MINT 709

CAPSTONE PROJECT

Project

Enabling MPLS-centric MEF services across Service Provider Networks.

Name: Syed Najm us Saqib Tariq

Supervisor: Mr. Juned Noonari

TABLE OF CONTENTS

LIST OF FIGURES

ABSTRACT

Today almost every service provider use Multi-Protocol Label Switching (MPLS) on its core network, because it is one of the technologies that are easily scalable, with more flexibility to work with existing technologies and better compatibility for service providers carrying traffic with QoS and traffic engineering options make MPLS more demanding.

Similarly, on the other hand Ethernet is one of the most widely deployed technologies across the globe with so many advancements are already in its account. It is very simple and has a very low operating cost which makes it more preferable option for service providers and subscribers to work with.

The prime objective behind this project is to further investigate MPLS and MEF services to enable Ethernet Services over a service provider's MPLS core network.

Therefore, a detailed study of MPLS is required for Layer 2 services and then Ethernet services will be taken into consideration before moving on to the deployment phase.

After thorough study is done on MPLS & Ethernet, The MEF and IETF standards and their requirements for each service will be taken under consideration so that each service should meet their requirements.

Before moving on to the LAB Demo it will be important to select the supporting hardware for configuring these services. It is recommended to use MEF certified hardware depending upon the availability.

After successful deployment of MPLS would be done on a test bed will be created in lab environment for testing of MPLS. After that Ethernet Services E-LINE, E-LAN and E-TREE would be configured one by one on the same generic test bed which have MPLS configured.
Lastly, a complete network test will conducted for MEF standards and L2 C-PE compliance.

2 - INTRODUCTION TO MPLS

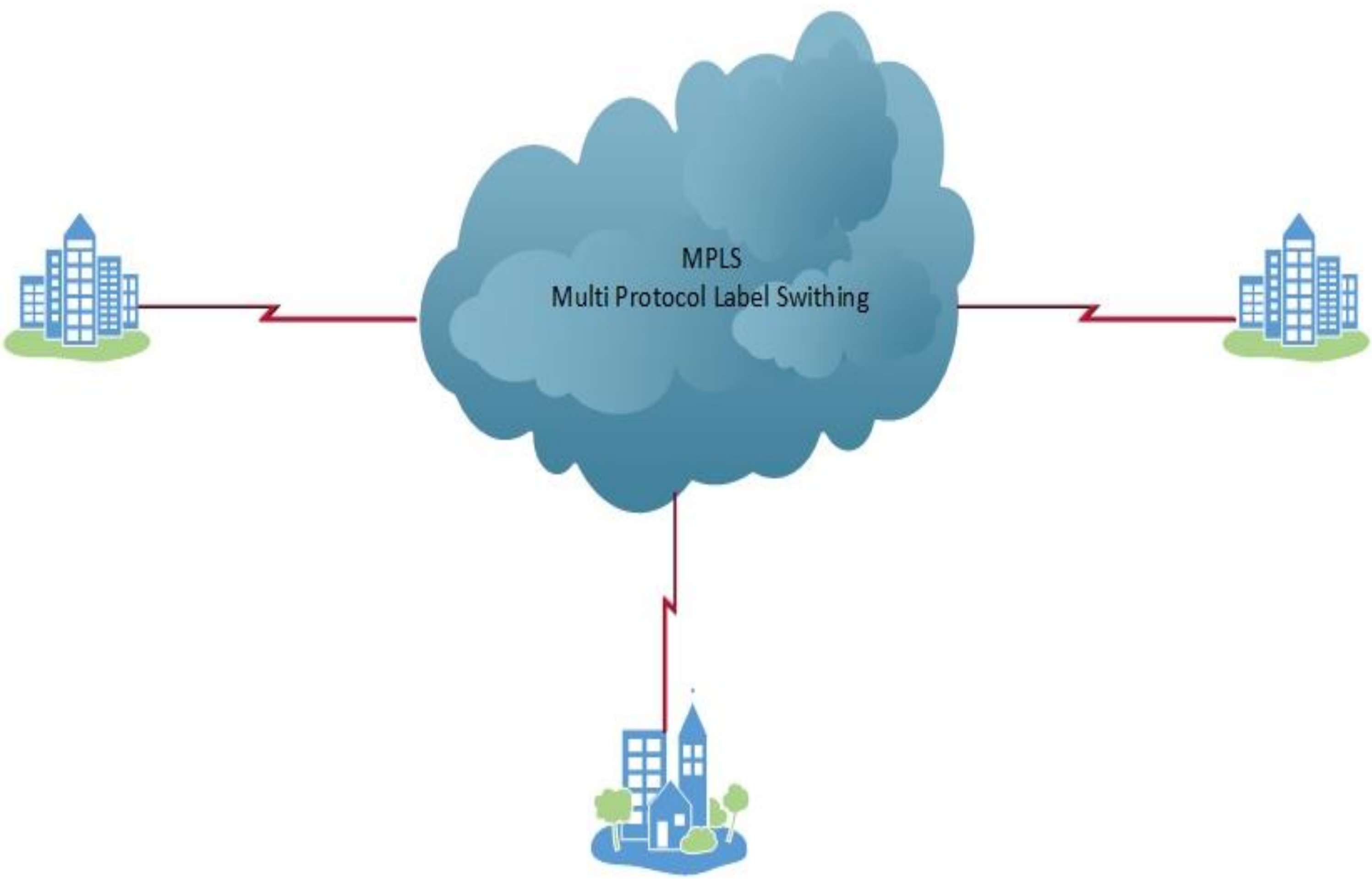
MULTI PROTOCOL LABEL SWITCHING

2.1 Introduction

MPLS is the technology that has been an integral part of the service provider networks for past few years. MPLS is a switching technology, but works quiet differently. MPLS uses labels to forward packets from one network to another over the WAN. MPLS defines a label to label network that can provide optimal traffic flow.

Some of the key benefits of MPLS are as follows:

- Efficient Traffic Engineering
- Scalability
- Better Quality of Service
- Optimal Traffic Routing



2.2 Significance of MPLS

Multi-Protocol Label Switching is industry standard used by service providers to give their clients Quality of service as well as provides possibility for the availability of network to far ends. As growing businesses cause growth in networks causing connectivity from one branch to other city to city. This may cause issues for service providers to control multiple clients having multiple branches place to place. MPLS gives easy management, flexibility and cost effective solution.

MPLS provides separate virtual route forwarding for different subscribers that end the problem of duplicate addressing over same router by different subscriber. Moreover MPLS is also used for load balancing over multiple links with different bandwidth over different links. MPLS is more oriented towards Service Providers, a customer network does not need to know MPLS and for most of the cases a default route from subscriber router is enough. While a provider can address the network scalability and redundancy issues where as subscriber can concentrate on his core business without having bothered about network connectivity.

MPLS brings perfect flexibility as it is difficult to make all these technologies to work together but MPLS can be used with various technologies. With Any Traffic over MPLS (AToM) a Service Provider can shift Layer 2 frames over MPLS backbone, even with Interworking IP, one can have a Layer 2 VPN with Serial link on one side and Ethernet on the other side. More over the customers who want to manage their routing can do it themselves with Layer 2 VPN and others can use Layer 3 VPN.

MPLS provides quality of service in cases where priority is real concern such as IP based voice service needs to have more priority as it is very sensitive to delay, jitter etc.

2.3 MPLS HEADER:

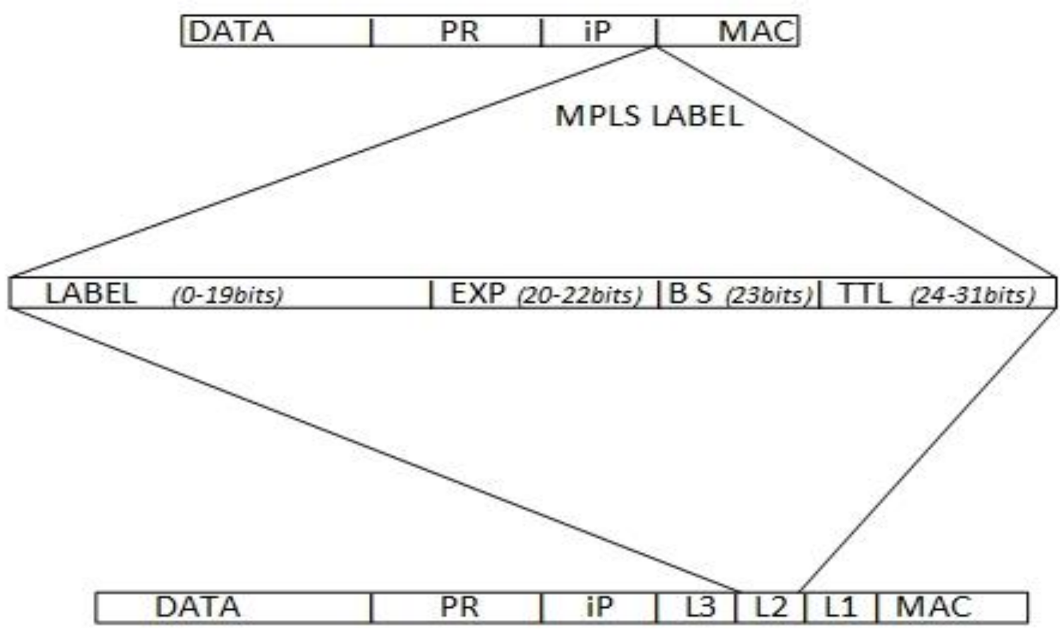
MPLS header works between Layer2 and Layer3 headers. It is often known as Shim Header, because it is inserted between the network and IP headers. It is a 32-bit header in which first 20 bits are the actual label, next 3 bits are for experimental purposes, 1 bit for Bottom-of-Stack, and an 8 bit for TTL.

Label: 20-bit label value, which is used for determining where to forward the packet and what operation to perform.

Exp: 3-bit value, used for experimental purposes. Different vendors use it for different Class of Service. E.g. Cisco Systems use it for Quality of Service (QoS).

BS: 1-bit value, can be set either 1 or 0. When set to 1, it means that it is the last entry of the label stack. Else, zero is set of all label stack entries.

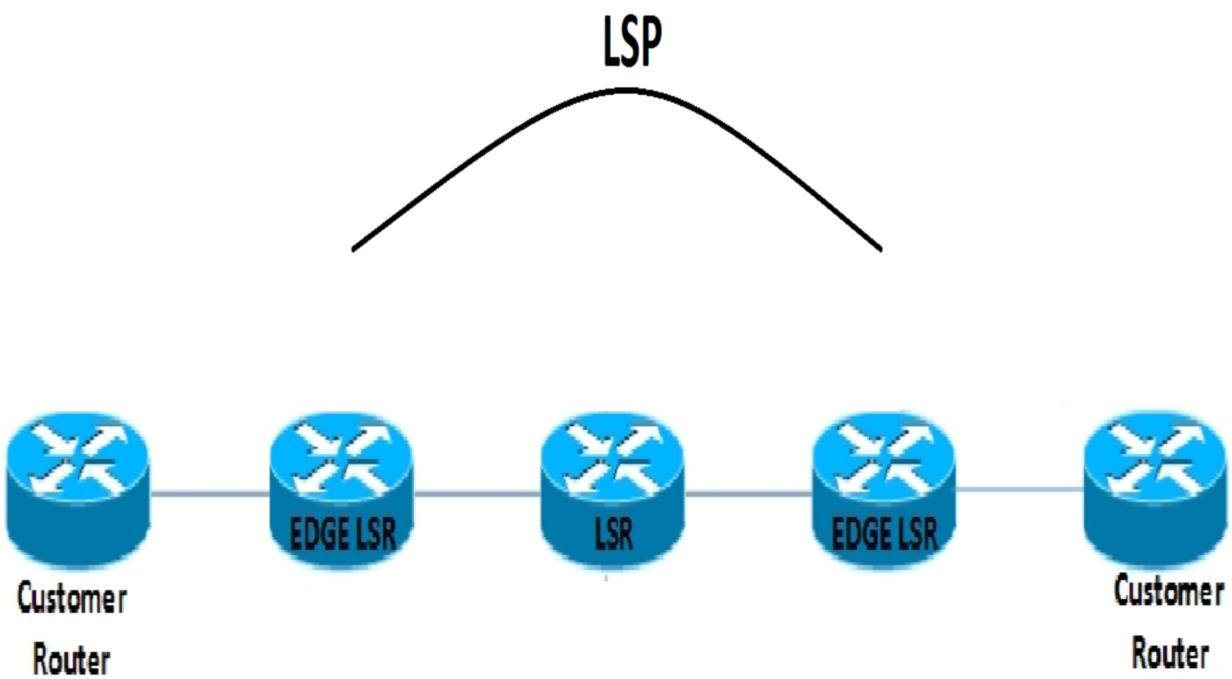
TTL: 8-bit value, for path tracing and visibility. It is also used for avoiding forwarding loops.



2.4 Label Switched Path LSP

LSP Label Switched Path is a unidirectional path created using LDP or RSVP. It is actually the path of multiple Label Switched Routers LSRs that are responsible to switch a labelled packet through an entire MPLS network or through some limited part of MPLS network.

The end routers of the path from which a label is ingress or egress are called Edge-LSR Label Edge Router or ingress LSR Label Switch Router and egress LSR Label Switch Router and all the routers in between are called the LSR Label Switched Router.



A label Switch router is that router that is capable of understanding the MPLS labels in the network and can perform three tasks Pop, Push and Swap.

Pop: It is capable of popping one or more labels before switching the packet.
Push: Capable of pushing the label into the packet.

Swap: And is eligible to swap a label.

A Label Switched Path can also be a Nested LSP as it is not compulsory that the ingress label router is always the first router where labels are assigned labels can be assigned even before that router and we call this a Nested LSP.

Since MPLS is a service provider technology and customer should not receive MPLS labeled packets, therefore the labels are striped off from the frame by the service provider router known as Edge Label Switch Routers before forwarded towards the client router. These routers are one the edge just before the client router. The routers just used for forwarding tagged packets are known as LSR Label switched routers. These routers are the core service provider routers and just used to forward Labels from one router to other router.

2.4 FEC Forwarding Equivalence Class:

FEC Forwarding Equivalance Class is a clasification done on the basis of policies to deal with in coming packets. The packets classified in a same FEC are given the same forwarding treatment for that entire class. When a packet is received its certain charactherstics are mapped in the FEC and then the packet is forwarded accrodingly. For example Layer 2 packets received from a perticular EVC at the ingress are forwarded through a particular EVC to a specific egress LSR.
A certain FEC Forwarding Equivalance Class packets can have a same label but all packets containing identical labels can belong to different FECs because there EXP value can differ.

2.5 Label Distribution Protocol

When MPLS was introduced the decision was to be made weather to emend the existing routing protocol or to make new official protocol for label information known as Label Distribution Protocol.

Label Distribution Protocol consist of

- **Forwarding Information Base Table (FIB)** table moves routing table in to cache structure where it keeps the date base of the network with the next label to get there.
- **Label Information Base Table (LIB**) table only consist of label information of the neighboring routers.
- **Label Forward Information Base Table (LFIB)** It is the combination of FIB and LIB table. It is the action table, which label should go to which router and if router receives, which labels from which router.

1. First Router adds Route in Routing table
2. The MPLS Enable Routers Assign Labels to each router (information for FIB table).
3. The routers advertise their Labels to or router (information for LIB table).
4. From this information FIB, LIB and LFIB table is formed.

2.6 RSVP (Resource Reservation Protocol)

RSVP is a signaling protocol that can control bandwidth allocation and is used true traffic engineering over MPLS network. LDP, RSVP both uses discovery advertisements to find the path from one client branch to other. RSVP has an additional feature that controls the flow of traffic through an MPLS network, while LDP is restricted to using the configured IGP's shortest path. RSVP uses a combination of the Constrained Shortest Path First (CSPF) algorithm and Explicit Route Objects (EROs) to find how traffic should flow.

Explicit Route Objects (EROs) limits LSP routing to a limited list of LSRs. By default, RSVP path that is defined by the network IGP's shortest path.

EROs consists of two types of instructions:

Loose hop is configured, it identifies one or more transit LSRs through which the LSP must be routed. The network IGP determines the exact route from the inbound router to the first loose hop, or from one loose hop to the next. The loose hop specifies only that a particular LSR be included in the LSP.

Strict hop identifies an exact path through which the LSP must be routed. Strict-hop EROs specifies the exact order of the routers through which the RSVP messages are sent.

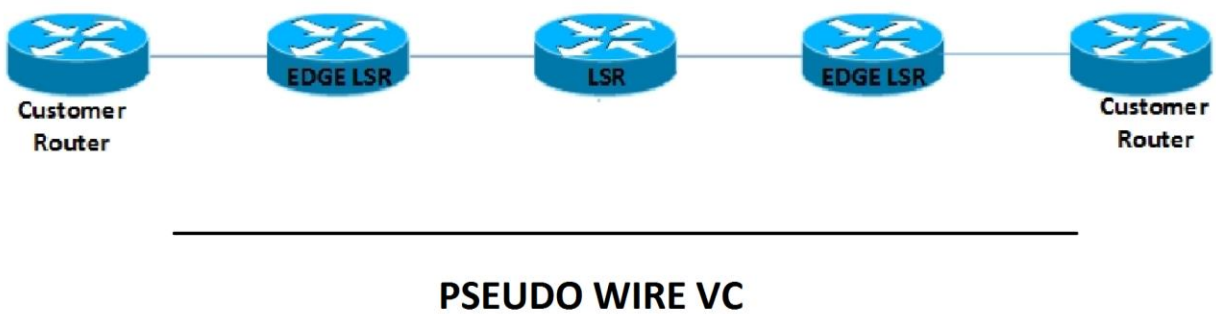
Constrained Shortest Path First algorithm to decide traffic is routed within the network, RSVP uses the Constrained Shortest Path First (CSPF) algorithm to calculate traffic paths that are subject to the following constraints:

- LSP attributes—Administrative groups such as link coloring, bandwidth requirements, and EROs
- Link attributes—Colors on a particular link and available bandwidth

2.7 Pseudo-wire

A Pseudo-wire is a strictly point to point service, It is normally used with attachment circuits. It contains two unidirectional LSPs which are represented by Virtual Circuit Labels (VC Label) or PW Labels. Pseudo Wire is used to transport Layer 2 frames over a MPLS network. It uses LDP signaling. Pseudo wires normally can be used in VPWS (Virtual Private Wire Service) or with VPLS.

Pseudo wire can be used with either VLAN tags or without VLAN tags. If we are using VLAN tags then they should be same on ingress and egress of same EVC. It can also carry VLAN tags for service providers with QinQ encapsulation.



2.8 VPLS Virtual Private LAN Service

Virtual private LAN service VPLS is a multipoint service. It is able to transport non IP data. Basically VPLS is Layer 2 multipoint VPN that permits more than one sites to be connected in a single bridged domain over a service provider's managed IP MPLS network.

All subscriber sites in a VPLS instance seems to be similar in the Local Area Network regardless of their actual locations. VPLS uses an Ethernet interface with customer, this modifies the LAN, WAN boundaries and permits quick and flexible service provisioning.

Generally a VPLS capable network is consist of 3 main components

- Customer Edges or CEs
- Provider Edges or PEs
- Core MPLS Network

The CE device is router or switch terminated at Customer's premises. However, The PE device is in which all the VPN intelligence and VPLS information is stored. Also PE's are devices where all the necessary tunnels are established to connect all other PEs. The IP MPLS Core Network interconnects Provider Edges and it does not really take part in the VPN operations. Traffic is simple switched based on MPLS labels.

Multipoint VPN service such as, Virtual private LAN service is the full mesh of the MPLS tunnels that are laid among all the PEs participating in the VPN service for all VPLS instances. This full mesh of interconnected tunnels is knows as pseudo wires is created between in all the PEs that take part in the VPLS instance.

3 - INTRODUCTION TO ETHERNET SERVICES

Ethernet Services are very beneficial for a service provider because these services help service provider in increasing total revenue by carrying different applications and types of traffic with excellent network efficiency and are adorably improving customer experience.

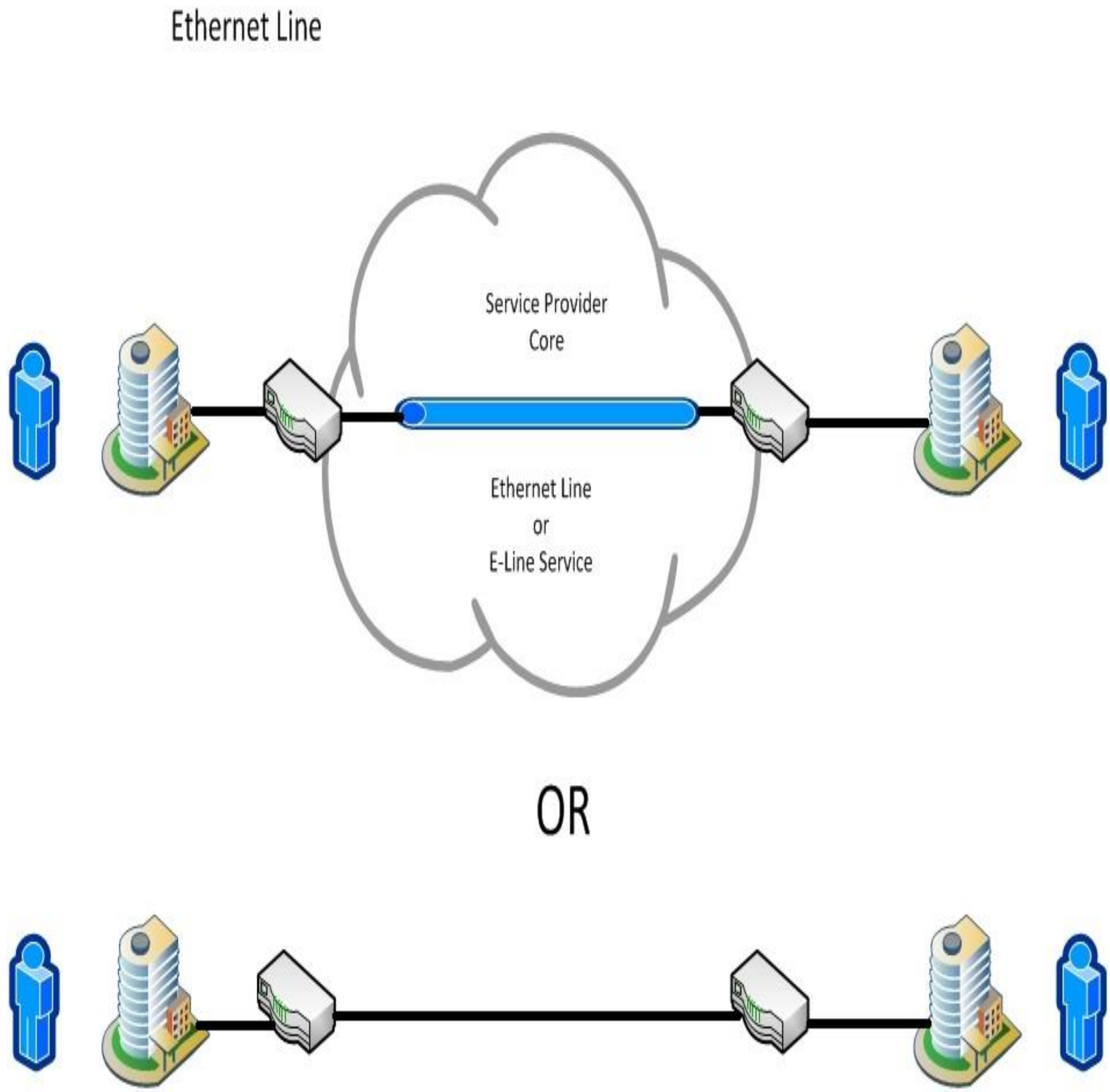
These Ethernet services also provide service provider with the opportunity for simple and efficient monitoring of entire network. By using OAM fault and performance management tools within a network and even across a network.

The other most beneficial service is Ethernet Access which has given Small to Medium business customers a very simple, reliable and secure way to carry there any type of traffic from one site to the other.

Currently the work is being done for the solution of Ethernet services over cloud Networks and there are some solutions and recommendations but still these services are not fully mature as per today's requirements. There is also on going work for making the monitoring of these services even better.

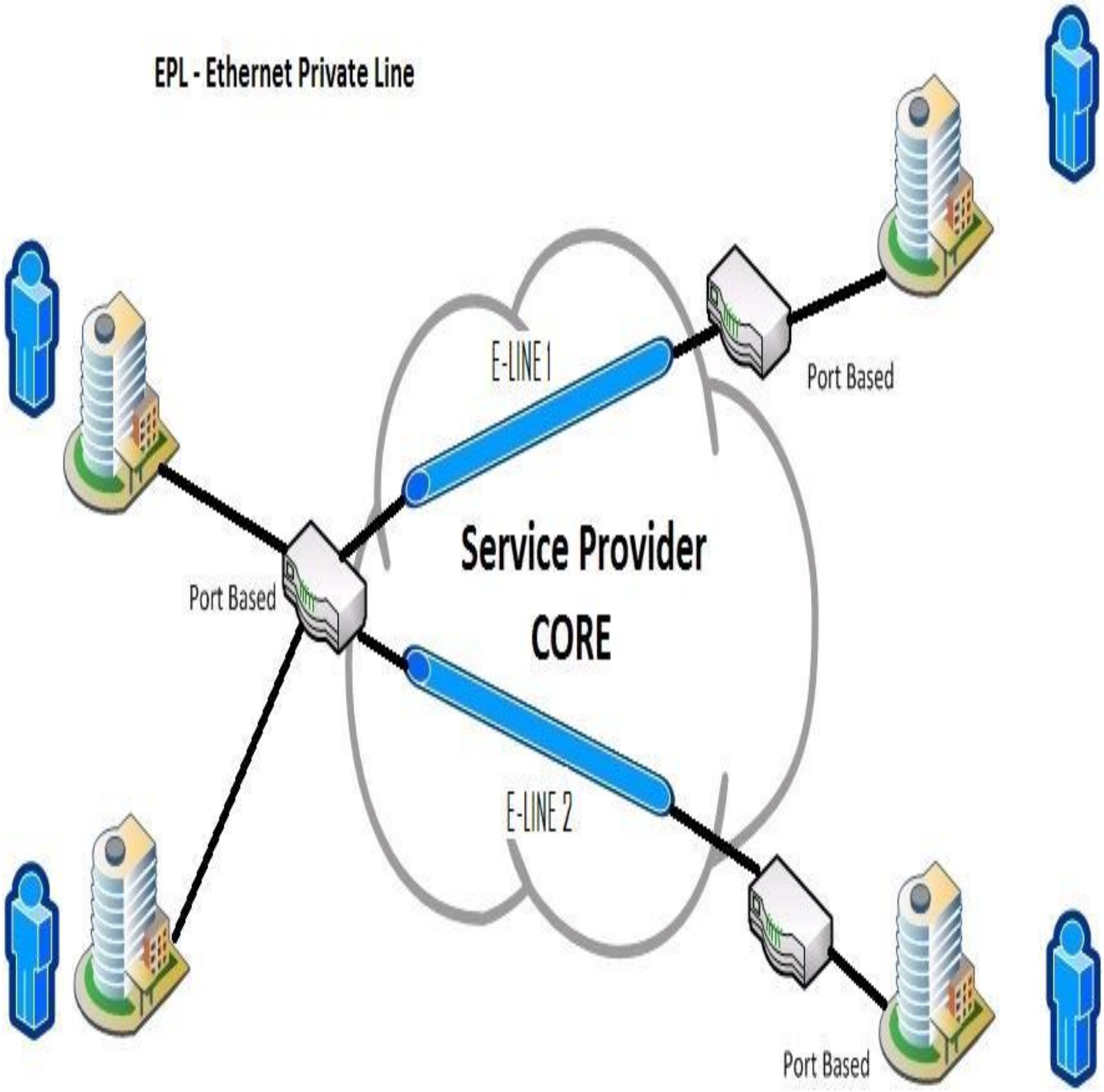
3.1 Ethernet Line or E-Line Service:

Ethernet Line (E-Line) service is purely a point-to-point Ethernet service. It is a transparent layer 2 service strictly between two UNIs. An E-Line has two different types of services, port based (Ethernet Private Line - EPL) and VLAN based (Ethernet Virtual Private Line - EVPL) as defined by the MEF in document 6.1. E-Line is also known as VLL which is Virtual Leased Line.



3.1.1 Ethernet Private Line:

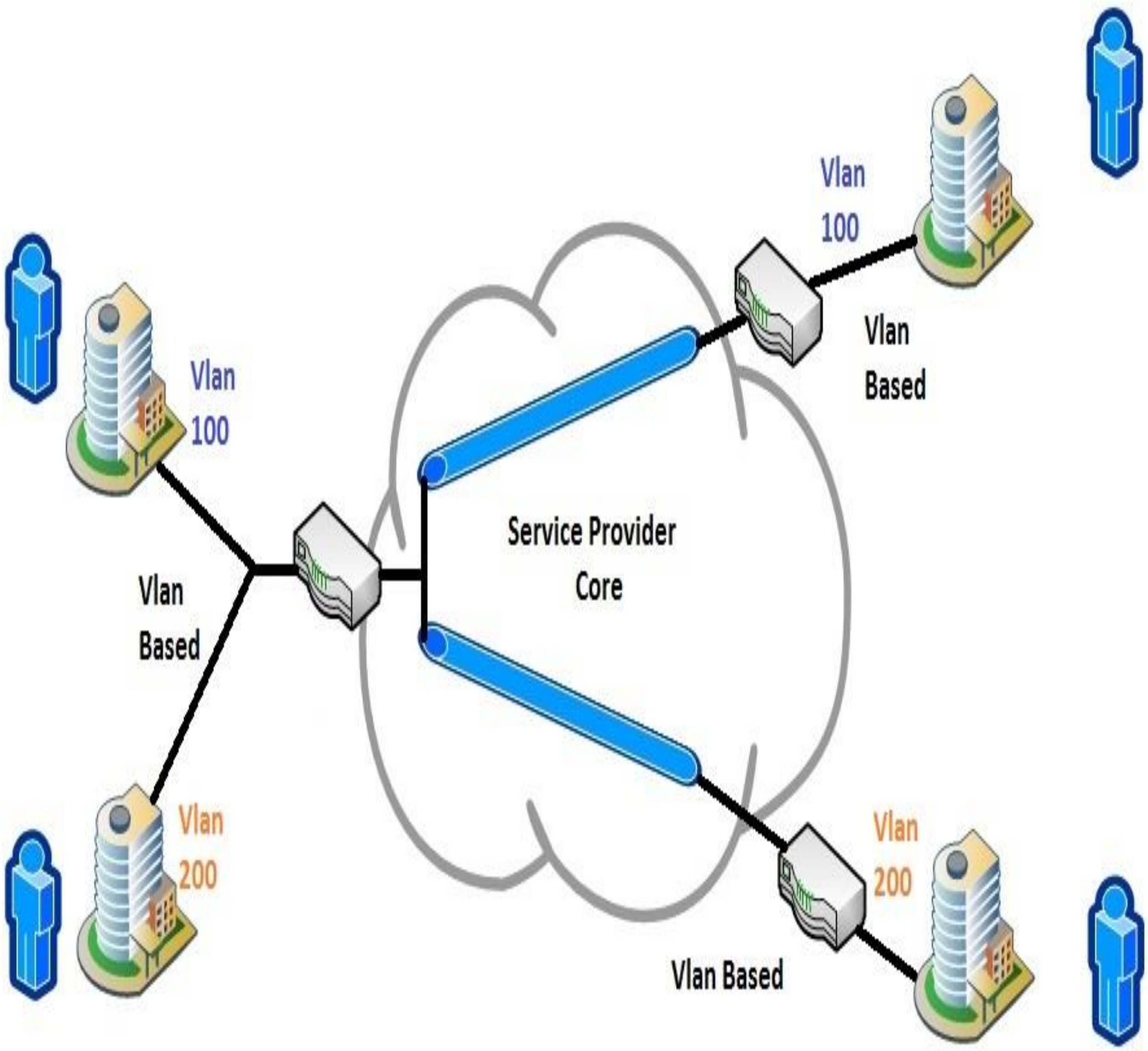
Ethernet Private Line is a port based E-Line service. Ethernet Private Line restricts service multiplexing by dedicating an independent UNI for each service.



As shown in the figure above each subscriber uses independent port based services.

3.1.2 Ethernet Virtual Private Line:

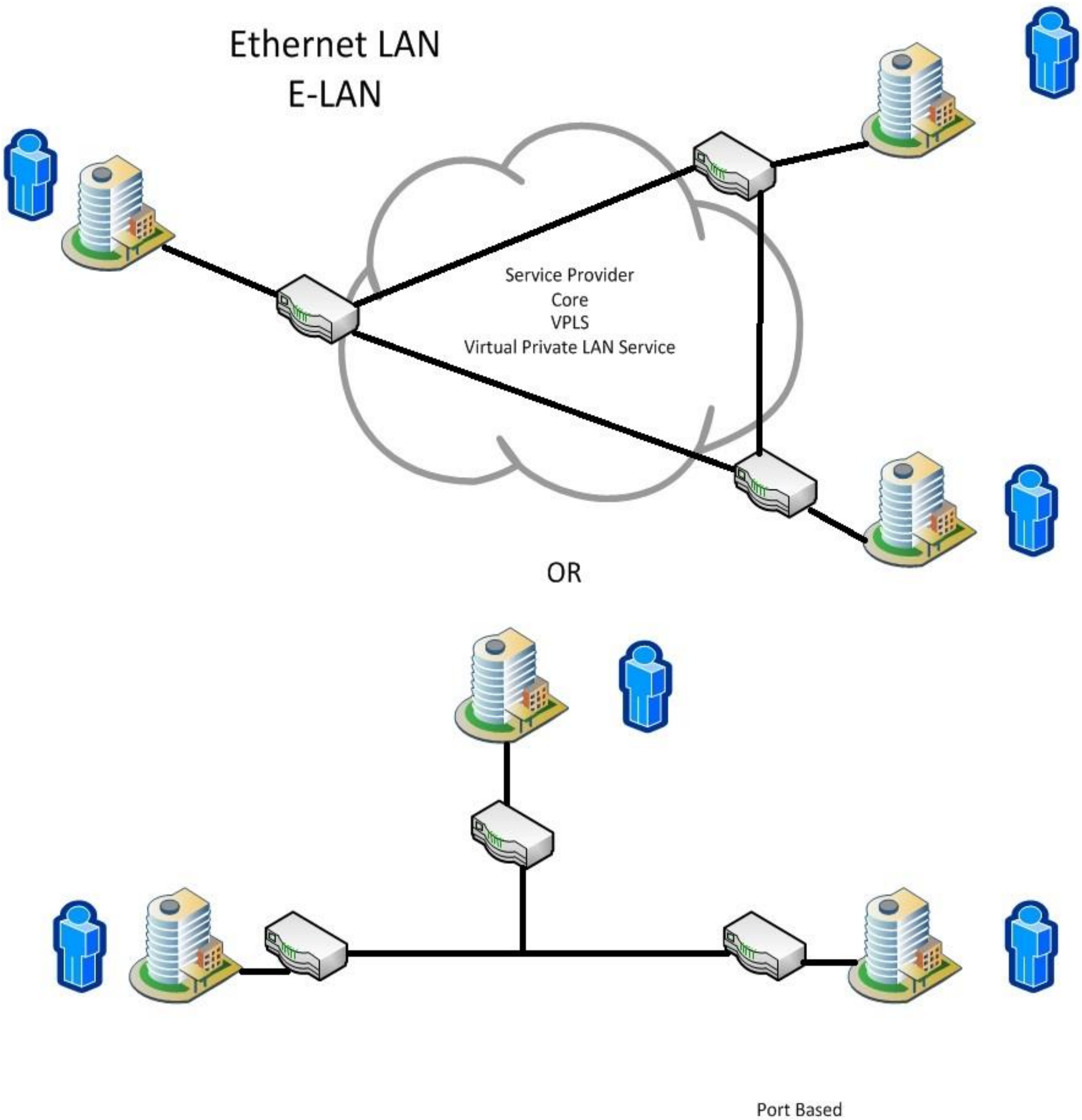
Ethernet Virtual Private Line is a VLAN based E-line service with different exemptions from Ethernet Private Line service. It is also configured as E-pipe on Alcatel routers. This type of service allows service multiplexing, each subscriber is mapped with different EVC (Ethernet Virtual Circuit) by VLAN IDs or TAGs on a common UNI then the service is EVPL which is Ethernet Virtual Private Line.



As shown in the figure above only one port is used to ingress two different subscribers, each is associated with different EVC Ethernet Virtual.

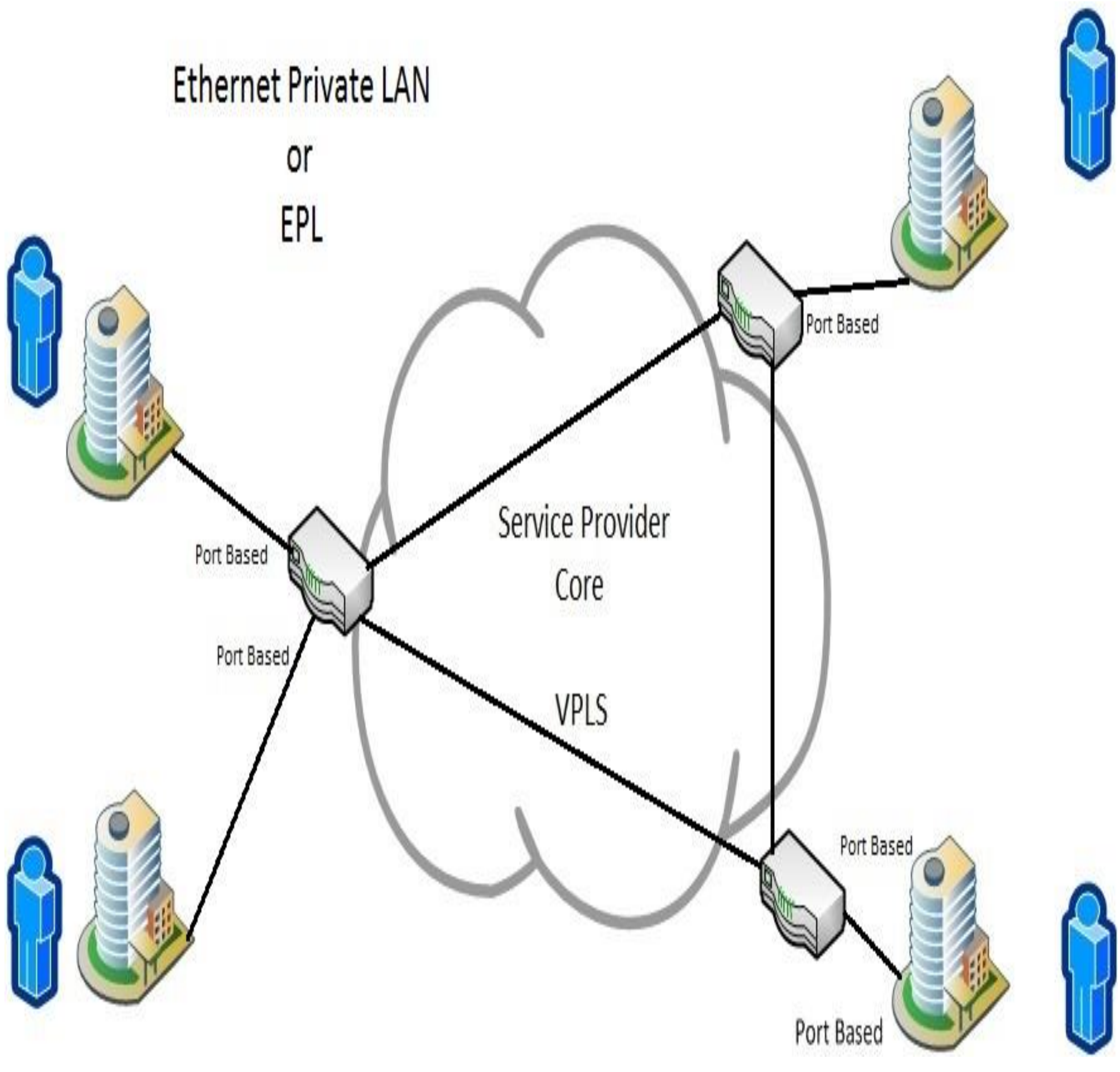
3.2 Ethernet LAN or E-Lan Service:

Ethernet LAN or E-LAN service is similar to a local LAN service, it is multipoint-to-multipoint service or in other word we can say any-to-any service. There are two different types of E-LAN services, port based and VLAN based. E-LAN is configured by enabling VPLS (Virtual Private LAN Service) over a service provider core network which learns MAC addresses and distributes Ethernet frames over a network.



3.2.1 Ethernet Private LAN:

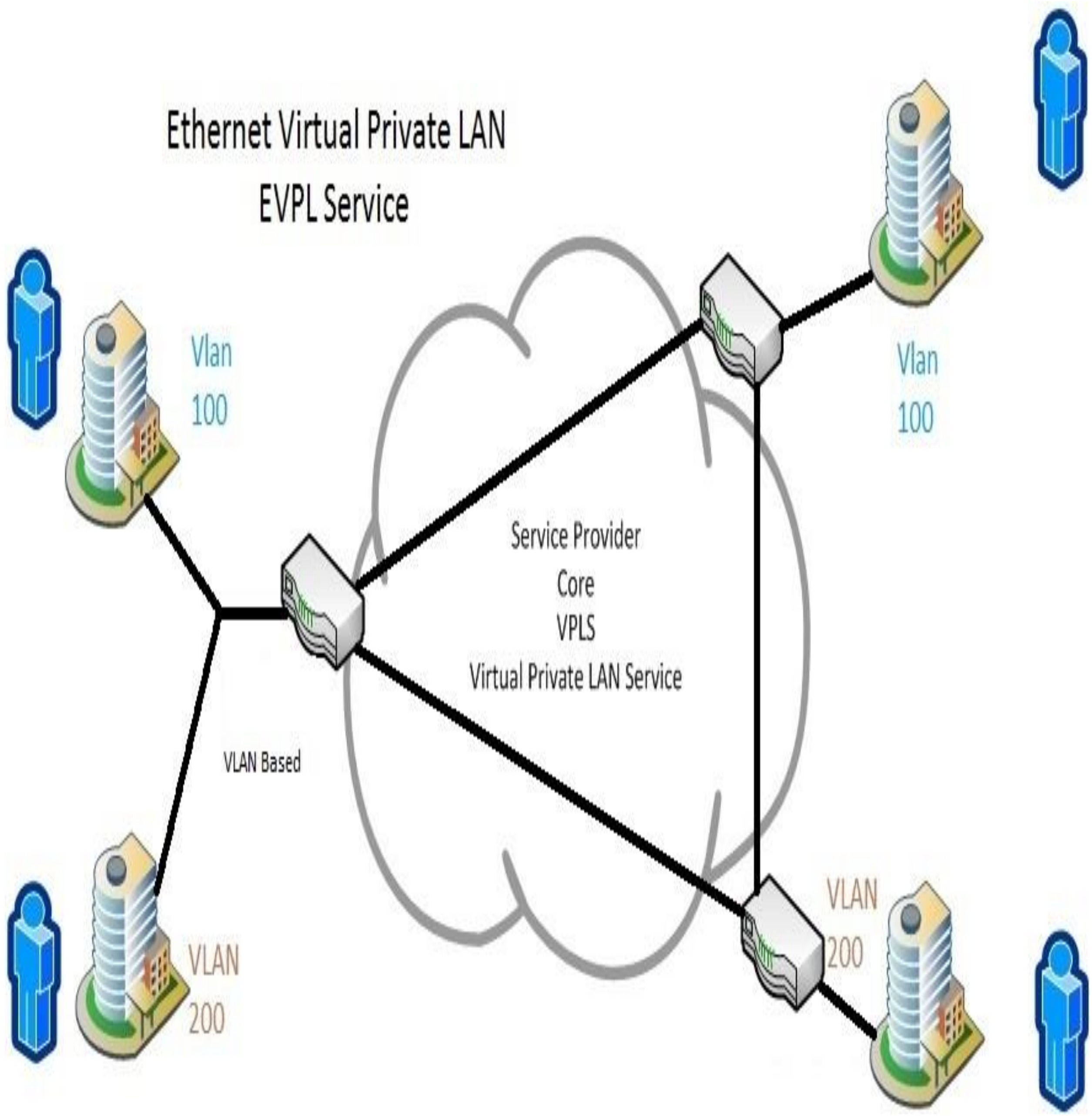
Ethernet Private LAN service is a port based E-LAN service. This type of service restricts service multiplexing by connecting each subscriber with independent port for ingress and the frames are Identical at each end with high transparency.



As figure illustrates that each subscriber has ingress port which is associated with its EVC.

3.2.2 Ethernet Virtual Private LAN:

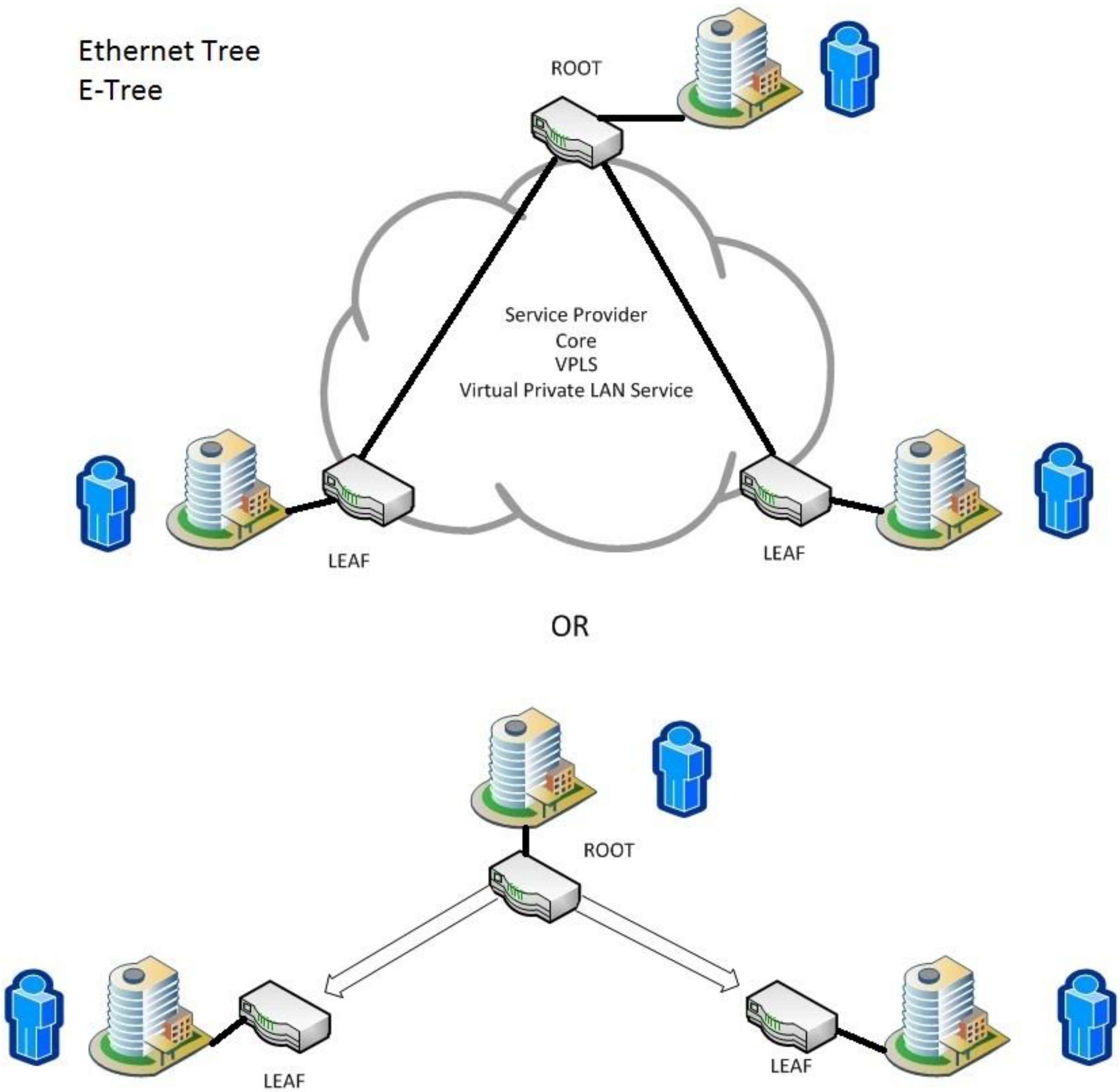
Ethernet Virtual Private LAN service is a VLAN based service. It allows the service providers for service multiplexing through which different subscribers can be mapped with their EVCs from a same UNI (Physical Port).



As figure illustrates different subscribers are ingress at same port.

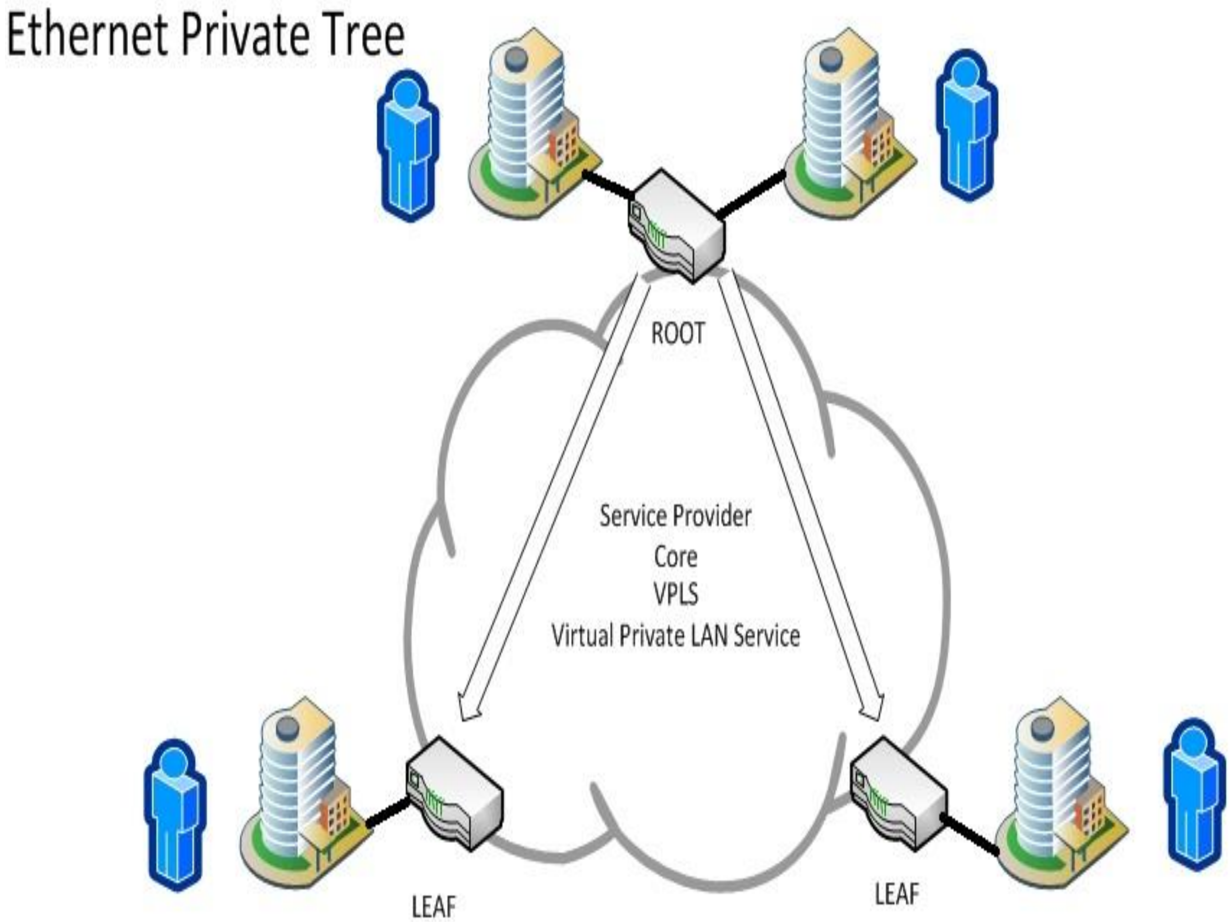
3.3 Ethernet Tree or E-Tree Service:

Ethernet Tree or E-Tree service is a point-to-multipoint or rooted multipoint service in which there are Leafs connected to a Root. In this type of service leafs can communicate with root but they cannot communicate with other leafs. It's is configured by enabling VPLS in such a way that traffic is directed from root to leaf.



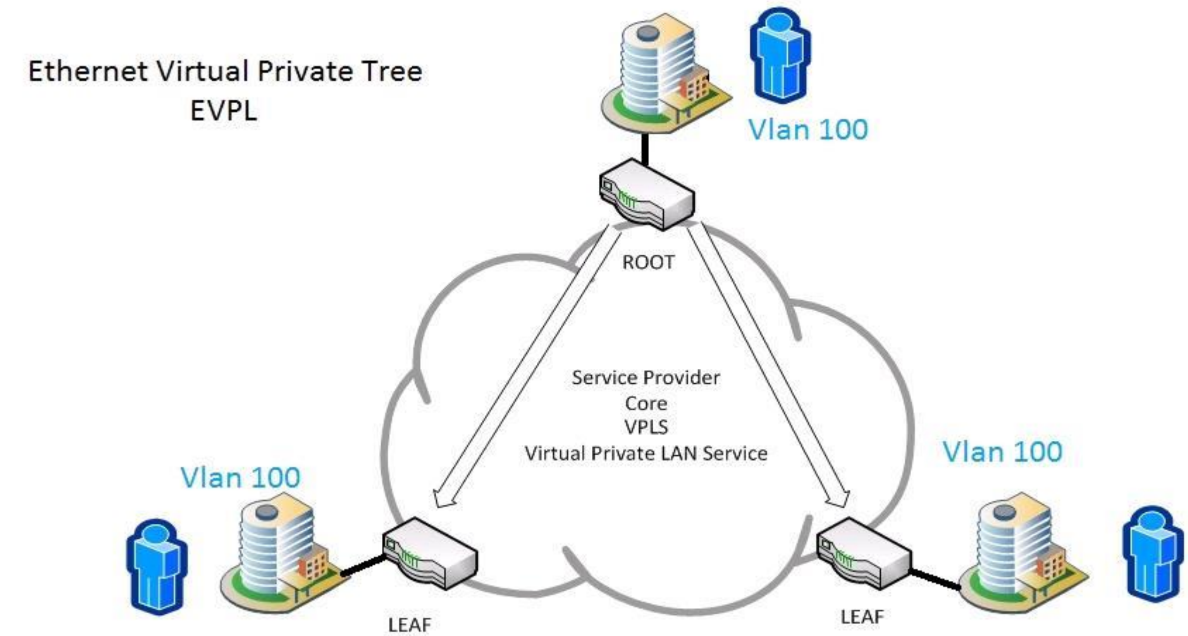
3.3.1 Ethernet Private Tree:

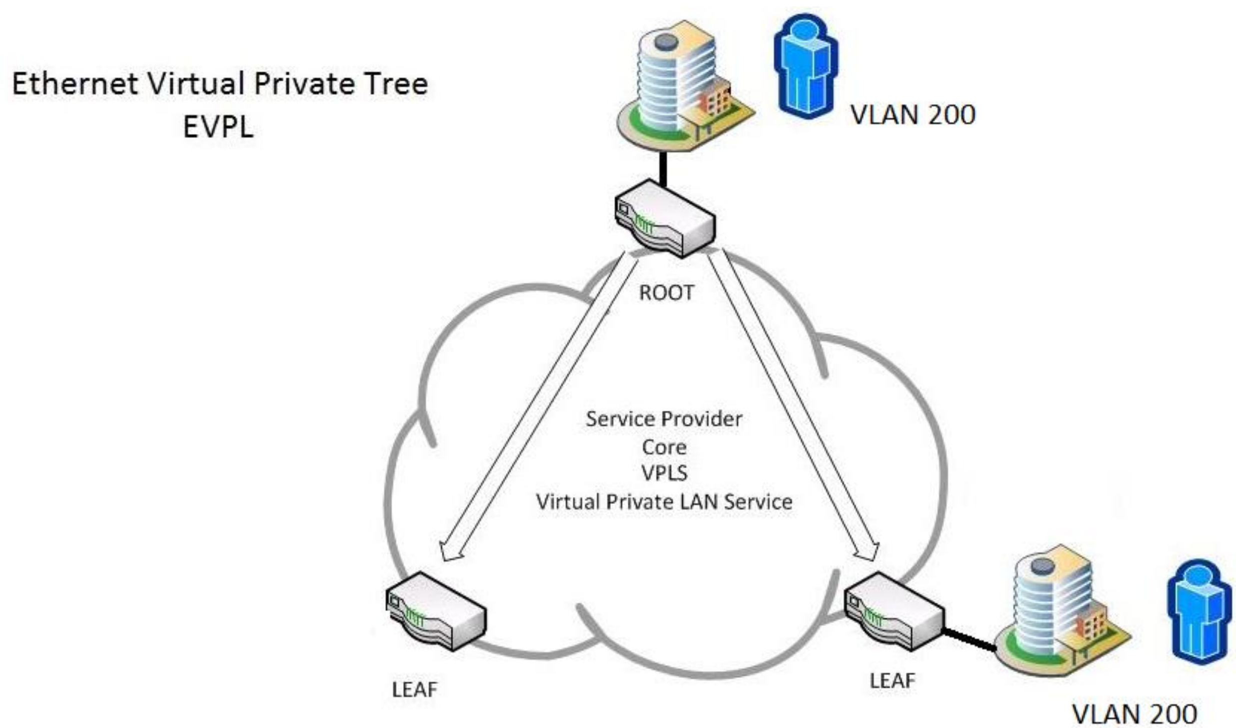
Ethernet Private Tree is a port based service which does not allows service multiplexing. Frames are highly transparent at both ends (Root & Leaf). A subscriber can configure different VLANs for different services or applications without notifying the service provider.



3.3.2 Ethernet Virtual Private Tree:

Ethernet Private Tree is a port based service in which access is a whole VLAN. Same port is associated with multiple EVCs , this is achieved by service multiplexing.





4 - MEF STANDARDS & REQUIREMENTS FOR ETHERNET SERVICES

4.1 INTRODUCTION:

Each service has its own specifications, minimum requirements and features which we have to ensure that it is rightly configured before utilization of each service. These specifications and requirements are set by MEF for each service.

This part of the report is taken from MEF Technical specifications document 6.1. This part shows the standards and requirements necessary to activate/configure each service and these standards and requirements are set by MEF for each service. So it is important to know the requirements and standards set by MEF before moving on to the services as it will ensure that the services configured are according to MEF.

Before going to the requirements we must understand some terms that are frequently used in requirements below. **(*All below terms and definitions are from MEF Technical Attributes document 6.1).***

UNI: User Network Interface.
EVC: Ethernet Virtual Connection.

MTU: Maximum Transmission Unit.

All to One Bundling: A UNI attribute in which all CE-VLAN IDs are associated with a single EVC.

Bandwidth profile per EVC: A bandwidth profile applied on a per-EVC basis.

Ingress Bandwidth Profile: A characterization of ingress Service Frame arrival times

and lengths at the ingress UNI and a specification of disposition of each Service Frame based on its level of compliance with the characterization.

Egress Bandwidth Profile: A service attribute that specifies the length and arrival time

characteristics of egress Service Frames at the egress UNI.

CE-VLAN ID / EVC Map: An association of CE-VLAN IDs with EVCs at a UNI.

CIR: Committed Information Rate. CIR is a Bandwidth Profile parameter. It defines the average rate in bits/s of Service Frames up to which the network delivers Service Frames and is committed to meeting the performance objectives defined by the CoS Service

Attribute.

CBS: Committed Burst Size is a Bandwidth Profile parameter. It limits the maximum number of bytes available for a burst of Service Frames sent at the UNI speed to remain CIR-conformant.

EIR: Excess Information Rate. EIR is a Bandwidth Profile parameter. It defines the average rate in bits/s of Service Frames up to which the network may deliver Service Frames but without any performance objectives.

CM: Color Mode.

Service Multiplexing: A UNI service attribute in which the UNI can be in more than one EVC instance.

Layer 2 Control Protocol Service Frame: A Service Frame that is used for Layer 2 control, e.g., Spanning Tree Protocol.

4.2 UNIs requirement for port based services:

Following tables illustrates the requirements at the UNIs for configuring each service.

UNI Service Attributes	Service Attribute Parameters Required For Each service		
	EP-LINE	**EP-LAN**	**EP-TREE**
UNI Identifier	Arbitrary text string to identify the UNI	Arbitrary text string to identify the UNI	Arbitrary text string to identify the UNI
Physical Medium	UNI Type 2 Physical Interface except for PON interfaces	UNI Type 2 Physical Interface except for PON interfaces	UNI Type 2 Physical Interface except for PON interfaces
Speed	10 Mbps, 100 Mbps, 10/100 Mbps Auto-negotiation, 10/100/1000 Mbps Auto-negotiation, 1 Gbps, or 10 Gbps	10 Mbps, 100 Mbps, 10/100 Mbps Auto-negotiation, 10/100/1000 Mbps Auto-negotiation, 1 Gbps, or 10 Gbps	10 Mbps, 100 Mbps, 10/100 Mbps Auto-negotiation, 10/100/1000 Mbps Auto-negotiation, 1 Gbps, or 10 Gbps
Mode	MUST be Full Duplex	MUST be Full Duplex	MUST be Full Duplex
MAC Layer	IEEE 802.3-2005	IEEE 802.3-2005	IEEE 802.3-2005
UNI MTU	MUST be ≥ 1522	MUST be ≥ 1522	MUST be ≥ 1522
Service Multiplexing	MUST be No	MUST be No	MUST be No
Bundling	MUST be No	MUST be No	MUST be No
All to one Bundling	MUST be Yes	MUST be Yes	MUST be Yes
CE-VLAN ID for untagged and priority tagged Service Frames	All untagged and priority tagged Service Frames at the UNI MUST map to the same EVC as is used for all other Service Frames	All untagged and priority tagged Service Frames at the UNI MUST map to the same EVC as is used for all other Service Frames	All untagged and priority tagged Service Frames at the UNI MUST map to the same EVC as is used for all other Service Frames
Maximum number	MUST be 1	MUST be 1	MUST be 1

of EVCs			
Ingress Bandwidth Profile Per UNI	MUST NOT specify	OPTIONAL. If supported, MUST specify <CIR, CBS, EIR, EBS, CM, CF>. MUST NOT be combined with any other type of ingress bandwidth profile.	OPTIONAL. If supported, MUST specify <CIR, CBS, EIR, EBS, CM, CF>. MUST NOT be combined with any other type of ingress bandwidth profile.
Egress Bandwidth Profile Per UNI	MUST NOT specify	OPTIONAL. If supported, MUST specify <CIR, CBS, EIR, EBS, CM, CF>. MUST NOT be combined with any other type of egress bandwidth profile	OPTIONAL. If supported, MUST specify <CIR, CBS, EIR, EBS, CM, CF>. MUST NOT be combined with any other type of egress bandwidth profile
Layer 2 Control Protocol Processing	MUST specify	MUST specify	MUST specify

(*All **ABOVE** standards in the table are taken from MEF Technical Specification document 6.1)*

4.3 UNIs requirement for VLAN based services:

Following tables illustrates the requirements at the UNIs for configuring each service.

UNI Service Attributes	Service Attribute Parameters Required For Each service		
	EVP-LINE	**EVP-LAN**	**EVP-TREE**
UNI Identifier	Arbitrary text string to identify the UNI	Arbitrary text string to identify the UNI	Arbitrary text string to identify the UNI
Physical Medium	UNI Type 2 Physical Interface except for PON interfaces	UNI Type 2 Physical Interface except for PON interfaces	UNI Type 2 Physical Interface except for PON interfaces
Speed	10 Mbps, 100 Mbps, 10/100 Mbps Auto-negotiation, 10/100/1000 Mbps Auto-negotiation, 1 Gbps, or 10 Gbps	10 Mbps, 100 Mbps, 10/100 Mbps Auto-negotiation, 10/100/1000 Mbps Auto-negotiation, 1 Gbps, or 10 Gbps	10 Mbps, 100 Mbps, 10/100 Mbps Auto-negotiation, 10/100/1000 Mbps Auto-negotiation, 1 Gbps, or 10 Gbps
Mode	MUST be Full Duplex	MUST be Full Duplex	MUST be Full Duplex
MAC Layer	IEEE 802.3-2005	IEEE 802.3-2005	IEEE 802.3-2005
UNI MTU	MUST be ≥ 1522	MUST be ≥ 1522	MUST be ≥ 1522
Service Multiplexing	SHOULD be supported at one or more UNIs	SHOULD be supported at one or more UNIs	SHOULD be supported at one or more UNIs
Bundling	Yes or No. If Yes, then CE-VLAN ID Preservation MUST be Yes.	Yes or No. If Yes, then CE-VLAN ID Preservation MUST be Yes.	Yes or No. If Yes, then CE-VLAN ID Preservation MUST be Yes.
All to one Bundling	MUST be No	MUST be No	MUST be No
CE-VLAN ID for untagged and priority tagged Service Frames	MUST specify CE-VLAN ID for untagged and priority tagged Service Frames in	MUST specify CE-VLAN ID for untagged and priority tagged Service Frames in	MUST specify CE-VLAN ID for untagged and priority tagged Service Frames in

	the range of 1-4094	the range of 1-4094	the range of 1-4094
Maximum number of EVCs	MUST be ≥ 1	MUST be ≥ 1	MUST be ≥ 1
Ingress Bandwidth Profile Per UNI	MUST NOT specify	OPTIONAL. If supported, MUST specify <CIR, CBS, EIR, EBS, CM, CF>. MUST NOT be combined with any other type of ingress bandwidth profile.	OPTIONAL. If supported, MUST specify <CIR, CBS, EIR, EBS, CM, CF>. MUST NOT be combined with any other type of ingress bandwidth profile.
Egress Bandwidth Profile Per UNI	MUST NOT specify	OPTIONAL. If supported, MUST specify <CIR, CBS, EIR, EBS, CM, CF>. MUST NOT be combined with any other type of egress bandwidth profile	OPTIONAL. If supported, MUST specify <CIR, CBS, EIR, EBS, CM, CF>. MUST NOT be combined with any other type of egress bandwidth profile
Layer 2 Control Protocol Processing	MUST specify	MUST specify	MUST specify

(*All* ***ABOVE*** *standards in the table are taken from MEF Technical Specification document 6.1)*

4.4 EVC requirement for port based services:

Following tables illustrates the requirements at the EVCs for configuring each service.

EVC Service Attribute	Service Attribute Parameters Required For Each service		
	EP-LINE	**EP-LAN**	**EP-TREE**
EVC Type	MUST be Point-to-Point	MUST be Multipoint-to-Multipoint	MUST be Rooted-Multipoint
EVC ID	An arbitrary string, unique across the MEN, for the EVC supporting the service instance	An arbitrary string, unique across the MEN, for the EVC supporting the service instance.	An arbitrary string, unique across the MEN, for the EVC supporting the service instance
UNI List	MUST list the two UNIs associated with the EVC. The UNI type MUST be Root for each UNI.	MUST list the UNIs associated with the EVC. The UNI type MUST be Root for each UNI.	MUST list the UNIs associated with the EVC. The UNI Type for at least 1 UNI MUST be Root. All UNIs that are not UNI Type Root MUST be UNI Type Leaf
Maximum Number of UNIs	MUST be 2	MUST be ≥ 2	MUST be ≥ 2
EVC MTU size	MUST be ≥ 1522	MUST be ≥ 1522.	MUST be ≥ 1522.
CE-VLAN ID Preservation	MUST be Yes	MUST be Yes	MUST be Yes
CE-VLAN CoS Preservation	MUST be Yes	MUST be Yes	MUST be Yes
Unicast Service Frame Delivery	MUST Deliver Unconditionally	Deliver Unconditionally or Deliver Conditionally. If Delivered	Deliver Unconditionally or Deliver Conditionally. If Delivered

		Conditionally, MUST specify the delivery criteria.	Conditionally, MUST specify the delivery criteria.
Multicast Service Frame Delivery	MUST Deliver Unconditionally	Deliver Unconditionally or Deliver Conditionally. If Delivered Conditionally, MUST specify the delivery criteria.	Deliver Unconditionally or Deliver Conditionally. If Delivered Conditionally, MUST specify the delivery criteria.
Broadcast Service Frame Delivery	MUST Deliver Unconditionally	Deliver Unconditionally or Deliver Conditionally. If Delivered Conditionally, MUST specify the delivery criteria.	Deliver Unconditionally or Deliver Conditionally. If Delivered Conditionally, MUST specify the delivery criteria.
Layer 2 Control Protocols Processing (only applies for L2CPs passed to the EVC)	MUST specify	MUST specify	MUST specify

(*All **ABOVE** standards in the table are taken from MEF Technical Specification document 6.1)*

4.5 EVC requirement for VLAN based services:

Following tables illustrates the requirements at the EVCs for configuring each service.

EVC Service Attribute	Service Attribute Parameters Required For Each service		
	EVP-LINE	**EVP-LAN**	**EVP-TREE**
EVC Type	MUST be Point-to-Point	MUST be Multipoint-to-Multipoint	MUST be Rooted-Multipoint
EVC ID	An arbitrary string, unique across the MEN, for the EVC supporting the service instance	An arbitrary string, unique across the MEN, for the EVC supporting the service instance	An arbitrary string, unique across the MEN, for the EVC supporting the service instance.
UNI List	MUST list the two UNIs associated with the EVC. The UNI type MUST be Root for each UNI.	MUST list the UNIs associated with the EVC. The UNI type MUST be Root for each UNI.	MUST list the UNIs associated with the EVC. The UNI Type for at least 1 UNI MUST be Root. All UNIs that are not UNI Type Root MUST be UNI Type Leaf.
Maximum Number of UNIs	MUST be 2	MUST be ≥ 2	MUST be ≥ 2
EVC MTU size	MUST be ≥ 1522	MUST be ≥ 1522	MUST be ≥ 1522
CE-VLAN ID Preservation	MUST be either Yes or No	MUST be either Yes or No	MUST be either Yes or No
CE-VLAN CoS Preservation	MUST be either Yes or No	MUST be either Yes or No	MUST be either Yes or No
Unicast Service Frame Delivery	Deliver Unconditionally or Deliver conditionally. If Delivered Conditionally, MUST	Deliver Unconditionally or Deliver conditionally. If Delivered Conditionally, MUST	Deliver Unconditionally or Deliver Conditionally. If Delivered Conditionally, MUST

	specify the delivery criteria.	specify the delivery criteria.	specify the delivery criteria.
Multicast Service Frame Delivery	Deliver Unconditionally or Deliver conditionally. If Delivered Conditionally, MUST specify the delivery criteria.	Deliver Unconditionally or Deliver conditionally. If Delivered Conditionally, MUST specify the delivery criteria.	Deliver Unconditionally or Deliver Conditionally. If Delivered Conditionally, MUST specify the delivery criteria.
Broadcast Service Frame Delivery	Deliver Unconditionally or Deliver conditionally. If Delivered Conditionally, MUST specify the delivery criteria.	Deliver Unconditionally or Deliver conditionally. If Delivered Conditionally, MUST specify the delivery criteria.	Deliver Unconditionally or Deliver conditionally. If Delivered Conditionally, MUST specify the delivery criteria.
Layer 2 Control Protocols Processing (only applies for L2CPs passed to the EVC)	MUST specify	MUST specify	MUST specify

(*All **ABOVE** standards in the table are taken from MEF Technical Specification document 6.1)*

(NOTE: Complete above section/chapter is taken from MEF Technical Specifications Document 6.1)

5 - LAB DEMO DETAILS & RESULTS

5.1 Implementation:

At the very first step the topology for test bed was decided that consisted of three routers and was a triangular topology which changed according to the need of services.

Following was configured in this part of report:
1) Interfaces

2) IGP – ISIS

3) MPLS
4) E-Pipe (E-Line)
i) EPL

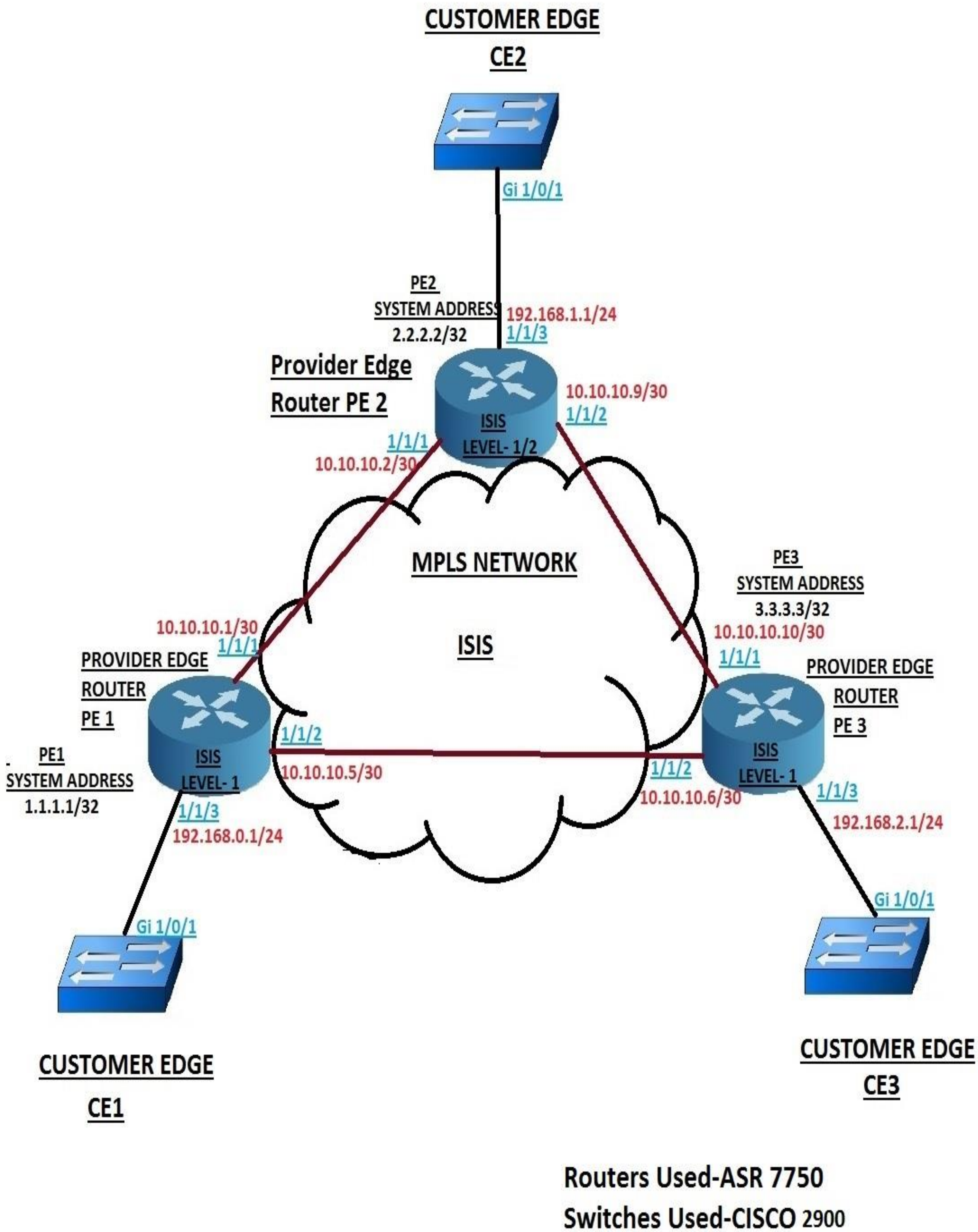
ii) EVPL

5)VPLS (E-Lan)
i) EPL

ii) EVPL

6) VPLS with traffic direct towards root to leaf (E-Tree)
i) EPT

ii) EVPT


CUSTOMER EDGE
CE2
Gi 1/0/1
PE2
SYSTEM ADDRESS
2.2.2.2/32
192.168.1.1/24
1/1/3
Provider Edge
Router PE 2
10.10.10.9/30
1/1/2
1/1/1
10.10.10.2/30
ISIS
LEVEL- 1/2
MPLS NETWORK
ISIS
PE3
SYSTEM ADDRESS
3.3.3.3/32
10.10.10.10/30
1/1/1
PROVIDER EDGE
ROUTER
PE 3
10.10.10.1/30
1/1/1
PROVIDER EDGE
ROUTER
PE 1
PE1
SYSTEM ADDRESS
1.1.1.1/32
ISIS
LEVEL- 1
1/1/2
10.10.10.5/30
1/1/2
10.10.10.6/30
ISIS
LEVEL- 1
1/1/3
192.168.2.1/24
1/1/3
192.168.0.1/24
Gi 1/0/1
Gi 1/0/1
CUSTOMER EDGE
CE1
CUSTOMER EDGE
CE3
Routers Used-ASR 7750
Switches Used-CISCO 2900

Initial configuration was done according to the following figure. Topology may slightly vary for Ethernet services.

5.2 Network Topology

- At the very first step the above topology was decided on which Ethernet Services were to be deployed.
- A triangular topology was considered in general as it is the best topology for the Ethernet services and for MPLS to work at the same time.
- Why ? – Because all the services are logically either point-to-point or multipoint-to-multipoint or rooted multipoint so it was reasonable for all three service and familiar topology makes it easier for the reader to understand the services.

5.3 Equipment used:

We configured a test bed for each service and we used the following equipment to configure and test each service.

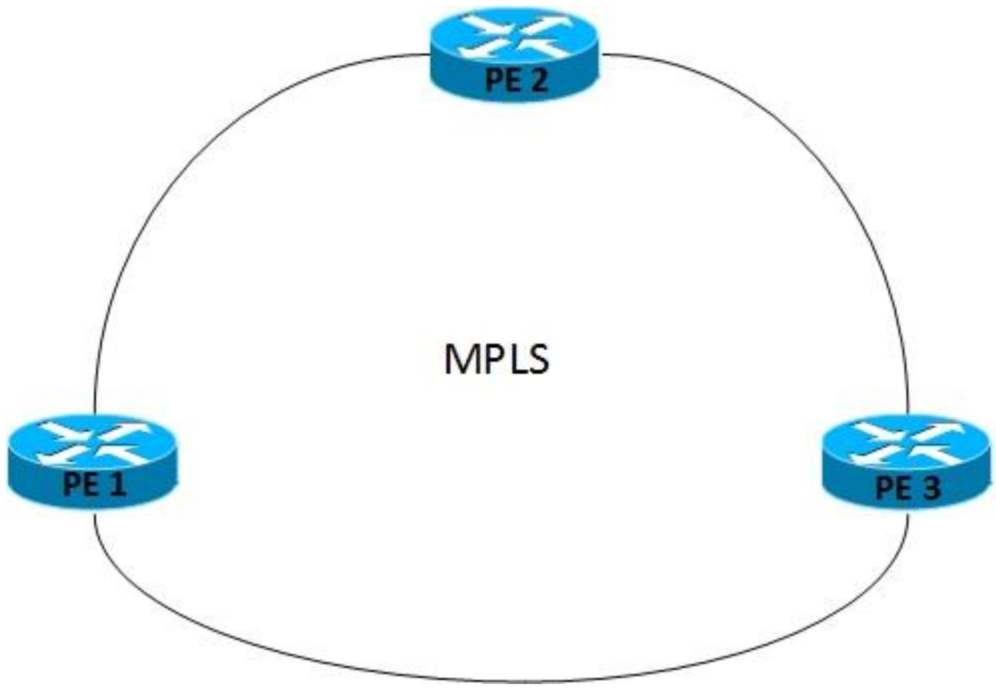
- Routers – ALU 7750
  (For MPLS Core)
- Switches - Cisco 2900
  (For End Customers Devices)
- Connectivity – Ethernet Cables with RJ-45 Connectors

Alcatel 7750 were used as part of core routers and Cisco 2900 was used as a C-PE (Customer-Provider Edge) device. The Alcatel equipment used is MEF certified.

5.4 Configuration:

- MPLS – Multi Protocol Label Switching
- E-Pipe – ELINE
  ii) EPL
  ii)EVPL
- VPLS – ELAN
  i)EPL
  ii)EVPL
- VPLS Traffic from Root to Leaf – ETREE
  i)EPT
  ii)EVPT

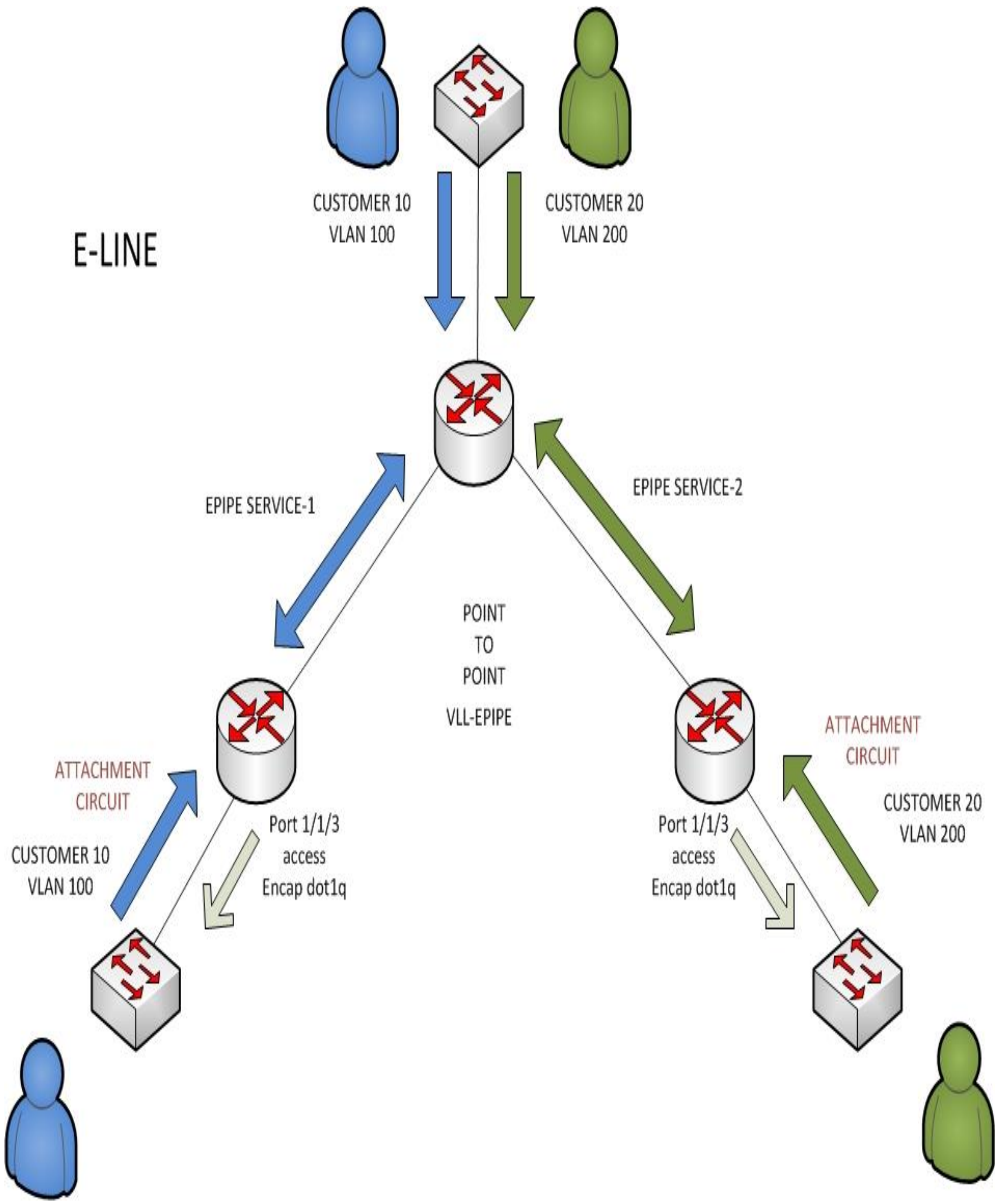
5.4.1 MPLS



- Configure IGP before MPLS.
- When configuring MPLS make sure the IGP is working.
- Check the end to end connectivity on the core.
- Now proceed with MPLS.
- Enable LDP for MPLS.
- Now check LDP bindings and MPLS status.
- Check the end to end connectivity.

5.4.2 E-Line (E-Pipe) configurations on Core

LOGICAL FLOW DIAGRAM



(a) E-LINE – (Epipe)

- MPLS is a pre-requirement for this service in this project.
- SDP should be configured with far end settings for each EVC.
- If MPLS and SDP are configured correctly then proceed with E-Pipe.
- SDP is used for L2 VPNs in ePipe therefore TLDP signaling must be enabled.
- Customers should be configured for e-pipe.
- Now start configuring E-pipe for respective customer.
- Configure/create spoke-sdp for EVC in e-pipe.
- Configure/create sap port for the port going to the C-PE.
- As MEF requirements change the MTU size

(b) Ethernet Private Line – EPL (E-Pipe)

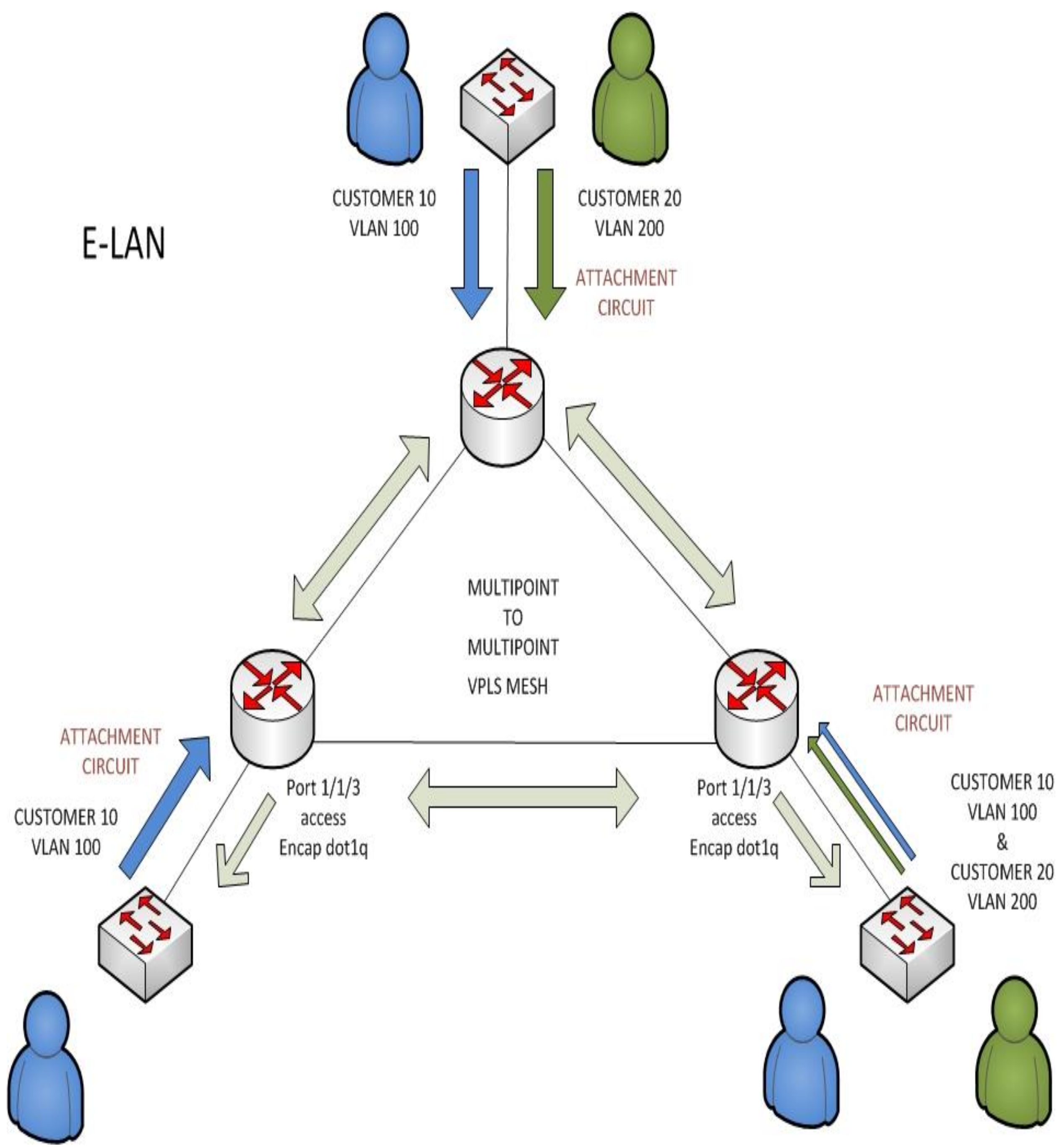
- The Ingress port going to the C-PE should be access.
- And same should be done on the C-PE.
- Each C-PE device should be connected on independent port.

(c) Ethernet Virtual Private Line – EVPL (E-Pipe)

- In E-pipe sap port should be matched to the VLAN tag used for that particular customer and the service provider VLAN tag if QinQ encapsulation is used.
- The Ingress port going to the C-PE should be trunk with encapsulation of dot1q or QinQ as per requirement of the SP.
- And same should be done on the C-PE.

5.4.3 E-Lan (VPLS) configurations on Core

LOGICAL FLOW DIAGRAM



(a) E-LINE – (VPLS)

- MPLS is a pre-requirement for this service in this project.
- SDP should be configured with far end settings for each EVC.
- SDP is used for L2 VPNs in VPLS therefore TLDP signaling must be enabled.
- If MPLS and SDP are configured correctly then proceed with VPLS.
- Customers should be configured for VPLS.
- Now start configuring VPLS for respective customer.
- Configure/create mesh-sdp for EVC in VPLS.
- Configure/create sap port for the port going to the C-PE.
- As MEF requirements change the MTU size by minimum 1522 or greater.

(b) Ethernet Private Lan – EPL (VPLS)

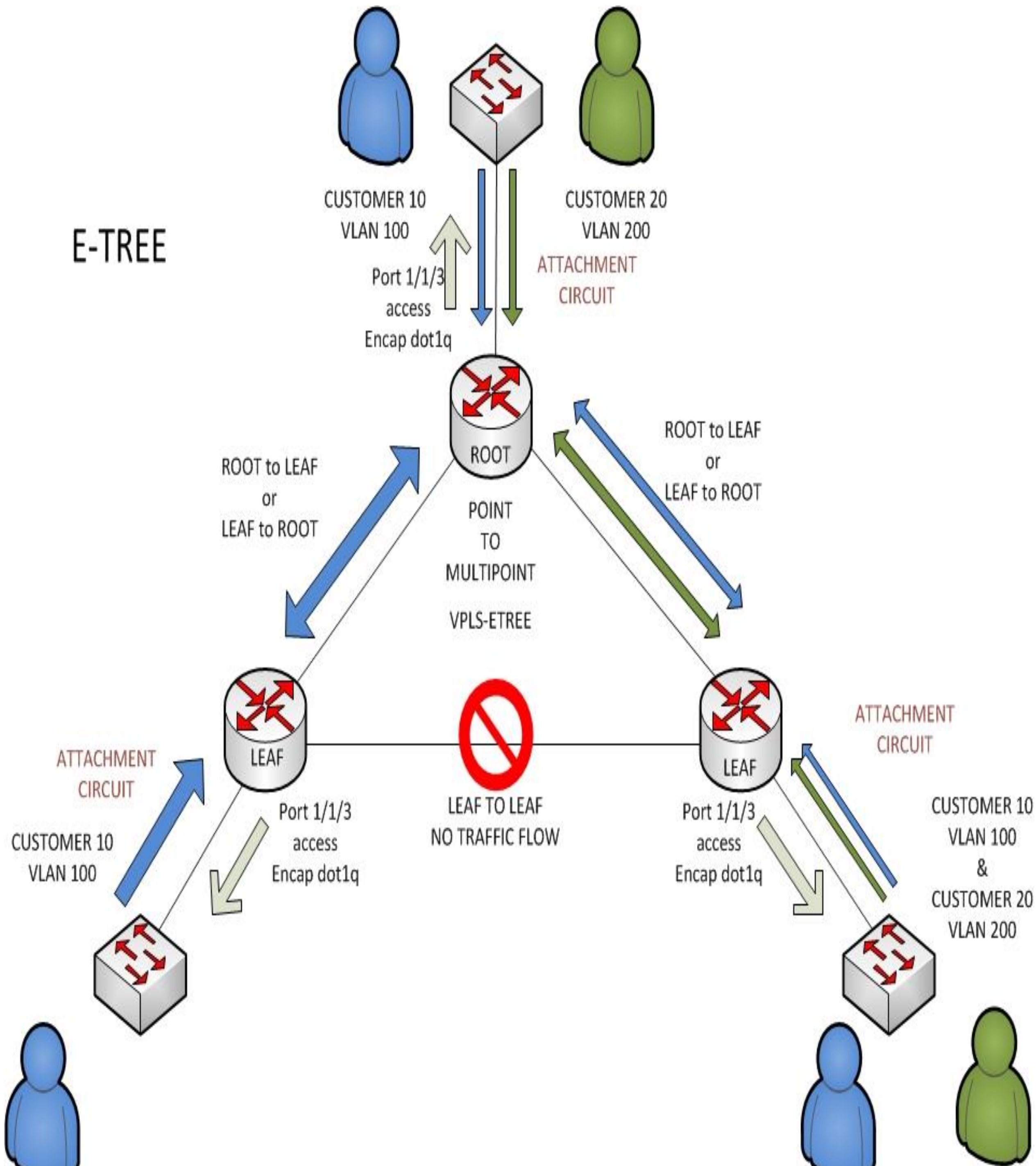
- The Ingress port going to the C-PE should be access.
- And same should be done on the C-PE.
- Each C-PE device should be connected on independent port.

(c) Ethernet Virtual Private Lan – EVPL (VPLS)

- In E-pipe sap port should be matched to the VLAN tag used for that particular customer and the service provider VLAN tag if QinQ encapsulation is used.
- The Ingress port going to the C-PE should be trunk with encapsulation of dot1q or QinQ as per requirement of the SP.
- And same should be done on the C-PE.

5.4.4 E-TREE (VPLS- Root to Leaf Flow) configurations on Core

LOGICAL FLOW DIAGRAM



(a) E-Tree – (VPLS Traffic directed from root to leaf)

- MPLS is a pre-requirement for this service in this project.
- SDP should be configured with far end settings for each EVC.
- SDP is used for L2 VPNs in VPLS therefore TLDP signaling must be enabled.
- If MPLS and SDP are configured correctly then proceed with VPLS.
- Customers should be configured for VPLS.
- Now start configuring VPLS for respective customer.
- Configure/create spoke-sdp for EVC in VPLS only directed towards root to leaf, no leaf to leaf is required.
- Each customer should be configured with split-horizon group.
- Configure/create sap port for the port going to the C-PE.
- As MEF requirements change the MTU size by minimum 1522 or greater.

(b) Ethernet Private Tree – EPT (VPLS – Root to Leaf flow)

- The Ingress port going to the C-PE should be access.
- And same should be done on the C-PE.

(c) Ethernet Virtual Private Tree – EVPT (VPLS – Root to Leaf flow)

In E-pipe sap port should be matched to the VLAN tag used for that particular customer and the service provider VLAN tag if QinQ encapsulation is used.

- The Ingress port going to the C-PE should be trunk with encapsulation of dot1q or QinQ as per requirement of the SP.
- And same should be done on the C-PE.

5.5 RESULTS

After configuring these services it is necessary to check each service with the MEF standards as the purpose of this project is to implement these services over MPLS network for a service provider under the guidance of MEF standards.

Checks	EPL	EVPL	EPLAN	EVPLAN	EPT	EVPT
ISIS	✓	✓	✓	✓	✓	✓
MPLS Status	UP	UP	UP	UP	UP	UP
LDP	UP	UP	UP	UP	UP	UP
VPLS Status	----		UP	UP	UP	UP
Service Status	UP	UP	UP	UP	UP	UP
MTU Size	>1522	>1522	>1522	>1522	>1522	>1522
End to End Conectivity	Success	Success	Success	Success	Success	Success
End to End Connectivity with df bit enabled	Success	Success	Success	Success	Success	Success
Leaf to Leaf communication	_____				No	No

5.5.1 MTU Size:

As minimum MTU size required for each service is 1522 which could pass without fragmenting the packet. We can set the MTU size to match the minimum requirement. VLAN tag for customers is included in 1522 but if a service provider requires to add its own VLAN tag by configuring QinQ then we have to add 32 more bytes so that the packet can be forwarded without fragmentation.

It was tested end to end ping with –df bit (do not fragment).

5.5.2 Bandwidth:

In practical scenarios, bandwidth for a particular customer is defined at a C-PE which is the end device of service provider.

5.5.3 Layer 2 Control Protocol Compliance Test Results Summary

I performed some tests for Layer 2 protocols to find out the characteristics of each service and how it responds to these protocols.
✓ **-** Represents that the PDU for that protocols were going through end to end.
X - Represents that the PDU for that protocols were NOT going through end to end.

PROTOCOL	EP-LINE	EVP-LINE	EP-LAN	EVP-LAN	EP-TREE	EVP-TREE
LACP	✓	✓	X	X	X	X
STP	✓	✓	✓	✓	✓	✓
MSTP	✓	✓	✓	✓	✓	✓
RSTP	✓	✓	✓	✓	✓	✓
MAC Leaning	✓	✓	✓	✓	✓	✓

LACP:

LACP didn't go through in any of the service other than E-Line because it is strictly a point-to-point protocol.

5.5.4 ETHERNET OAM

(a) 802.3ah - Link Layer OAM

This is specifically designed for single hop links. Its can work within a 1 mile range. In practical scenarios this is used in between Provider Edge and Customer Edge. It is strictly between a link and do not work beyond one link neither the OAM messages go beyond one link for this.

Following are its main parameters:

Discovery: It is basically the discovery of the C-PE.

Remote Failure Indication: This is used to inform the service provider that there is some sort of power outage or failure is detected in C-PE.

Fault Isolation: This locates the fault that where that fault is in Service Provider or Customer.
Port - Level Loopback: This checks traffic transmission performance.

Performance & Status Monitoring: This is very basic performance and monitoring with the capability of alarm support.

(b) 802.1ag / Y.1731 - Connectivity Fault Management

There are four main parameters for connectivity fault management each of them help is tracing or notifying the fault.

Fault Detection

The purpose of Fault Detection is to detect the service fault or failure within the network and it is achieved by Continuity Check Messages (CCM). Continuity Check Messages are sent periodically across the network by the source of the service and if the reply is not received within the timeout time then an alarm is created by both end points of the network.

Fault Verification

This parameter is used in verifying the fault. It is defined as unicast in 802.1ag and as multicast in Y.1731. This is achieved by send loopback messages to a device or the end point. This Fault Verification is very much similar to ping. A loopback message is sent and a reply is awaited if reply is received then the path till which the loopback message was sent is fault free but if the reply is not received then it means there is some kind of fault or service failure. This can also help in identifying the location of the fault if we send loopback messages device by device till the end point. But link trace is more efficient way of tracing the fault.

Fault Isolation

Fault isolation is used to detect the location of the fault. And this is achieved by sending Link Trace Messages (LTM). Link trace message works as it is send from one end point to the other and all the devices in between will reply accordingly for the link trace message and their reply is called Link Trace Response (LTR). And if the reply is not received then it means the fault is in between that device.

Fault Notification

Fault Notification is only defined in Y.1731 because this uses Alarm Indication Signals (AIS) which are not used in 802.3ah because of the RSTP and ring protection. AIS is send only to the endpoints from C-PE which tells which services are currently affected and to keep fail state these messages are transmitted periodically until fail state is changed.

(c) Y.1731 – Performance Monitoring

Y.1731 also supports performance monitoring in Ethernet OAM. It does it by following ways.

Frame Loss Ratio

Frame loss ratios are determined by Continuity Check Messages which are sent from service source to service endpoint. Frame loss ratio is calculated by having counter service senders and service receivers these are transmit and receive counters. Number of packets received vs number of packets drops determines the ratio.

Frame Delay - FD / Frame Delay Variation - FDV

One Way trip:

A Delay Measurement Test packet is sent from the service source to the service end point with a time stamp and Service source and service end point have synchronized clocks which helps in calculating latency whereas the delay variation the time difference between sent time and received time.

Round Trip:

A Delay Measurement Message DMM is sent from the service source to the service end point with a time stamp and a Delay Measurement Response DMR is sent back from the end point to the source with the time stamp of the source. When the source receives that message it calculates the delay by calculating the transmission time and receive time.

6 - CURRENT DEVELOPMENTS IN CARRIER ETHERNET AND ITS FUTURE

6.1 Current Developments:

The whole world of technology is developing itself in a very fast way across the globe. Along with it Ethernet is one of the most commonly and widely used technology throughout the globe. This is one of the main reasons for its quick advancements and Ethernet services are the one the main sign of Ethernet advancements.

In this report we discuss three Ethernet services which are part of Career Ethernet 2.0 as per MEF. But there is one more service which came with Carrier Ethernet 2.0 that is Ethernet Access.

Ethernet Access fulfills the requirement for everyday use of the small to medium wholesale business. As today each customer require the service provider to carry its Voice, Data, Video and iP VPN traffic with reliability and scalability. So this requirement is easily fulfilled by Ethernet Access.

Ethernet Access EPL service interconnects a dedicated UNI and an ENNI whereas Ethernet Access EVPL service uses a UNI that can support multiple service instances.

The

Latest development in Ethernet services is E-VPN or also known as BGP MPLS based Ethernet VPN. This is a great service that gives many advantages over MPLS. it's an alternate to VPLS. In this service MAC address learning is achieved with BGP over MPLS core and this is done in control plane. This service provides high scalability and virtualization in networks. This service uses Ethernet Tags along with labels used to identify broadcast domains. Ethernet tags are much similar to VLAN tags.

When compared to VPLS, This service provides the service provider with many advantages such as load balancing, Fast convergence from active failures, Multi homing, Policy based forwarding/distributions, Getting rid of flooding issues and Control plane based learning.

6.2 Future Work:

Carrier Ethernet 2.0 came into reality in year 2012 and since then there have been many advancements to make these services simpler, efficient, faster, reliable and easy to monitor but even today these services are not mature enough to meet the current user or service provider requirements and the development work is still on going to improve and achieve the goals for service providers and their subscribers.

Currently the major challenge is MAC address limitations and scaling, As MPLS networks collapse boundaries between two Layer2 network or is used to bridge layer2 networks so MAC limitations are inherited from layer 2. In other words a legacy layer2 network on different locations is bridged with MPLS which contains many devices and on the other hand the service provider router has MAC limitations plus this type of network extend the broadcast domain and loop prevention is also a problem. These problems restrict the network in scaling.

The other challenge is the automated management in the services along with dynamic provisioning for cloud services as today the era for cloud services is in play.

There is also on going work to make the characteristics of Ethernet services more flexible and responsive as it is highly necessary for these services to be flexible by not being hardware or vendor dependent so that these services can work with every service provider in any scenario and hardware.

SUMMARY

Alright, we’re finally concluding this project. In this project we learnt, several important technologies such as, MPLS, Carrier Ethernet and its services and their implementation for service providers.

We started from understanding MPLS and investigated its layer 2 services. Afterwards we studied and understood the Ethernet Services and their standards set by MEF and IETF. We actually learnt the mechanism and requirement for both MPLS and Ethernet Services.

Subsequently we moved on to the Implementation of MPLS followed by the deployment of Ethernet services. After Implementation, each service was tested under MEF requirements and tested for Layer2 Control Protocol compliance as well.

Lastly, a thorough research for OAM was conducted and is presented in this document for respective readers to better understand and make them more familiar with tools and techniques used for monitoring and maintaining a network.

References

Books:

MPLS-Enabled Applications **by** Ina Minei, Julian Lucek

MPLS and VPN Architectures, Volume II **by** Jim Guichard, Ivan Pepelnjak, Jeff Apcar
Layer 2 VPN Architectures **by** Wei Luo Carlos, Pignataro, Dmitry , A Chan

Networks and Services Carrier Ethernet, PBT, MPLS-TP and VPLS **by** Mehmet Toy

[1]MEF Documents:

MEF Technical Specifications:

Doc 6.1

Doc 6.1.1

Doc 10

Doc 10.1

Doc 10.2

Doc 6.1

Doc 6.1

Other Docs:

7750 SR OS Services Guide Alcatel

7750 SR OS MPLS Guide Alcatel

BGP MPLS Based Ethernet VPN-draft-ietf-l2vpn-evpn-06

VPLS Technical Tutorial Alcatel

RFCs:

RFC 4379

RFC 4364

RFC 4664

RFC 4762

RFC 3985

RFC 4447

RFC 4448

Web Links:

- https://infoproducts.alcatel-lucent.com/html/0_add-h-f/93-0076-HTML/7750_SR_OS_Services_Guide/services_VLL-Intro.html#2029682
- https://infoproducts.alcatel-lucent.com/html/0_add-h-f/93-0076-HTML/7750_SR_OS_Services_Guide/services_VLL.html#3070232
- http://metroethernetforum.org/carrier-ethernet/carrier-ethernet-services
- http://metroethernetforum.org/Assets/CE2.0/MEF_New_Generation_of_Carrier_Ethernet_-_Overview_2012-01-23.pdf
- http://www.cisco.com/en/US/products/ps6648/products_ios_protocol_option_home.html
- http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6557/ps6603/ps6646/prod_white_paper09186a00800a8442.html
- http://metroethernetforum.org/carrier-ethernet/technical-specifications
- http://metroethernetforum.org/
- www.fplfibernet.com
- www.wikkipedia.com
- http://metroethernetforum.org/Assets/CE2.0/Business_Case_for_CE2-0_2012-02-23.pdf
- http://www.fujitsu.com/downloads/TEL/fnc/whitepapers/EthernetService-OAM.pdf
- http://searchnetworking.techtarget.com/definition/pseudowire
- http://www.cisco.com/c/en/us/td/docs/ios/12_0s/feature/guide/vpls_qos.html#wp1039077
- metroethernetforum.org

Research Papers:

- Evolution of Carrier Ethernet – Technology

  Ashwin Gumaste, Naresh Reddy, Deepak Kataria, Nasir Ghani
- MEF E-Tree Service Over MPLS

  Simon Delord, Frederic Jounay, Raymond Key
- Supporting Ethernet Transport Services

  Written by Enrique Hernandez-Valencia

Videos:

CBT – Nuggets CCNA Training

CBT – Nuggets CCNP Training

Ethernet OAM by Accedian Networks