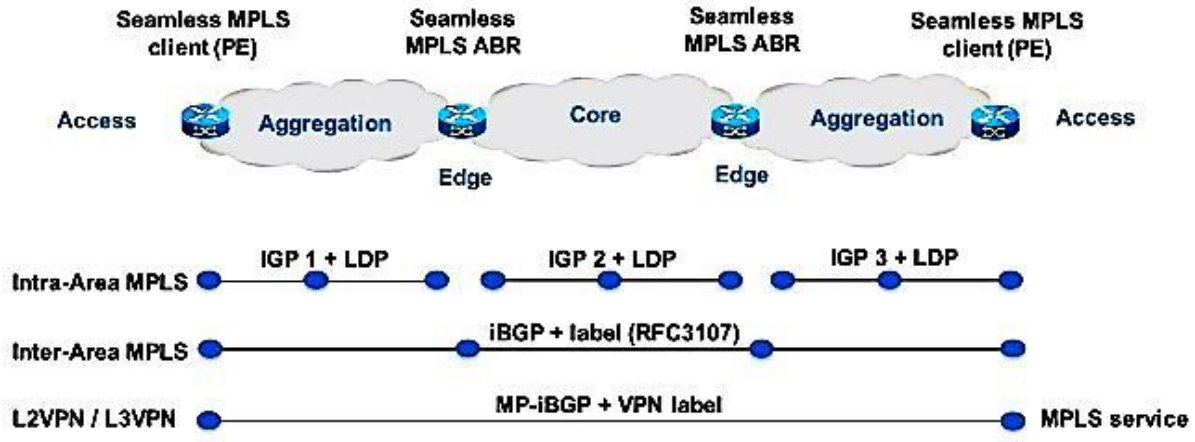

Figure 3 Seamless MPLS basic architecture

Ref: http://www.cisco.com/c/en/us/support/docs/multiprotocol-label-switching-mpls/mpls/116127-configure-technology-00.html#anc5

6. Seamless MPLS Architecture

The motivation of Seamless MPLS is to provide an architecture which supports a wide variety of different services on a single MPLS platform fully integrating access, aggregation and core network. With Seamless MPLS there are no technology boundaries and no topology boundaries for the services. Network (or region) boundaries are for scaling and manageability, and do not affect the service layer, since the Transport Pseudowire that carries packets from the Access Node (AN) to the Service Node (SN) doesn't care whether it takes two hops or twenty, nor how many region boundaries it needs to cross. The Seamless

MPLS architecture therefore decuples the service and transport layer and integrates access, aggregation and core into a single platform.

With Seamless MPLS it is not necessary to use service specific configurations on intermediate nodes; all services can be deployed in an end to end manner. Interior Gateway Protocol (IGP) or MPLS signaling information is not contained within the region and is exchanged across regions. This increases the size of routing/forwarding tables as well as the MPLS state within individual routers. The Seamless MPLS model addresses this challenge by introducing a hierarchy of transport and service layers. The Seamless MPLS transport layer consists of an inter-region tunnel and an intra-region tunnel.

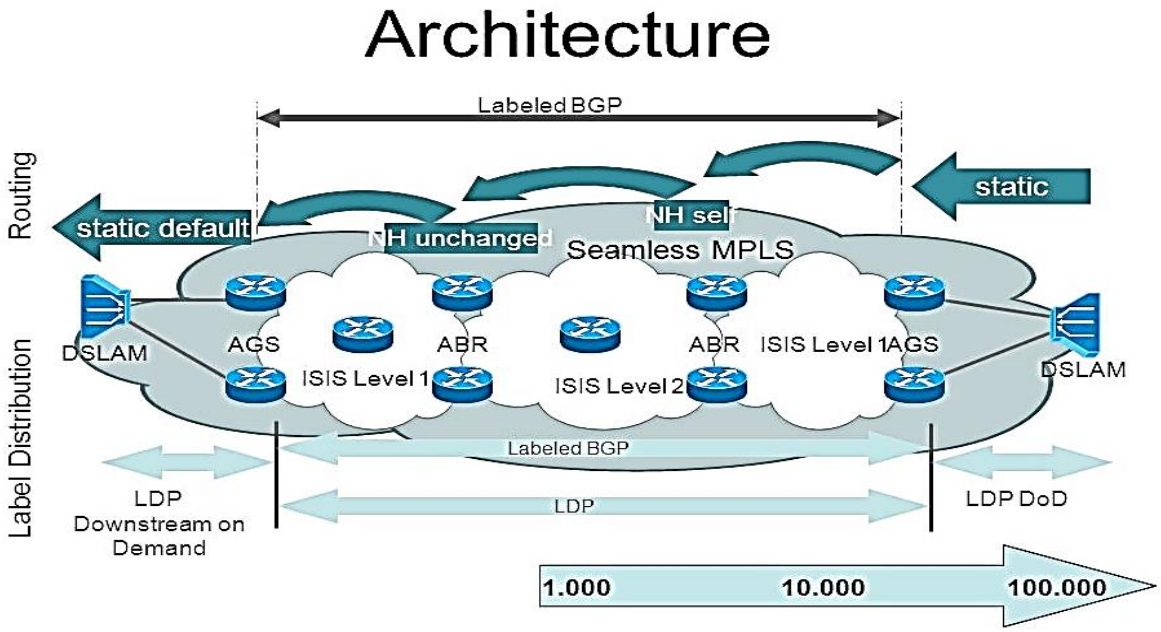

Figure 4 Seamless MPLS Architecture representation

Ref: http://slideplayer.us/slide/721469/

6.1.Access Layer

● Access networks consist of many more devices than those found in core or aggregation networks. Typical access networks can span 100,000 devices or more, whereas core networks consist of hundreds of devices or fewer.

● Access networks have very simple topologies, either hub-and-spoke, as in the case of wireline central-office-based access, or ring topologies in the case of cell sites and Fiber-to-the-x (FTTx) implementations. This is very different from the much more comprehensive connectivity typically found in core networks.

● Devices in the access network must be optimized for cost, size, and power consumption. This tends to limit their control-plane processing capability when compared to core network devices.

● Due to the large number of devices in access networks, simple operation with cost-optimized network elements is an absolute necessity for operators to cost-effectively deliver service.

● Fast restoration (less than 1 second) is required, without adding protocol complexity to the design.

6.2.Aggregation Layer

The aggregation network aggregates traffic from access nodes and must have functionalities that enlarge the scalability of the connected simple access nodes. The Aggregation Layer must be with a link state based Interior Gateway Protocol (IGP) with each aggregation area separated. All routes that are inter-area should use an Exterior Gateway Protocol (EGP) to keep the IGP small. The aggregation node must have the full scalability concerning control plane and forwarding. The support of load balancing for layer 2 services must be implemented.

6.3.Core Layer

The core connects the aggregation areas. The core network elements must have the full scalability concerning control plane and forwarding. The IGP must be link state based. The core area must not include routes from aggregation areas. All routes that are inter-area should use an EGP to keep the IGP small. Each area of the link state based IGP should have less than 2000 routes. The support of load balancing for layer 2 services must be implemented.

7. Building End to End Transport Layer

Consider the following figure for understanding and explanation

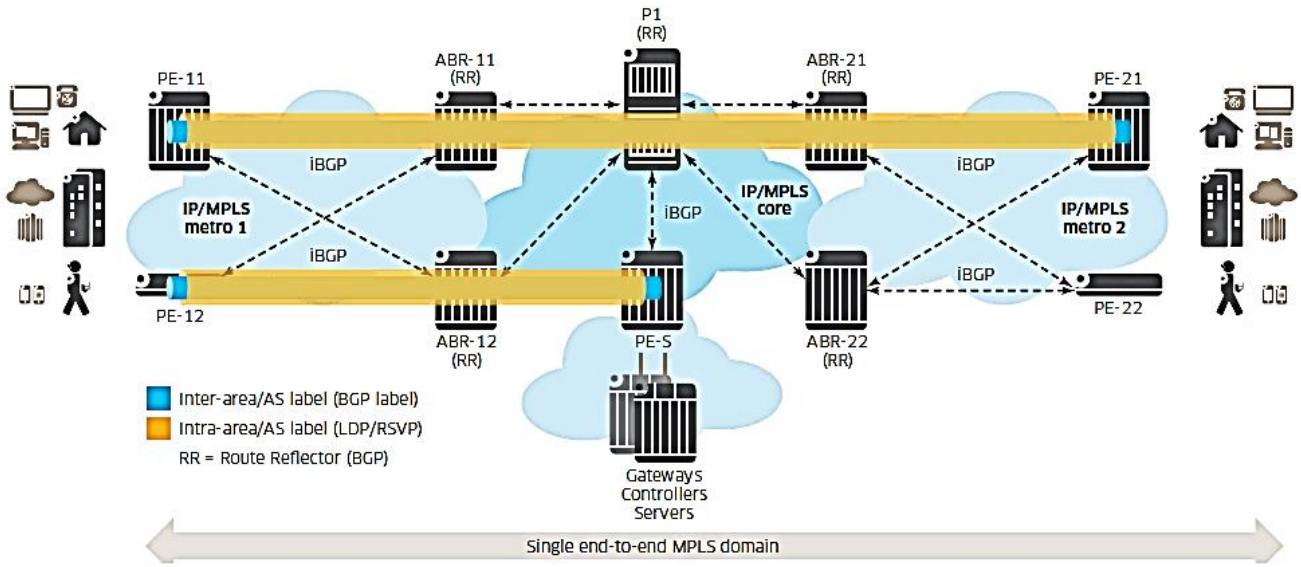

Figure 5 Creating End to End Transport Layer using Seamless MPLS

Ref: Evolving to "end-to-end MPLS" Architecture. Alcatel Lucent. Technical White Paper

RFC 3107 (Carrying Label Information in BGP 4) specifies a way in which label mapping information can be piggybacked in the same Border Gateway Protocol (BGP) update message that

is used to distribute the route itself. When BGP is used to distribute routes, it can be used to distribute an MPLS label which is mapped to that route. Label distribution can be piggy backed in the BGP update message by using the BGP-4 Multiprotocol Extension Attribute. The Label is encoded in the Network Layer Reachability Information (NLRI) field of the attribute and the Subsequent Address Family Identifier (SAFI) field is used to indicate that NLRI contains a label. RFC [2283]. The fact that NRLI field carries a label, the SAFI value is set to 4. A region may represent an Open Shortest Path First (OSPF) area, Intermediate System to Intermediate System (IS-IS) level, OSPF/IS-IS instance, or even an autonomous system (AS). The Area Border Router (ABR) nodes act as Route Reflectors (RRs) for the region and act as a RR client to the core RRs.

7.1 Inter Region Transport Tunnel

The inter-domain routing is responsible for establishing connectivity between and across all MPLS domains. The inter-domain routing should establish a routing and forwarding hierarchy in order to achieve the scaling goals of seamless MPLS.

Figure 5 depicts two inter-region transport tunnels:

1. Inter-region tunnel between PE-11 and PE-21
2. Inter-region tunnel between PE-12 and PE-S

These tunnels provide the PE to PE reachability across regions and provide the inner tunnel label of the transport layer hierarchy. For tunnel 1, the ABR nodes (ABR-21/ ABR-22) receive the loopback and advertise the loopback and a label with next hop self to ABR-11 and ABR-12. These ABRs, in turn, advertise the loopback with next hop self to PE-11. Note: The Seamless MPLS draft (draft-ietf-mpls-seamless-mpls-07) suggests that only the local ABRs change the next hop to self (e.g. for PE-21 loopback, ABR-21 changes the next hop to self but not ABR-11).

When reflecting routes from the core into the aggregation domain, the ABR SHOULD NOT change the BGP NEXT-HOP addresses (next-hop- unchanged). When reflecting routes from the aggregation into the core, the ABR MUST set then BGP NEXT-HOP to its own loopback addresses (next-hop- self). While this approach has some scalability advantages, it requires that PE routers in metro 1 have RSVP or LDP reachability to all ABR nodes in the core area.

A key benefit of the BGP-based approach is the ability to use BGP policies to limit (permit/deny) propagating loopback reachability to different parts of the network on an as-needed basis. BGP filtering policies based on IPv4 prefixes or BGP communities may be configured on specific nodes within the network to prevent loopback propagation (and hence BGP tunnel creation beyond that point).

7.2 Intra Region Transport Tunnel

The intra-region transport tunnels provide transport for the inter-region BGP tunnel within each region. These tunnels provide the outer tunnel label of the transport layer hierarchy. This intra-region tunnel may use LDP or Resource Reservation Protocol with Traffic Engineering (RSVP-TE) and is used to switch the packet between BGP peers (i.e. routes point to the BGP next hop).

The intra-domain routing within each of the MPLS domains (i.e. aggregation domains and core) should utilize standard IGP protocols like OSPF or ISIS.

The intra-domain MPLS LSP setup and label distribution should utilize standard protocols like LDP or RSVP. It also assumes relatively simple MPLS implementations on access nodes. The core uses ISIS L2 to distribute routing information for the loopback addresses of all core nodes. The border routers (ABR) that connect to the aggregation domains are also part of the respective aggregation ISIS L1 area and hence ISIS L1L2.

LDP Downstream Unsolicited (DU) is used to distribute MPLS label binding information for the loopback addresses of all core nodes. The core uses ISIS L2 to distribute routing information for the loopback addresses of all core nodes. The border routers (ABR) that connect to the aggregation domains are also part of the respective aggregation ISIS L1 area and hence ISIS L1L2. LDP DU is used to distribute MPLS label binding information for the loopback addresses of all core nodes.

7.3 Downstream On Demand (DoD)

In general, MPLS routers implement LDP Downstream Unsolicited (LDP DU) label advertisements [RFC5036] and advertise MPLS labels for all valid routes in their RIB tables. LDP DoD enables on-demand label distribution ensuring that only required labels are requested, provided, and installed. In most cases, access nodes connect to the rest of the network using very simple topologies. Here, static routing is sufficient to provide the required IP connectivity. In line with the Seamless MPLS design, static routes configured on aggregation nodes and pointing towards the access network are redistributed in either IGP or BGP labeled IP routes [RFC3107].

7.4 Extending MPLS To The Access Network

Two challenges must be overcome before traditional IP/MPLS can be applied to any type of access network.

First, for traditional IP/MPLS, each endpoint requires a unique identifier within the network, which is usually a /32 loopback address that cannot be summarized within the network. As the application of this technology grows to tens or hundreds of thousands of endpoints in access networks, the burden on the routing protocol of having a link-state database containing a /32 address for each endpoint becomes too great.

The second barrier to overcome when deploying MPLS in access networks is that, in order for traditional IP/MPLS networks to deliver 50-millisecond restoration, traffic engineering is required. This increases protocol complexity due to the need to add RSVP to the network and design a fast reroute tunnel overlay.

The choice of technologies to overcome these two barriers is most naturally determined by the capabilities of the access nodes being deployed in the network, and the operator's preference for a dynamic or static control plane.

Label allocation Downstream on Demand offers an alternative approach for bringing MPLS to access networks, using a simple label distribution protocol implementation without the need to increase routing protocol complexity. LDP Download on Demand keeps the access node extremely simple and eliminates propagation of /32 host routes within the network. This simple mechanism requires very little processing capability within the access node, with no routing protocol requirements. Restoration with LDP Download on Demand is fast, but depending on the capabilities of the access nodes, it may not reach the 50-millisecond threshold. The main point to understand here is that LDP Download on Demand allows very simple devices with limited memory and CPU resources to participate in end-to-end MPLS with acceptable operational characteristics.

If the access devices support Interior Gateway Protocol (IGP) and per-prefix label allocation, LFA for IP/MPLS can offer 50-millisecond restoration with no additional configuration required on the access device. To support Pseudowire operations, LFA will need to be configured with knowledge of all /32 host identifiers in the routing domain. However, a multi-segment Pseudowire approach provides a way to limit propagation of /32 addresses while still offering end-to-end label-switched paths. The mechanism LFA uses to deliver simple 50-millisecond

restoration is similar to the Enhanced Interior Gateway Routing Protocol (EIGRP) concept of a feasible successor. An LFA-enabled routing protocol (either OSPF or IS-IS) will predetermine a backup path and, should the primary path fail, start using the backup path immediately when a failure is recognized in the primary path. LFA uses a very simple approach to determine a loop-free path: it is any path that does not point back through itself. Because this logic is implemented within the router as part of the routing computation process, it presents no interoperability issues, as all communications between network elements remain the same.

7.5 LDP FEC to BGP Stitching

Consider the following Figure for better understanding.

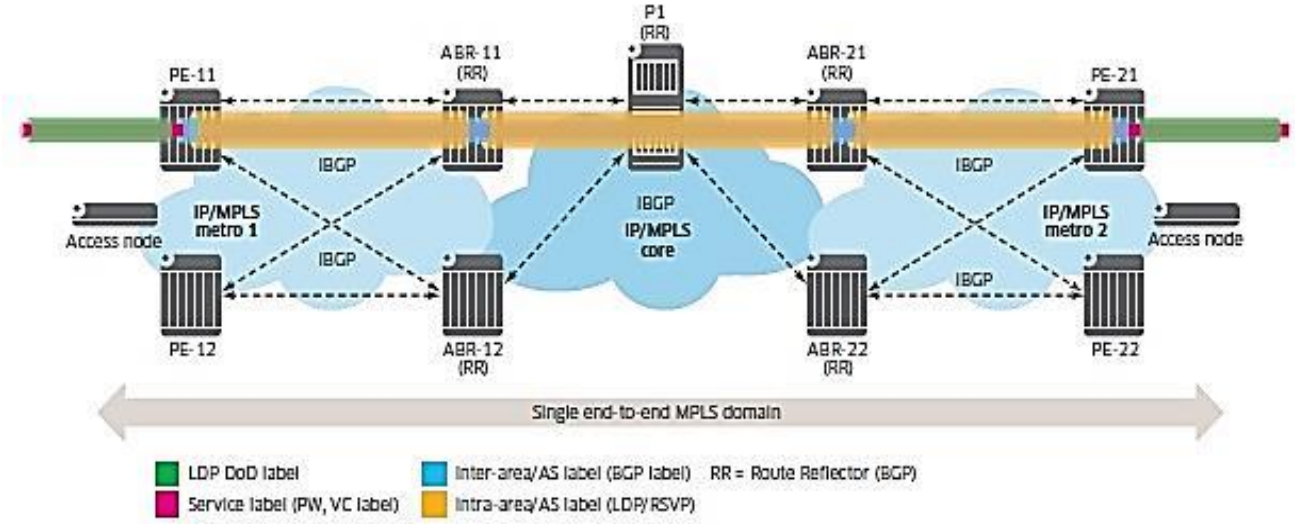

Figure 6 Extending MPLS to Access

Ref: Evolving to "end-to-end MPLS" Architecture. Alcatel Lucent. Technical White Paper

LDP FEC to BGP stitching may be used along with LDP DoD or LDP DU.

In figure 6 perform a translation (LDP FEC to BGP stitching) function.

• PE-11 can export an access node LDP Forwarding Equivalence Class (LDP FEC) into BGP and advertise this as a label route using RFC 3107.

• PE-21 translates the /32 BGP labeled routes into LDP FEC and redistribute this FEC to LDP-DU peers and to LDP-DoD peers (access nodes), if requested.

The outermost label represents the LDP tunnels used to switch the packet between BGP peers within the region (intra-region tunnel).The middle label (inter-region BGP tunnel) is used to switch the packet to the destination PE (PE-11 or PE-21 depending on traffic direction). The innermost label is the MPLS service label between the access nodes. By implementing RFC 3107 at the aggregation point, where access networks are aggregated toward the core, BGP label allocation eliminates the need for core devices to learn all of the prefixes in the access domains as routes are summarized.

7.6 BGP Fast Reroute (FRR) or BGP Prefix Independent Convergence (PIC)

BGP fast reroute (FRR) or Edge PIC (Prefix Independent Convergence) is a feature that brings together indirection techniques in the forwarding plane and pre-computation of BGP backup paths in the control plane to support fast reroute of BGP traffic around unreachable/failed next-hops. When BGP fast reroute is enabled, the control plane attempts to find an eligible backup path for every received IPv4 and/or IPv6 prefix, depending on configuration.

BGP Prefix Independent Convergence (PIC) is the technology that enables RFC 3107 procedures to be implemented with dramatically improved re-convergence characteristics. Prior to BGP PIC, BGP convergence was slow, potentially resulting in minutes of outage. BGP PIC brings convergence into the range of 50 to 300 milliseconds, depending on topology, with no additional configuration required. This is quicker than doing a prefix-by-prefix calculation, as with the new mechanism, only one pointer must be updated for all the paths that will use that new next-hop

address. It is this function of updating a single pointer that is shared by all prefixes using the same next hop that makes this feature prefix-independent.

8. MPLS Transport Profile (MPLS-TP)

With respect to the Seamless MPLS which focus to provide end to end connection, we will see how MPLS-TP has evolved to do the same. A question that could possibly be asked here is; MPLS-TP has been evolving even before seamless MPLS; so, why is seamless MPLS becoming the talk of the next possible networking generation? The answer to this question shall be easily understood once we comprehend how both of them differ and how MPLS-TP functions in order to analyse both these technologies.

The basic concept behind the evolution of Seamless MPLS and MPLS-TP remain quite similar, i.e. applications such as IPTV and mobile video, coupled with the pressure to minimize the cost per bit and maximize the value per bit, is forcing carriers to transition their transport networks from circuit-based technologies to packet-based technologies. With this initiative, MPLS-TP reuses most of the existing protocols from the rich MPLS/GMPLS (generalized MPLS) suite, and then adds a few enhancements, most notably in the area of Operation, Administration, and Management (OAM). The MPLS-TP enhancements increases the applicability of MPLS overall, allowing it to serve both the transport (access and core) and the services networks.

Hence MPLS-TP is a profile of MPLS for transport network. It takes a subset of MPLS/GMPLS protocol suite and adds a few extensions to address transport network requirements. Therefore, we can see that it has all the features and benefits of traditional MPLS and adds few more to improve it. MPLS-TP refers to a set of compatible enhancements to the MPLS protocol suite. These protocols and new enhancements can be separated into the following categories:

• Network Architecture—Covers the definition of various functions and the interactions among them.

• Data Plane—covers the protocols and mechanisms that are used to forward the data packets.

This can further be divided into the following subcategories:

- Framing, forwarding, encapsulation
- OAM (Operation, Administration and Management)
- Resiliency (protection and restoration)
- Control Plane—Covers the protocols and mechanisms used to set up the label-switched paths (LSPs) that are used to forward the data packets.
- Management Plane—covers the protocols and mechanisms that are used to manage the network.

8.1 MPLS and MPLS-TP Components

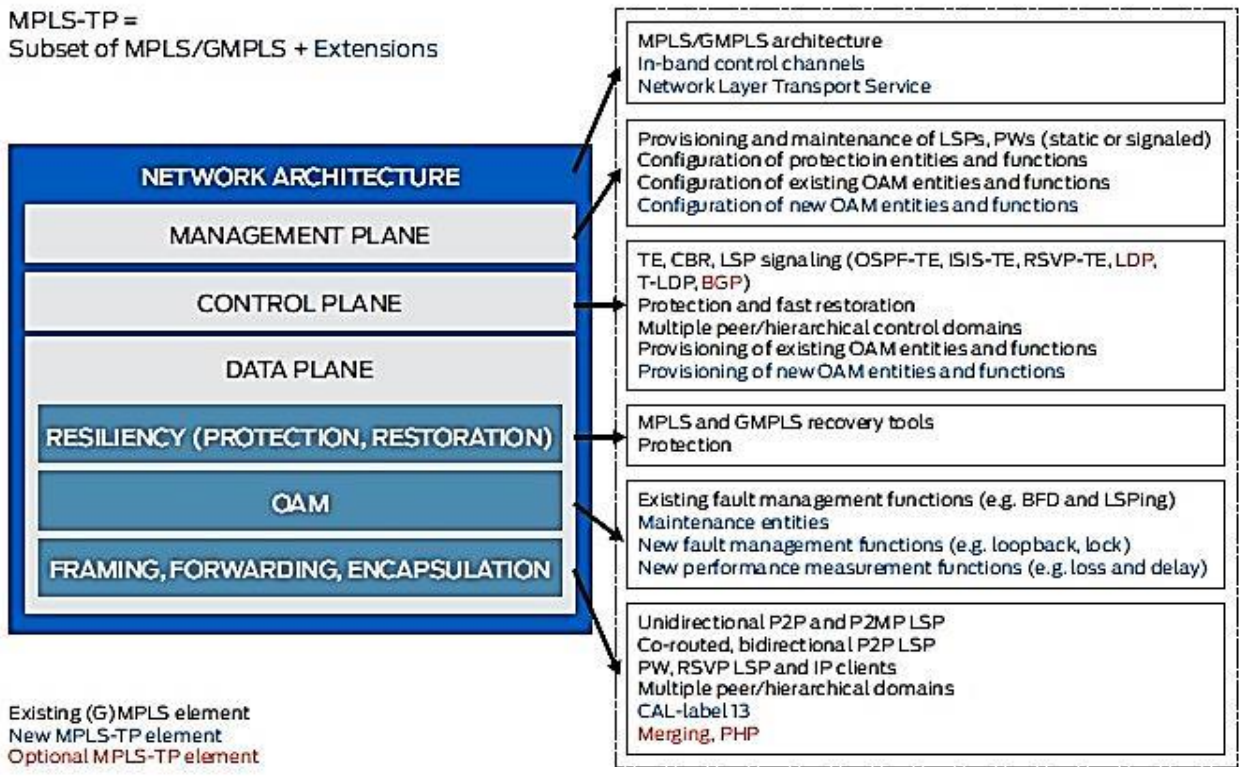

Figure 7 MPLS- TP components

Ref: MPLS transport profile (MPLS-TP), Juniper Networks, Tech White Paper

Consider Figure 7. The protocol and mechanisms highlighted in blue are being added to the MPLS/GMPLS protocol suite as part of the MPLS-TP effort. The protocols and mechanisms highlighted in red might not be needed for the transport networks and are, therefore, being made optional.

8.2 Operations, Administration and Management

The OAM functions being added as part of MPLS-TP are fault detection (e.g., connectivity check, connectivity/path verification), fault localization (e.g., loopback, lock), and performance monitoring (e.g., delay and loss measurement). Note that the existing MPLS tools such as Bidirectional Forwarding Detection (BFD), LSP ping, and LSP trace are being extended to support these new OAM functions. Since MPLS-TP is designed to work in devices where IP routing is not supported, these OAM functions need to operate without any IP layer functionalities. In order to make that possible, the framing, forwarding, and encapsulation component of the MPLS protocol suite is being enhanced with Generic Associated Channel (G-ACh) and G-ACh Label (GAL) to carry the OAM packets without any reliance on IP. Also, the OAM packets need to traverse the same path as the data packets. To support this requirement, the network architecture component of the MPLS protocol suite is being enhanced to support the in-band control channels.

G-ACh is simply a header in the packet that provides the DE multiplexor function for OAM packets for appropriate handling. Note that the existence of ACh was negotiated when the Pseudowire was set up, which is not feasible if static provisioning is used. This problem has been solved by using one of the reserved labels for this purpose. RFC 5586 identifies the reserved value 13 as a G-ACh label (GAL), thus providing the necessary tagging. Use of GAL for tagging

OAM packets also enables easy extraction of the OAM packets at either a midpoint or an endpoint of an LSP or a Pseudowire.

8.3 MPLS-TP Control Plane

The MPLS-TP control plane is based on a combination of the MPLS control plane for pseudo wires and the GMPLS control plane for MPLS-TP LSPs, respectively. MPLS-TP may utilize the distributed control plane to enable fast, dynamic and reliable service provisioning in multi-vendor and multi-domain environments using standardized protocols that ensure interoperability. The distributed MPLS-TP control plane provides the following basic functions:

- Signaling
- Routing
- Traffic engineering and constraint-based path computation
- Moreover, the MPLS-TP control plane is capable of performing fast restoration in the event of network failures.

The current transport networks, however, have been using a static control plane, i.e., the circuits are statically provisioned by an intelligent network management system (NMS). Dynamic control plane is optional with MPLS-TP. The GMPLS control plane, or its ITU-T counterpart, Automatically Switched Optical Network (ASON) [G.8080], supports connection management functions as well as protection and restoration techniques and thus providing network survivability across networks comprising routers, MPLS-TP LSRs, optical ADMs, cross connects, and WDM devices. MPLS has a rich set of protection and restoration mechanisms such as LSP fast reroute, Pseudowire redundancy, and path protection.

8.4 Analysis of MPLS-TP for End to End Connection

We have seen above that MPLS-TP could provide the end to end connection. The goal of MPLS-TP is to provide connection-oriented transport for packet and TDM services over optical networks leveraging the widely deployed MPLS technology. The technology in itself was designed for this purpose. Now, talking about end to end connection across the access, aggregation and core having just one convergence protocol to make this possible is the key talk of this project.

There are pretty many reasons why seamless MPLS is preferred over MPLS-TP; some of them are:

- Penultimate hop popping is not supported. Only ultimate hop popping is supported, because label mappings are configured at the MPLS-TP endpoints.
- Ethernet sub interfaces are not supported.
- IPV6 addressing is not supported.
- L2VPN interworking is not supported.
- PW ID Forward Equivalence Class (FEC) (type 128) is supported, but generalized ID FEC (type 129) is not supported.
- Ping for Static Pseudo wires over MPLS-TP tunnels is not supported.
- Optional Reverse Path Connectivity verification is not supported.
- MPLS-TP requires a more complex access layer compared to seamless MPLS when implemented with DoD.

There is still a great deal of "compartmentalization" between the parts of the network where MPLS-TP is used and where more dynamic functions of MPLS are used. MPLS-TP usage tends to be focused on the access and aggregation while MPLS usage tends to be focused on the

aggregation and core. Yet regardless of the network architecture, the networks need to provide end to end service with the guarantees and diagnostics as though there were a unified network.

9. Provider Backbone Bridging- Traffic Engineering (PBB-TE)

Ethernet's initial successes were mainly because of the massive adoption in Enterprise networks, its low cost and ease of deployment. Over the years Ethernet has evolved, initially running over coax cables at low speeds and nowadays over copper and fiber with speeds ranging up to 100Gbps and even more. Because of several enhancements Ethernet became an attractive technology in Service Provider (SP) and other Telecommunication environments. Originally designed as a local-area network (LAN) communication protocol, Ethernet allows computers and nodes to be interconnected within a small network. But to expand its reach into the core infrastructure, Ethernet needed to offer carrier-grade quality of service (QoS) guarantees and reliability to thousands of computers across metropolitan, national and global distances without affecting its simplicity and cost-efficiency.

In the past it was difficult for Carrier Networks to adopt Ethernet in the WAN or MAN, because:

- Native Ethernet does not support scaling up to millions of customers' MAC addresses.
- Native Ethernet frames do not have fields available for Class of Service (CoS)
- Identification Redundant Ethernet connections relied on the spanning tree protocol. The spanning tree protocol does not scale very well in large networks
- Lack of Operations Administration and Maintenance (OAM) support.

To address the above issues and meet carrier requirements, the IEEE defined several adaptations of Ethernet in amendments to the 802.1 standard. These changes comprise additional headers as well as changes of the Ethernet operational principles.

This technology can also be implemented over the network to provide End to End connection like the Seamless MPLS. We will analyse this further once we have seen through the Evolution, structure and working of PBB-TE.

9.1 PBB-TE: An Evolution to Legacy Ethernet

1. **802.1Q Vlan**

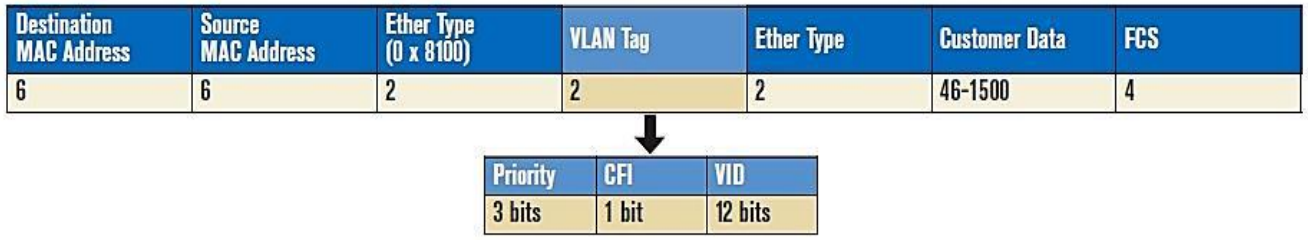

Figure 8 Ethernet Frame 802.1Q Vlan

Ref: Provider Backbone Bridge with Traffic Engineering, Thiemo Diallo, Application Note 210

The 802.1q VLAN tagging standard scales up to 4096 separated broadcast domains. So in theory with 802.1q it is possible to support 4096 customers within the provider network. With 802.1q the provider assigns VLANs, which the customers must use to avoid VLAN ID overlap in the provider network, which is inefficient and complex to coordinate. The 802.1q standard supports Class of Service (CoS) through the usage of three dot1p priority bits (PCP) in the VLAN header. The provider network needs to interact with customer layer 2 loop prevention mechanisms and makes forwarding decisions based on the learned customer MAC addresses. This is a potential security risk, as the provider core switches must act on the information received from the customer space (for example excessive MAC learning, spanning tree interaction). These

limitations caused the 802.1q standard not to be adopted by providers as a carrier grade transport technology.

9.2 Ethernet 802.1ad Provider Bridge

Destination MAC Address	Source MAC Address	Ether Type 0 x 8100 0 x 9200 0 x 9100 0 x 9300	S-VLAN	Ether Type 0 x 8100 0 x 9200 0 x 9100 0 x 9300	C-VLAN	Ether Type	Customer Data	FCS
6	6	2	2	2	2	2	46-1500	4

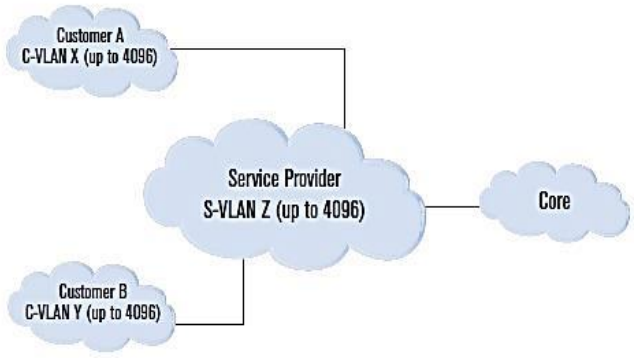

Figure 9 Ethernet Frame 802.1ad Provider Bridge

The Provider Bridging (802.1ad) standard has some major improvements over the 802.1q standard as it uses two stacked VLAN tags, the service provider tag (S-TAG or outer tag), which represents a customer or service instance in the provider network and the customer (C-TAGS/ inner tag) representing the customer VLANs. The main advantage over 802.1q is that customer VLANs can be reused and are non-overlapping as long as the S-TAG is different. Forwarding based on the S-TAG allows for a maximum of 4096 customer/ service identifiers in the provider networks. The dot1p value in the S-TAG and C-TAG makes it possible to preserve customer Class of Service (CoS) markings, hence the ability to provide CoS transparent services towards customers. Like the 802.1q standard, with Provider Bridging the customer MAC addresses are still used for forwarding purposes in provider networks. An increase in customer MAC addresses

results in an increase in the amount of MAC addresses learned in the provider network. This might result in scaling issues in the provider hardware or even cause outages due to broadcast storms (flooding). So although the 802.1ad standard has major benefits over the 802.1q standard, the 802.1ad standard still could not cope with the scaling and stability requirements needed in large carrier networks.

9.3 Ethernet 802.1ah Provider Backbone Bridge (PBB)

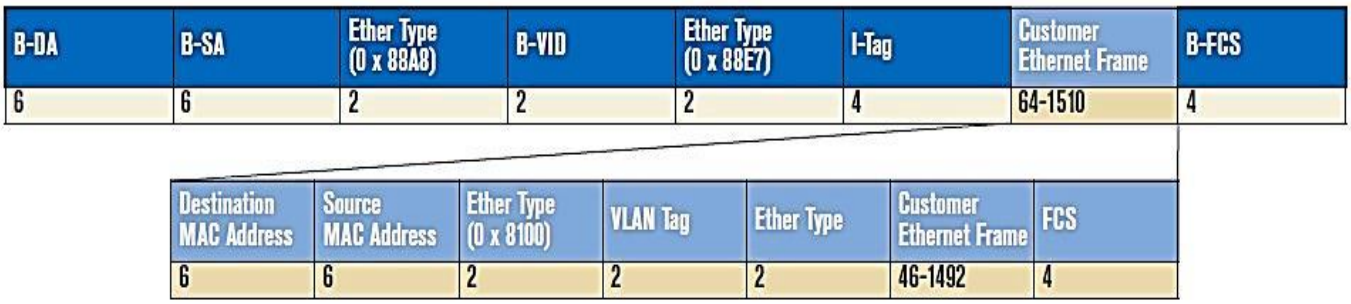

Figure 10 Ethernet 802.1ah frame- Provider Backbone Bridge

Ref: Provider Backbone Bridge with Traffic Engineering, Thiemo Diallo, Application Note 210

As networks grew, core switches needed to manage a greater number of medium access control (MAC) addresses in the forwarding tables.

Combined with the limited number of VLANs, this increased the complexity of the networks.

The 802.1ah PBB approach proposed encapsulates a customer's Ethernet frame into a carrier Ethernet frame, complete with its own MAC address space. Within a PBB network, frames are switched according to the destination backbone switch MAC.

The main advantage of this approach is the complete separation of customer and carrier domains, enabling the customer's Ethernet frames to be transparently transported in the carrier's Ethernet

frames. This greatly reduces the complexity of the switch-forwarding tables, as the entries are limited to the carrier's network switches.

PBB also added a unique field called I-Tag, which allows the carrier to assign QoS parameters and define a unique customer identifier (I-SID).

Therefore, traffic flows are assigned a unique I-Tag per customer, and QoS can be performed per customer instead of per VLAN. Moreover, since the I-SID is 24 bits long, there are up to two million service identifiers.

There is a clear separation between the customer space and provider space. Customer MAC addresses are learned only on the provider Backbone Edge Bridges (BEB) and are not used in provider Backbone Core Switches (BCB) for forwarding decisions. This is accomplished by having the BEB encapsulate the customer frames that are received on the UNI-N in a provider MAC header. A UNI or ENNI provides various data; control and management plane capabilities required by Carrier Ethernet providers and demarcate different network domains. A UNI can be of two types (UNI-C and UNI-N). A UNI-C is located on Customer edge equipment whereas the UNI-N is located on the Provider equipment. A UNI-C and UNI-N interface are always connected.

In a PBB network, forwarding is solely based on the Backbone VLAN (B-VID), which is a dedicated reserved Service Provider VLAN (S-VLAN). This means that the B-VID must be unique on each NNI within the PBB network. BCBs do not need to be PBB capable, as they just need to forward frames based on the B-VID. In other words, BCBs need at least 802.1q support to transport 802.1ah (PBB) tagged frames.

With PBB, carrier grade resiliency can be achieved using technologies like Transparent Interconnection of Lots of Links (TRILL) or Shortest Path Bridging Mac (SPBM), instead of

using a STP flavor for layer-2 loop avoidance. However these protocols currently do not have Traffic Engineering (TE) capabilities as with PBB-TE. With PBB, the number of transport tunnels is limited to 4096, as forwarding is based on a 12-bit B-VID only.

9.4 Ethernet 802.1Qay Provider Backbone Bridge- Traffic Engineering (PBB-TE)

This latest standard is based on the Nortel technology known as Provider Backbone Transport (PBT). Essentially based on the PBB frame format, the PBB-TE standard focuses on frame transport within the network as it replaces the existing spanning tree protocol (STP) with a connection-oriented and pre-established path configured by the user.

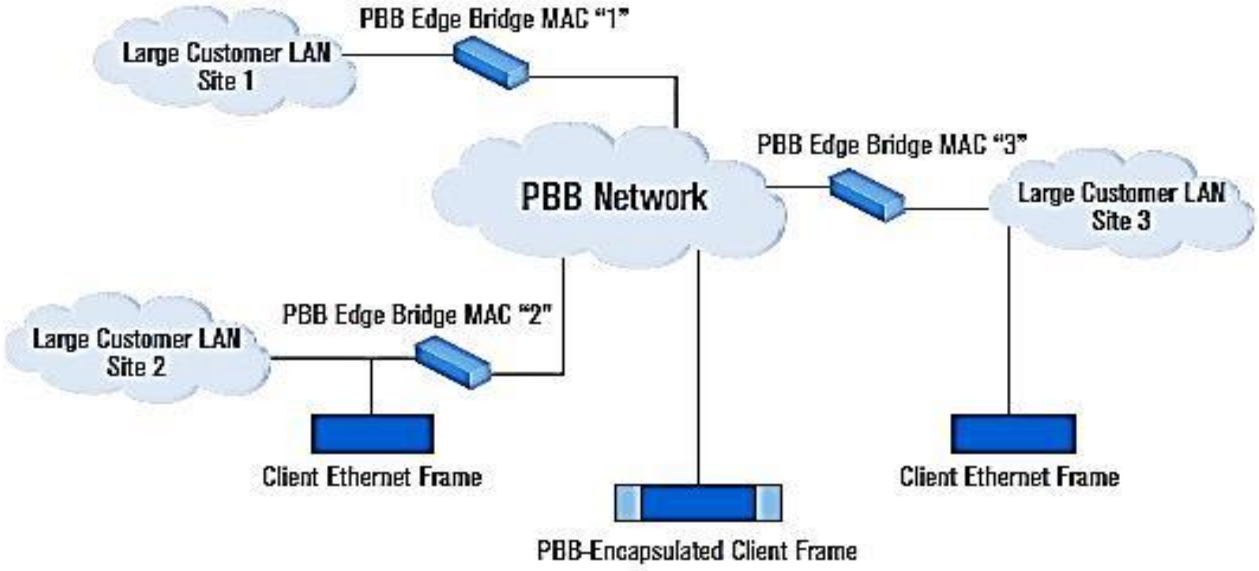

Figure 11 Ethernet 802.1Qay – Provider Backbone bridging with Traffic Engineering

Ref: Provider Backbone Bridge with Traffic Engineering, Thiemo Diallo, Application Note 210

In the figure above (Figure 11), the spanning tree is disabled, so the PBB forwarding devices only need to "learn" the MAC addresses of the edge devices to transmit the frames properly.

9.5 PBB-TE Architecture

The edge bridge is the interface between the customer network and the service provider network as shown in figure 12. This device is responsible for the encapsulation or de-encapsulation of the customer's Ethernet frames with PBB headers as well as the insertion of the proper backbone and I-Tag.

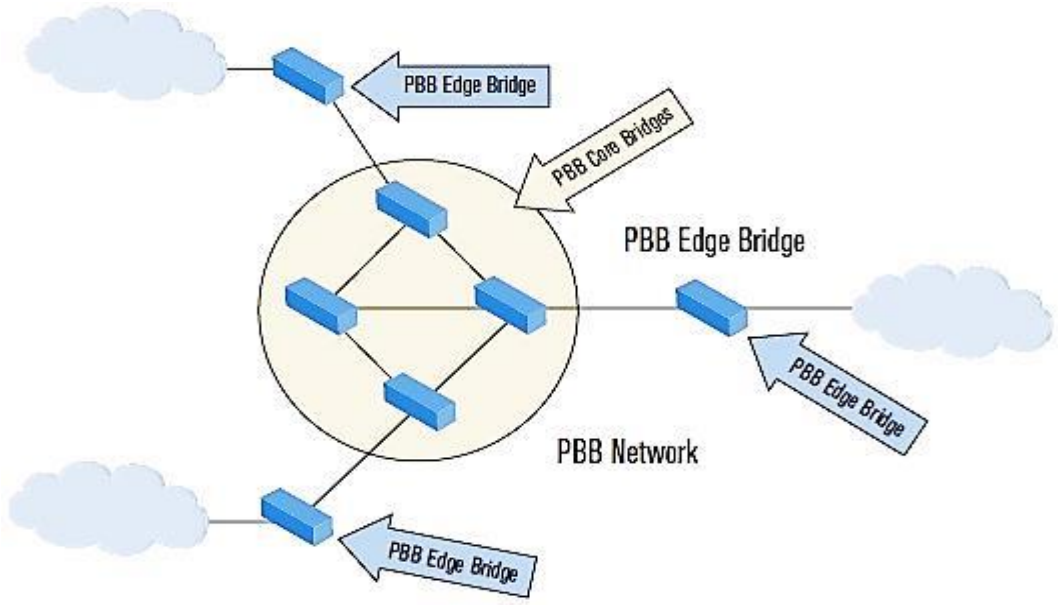

Figure 12 PBB-TE Architecture

Ref: Provider Backbone Bridge with Traffic Engineering, Thiemo Diallo, Application Note 210

These fields are mandatory, as the frames will be switched within the PBB-TE network based on the backbone destination MAC address (B-DA) and the backbone VLAN ID (B-VID). The I-Tag is used to identify QoS levels as well as the customer carried by the PBB frames via the service ID.

The backbone switch is responsible for the forwarding of PBB frames within the PBB-TE network using predefined routes according to the B-VID. These switches differ from normal Ethernet switch in that they lack STP (and its variant, rapid spanning tree protocol, or RSTP) measures.

9.6 PBB-TE Frame Forwarding

In PBB-TE, switches are configured with static routes by the network operator, ensuring that frames take predetermined paths within the network. The user must configure all the backbone switches in the forwarding table using external management software. In such a situation, frames with destination MAC addresses not yet associated in the port-MAC table will be dropped; they will not be forwarded. Since broadcast frames are not supported in PBB-TE networks, they will also be dropped by the backbone switches.

In PBB-TE forwarding is based on 46 bits of the 48 bit Destination BEB MAC address + the B-VID (12 bits), so 58 bits in total. Unlike PBB, with PBB-TE the B-VID may be reused on the NNI as long as the Destination BEB MAC is different. This means that with PBB-TE it is possible to have 4096 ESPs towards the same destination BEB, whereas with PBB the maximum is 4096 tunnels for the whole PBBN (assuming per hop BVID rewriting is not used, which buys some additional room due to BVID re-usage).

The PBB-TE management plane (NMS) ensures that the PBB-TE network is loop free, which means that STP is not needed and must be disabled for the PBB-TE VLAN range used in the PBBN. Carrier grade service resiliency (sub 50ms failover) is supported, by providing pre-provisioned backup paths (each with a different B-VID) in combination with OAM (CFM) for fault detection and service failover. Several drafts are proposed for dynamic control plane support for PBB-TE, where GMPLS is used to signal the bi-directional Ethernet Label Switched Paths (ESPs) and provisions OAM functions in the network.

As all PBB-TE paths are statically provisioned by the NMS, there is no need to support the forwarding of broadcast and or unlearned frames for BEB MAC address reachability. These broadcast or unlearned frames are either dropped or forwarded as unicast traffic to remote BEBs.

From a services perspective, PBB-TE only supports point-to-point services, thus E-LAN and E-TREE services are not natively supported. This does not mean that E-LAN services cannot be provisioned, however the design and applicability is often very limited and heavily relies on vendor specific / proprietary features.

9.7 PBB-TE: Connectivity Across the network (Edge to Edge)

Since PBB-TE requires the network operator to configure the path taken by frames across the network, this important test ensures that all nodes of the PBB network can be reached from any other node. More specifically, it ensures connectivity between edge switches, intrinsically measuring the route configured by the user.

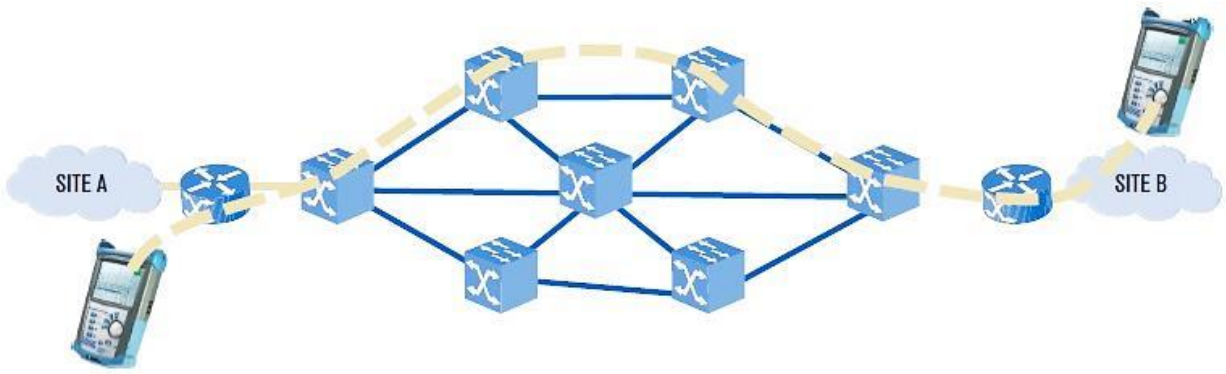

Figure 13 PBB-TE Edge to Edge connection

Ref: Provider Backbone Bridge with Traffic Engineering, Thiemo Diallo, Application Note 210

As protection or working paths are used according to VLAN settings, it is important to ensure that the edge and core switches are able to discriminate between specific VLANs and forward them correctly. Recognized VLANs must be forwarded as defined by the customer, while unrecognized VLANs should be discarded.

9.8 Analysis of PBB-TE for End to End Connection

Both PBB-TE and MPLS-TP are carrier grade transport technologies providing more or less the same functionality. From a management plane perspective, both technologies use the concept of static provisioning and monitoring through an NMS and have the option for a dynamic control-plane.

Comparing this to Seamless MPLS, the major advantage is; Seamless MPLS has dynamic provisioning and do not need provisioning at intermediate nodes unlike MPLS-TP and PBB-TE. Deploying a service from one metro region to another requires provisioning at several intermediate points in the end-to-end network, making troubleshooting and fault recovery more complex.

Both Seamless MPLS and MPLS-TP use a concept of forwarding based on per interface specific 20 bits labels, which is inherited from the MPLS standard and highly scalable. They allow stacking of (in theory) unlimited labels, where eventually hardware limitations, applicability and MTU considerations would become the limiting factor. In case of PBB-TE the hierarchy is limited to only one transport identifier (B-VID) and one payload identifier (I-SID).

PBB-TE does not support E-LAN services, whereas Seamless MPLS and MPLS-TP standards have support for E-LAN and E-TREE services.

Of all, the most important discussion here is the end to end connectivity. Though both PBB-TE and Seamless MPLS can provide the necessary services, their architecture is completely different. MPLS is so widely and popularly used and implemented in the core and aggregation layer that, people seem to focus on it. On the other hand, PBB-TE is used according to what type of specific service is required. MPLS is commonly known as the single convergence Protocol where it converges any protocol to the MPLS format by simply adding tags and carries it over the

network. It's interoperability with IP made it so easy and popular to use that almost every service provider has implemented it and made it as a standard. To look in to a greater picture, it would be way easier to implement Seamless MPLS over the already established standard of MPLS rather than going for an alternative to achieve the end to end connectivity.

10. Seamless MPLS: Design Use Case

10.1 Design

- Split the network into regions: access, metro/aggregation, edge, core
- Single IGP with areas per metro/edge and core regions
- Hierarchical LSPs to enable e2e LSP signaling across all regions
- IGP + LDP for intra-domain transport LSP signaling
- RSVP-TE alternative to LDP
- BGP labeled unicast for cross-domain hierarchical LSP signaling
- LDP Downstream-on-Demand for LSP signaling to/from access devices
- Static routing on access devices

10.2 Properties

- Large scale achieved with hierarchical design
- BGP labeled unicast enables any-to-any connectivity between >100k devices – no service dependencies (e.g. no need for PW stitching for VPWS service)
- A simple MPLS stack on access devices (static routes, LDP DoD)

10.3 Use Case: End to End connection Simplicity with Control and Data Plane

Access Node (AN) to Aggregation Node (AGN) which is part of the transport Node (TN) Via Downstream on Demand (DoD) – RFC5036

LDP DoD enables on-request label distribution ensuring that only required labels are requested, provided and installed.

Aggregation Node (AGN) to Area Border Routers (ABR) i.e. the Core Border Nodes (BN) via Downstream Unsolicited (DU). – RFC 5036 for advertising MPLS labels for all routes in their RIB. This is very insufficient for Access Nodes. Mostly stub nodes can rely on static routing and need reachability to a small subset of total routes (labels).

BGP-LU enables distribution of /32 router loopback MPLS FECs – RFC 3107 is used between Seamless MPLS regions for any2any MPLS reachability. This enables large scale MPLS network with hierarchical LSPs

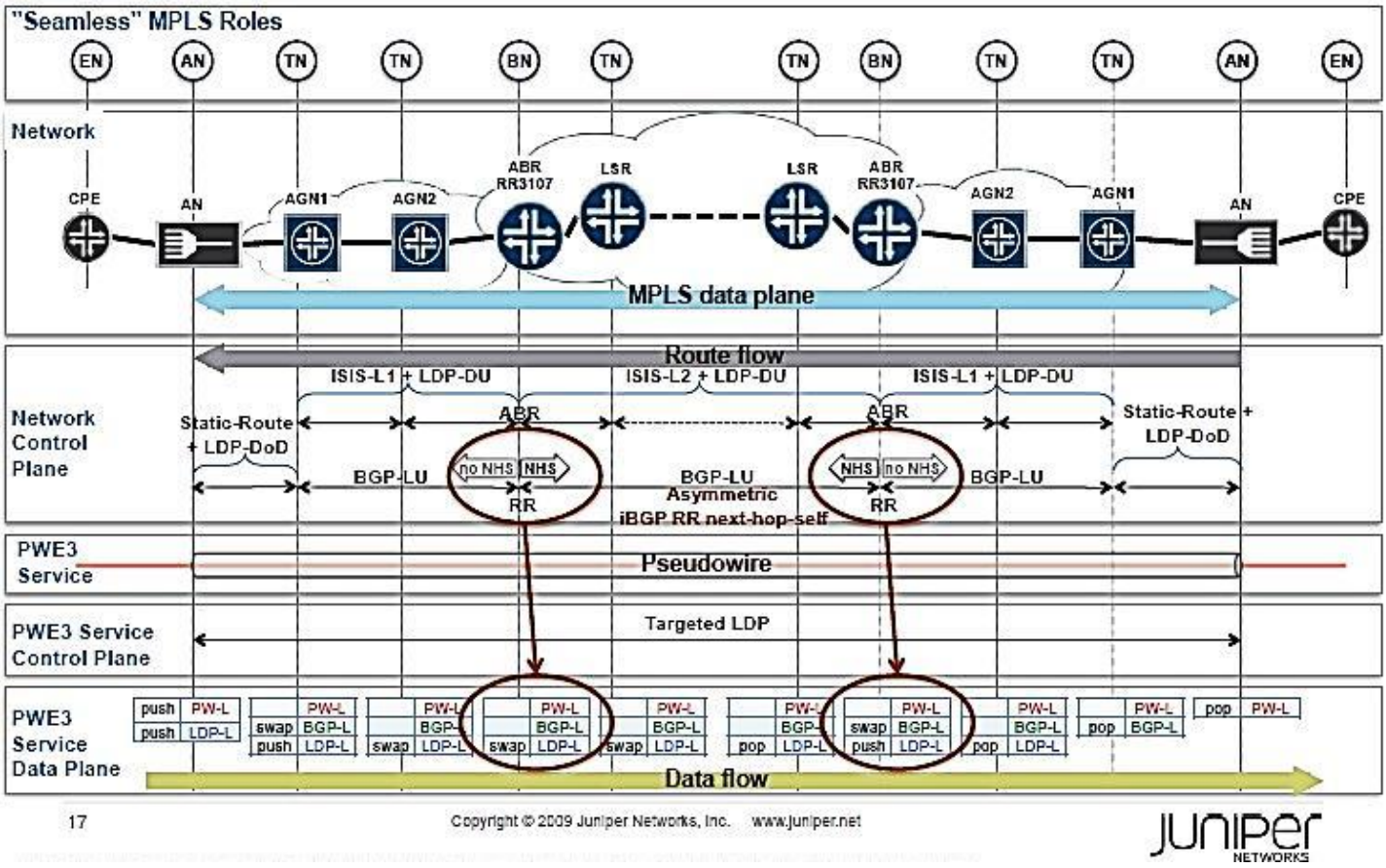

Figure 14 Seamless MPLS control plane and MPLS Data plane per Deployment Scenario #1 in draft-mpls-seamless-00 (Juniper Networks)

10.4 Labeled iBGP next-hop handling

The ABR nodes run labeled iBGP both to the core mesh as well as to the AGN1 nodes of their respective aggregation domains. Therefore they operate as iBGP route reflectors, reflecting labeled routes from the aggregation into the core and vice versa.

When reflecting routes from the core into the aggregation domain, the ABR SHOULD NOT change the BGP NEXT-HOP addresses (next-hop unchanged). This is the usual behaviour for iBGP route reflection.

In order to make these routes resolvable to the AGN1 nodes inside the aggregation domain, the ABR MUST leak all other ABR and core PE loopback addresses from ISIS L2 into ISIS L1 of the aggregation domain. Note that the number of leaked addresses is limited so that the overall scalability of the seamless MPLS architecture is not impacted. In the worst case all core loopback addresses COULD be leaked into ISIS L1, but even that would not be a scalability problem.

When reflecting routes from the aggregation into the core, the ABR MUST set then BGP NEXT-HOP to its own loopback addresses (next-hop self) NHS. This is not the default behaviour for iBGP route reflection, but requires special configuration on the ABR. Note that this also implies that the ABR MUST allocate a new local MPLS label for each labeled iBGP FEC that it reflects from the aggregation into the core. This special next-hop handling is essential for the scalability of the overall seamless MPLS architecture since it creates the required hierarchy and enables the hiding of all aggregation and access addresses behind the ABRs from an IGP point of view.

An access node is commissioned without any services provisioned on it. The AN can request labels for loopback addresses of any AN, AGN, or other nodes within the Seamless MPLS network for operational and management purposes. (RFC 7032)

11. CONCLUSION

This project on Seamless MPLS provided the Technical Approach towards Seamless MPLS control Plane in detail projecting End to End Connectivity. The scope and business feasibility was just not constrained to this approach, but other networking technologies such as MPLS-TP and PBB-TE were compared in this project with technical approaches, to provide connectivity from source to destination Node without any barriers. Though all these technologies could possibly perform almost similar behavior in terms of resolving connections during failures, results and throughput, the Project showed why Seamless MPLS is on the rise and is in demand in the future of networking.

A major fact that is to be essentially noted is that, both MPLS-TP and PBB-TE are not ignored technology protocols, but are essential to certain use cases wherever it fits best. The point of this project was to gape through the technologies for an end to end connectivity. Furthermore both MPLS-TP and PBB-TE can run in the underlining Seamless MPLS protocol without any hassle and can be used to configure the Access Nodes to the Aggregation nodes.

This Project also showed how seamless MPLS overcomes the different barriers of the traditional IP- MPLS and other barriers by MPLS-TP and PBB-TE. One of the main reasons of its popularity is the ease of implement considering MPLS already being implemented almost at every Service Provider’s Aggregation and Core Layer.

List of Abbreviations

1	IP	Internet Protocol
2	MPLS	Multi-Protocol Label Switching
3	LTE	Long Term Evolution
4	MAN	Metropolitan Area Network
5	WAN	Wide Area Network
6	QoS	Quality of Service
7	PBB-TE	Provider Backbone Bridging- Traffic Engineering
8	LER	Label Edge Router
9	PER	Provider Edge router
10	LSR	Label switching routers
11	LSP	Label Switched paths
12	FEC	Forward Equivalence Class
13	CER	Customer Edge Routers
14	RIB	Routing information Base
15	LIB	Label information Base
16	FIB	Forwarding information Base
17	LFIB	Label forwarding base
18	TDP	Tag Distribution Protocol
19	BGP	Border Gateway Protocol
20	RSVP	Resource reservation Protocol
21	VPN	Virtual Private Network
22	ATM	Asynchronous Transfer Mode
23	SONET	Synchronous Optical Networking
24	FMC	Fixed and Mobile Network convergence
25	AN	Acces Node
26	AGN	Aggregation Nodes
27	TN	Transport Node
28	SN	Service Node
29	IGP	Interior Gateway Protocol
30	EGP	Exterior Gateway Protocol
31	NLRI	Network Layer reachability information
32	SAFI	Subsequent Address Family Identifier
33	OSPF	Open shortest path first
34	AS	Autonomous system
35	ABR	Area Border Router

36	RR	Route Reflector
37	ISIS	Intermediate system- Intermediate System
38	DU	Downstream Unsolicited
39	DoD	Downstream on Demand
40	FRR	Fast Re route
41	CPU	Central Processing Unit
42	LFA	Link Failure Alternative
43	EIGRP	Enhanced Interior gateway routing protocol
44	PIC	prefix independent convergence
45	TP	transport Protocol
46	GMPLS	Generalized MPLS
47	OAM	Operation, Administration and Management
48	P2P	Point to Point
49	P2MP	point to multi-point
50	PW	Pseudo Wire
51	BFD	Bidirectional Forwarding Detection
52	G-Ach	Generalized Associated Channel
53	GAL	G-Ach Label
54	ASON	Automatically Switched Optical Network
55	ADM	Add-Drop Multiplexer
56	WDM	Wavelength division Multiplexing
57	SP	Service Provider
58	LAN	Local Area Network
59	CoS	Class of Service
60	MAC	Media Access Control
61	Vlan	Virtual LAN
62	PCP	Priority Code Point
63	SID	Service Instance VlanID
64	BEB	Backbone Edge Bridges
65	BCS	Backbone Core Switches
66	UNI	User to Network Interface
67	TRILL	Transparent Interconnection of Lots of Links
68	SPBM	Shortest Path Bridging Mac
69	VID	VLAN ID
70	STP	Spanning Tree Protocol
71	B-DA	Backbone Destination MAC Address
72	NNI	Network to Network Interface

73	PBBN	Provide Backbone Bridging Network
74	CFM	Connectivity Fault Management
75	NMS	Network Management System
76	ESP	Ethernet Label Switched Paths

References

1. Seamless MPLS Architecture draft-ietf-mpls-seamless-mpls-07, June 28, 2014, MPLS Working Group, Internet-Draft.
2. BGP Prefix Independent Convergence draft-rtgwg-bgp-pic-02.txt, October 21, 2013, Network Working Group, Internet Draft.
3. Achieving Sub Second IGP Convergence in Large IP Networks, Pierre Francois Dept CSE, Universit ´e catholique de Louvain (UCL), Clarence Filsfils and John Evans Cisco Systems, Olivier Bonaventure Dept CSE, Universit ´e catholique de Louvain (UCL).
4. Loop-Free Alternate (LFA) Applicability in Service Provider (SP) Networks, June 2012, Internet Engineering Task Force (IETF).
5. RFC 5286, Basic Specification for IP Fast Reroute: Loop-Free Alternates, September 2008, Network Working Group.
6. RFC 3107, Carrying Label Information in BGP-4, May 2001, Network Working Group.
7. RFC 4364, BGP/MPLS IP Virtual Private Networks (VPNs), February 2006, Network Working Group.
8. Implementing Seamless MPLS, Maciek Konstantynowicz, Internet Engineering, Juniper Networks, March 2011.
9. Network Scaling with BGO Labeled Unicast, Design and Configuration Guide, Juniper Networks.
10. RFC 5036, LDP Specification, October 2007, Network Working Group.
11. RFC 5283, LDP Extension for Inter-Area Label Switched Paths (LSPs), July 2008, Network Working Group.

12. RFC 5151, Inter-Domain MPLS and GMPLS Traffic Engineering – Resource Reservation Protocol-Traffic Engineering (RSVP-TE) Extensions, February 2008, Network Working Group.
13. Scaling MPLS – Seamlessly resilient service enablement at massive scale using standard protocols, RIPE65 – Amsterdam, NL September 24, 2012, Christian Martin, Juniper Networks.
14. RFC 7032, LDP Downstream-on-Demand in Seamless MPLS, October 2013, Internet Engineering Task Force (IETF).
15. Connection Oriented Ethernet Vs MPLS-TE: An Ethernet Transport layer TCO Comparison, Management Consultants to the Networking Industry, Network Strategy Partners, March 2009.
16. MPLS Transport Profile, July 15, 2011, Cisco.
17. MPLS Transport Profile (MPLS-TP)- A Set of Enhancements to the Rich MPLS Toolkit, Juniper Networks, White paper.
18. MPLS in Next-Generation Transport Networks, A Light Reading Webinar Sponsored by Cisco, Ericsson, Metaswitch Networks, IXIA and ECI.
19. Evolving to "End to End MPLS" Architecture Alcatel-Lucent Enables Seamless, Scalable, Resilient MPLS Networks Technical White Paper.
20. Provider Backbone Bridge with Traffic Engineering: A carrier Ethernet Technology Overview By Thierno Diallo, Product Specialist
21. RFC 3916, Requirements for Pseudo-Wire Emulation Edge-to-Edge (PWE3), Network Working Group

22. SURFnet7: PBB-TE and MPLS-TP technical description and comparison by Jörg Buesink, December 24th, 2013
23. RFC 3209, RSVP-TE: Extensions to RSVP for LSP Tunnels, Network Working Group, Decmeber 2001
24. RFC 3724, The Rise of the Middle and the Future of End-to-End: Reflections on the Evolution of the Internet Architecture, March 2004, Network Working Group
25. RFC 4090, Fast Reroute Extensions to RSVP-TE for LSP Tunnels, May 2005, Network Working Group
26. Seamless MPLS: Flexible Service Delivery, Juniper Networks
27. Seamless MPLS, Juniper Networks, Whitepaper
28. Scaling MPLS – Seamlessly resilient Service Enablement at massive scale using standard Protocols , Juniper Networks
29. http://blog.ine.com/2010/06/28/mpls-components-part-2/#more-3968
30. http://networkstatic.net/the-control-plane-data-plane-and-forwarding-plane-in-networks/
31. http://www.cisco.com/c/en/us/support/docs/multiprotocol-label-switching-mpls/mpls/116127-configure-technology-00.html#
32. http://slideplayer.us/slide/721469/