Carrier Ethernet Technologies

Table of Contents

List of Figures

List of Tables

Executive Summary

Carriers are deploying Ethernet in metro and core networks. Carrier Ethernet have been developed from Ethernet for LAN with alterations to enable its use in MAN and WAN environments. The Ethernet standard has grown to include new technologies as computer networking has far developed and there is growing demand of high-bandwidth applications at increasingly lower costs.

Carrier Ethernet technology can be implemented over many different types of transport network technologies to support both existing and emerging services. There are multiple solutions that can be used to deliver Carrier Ethernet over Service Provider networks, each with its own specific standard and goal, and accordingly, different in how the Carrier Ethernet solution is offered.

The information has been accumulated from different resources publicly available, that includes documents and drafts from IETF, RFCs, MEF, IEEE and ITU-T.

Carrier Ethernet technologies discussed in this report are:

1. **Ethernet over Internet Protocol/Multi-protocol Label switching(EoMPLS)**
   Ethernet over IP/MPLS is a mechanism that allows an Internet Service Provider to transport Layer 2 Ethernet frames over provider's backbone network; here Ethernet packets are encapsulated inside IP/MPLS packets. EoMPLS service enables customers to improve their bandwidth costs against usage ratio by constructing out a virtual infrastructure between their points of presence. This report covers description of three services VPWS, VPLS and VPMS, improvements in OAM functionality and Traffic protection and restoration.

2. **Multiprotocol Label Switching Transport Profile (MPLS-TP)**
   MPLS-TP is a profile of MPLS protocols that are being defined in IETF. It is designed for use as a network layer technology in transport networks. It offers existing MPLS implementation, by removing some functions such as Equal Cost Multi Path (ECMP) and Penultimate Hop Popping (PHP) that are not relevant to connection-oriented applications. Also, it is based on existing MPLS standards such as Pseudowire, forwarding mechanisms, Label Switched Paths constructs, performance monitoring, and protection switching that provides support to transport network requirements. MPLS-TP links the gap between packet and transport network.
   MPLS-TP provide service providers with integrated network management and provisioning, and single packet switching technology that can be used across several transport networks, that reduces the total operational cost. This report demonstrates that although MPLS and MPLS-TP has the same forwarding mechanisms but MPLS-TP has enhanced OAM

functionalities and protection capabilities and based on these features how MPLS-TP can become a true Carrier Class transport Technology.

3. **Provider Backbone Bridge –Traffic Engineering (PBB-TE)**
   Provider Backbone Bridge Traffic Engineering (PBB-TE) is the technology developed by the IEEE with the purpose of giving service providers a Layer 2 carrier-grade transport based on Transport Carrier Ethernet Services. PBB-TE is based on PBB as it uses layered VLANs and MAC-in-MAC forwarding scheme encapsulation. PBB-TE extends the functionality of PBB by adding a connection-oriented mode using point to point tunnels traversing the core from one PBB to another. This report provides a brief description about how PBB-TE is different from previous two standards PB and PBB architecture.

4. **Optical Transport Network (OTN)**
   OTN was designed with the purpose of combining the benefits of SONET/SDH with the bandwidth expanding capabilities of DWDM. OTN was created to be a carrier technology and importance was given to enhance transparency, scalability and monitoring of signals carried over large distances over several domains. Transport of Ethernet frames over OTN is highly transparent. OTN improves transport network performance, bit rate efficiency and resiliency at high capacity. It offers innovative optical communication technologies such as optical paths and forward error correction (FEC).
   This report explain the transport architecture of OTN and demonstrate how it combines the benefits of SONET/SDH with DWDM bandwidth-expanding capabilities and why OTN is called digital wrapper as different types of traffic are multiplexed onto and carried over a single Optical transport unit frame.

The purpose of this project report is to provide in-depth analysis of the improvements which are introduced in the four Carrier Ethernet technologies, like Traffic Engineering, Protection and Restoration, QOS, Resilience and OAM etc. There is a detailed analysis of the above mentioned four technologies on basis of Carrier Ethernet's five different attributes that are Standardized services, Scalability, Reliability, Quality of Service and Service management. At the end there is Comparison and Contrast between different Carrier Ethernet Technologies described in the project.

1. Introduction

Ethernet simplicity and its widespread use made it de-facto standard in current data communication networks. Over the last three decades, Ethernet proceed as the leading LAN technology and now Carrier Ethernet commit to do the same in the MAN and WAN environments. The Ethernet standard has grown to include new technologies as computer networking has far developed and there is growing demand of high-bandwidth applications at increasingly lower costs. The evolution of Ethernet from LAN to WAN also present different challenges and created ambiguity and confusion for network specialist to talk about Carrier Ethernet and its different flavor.
Carrier Ethernet technology can be implemented over many different types of transport network technologies to support both existing and emerging services. There are multiple solutions that can be used to deliver Carrier Ethernet over Service Provider networks, each with its own specific standard and goal, and accordingly, different in how the Carrier Ethernet solution is offered.

1.1 Carrier Ethernet Overview

Carrier Ethernet essentially expands traditional Ethernet with Carrier-class capabilities which make it optimal for deployment in Service Provider Access, Metro Area Network and to the Wide Area Network.
According to Metro Ethernet Forum, Carrier Ethernet is ubiquitous, standardized, carrier-class service with the following attributes:

- Standardized Services
- Scalability
- Reliability
- Quality of Service
- Service Management

An Ethernet frame originating at a device in the LAN continues to traverse across MAN or WAN networks and terminates at a device in a remote LAN. Examples of basic transport mechanisms that could be used are: Ethernet over fiber, Ethernet over SONET/SDH, Ethernet over PDH, Ethernet over MPLS, Ethernet over OTN, and Ethernet over WDM. The emerging Metro Ethernet market will continue to revolutionize communications well into the future.

1.2 Benefits of Carrier Ethernet

- Customers have the ability to subscribe to multiple services and applications for example Internet access, VoIP, etc. over the same port.

- The operational costs are reduced by up to 80% and Capital costs by up to 70% due to single connection instead of managing several different types of connections.
- It can be carried over underlying technologies: Multiprotocol Label Switching (MPLS), SONET / SDH, Generic Framing Procedure (GFP), Dense Wave-length Division Multiplexing (DWDM).
- Support both existing and emerging services, including business services, residential services, mobility services, and wholesale services.
- Enables new applications requiring high bandwidth and low latency that were previously not possible due to high cost.
- Support all the application services including video, voice, data services for Internet access, private IP, or Ethernet VPNs.
- Demand of High bandwidth applications at low rates.
- Simplicity and Flexibility.
- Simplified premise equipment management by using single interface for all services, improves profitability.

1.3 Carrier Ethernet Applications

The application of Carrier Ethernet includes VoIP, LAN expansion, Business Ethernet, Dedicated Internet Access, Disaster Recovery, Packet video, Point-to-point connections with guaranteed bandwidth, Converged IP Transport, Layer 2 VPNs, IPTV, Extranet connectivity, Business continuity, and wireless backhaul.

1.4 Fundamental Ethernet Service Components

- **Ethernet Ports** (Ethernet UNI): It is the physical interface that is used to interconnect customer and the Ethernet service provider. The UNI type is selected based on the type of Ethernet port and the speed of the port. Standard Ethernet speeds are 10Mbs, 100Mbps, 1Gbps, 10Gbps or 100Gbps.

- **Ethernet Connectivity**: Connects two or more User network interfaces. The MEF has defined the Ethernet Virtual Connection (EVC) to represent Ethernet connectivity. EVC prevents data transfer between sites that are not part of the same EVC. There are three types of connectivity:
    1. Point-to-Point
    2. Multipoint-to-Multipoint
    3. Rooted-Multipoint (Point-to-Multipoint)

- **Ethernet Service Bandwidth**: This specifies a limit on the rate at which Ethernet frames can be send to or receive from the network. Ethernet service bandwidth is specified using a Committed Information Rate (CIR) and Excess Information Rate (EIR)

1.5 Carrier Ethernet Services

A Carrier Ethernet service is defined as a connectivity service based on Carrier Ethernet which is delivered over MEN using different technologies to an organization by an Ethernet Service Provider. The purpose of an Ethernet service is to connect one or more remote sites to an Ethernet service provider, in a reliable, scalable and manageable manner.
There are different service types that describe the basic connectivity options of a Carrier Ethernet services:

- **E-Line**: An E-Line is a point to point EVC service that connects exactly two UNIs. Those two interfaces can communicate only with each other. E-Line is the most popular Ethernet service type due to its simplicity. E-Lines are used to create:-
    1. Ethernet Private Lines (EPL)
    2. Ethernet Virtual Private Lines (EVPL)
    3. Ethernet Internet access

- **E-LAN**: An E-LAN is a multipoint to multipoint EVC that connects a number of UNIs. Each UNI is connected to a multipoint EVC that can communicate with any other UNI that is connected to that Ethernet service. E-LANs are used to create:-
    1. Multipoint Layer 2 VPNs
    2. Transparent LAN services
    3. Layer 2 VPNs
    4. Multicast networks

- **E-Tree**: An E-Tree is a rooted multipoint EVC that connects a number of UNIs. UNI are distributed between a root and leaves of a tree. At the difference of E-Line and E-LAN where there are no communication restrictions between endpoints, on E-Tree root can communicate with all other endpoints on the E-Tree, however leaf can only communicate with roots but not leafs. E-Trees are used to create:
    1. Rooted multi-point Layer 2 VPN
    2. Multicast Service Operators
    3. Broadcast networks
    4. Video on demand
    5. Mobile backhaul services

- **E-Access:** An E-access is a service type that defines services that use a point-to-point OVC which has one OVC End Point at an ENNI and one at a UNI. E-Access is used to create:
    1. Wholesale Access Services
    2. Access EPL
    3. Access EVPL

2 Carrier Ethernet Technologies

With spreading offerings of Ethernet services, service providers started computing how to add more capabilities to entertain growing variance of Ethernet services and develop the capabilities for Ethernet to be a feasible transport for metro and long-haul networks. Service Providers can offer smooth Ethernet services to the end user across multiple underlying solutions because of the common Carrier Ethernet layer. Carrier Ethernet technology can be implemented over many different types of transport network technologies to support both existing and emerging services.
There are multiple solutions that can be used to deliver Carrier Ethernet over Service Provider networks, each with its own specific standard and goal, and accordingly, different in how the Carrier Ethernet solution is offered. Some of these solutions are more useful than others in specific framework.
When joined with existing, familiar technologies such as SONET/SDH, IP, and MPLS, Ethernet has huge potential for providing excellent-bandwidth connectivity and service over the range of service provider offerings. The fundamental service definitions can be same, providing the end user with a seamless Ethernet experience even though there are a variety of distinct access technologies operative at that time.
For a Service Provider, choosing the suitable Carrier Ethernet delivery platform means better profitability, satisfies customer demand, and simplifies their networks and a higher level of competitiveness, whereas for end-user, choosing the right delivery platform can mean minimizing their communication costs and taking benefit of the required scalability, adaptability and robustness.

2.1 Transport Technologies

Carriers take advantage of Ethernet as a transport for their network backbone, delivering numerous profitable services and their service media. Carrier Ethernet services are designed to be delivered over all deployed transport frameworks and they can be implemented over any network based on the following transport technologies:

- Ethernet over Copper
- Ethernet over PDH
- Ethernet over Multi-Protocol Label Switching (MPLS)
- Multiprotocol Label Switching – Transport Profile (MPLS-TP)

- Ethernet over Passive Optical Networks (PONs)
- Ethernet over Fiber
- Ethernet over SDH/ SONET
- Provider Backbone Bridging with Traffic Engineering (PBB-TE)
- Optical Transport Network (OTN)
- Wireless Ethernet (WiMAX, Broadband Wireless)
- Ethernet over Resilient Packet Ring (RPR)

When evaluating the implementation choices for Carrier Ethernet, it is important to consider the organization's skill set available to deploy, geographical extent, operational constraints and maximum bandwidth that can be transported over each technology. Carrier Ethernet technologies discussed in this report are:

1. Ethernet over Internet Protocol/Multi-protocol Label switching(EoMPLS)
2. Multiprotocol Label Switching Transport Profile (MPLS-TP)
3. Provider Backbone Bridge –Traffic Engineering (PBB-TE)
4. Optical Transport Network (OTN)

3 Ethernet over Internet Protocol/Multi-Protocol Label Switching (EoMPLS)

Ethernet over IP/MPLS is a mechanism that allows an Internet Service Provider to transport Layer 2 Ethernet frames over provider's backbone network; here Ethernet packets are encapsulated inside IP/MPLS packets. EoMPLS service enables customers to improve their bandwidth costs against usage ratio by constructing out a virtual infrastructure between their points of presence.

3.1 MPLS overview

MPLS is a packet switching technology used by routers for speeding up network traffic flow and making it easier to manage. In an MPLS network, data packets are assigned labels which are distributed using (Label distribution protocol) LDP and when MPLS device accepts traffic, the device make forwarding decisions based on the label value in the MPLS encapsulation header. This allows creating end-to-end circuits over any kind of transport medium, using any protocol. In MPLS data encapsulation, the MPLS header is inserted between the second and third layers of the OSI model, Thus MPLS is often referred to as a Layer 2.5 protocol.

MPLS is a mature standard and popular as it is has been around for more than 10 years with successful deployment by big provider networks. MPLS networks are reliable, scalable and dynamic, moving traffic faster overall, support quality of service, and can be traffic engineered

to utmost use of service provider infrastructure at the same time preserving customer Service Level Agreements. They can also be arranged to provide protection and recovery, to provide flexibility in the case of link or network failure. And MPLS provides an excellent solution to the Carrier Ethernet requirements which has also contributed towards its use as an internal provider technology for providing Ethernet as a service for end customers.

3.2 Features of EoMPLS

EoMPLS implementation is based on several features of MPLS which can be characterised as carrier grade that makes Ethernet service itself carrier grade quality. Those features are as follows:

- MPLS offers a range of QoS mechanisms that guarantee performance under all network conditions.
- An assembled network protocol that can encapsulate any layer 2 protocol like Ethernet, frame relay, ATM, PPP and carry layer 3 IP protocol using pseudowire tunnel.
- Advanced Traffic Engineering capabilities using RSVP-TE.
- Create Ethernet Virtual LAN services which allow multiple services like transparent LAN services, IP VPN services, and transport of protocols without interfering with the routing of the site.
- Supports all network topology ring, multiple rings, mesh, star and dual.
- EOIP/MPLS is added to existing IP/MPLS network which offers Ethernet services over existing IP networks.

3.3 Pseudowires

A Pseudowire (PW) is an emulated point-to-point Layer 2 connection between two Provider Edge routers. The draft-martini approach forms the basis of the pseudowire architecture. Originally PW was key enabling technology designed for delivering Ethernet services over MPLS and now it is extended for many other services like ATM, FR, Ethernet, and TDM. Pseudowires may be established either using static configuration or using LDP signalling between the PEs at either end of the pseudowire.

The important feature of the Pseudowire technology is that transmitted streams are encapsulated in packets upon entering the network and then reconstructing Pseudowire edge of network. As a result, real time traffic is delivered transparently without distortion, avoiding the complexities of translating signaling data, while ensuring that synchronization criteria are met. With the Pseudowires approach one can maximise reuse of existing hardware and software technology.

3.4 Ethernet Pseudowires

In Ethernet pseudowire all packets received from the attachment circuit at the ingress PE are forwarded over the pseudowire and transmitted over the attachment circuit at the egress PE. It allows Ethernet Protocol Data Units to be carried over a MPLS network. Ethernet pseudowire can operate in either tagged mode or raw mode:

- **Tagged mode:** In this mode, each frame must contain at least one 802.1Q VLAN tag, and both PE must agree how to process the tag. The tag value is processed based on a predefined rule or algorithm at the two pseudowire end points.
  This mode exists because many routers available at the time the original draft-martini was written were unable to add and remove VLAN tags. If the VLAN tag is different on the ingress and egress PE, then the tag is rewritten at egress—though it may be rewritten at ingress if the egress PE has signaled the optional requested VLAN ID and if the ingress PE is able to rewrite the tag at ingress.

- **Raw mode**: In this mode, if a frame contains an 802.1Q VLAN tag and the tag is not suitable to be processed at the two pseudowire end points, it passes transparently through them without modification.

In general, the tagged mode is used for VLAN-based services and the raw mode for port-based services, though the raw mode may be used for VLAN-based services if the tag is stripped at ingress and a new tag added at egress.

3.5 EoMPLS Packet Format

Tunnel and pseudowire labels comprise the two levels of Label stack. The third is a Control Word that is optional depending upon the type of layer 2 transport and is used to deliver payloads in order. Pseudowire set-up can be done by either LDP or RSVP-TE if bandwidth guarantees are provided.

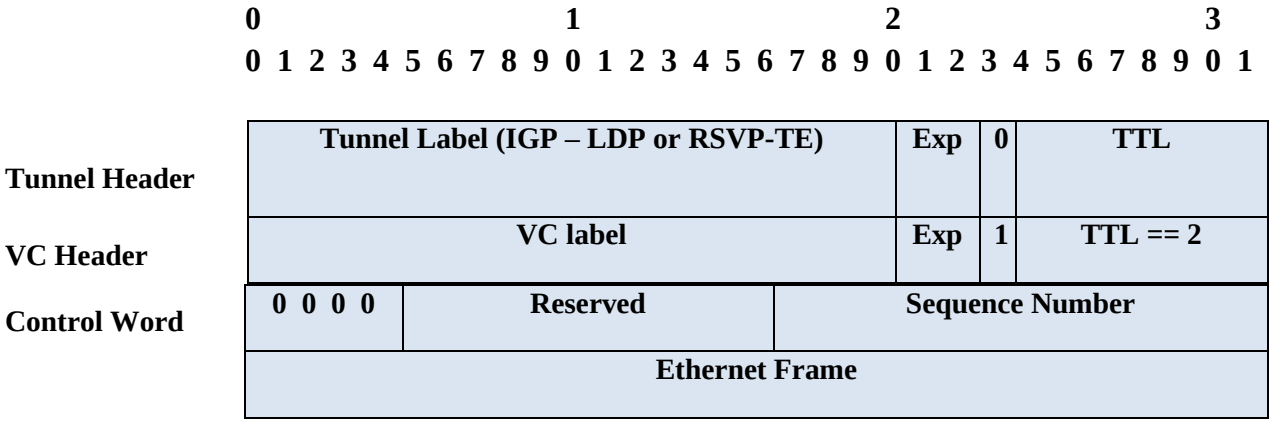

Figure 1: EoMPLS Packet Format [7], p.14

The tunnel label forward packets across the network from the ingress PE to the egress PE. The ingress LSR sets the VC label's Time to Live (TTL) field to a value of 2 and it sets the TTL of the tunnel label to 255. VC label bind the Layer 2 interface where packets must be forwarded. To indicate that the VC label is at the bottom of the stack, the ingress PE marks the VC label's end-of-stack bit with the value of 1. Control word is used to detect packet loss and when there is a possibility of mis-ordering of user frames.

3.6 Services

The Metro Ethernet Forum (MEF) has defined three types of Carrier Ethernet services based on MPLS working within a provider network:

- E-Line can be provisioned as Virtual Private Wire Service (VPWS).
- E-LAN can be provisioned as Virtual Private LAN Service (VPLS).
- E-Tree can be provisioned as Virtual Private Multicast Service (VPMS).

These services are mentioned in RFC 4664 as Layer 2 Virtual Private Networks (L2VPN) and can operate over any physical topology like mesh, partial mesh, and tree.

3.6.1 Virtual Private Wire Service (VPWS)

VPWS is a point-to-point connection between any two end-users or Customer Edge (CE) devices. To provide this service VPWS uses a pseudowire that connects two Provider Edge devices with interface user networks through a provider core. The Provider Edge (PE) device does a simple mapping between the pseudowire and a physical or logical access interface, allowing the creation of the Ethernet Private Line (EPL) Service or the Ethernet Virtual Private Line (EVPL) Service as defined by the Metro Ethernet Forum in [MEF6.1]. EPL service is created with the use of a physical interface and EVPL Service is created with the use of logical interfaces – VLANs.
The VPWS is completely transparent to the end-user data and application protocol. From the customer’s perspective, the service provider’s network that provides the VPWS service behaves like a wire (pseudowire) and connects the two sites. Therefore, VPWS is also referred to as Virtual Leased Line (VLL).
VPWS service offers service for interworking for Ethernet, ATM, Frame-Relay and TDM across a common IP/MPLS networks. VPWs are also called pipe services because they behave like a point to point pipe. The following are examples of several VPWS services:

- Apipe — ATM point-to-point service between two ATM node
- Cpipe — TDM leased line service point-to-point between two TDM node
- Fpipe — Frame-Relay point-to-point service between two Frame-Relay node
- Epipe — Ethernet point-to-point service between two Ethernet node
- Ipipe — Point-to-point service between two nodes that has different technologies.

The VPWS is the simplest type of Virtual Private Network to extend with least resource consumption as it is a preferred solution for any point-to-point connectivity requirements. The technology does not make use of customer MAC addresses, which reduces the amount of information that must be stored by the PE devices.

3.6.2 Virtual Private LAN Service (VPLS)

VPLS is a provider service that creates an Ethernet multipoint switching service over MPLS and follows the full functionality of a traditional Local Area Network (LAN). A VPLS makes it possible to interconnect multiple LAN sites over a packet-switched network and provides connectivity between multiple sites as if these sites were attached to the same Ethernet LAN. [RFC4026].
VPLS is another example of a L2VPN that bridges customer Ethernet traffic between geographically dispersed areas. VPLS is also referred to as Metro-Ethernet service as well as Transparent LAN Service.
VPLS like VPWS uses pseudowires. However, each VPLS instance uses its own set of pseudowires. The basic VPLS architecture consists of a set of PEs. Each set of pseudowires provides the full mesh connectivity for PEs. These fully meshed pseudowires in the VPLS network obey the split-horizon forwarding rule that is they do not exchange traffic between each other, but only with PEs. Forwarding decisions are based on MAC addresses which are learned from the source addresses of frames. Ethernet frames are forwarded toward all CE devices connected to a VPLS with broadcast, multicast or unknown destination addresses.
There are two standardized VPLS implementations using two different label-signaling protocols:

- **BGP based VPLS:** This implementation uses the Multi-Protocol Border Gateway Protocol to signal the service-labels for each VPLS instance. BGP-VPLS provides both signaling and auto discovery of VPLS tunnels that help to avoid complexity of configuration at the expense of running BGP protocol between VPLS routers.
- **LDP based VPLS:** This implementation uses Targeted LDP to signal the service-labels among PE routers within the same VPLS service. LDP-VPLS provides only signaling, but not auto discovery so it requires a manual specification of each PE device participating in a VPLS instance. This procedure is time-consuming and error-prone procedure.

VPLS is deployed in converged IP/MPLS network, along with other services like IP VPN. By using VPLS services, customers can significantly extend the coverage of their private LAN while keeping the routing topology design to themselves. VPLS service interconnects multiple customer routers that offers simpler configuration and fewer restrictions than interconnecting the routers over Ethernet pseudowires.

3.6.3 Virtual Private Multicast Service (VPMS)

VPMS is L2VPN service that provides point-to-multipoint connectivity for a variety of link layers, including Frame Relay, ATM, Ethernet, PPP, etc., across an IP or MPLS-enabled IP Packet Switched Network.
Framework and Service level requirements for the service are under development and have been proposed in an IETF Internet Draft (draft-ietf-l2vpn-vpms-frmwk-requirements).

VPMS allows a single coverage of Ethernet frames transmitted by a transmitter to be copied in the provider network and delivered to multiple receivers connected to the same VPMS instance. VPMS is not MAC-based forwarding. A VPMS is an E-Tree service as defined by MEF.

3.7 EoMPLS QoS

QoS in EoMPLS enables network Service providers to provide differentiated types of service across an MPLS network and guarantee delivery.
QoS architectures may be divided into two major classes:

- **Integrated Services (IntServ):** IntServ framework was developed within IETF to provide per-flow QoS guarantees to individual sessions and uses Resource Reservation Protocol (RSVP) as the signalling mechanism. This protocol involves prior reservation of resources before sending between receiver and transmitter using end-to-end signaling, in-order to achieve the required QoS. This model is less scalable as prior flow reservations are required, but can be used to enable a firm guarantee that a traffic contract will be met.
- **Differentiated Services (DiffServ):** DiffServ framework defines a QoS architecture, which is based on aggregation of flows and requires traffic to be marked with priority and send it to the network. It is up to the network operator whether the required priority treatment for QoS is given or not. There is no prior reservation of resources in DiffServ. This model is more scalable that IntServ as there is no need for prior flow reservation. It is applicable to connectionless and connection orientated forwarding, but is unable to provide guaranteed forwarding behavior.

QoS for EoMPLS traffic uses strict priority or weighted round robin scheduling in the egress interface of both ingress and egress router. EoMPLS QoS priority can be set by using 3 experimental bits (EXP bits) in the MPLS label to determine the priority of packets. MPLS QoS enables service providers to classify packets according to their type, input interface, and other factors by marking each packet within the MPLS experimental field. IP Precedence or DSCP bits can be used to specify the QoS for an IP packet and MPLS experimental bits can be used to specify the QoS for an MPLS packet.

3.8 EoMPLS OAM

OAM (Operations, Administration, and Maintenance) is a mechanism that is used for connectivity verification, path discovery, remote fault detection, and provide proactive detection of service degradation, performance monitoring and SLA verification. It also allows immediate detection of a link or node failure that affects the service and provides the ability to monitor and troubleshoot the network. There are a variety OAM tools and protocols have been defined to enable detection of EoMPLS failures and fault detection:

- **LSP Ping**: LSP Ping is used to detect data plane failure and to check the consistency between the data plane and the control plane. LSP ping mode can used to ping a LSP periodically to verify connectivity, and if the ping fails, then LSP traceroute mode can be used to diagnose the location of the fault. LSP Ping verifies that packets that belong to a particular Forwarding Equivalence Class (FEC) actually end their MPLS path on a LSR that is an egress for that FEC. LSP Ping sends MPLS echo requests following the same data path that normal MPLS packets would traverse. LSP ping is defined in RFC 4379.
  LSP Ping uses echo request and echo response UDP packets encapsulated into tested LSP frames. An MPLS echo request packet is sent by the router to test LSP of a given FEC, that is a UDP packet with the destination address randomly chosen from the 127/8 range and the destination port set to 3503 (for MPLS echo requests). The IP TTL value of MPLS echo request packets is set to 255 for LSP ping and it starts with 1 and the Router Alert option is set in the IP header. A router that receives an MPLS echo request sends an MPLS echo reply packet to the sender of the echo request. An MPLS echo reply packet is a UDP packet with a destination IP address and a destination port copied from the source IP address and the source port of the echo request. The IP TTL value of this packet is set to 255. Each packet indicates how its recipient should send its reply; because MPLS LSP is usually unidirectional, the reply can't be sent back over the LSP. The replying mode is determined by the echo request, which may be one of four reply modes:
  1. IP reply
  2. No reply
  3. Reply with the Router Alert option
  4. Associated control channel

- **Bidirectional Forwarding Detection (BFD):** BFD is a detection protocol designed to detect faults in the bidirectional paths between two forwarding systems, including data links. It provides fast forwarding path failure detection mechanism which is independent of media, encapsulations, topologies, data protocols and routing protocols.
  BFD packets are sent at intervals over a transmission path between the two systems and path failure is detected when BFD packets stop arriving.
  There are two BFD operating modes:

1. **Asynchronous mode**: In this mode device periodically send Hello packets to each other. If a system stops receiving packets for long enough, the path is assumed to have failed.
2. **Demand mode**: In this mode no periodic Hello packets are exchanged after the session is established unless one system initiates a Poll/final sequence. It is assumed that the system have another way to verify connectivity to each other.
   BFD can be used in combination with LSP Ping to provide faster data plane failure detection and make it possible to provide failure detection on a greater number of LSPs. BFD is the primary mechanism to make fast switchover and meet transport requirements. BFD could be used to complement or replace use of RSVP hellos for MPLS Fast reroute Node protection.

3.9 Traffic Protection and Restoration

In MPLS there are several protection and restoration features that differ in the way they restore a data path using alternative paths and the time that is needed for restoration. The main task of the MPLS traffic protection is controlling the traffic flow in the network and finding the best way for detour path to protect against a network failure.
MPLS fast Reroute (FRR) provides path restoration to LSPs. It repairs failures at the point of failure, rather than waiting for the PathErr to propagate to the ingress LSR. In FRR mechanism, each router along the LSP creates a detour path along main MPLS LSP. The upstream router immediately sends traffic to its detour LSP to protect against a link or node failure. The router also notifies the ingress router for the path that part of the main LSP has failed, so that it can then redirect traffic along new path. The reroute decision is completely a function of Resource Reservation Protocols used for creating LSPs in an IP/MPLS network. In Fast reroute detection and recovery is expected under 50 milliseconds.
MPLS supports several failover mechanisms:

- **Path Protection:** It provides full path failure recovery protection for MPLS tunnels. In MPLS path protection mechanism a backup path is built along the primary LSP, ideally disjoint from the primary path signaled for the LSP. In case of failure upstream router immediately sends traffic to its backup path. No path computation and signalling of the new LSP once the failure has been detected and propagated to the head-end.
  This kind of protection switching is much faster than a traditional re-routing which involves OSPF-TE or IS-IS-TE calculations. The main advantages of path protection are control over where the traffic goes after a failure and minimum packet loss when combined with fast reroute.
- **Node Protection:** In this mode, the backup path is created from each node on a path to the egress router of the path. The main purpose of the backup path is to protect against a failure of the downstream node. This technique also protects against a link failure

because backup tunnels bypass the failed link and the node. It is the most efficient protection scheme providing protection in 50ms in case of link and node protection.

- **Link Protection:** In this mode each link used by an LSP is provided protection by pre-established backup paths. Link protection offers per-link traffic protection. They protect LSPs if a link along their path fails by rerouting the LSP's traffic to the next hop using backup paths. These are referred to as next hop backup tunnels because they terminate at the LSP's next hop beyond the point of failure.
  This mechanism allows protection of a link but cannot be used in case of a failure of a node in the network. It works faster than a path protection, usually in the 50ms range. It is a kind of MPLS fast re-route feature.

3.10 EoMPLS Meets the Carrier Ethernet Attributes defined by MEF

- **Standardised Services**:
  1. EoMPLS is an Internet Engineering Task Force (IETF) standard-track protocol based on the Martini draft. IETF standardise MPLS, pseudowires, and VPLS (VPLS-LDP and VPLS-BGP) to guarantee that service providers can develop practical equipment that offers EoMPLS services. It resolves interoperability challenges in multi-vendor networks.
  2. Ethernet PWs implement the MEF's E-Line service (Point to point) and VPLS implements the MEF's E-LAN service (multipoint to multipoint).
  3. Pseudowire emulation edge-to-edge (PWE3) provides a tunneling service over a MPLS core.
  4. A Layer 2 circuit is allocated a label and LDP is used to distribute the label-circuit mapping.
  5. EoMPLS does not require any changes to customer LAN equipment.

- **Scalability:**
  1. With EoMPLS, data is transferred over any combination of Layer 2 technologies, using any Layer 3 protocol, with increased scalability.
  2. It supports huge number of services in every network by layering different services onto each MPLS Label Switched Paths and distributed network architecture.
  3. Highly scalable based on number of VLAN supported by the platform, it can scale to thousands/Ten thousands of VLANs per framework.
  4. EoMPLS provides easy interfacing to current wired and wireless networks.
  5. Rapid bandwidth scaling without equipment changes for ample flexibility and scalability.

6. It offers end-to-end network bandwidth guarantees and increased bandwidth efficiencies by providing protection at layer 2.
7. Large number of customers over a common infrastructure.
8. The spread of the Layer 2 connection on the Layer 3 transport hides any physical convergence and this increases overall stability of Layer 2.
9. Services can be provided across geographic diverse locations since IP/MPLS networks may be global in reach and one service may be provided over multiple service providers networks.

- **Reliability:**
    1. The Fast Reroute (FRR) structure is used for providing network protection and recovery from failures that occurs in less than 50 milliseconds. FRR allows rerouting around a failed link or node.
    2. EoMPLS model secure against network failures at the network layer and generates fault notification to the service layer when the fault is unrecoverable.
    3. Fast software upgrade to offer a very high availability service to the end user.
    4. MPLS provides several failover mechanisms like Path protection, Head-end path restoration, Node protection and Link protection.
    5. Different level of protection may be applied to various classes of traffic.
    6. Capability to rapidly detect and recover from different failures meets the most demanding quality requirements for the delivery of high-quality voice and video services.
    7. EoMPLS can also utilise Link aggregation or Resilient Packet Ring where appropriate to add link redundancy and recovery in distribution networks.

- **Quality of Service:**
    1. EoMPLS model offers means of aggregating QoS (Quality of Service) reservations through the network core by layering services on MPLS Label Switched Paths. It provides a range of Bandwidth and QoS options.
    2. There are two basic QoS models in EoMPLS:
        i. E-LSP (EXP-inferred-PSC LSP) model uses the EXP or experimental field to infer QoS. It offers a scalable soft QoS mechanism suitable for most services.
        ii. L-LSP (Label-only-inferred-PSC LSP) model infers QoS from the label and, optionally, also from the EXP field. It offers the hard QoS to guarantee performance under all network conditions.
    3. By using traffic engineering (TE) service providers can provide various levels of QoS for different types of services such as packet delays and loss and guarantee traffic flow. EoMPLS supports the establishment of Traffic Engineering paths in different ways:

i. Control plane based
ii. Network Management System based
iii. Manually configured

4. Multiple classes of traffic with guaranteed Service Level Agreements (SLA) can be offered to deliver the performance required for a target application.

- **Service Management:**
  1. Service Providers can effectively troubleshoot and diagnose network problems.
  2. Essential monitoring and management stations.
  3. EoMPLS manages tunnels and services that can benefit from user friendly provisioning service and management:

i. NMS-based service provisioning
ii. Combined NMS and MPLS signaling

4. EoMPLS tools for service management have been standardised through IETF RFCs.
5. In IEEE there are two standards for OAM:

i. IEEE 802.3ah Ethernet Operations, Administration, and Maintenance **(**E-OAM)
ii. IEEE 802.1ag Ethernet Connectivity Fault Management (E-CFM)

These standards provide the tools to control a network in the data plane and the control plane over an Ethernet services and to check continuity, connectivity, and performance.

3.11 Applications for Ethernet over MPLS

- EoMPLS is a popular method for creating Ethernet Virtual LAN services because it allows transparent LAN services, bridging between sites and IP VPN services, without interfering with the routing of the site.
- EoMPLS was originally developed for carriers to offer point to point Ethernet services to internet service providers that wanted high bandwidth. VPLS provides powerful tools to allow Ethernet to extend to the WAN as a sophisticated and scalable connectivity service.
- It offers a way to provide Point to point Layer 2 connections between customer locations over an IP network. Such connections are replacing the point-to-point services provided in legacy technologies like Frame Relay, TDM, ATM and SONET/SDH.
- When providing point-to-point customer connections the provider equipment does not use any of customer address for switching traffic as they are unaware of customer MAC address. Provider equipment does not store any addressing information that reduces memory utilisation and makes the network scale to a virtually unlimited number of services.
- EoMPLS provides residential and business services like VPLS, VPWS, VPMS, L3VPN and private line. Residential multiple play services like voice, video, data and mobile.

- EoMPLS connect different work stations of an organisation, giving the organisation full control of their Layer 3 routing although holding the communication of customer information under the authority of the network operator.
- Revenue generation by adding new services like Triple play and 3G mobile aggregation.
- Carriers wishing to offer all services over a common platform are now deploying multi-service PE devices. These enable them to offer IP services, and legacy services over the same network using EoMPLS for IP services, Ethernet services and pseudowires for legacy services migration.

3.12 Advantages of EoMPLS

- EoMPLS enables providers to offer carrier-class Ethernet services to their customers over existing IP networks; it enables the service provider to provide multiple physical connections that transport all types of traffic over single virtual network and accommodate all types of customers.
- Online performance monitoring to get current detailed information about the performance of each port used for a connection.
- EoMPLS is highly scalable as addition or removal of VCs is easier.
- Transparent IP services and LAN services.
- Reduces Operational cost and capital cost through the aggregation and interoperability of multiple Carrier Ethernet services over a single physical connection.
- The Edge Routers switch traffic based on port or VLAN, there is no need of learning MAC addresses.
- Statistical multiplexing of traffic from different services and different customers allows most efficient utilisation of bandwidth.
- Upgrading to EoMPLS is transparent IP service to the customer. Because the service-provider network is separate from the customer network, the service provider can upgrade to EoMPLS without disruption of service to the customer. The customers assume that they are using a traditional Layer 2 backbone.
- MPLS offers a variety of Quality of service mechanisms that can be applied to EOIP/MPLS service which guarantee performance under all network situations.
- Ease of configuration and lower cost of bandwidth.
- Layer 2 and Layer 3 provisioning flexibility.

3.13 Limitations of EoMPLS

- EoMPLS does not support packet fragmentation and reassembly. Therefore, the maximum transmission unit (MTU) of all links between endpoints must be sufficient to

transmit the largest Layer 2 VLAN received. The ingress and egress provider-edge routers must have the same MTU value.

- VPLS design assumes that all PE devices are fully meshed over Ethernet pseudowires. If any pseudowire breaks due to some failure, then the VPLS service does not offers full connectivity between all attached devices. This will upset IP routing protocols that rely on multicast to transport network reachability information.
- EoMPLS supports VLAN packets that follow the IEEE 802.1Q standard that establishes a standard method for inserting VLAN membership information into Ethernet frames. The Inter-Switch Link protocol is not supported between the Provider Edge and customer edge routers.

4 Multiprotocol Label Switching Transport Profile (MPLS-TP)

4.1 Background

MPLS has been one of the most successful connection oriented technology of the past decade due to its key features like Scalability, Efficient Packet Forwarding, Protocol neutrality and QoS. The success of MPLS in the packet based network motivates service providers to enhance MPLS beyond the packet based network to enable higher reliability to packet transport networks, as these networks are best suited for carrying packets.
The ITU-T and the IETF jointly work on different improvements to MPLS that allow it to be applied to transport network and mobile backhaul. The set of these new formulations of MPLS enhancements is called MPLS Transport Profile (MPLS-TP) that is standardized by developing Technologies. MPLS-TP provides SONET/SDH like OAM and resiliency features to packet transport network -scalable operations, high availability and performance monitoring. In addition to adopt supporting QoS in transport technologies, it also provides simple managed bandwidth services and in-band OAM protection mechanisms.

4.2 Overview

MPLS-TP is a profile of MPLS protocols that are being defined in IETF. It is designed for use as a network layer technology in transport networks. It offers existing MPLS implementation, by removing some functions such as Equal Cost Multi Path (ECMP) and Penultimate Hop Popping (PHP) that are not relevant to connection-oriented applications. Also, it is based on existing MPLS standards such as Pseudowire, forwarding mechanisms, Label Switched Paths constructs, performance monitoring, and protection switching that provides support to transport network requirements. MPLS-TP links the gap between packet and transport network.

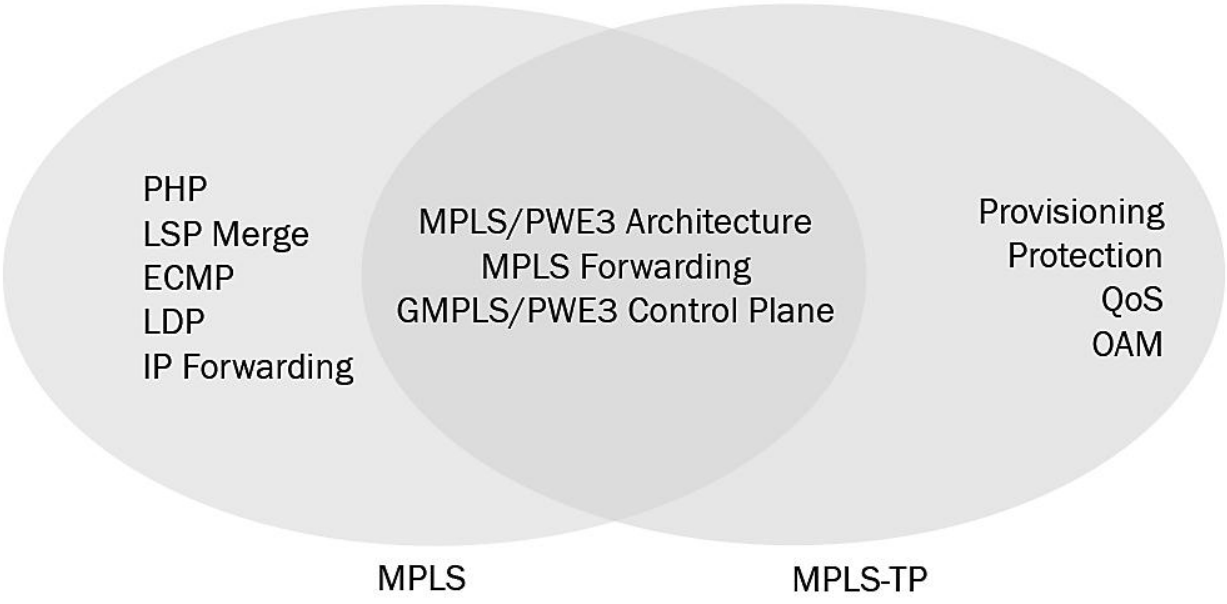

Figure 2: Relationship of MPLS and MPLS-TP [16], p.31

MPLS-TP presents features related with transport networks such as transport grade OAM functions, protection switching, and performance monitoring. MPLS-TP offers service providers with a reliable packet based technology that is based upon circuit based transport networking. These features bring evolution to connection-oriented packet transport network by providing efficient packet switching though allowing transport-grade operations. MPLS-TP has enhanced OAM functions and protection features like fault detection, fault localization, troubleshooting, SLA verification, performance monitoring which allows quick detection and correction for any SLA violations.

MPLS-TP provide service providers with integrated network management and provisioning, and single packet switching technology that can be used across several transport networks, that reduces the total operational cost. MPLS-TP operate without any IP layer functionalities as it is intended to reduce network operational complexity and designed to work in devices where IP routing is not supported.

4.3 Features of MPLS-TP

MPLS-TP provides key enhancements to MPLS that provides benefits to Service Providers. Some of the key characteristics features are mentioned below:

- MPLS-TP interoperates with existing MPLS architecture and forwarding mechanism, it reuses pseudowire and MPLS Label Switched Paths constructs.

- It is strictly connection oriented protocol with traditional protection schemes.
- MPLS-TP can carry any type of customer traffic such as Layer3, Layer2, Layer 1, Asynchronous Transport Mode (ATM), SDH and Ethernet services.
- MPLS-TP uses Label Switched Paths and Pseudowires to deliver point to point services as well as point to multipoint and multipoint to multipoint services.
- It provides SONET/SDH like OAM and resiliency features to packet transport network - scalable operations, high availability and performance monitoring.
- OAM functions are integral part of the MPLSTP data plane and are independent from management or control plane.
- MPLS-TP allows optimization of packet transport to reduce overall network cost, allowing a more reasonable and efficient network infrastructure.
- MPLS-TP uses Generic Associated Channel (G-ACh) to support Fault, Accounting, Performance and Security functions. G-ACh can be used to send traffic as well as data.
- Meets functional requirements of service provider transport networks.

4.4 MPLS-TP Architecture

MPLS-TP technology is subset as well as an extension of the MPLS protocol and uses the same forwarding mechanisms and architecture as traditional MPLS. There are different elements forming an MPLS-TP network. These elements do not introduce new functionality to MPLS-TP and have same behaviour as in MPLS.

MPLS-TP network includes the following elements:

1. MPLS-TP Label Switching Router
2. MPLS-TP Label Edge Router
3. MPLS-TP Provider Edge Router
4. MPLS-TP Provider Router
5. MPLS-TP Customer Edge Router

In order to ensure proper operational control, MPLS-TP network elements exchange OAM packets that follow the same path as data packets, with a set of tools running at each LSP. MPLS-TP has new enhancements to MPLS architecture those are In-band control channels and Network Layer Transport Service. MPLS-TP includes control plane, protection, and network management as part of its architecture.

To ensure compatibility between the OAM packets and the data path, the OAM packets use in-band control channels. In MPLS-TP OAM functions like framing, forwarding, and performance monitoring need to operate without any IP layer functionalities, because MPLS-TP is designed to work where IP routing is not supported. MPLS-TP makes it possible with Generic Associated Channel (G-ACh) and G-ACh Label (GAL) to carry the OAM packets.

1. **Generic Associated Channel (G-ACh):**

G-ACh allows control packets to be multiplexed transparently over LSPs or MPLS-TP segments. G-Ach provides mechanism to allow management and OAM information run in-band. Multiple control channels can exist between end points.

2. **G-ACh Label (GAL):**

GAL is used to identify the OAM control packets. It is defined by assigning a reserved MPLS label value. If a GAL is found anywhere in the label stack it enables easy extraction of the OAM packets at point of an LSP. RFC identifies new reserved label – Label 13 as a G-ACh label for providing necessary tagging.

4.5 MPLS-TP Packet Format

The MPLS-TP Packet format is depicted in the Figure below.

- **GAL – Generic Alert Label: A**llows any type of traffic and OAM packets to be directed to an intermediate node on a LSP or PWE. The GAL is used in MPLS-TP LSPs to flag the G-ACh. In MPLS-TP, the GAL must always be at the bottom of the label stack i.e. S bit is set to 1.

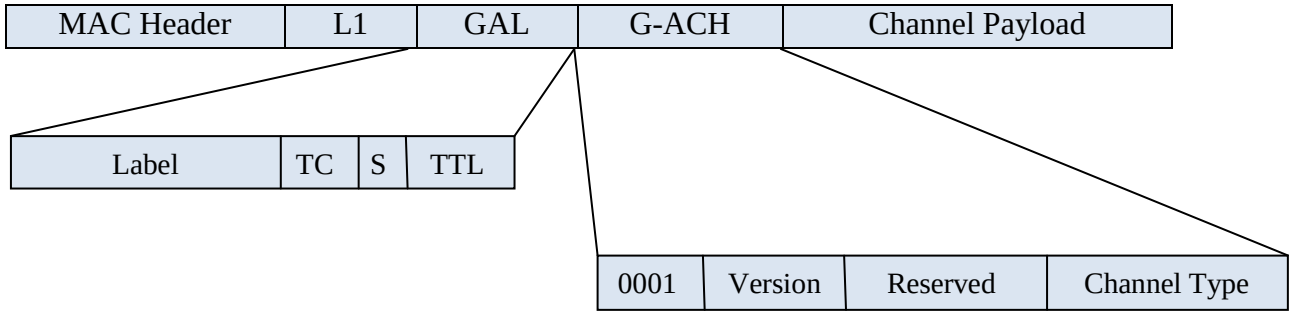

Figure 3: MPLS-TP Packet Format

- **Label-** Label Value, 20 bits
- **TC -** Traffic class field, 3 bits. TC is used for QoS related functions.
- **S -** Bottom of stack, 1 bit. This field is used when more than one label is assigned to a packet.
- **TTL -** Time to Live, 8 bits. MPLS-TP LSPs use TTL field that serves as a hop counter. At every routed hop, the TTL value is decremented by one; if the TTL reaches zero before the packet reaches its destination node, the packet is discarded.
- **G-ACH – Generic Associated Channel:** The G-ACh is used in both PWs and MPLS-TP LSPs. G-ACH defines what packet function using channel type field.

4.6 MPLS-TP Control Plane

The control plane mechanism is responsible for the setup of end to end Label switched paths automatically across a packet switched network. Also used for determining and defining primary and backup paths, configuring the OAM functions along the path. MPLS-TP control plane is capable of carrying out fast restoration in the incident of network failures.
Control plane functionality is optional in MPLS-TP. IETF defined Generalised MPLS (GMPLS) as a MPLS-TP control plane protocol to be applied to packet switched networks. GMPLS control plane supports connection management functions as well as protection and restoration techniques making MPLS-TP more dependable transport protocol.
MPLS-TP can operate in two modes – static provisioning of LSPs with network management system, and dynamic provisioning with a GMPLS control plane. It is estimated that both modes will be deployed, depending on network type and carrier preference.

- **Static provisioning with network management system:**

The static provisioning model is the simplified version and commonly known as static MPLS-TP. In this approach operators can set up LSPs and PWs statically using a Network Management System (NMS), similar to the manner it is done in legacy transport networks. It establishes bi-directional LSPs. With Static Provisioning there is no dependency on routing protocols or signaling. Since the signaling is static it does not implement some MPLS functions, such as LDP and RSVP-TE.
The static control plane has applicability in situations where some equipment used at the edges of the network, does not support a dynamic control plane. Static configuration is preferred sometimes for security reasons.

- **Dynamic provisioning with a GMPLS control plane:**

Dynamic provisioning approach a control plane is used. Here LSPs and PWs are created by the network using GMPLS as a signaling mechanism and Targeted Label Distribution Protocol (T-LDP) respectively. Dynamic Control Plane establishes bidirectional RSVP LSP setup within GMPLS framework.
The dynamic control plane offers some important benefits:

1. maximum flexibility for path computation and routing decisions
2. advanced protection functions such as LSP tail-end protection
3. may also be used to set up the OAM function
4. Multi-vendor interoperability
5. Define recovery mechanisms

4.7 MPLS-TP QoS

The main aim of MPLS-TP is to enable Service Providers to guarantee Service Level Agreement (SLA). QoS mechanism is an essential part of MPLS-TP to guarantee network bandwidth, packet loss and to control jitter and delay.
MPLS-TP uses the DiffServ QoS approach in which edge routers do traffic conditioning and internal routers do different QoS treatment to packets based on their markings. The marking information is carried in the label header in a 3-bit field that defines the QoS treatment (per-hop behaviour) that a node should give to a packet. MPLS & MPLS-TP label has a 3 bit field usually known as Traffic Class field. These 3 bits define the QoS treatment (per-hop behaviour) that a node should give to a packet.
QoS mechanisms include:

- DiffServ traffic types and traffic class separation
- provisioning end-to-end bandwidth
- supports DiffServ with Traffic Engineering capabilities
- flexible Bandwidth allocation
- provision for delay and jitter sensitive services
- guarantee of fair access to shared resources

MPLS-TP is a multi-layer technology and defines three mechanisms for multi-layer QoS management:

- **Uniform mode:** Uniform mode is used when the customer and service provider are under same DiffServ domain.
- **Short pipe mode:** Short Pipe Mode is used when the customer and service provider are in different DiffServ domains. This mode is useful when the service provider wants to implement their own QoS policy independent of their customer's QoS policy. Short pipe mode uses an inner header for forwarding.
- **Pipe mode:** Pipe mode is identical to short pipe mode. The pipe and short pipe mode differ in the header that the tunnel egress uses when it determines the Per Hop Behaviour of an incoming packet. Pipe mode always uses the outermost label for forwarding.

Only pipe mode and short pipe mode are supported by MPLS-TP. Uniform mode is not supported due to the hierarchical structure of MPLS-TP.

4.8 MPLS-TP OAM

MPLS-TP is based on a profile of the MPLS architectures enhanced with additional OAM procedures and protection features for fault detection, fault localization and performance monitoring for packet transport application that do not rely on the presence of a control plane or IP functionality. IETF MPLS-based MPLS-TP OAM tools meet transport requirements.
MPLS-TP strives to be a carrier-grade transport network so it has strong OAM requirements. OAM is nowadays becoming more significant, as service providers are requiring a strong and stable set of tools to maintain transport network services, in order to deliver better services and to comply with the SLAs guaranteed with their customers. Service Providers themselves profit

from introducing OAM functionality into their networks. Failures and possible problems are detected faster and more efficiently, reducing the time to repair and consequently reducing their Operational cost.
The OAM is designed to address the quality of network issues and provides the following necessary functions:

- Test, identify and locate failure within the network
- Monitor network performance tests and measure packet loss rate, delay, jitter and other performance issues
- Reduce network operational complexity related with network performance monitoring and protection switching.
- Find failures and activate the protection switchover
- Loop-back testing properly locates the fault on a port

In addition to MPLS functionalities, MPLS-TP provides network operators with full command over their packet networks. Additional transport functionalities being added as a part of MPLS-TP are:

- Comprehensive OAM capabilities
- Fault detection fault localization
- Data-plane/control-plane separation
- Static provisioning of bidirectional services
- Performance monitoring

4.8.1 OAM Architecture

OAM and monitoring in MPLS-TP is based on the concept of maintenance entities. The OAM architecture is described in the OAM Framework document that defines the following functional components:

- **Maintenance Entity (ME):** These are relationship between those points of a transport path that requires management. It is bounded by two Maintenance End Points.
- **Maintenance Entity Group (MEG):** A collection of one or more MEs that belong to the same transport path those are managed and monitored as a group.
- **MEG Endpoint (MEP):** These are points where messages for fault management and performance monitoring are originated or terminated.
- **MEG Intermediate Point (MIP):** MIP is a maintenance entity that is located at intermediate points along the end-to-end path. MIP does not initiate any OAM messages, but may react and process them.
- **Tandem Connection:** It is part of a transport path that can be monitored independently of the end-to-end monitoring.

4.8.2 OAM Tools

OAM tools are the functions that are used to perform fault management and performance management. MPLS-TP supports the following OAM function:

- **Fault Management**
  1. **Continuity Check and Connectivity Verification (CC & CV):** This operation allows fast detection of loss of connectivity and misconnections between MEPs. To provide CC & CV, extended Bidirectional Forwarding Detection (BFD) and extended LSP-Ping tools are used.
  2. **Remote Defect Indication (RDI):** RDI is an indicator sent by an MEP to its peer MEPs to notify that a defect has been detected on connection between them. Extended BFD to include the RDI function within the CC & CV messages.
  3. **Alarm Reporting:** It enables fault localization and suppresses alarm when there is a failure condition so that there is not unnecessary alarms propagation. Alarm reporting is used successively with Alarm Indication Signal
  4. **Lock Reporting:** When an MEP is administratively locked it transmits Lock signal to inform the administrative locking condition to its sub layer MEP. It is used to suppress alarms at the MPLS-TP layer and allows MEP clients to differentiate between the defect conditions and intentional administrative actions at the server layer MEP.
  5. **Loopback messages:** MEPs send loopback messages to authenticate connectivity with other MEPs on the transport path. Loopback messages are used for out of service testing and to check reachability to different points.

- **Performance management**
  1. **Packet Delay Measurement:** It is used to measure delay in forwarding the packets between two endpoints.
  2. **Packet Loss Measurement:** It is used to measure packet loss on an established path between two endpoints.
  3. **Client Fault Indication:** This function is used to indicate the presence of fault to the far-end client. Applications of Client fault indication is far-end performance monitoring.

4.9 Traffic Protection and Restoration

MPLS-TP is Packet based technology that is intended to decrease network operational complexity, and ensuring network reliability and high availability. Protection and restoration is known as network survivability, it is the ability of a network to restore from failure of network. MPLS-TP provides similar protection switching mechanisms which are used in traditional transport technologies such as SONET/SDH transport networks. A protection mechanism for MPLS-TP includes following:

- Protection State Coordination (PSC) protocol to coordinate the both ends on protection state and commands
- Protection for both unidirectional and bidirectional paths
- End to end protection for LSPs and PWs layers
- In case of failure in the data plane switching time is less than 50 ms
- Provides 1+1, 1:1 and n:1 protection schemes architecture
- Protection switching is triggered automatically upon detection of Signal or network failure
- Manual protection commands e.g. manual switch, lockout, clear

Restoration is re-routing that requires computation of a new transport path. Restoration operations can be supported in following four different ways:

- Manual control: Triggered by operator
- Failure-triggered actions: started upon detection of a signal failure in the network
- OAM signalling: Data plane OAM message exchange. These messages can be used trigger a recovery operation.
- Control-plane signalling: manage detection, localization, and reaction to network failures and accordingly start recovery operations.

MPLS-TP supports enhanced protection switching and restoration mechanisms at different levels, to recover from failed network and to support the protection switching. All existing GMPLS and MPLS recovery mechanisms are applicable to MPLS-TP.

4.9.1 Protection Topologies

MPLS-TP network enhances the resiliency mechanism of MPLS by adding provision for OAM-triggered protection and enhancing protection in ring topologies. There are different methods of attaining protection depending on the type of service, type of mechanism or level of protection. It supports general mechanisms like alternate paths or bypass tunnels, and in some situations optimized mechanism if network topologies require it.

There are different protection topologies:

- **Linear Protection:**

Linear protection provides a fast and simple end to end protection switching mechanism. It provides protection to transport paths, that can be unidirectional and bidirectional. Linear protection fits best in mesh networks.

Types of linear protection schemes are:

1. **1+1 linear protection scheme:** A fully dedicated protection path is allocated for recovery. At the source to traffic is copied and transmitted on both working as well as protection path. 1+1 protection scheme does not allow protection channel to carry any extra traffic.

2. **1:1 linear protection scheme:** A protection path is allocated to protect against failure in a working path. In normal situations, data traffic is transmitted over the working path, while the protection path is reserved for future use and stays in idle. When a failure occurs on the working path traffic is switched to the protection path. It needs an additional facility to switch the traffic from a working channel to a protection channel, thus affecting restoration speed.
3. **1: n linear protection scheme:** One protection path is allocated to protect n number of working paths. This can only protect one working path at a time. The protection path might not have enough resources to protect all the n working paths that are affected by fault at certain time. In order to guarantee protection the protection path should support enough resources.

These protections schemes are defined for both uni-directional and bi-directional paths. In Bidirectional protection scheme both the directions will be interchanged at the same time even if the fault applies to only one direction of the path. In unidirectional protection scheme protection switching is done independently for each direction of a bidirectional transport path.

- **Ring Protection**

Ring topologies are used in transport networks due to their ability to easily support both point to point and point to multipoint transport paths. Service Providers express great interest in the operation of MPLS-TP in ring topologies and they require a high degree of survivability functionality ring topologies. Various optimizations and schemes such as wrapping and steering have been developed as part of MPLS-TP work to provide efficient protection in ring topologies. Types of ring protection schemes are:

1. **Facility bypass ring protection:** A single facility bypass path protects all paths over a particular link by wrapping traffic. In this mechanism when a fault is detected on the transport path that would prevent forwarding of the data along the data path. It wraps all data traffic around the ring, on an appropriate bypass channel, until arriving at the LSR that is on the opposite side of the fault. The facility bypass technique allows the protection of many paths that pass through the same links via the same bypass tunnel.
2. **Detours ring protection:** When a network failure occurs on the current path, the traffic is quickly routed to one of the detours path. A detour path can be used for optimal traffic delivery to the destination point. This is one-to-one backup and each LSP is protected separately.

- **Mesh protection**

Shared mesh protection is a protection and recovery mechanism in transport networks in this multiple recovery paths can share network resources for protection of working paths. This protection scheme can make efficient use of network resources, however needs careful management to ensure that only one set of traffic is switched to the protection resources at specific time.

4.10 MPLS-TP Meets the Carrier Ethernet Attributes defined by MEF

- **Standardised Services**:

Firstly, the ITU-T started to enhance MPLS for transport networks under the name T-MPLS. Due to concerns about T-MPLS not being compatible with existing MPLS, ITU-T terminates further work on T-MPLS. MPLS-TP standardisation is outcome of a joint effort between the IETF and the ITU-T. These teams work together in order to bring transport network requirements to the existing MPLS technology. The Joint Working Group (JWT) on the following main categories:

1. OAM
2. Control plane
3. Network Survivability
4. Network management

It support for end to end QoS, strict Committed Information Rate, guaranteed frame delay, frame delay variation and packet loss ratio. There is still work in Progress regarding extensions to the Label Distribution Protocol (LDP) to configure and control proactive OAM functions, suitable for dynamic Single-Segment Pseudowire (SS-PW) and Multi-Segment Pseudowire (MS-PW). (source [draft-ietf-pwe3-oam-config-01])

- **Scalability:**

1. MPLS-TP scales well with increase in end-points, number of services and bandwidth.
2. MPLS-TP is a multi-client technology that supports different technology types such as Ethernet, SDH and ATM. It provides carriers with a low-cost, highly scalable solution without the need for investing in new technology.
3. MPLS-TP uses Label Switched Paths and Pseudowires to deliver point to point services as well as point to multipoint and multipoint to multipoint services.
4. MPLS-TP interoperates with existing MPLS and pseudowire emulation edge-to-edge (PWE3) networks. It helps to extend IP/MPLS networks beyond their geographical limits to deliver end-to-end services.
5. In MPLS-TP by moving all database of network topology to a central Network Management System, it increases the scalability of the network. Automated or manual provisioning can be done with network management system.
6. OAM functions are integral part of the MPLSTP data plane and are independent from management or control plane.

- **Reliability:**

1. In case of failure in the data plane, protection switching time of LSP is less than 50 ms
2. End to end linear protection for LSP and PW layers

3. Protection State Coordination (PSC) protocol to coordinate the both ends on protection state and commands.
4. MPLS-TP network enhances the resiliency mechanism of MPLS by adding provision for OAM-triggered protection and enhancing protection in ring topologies.
5. It provides SONET/SDH like OAM and resiliency features to packet transport network - scalable operations, high availability and performance monitoring.
6. Provides 1+1, 1:1 and n: 1 protection schemes architecture.

- **Quality of Service:**

1. MPLS-TP supports number of services to enable service providers to guarantee service level agreements.
2. Flexible BW allocation
3. Provisioning end-to-end bandwidth
4. Support for delay and jitter sensitive services

- **Service Management:**

1. It provides static provisioning with NMS and dynamic provisioning with GMPLS
2. OAM and data packets are carried on the same path, it allows simpler and faster monitoring of the PW and LSP layers.
3. MPLS-TP OAM functionality can be configured by management or control plane
4. End-to-end protection scheme triggered by OAM
5. MPLS-TP uses Generic Associated Channel (G-ACh) to support Fault, Accounting, Performance and Security functions. G-ACh can be used to send traffic as well as data.

4.11 Applications of MPLS-TP

MPLS-TP is a subset of IP/MPLS designed to meet transport network operational requirements. It takes basic elements from IP/MPLS such as Pseudowire Emulation Edge to Edge (PWE3) architecture and forwarding mechanisms, and provides additional functionality such as performance monitoring, transport grade OAM, and protection switching. MPLS-TP meets functional requirements of service provider transport applications. Due to its widespread features, MPLS-TP is very flexible and can be used for many different applications:

- MPLS-TP is fully compatible with IP/MPLS networks. It can carry any type of customer traffic such as Layer3, Layer2, Layer 1, Asynchronous Transport Mode (ATM), SDH and Ethernet services.
- Applicable to situations where reliability, QoS and OAM are the main requirements.
- Converge diverse fixed and mobile services on a common high performance infrastructure
- Residential Broadband Access
- Business and Enterprise service

- Service providers can extend the MPLS edge to metro networks, and to mobile backhaul providing a single end-to-end MPLS-TP transport network.
- Integrated IP and transport platform for next-generation common access and transport solution
- Service providers are moving their metro core networks to packet transport network to support utility networks.
- MPLS-TP technology is used for service transport and mobile data backhaul
- Mobile video and IPTV
- Backhaul of mobile traffic over packet network infrastructure
- Providers are likely to adopt to MPLS-TP since they already use MPLS in their networks
- It can be operated and controlled via network management or a control plane

4.12 Advantages of MPLS-TP

- Carrier-grade and multi-vendor common packet transport network
- Supports high accuracy timing and clock
- OAM functions are independent from management or control plane
- It allows service providers to migrate all their transport services to a converged MPLS-TP core network
- Carrier-class feature such as traffic engineering, QoS, and connection oriented provisioning
- High performance timing synchronization & distribution network to meet 3G mobile requirement
- There is no IP in the forwarding plane
- Simplified service provisioning
- High reliability, equipment protection and network protection in less than 50ms
- Without requiring the use of multiple networks it can achieve different characteristics for key applications
- Provides SONET/SDH like OAM and resiliency features to packet transport network - scalable operations, high availability and performance monitoring
- Reduce network operational complexity associated with network performance monitoring and management, fault management, and protection switching
- MPLS-TP allows optimization of packet transport to reduce overall network cost, allowing a more reasonable and efficient network infrastructure
- Packet based networking with statistical multiplexing that improve bandwidth efficiency and flexibility

5 Provider Backbone Bridge –Traffic Engineering (PBB-TE)

5.1 Overview

There has been increasing demand for data services from last few years. Carriers are looking for new, less expensive methods to transmit data services, even though still guaranteeing end-to-end connections and Service level agreements. Provider Backbone Bridge Traffic Engineering (PBB-TE) is the technology developed by the IEEE with the purpose of giving service providers a Layer 2 carrier-grade transport based on Transport Carrier Ethernet Services.
There are several IEEE protocols that can be used to provide Carrier Ethernet services in metro networks:
Provider Bridge 802.1ad (PB)
Provider Backbone Bridges 802.1ah (PBB)
Provider Backbone Bridged - Traffic Engineering 802.1Qay (PBB-TE)

5.1.1 Provider Bridges (PB)

Provider Bridge also known as Q-in-Q standard targets to solve the challenging coordination of VLAN IDs between service providers and customers that is required in bridging. It allows multiple VLAN headers to be inserted into a single frame. The expanded VLAN space allows the service provider to provide certain services on specific VLANs for specific customers and yet still allow service provide to provide other types of services for other customers on other VLANs.
PB separates service provider's VLAN tag (S-tag) from customer tag (C-tag). By dong this way C-tag is untouched and the provider could differentiate customers as well as provide services. PB standard have scalability issues due to availability of only 4094 addresses in service provider network.

5.1.2 Provider Backbone Bridges 802.1ah (PBB)

Provider Backbone Bridges (PBB) was designed to solve the problem of scaling to more than 4094 services in a Provider Bridged network and provide additional capabilities. Basically, PBB adds a PBB header containing new destination and source MAC addresses also referred to as MAC-in-MAC.
A PBB re-encapsulates the PB traffic with an outer Ethernet header that includes source and destination MAC addresses of the PBB devices, i.e. service identification tag called I-SID. The I-ID is a 24-bit field that is used to uniquely identify maximum of 16 million service instances thus solving the scalability issue. PBB also provides a new feature called Backbone VLANs (B-Tag) that is used to make traffic forwarding decisions.
PBB makes customer domain completely separate from and provider domain enabling the customer Ethernet frames to be transparently transported in the carrier Ethernet frames.

Minimizing the number of MAC addresses that need to be learned reduces relearning of MAC addresses, reducing the complexity, enhanced security, enhancing end-to-end performance, and making the network more stable as far as forwarding Ethernet frames is concerned.

5.1.3 Provider Backbone Bridge – Traffic Engineering 802.1Qay (PBB-TE)

PBB-TE is a recent technology that provides a Carrier Grade Ethernet Transport network solution. PBB-TE is also popularly known as PBT (Provider Backbone Transport) and it supports connection oriented forwarding using Ethernet. PBB-TE is based on PBB as it uses layered VLANs and MAC-in-MAC forwarding scheme encapsulation. It varies from PBB in eliminating MAC learning functionality, MAC address flooding and spanning tree protocol. PBB-TE extends the functionality of PBB by adding a connection-oriented mode using point to point tunnels traversing the core from one PBB to another. Traffic engineered tunnels are created by the control plane that carry client frames across the network with deterministic service parameters like resiliency, performance and QoS.
With the use of global VLAN tags the address space is limited, so MAC learning functionality to identify source-destination pairs is disabled in PBB-TE. PBB-TE assigns a range of VIDs and MAC addresses to categorize specific paths through the network. PBB-TE takes the combination of B-VID (Backbone VLAN ID) and B-MAC (globally unique MAC address), leading to 60 bit (12+48) unique addresses. The 60-bit address is used to identify the Ethernet path for destination.

5.2 Features of PBB-TE

PBB-TE is a connection oriented packet network and its objective is to provide carrier class features over Ethernet networks. The main features of PBB-TE are:

- PBB-TE may be a new name but it’s just Ethernet, it reuses existing Ethernet header and hardware.
- Connection-Oriented Ethernet that deliver point-to-point services with high level of service reliability, manageability and scalability.
- Adapts Ethernet technology to packet transport networks
- Support Protection Switching and Traffic Engineering for deterministic point-to-point Backbone VLANs also known as tunnels
- It has ability to provision protected virtual circuits
- Maximum utilization of core network with engineered paths
- With the elimination of broadcasting packets flooding the network, the management of the network goes better
- PBB-TE is independent of service and transport layer, the services inside the tunnel could be Ethernet, IP, MPLS pseudo-wires, or VPLS.

- Allows carriers to engineer and provision deterministic, protected and secured connection-oriented tunnels and services within the Ethernet networks.
- Customer MAC addresses tunneled on provider network enhance security and scalability
- The forwarding table is statically configured by network management system.
- PBB-TE position Ethernet as replacement of the IP/MPLS networks in the metro
- It provides link protection with pre-calculated paths, which are stored on the switches. Protection path switching between working and protect tunnels aimed at 50 msec restoration of service

5.3 PBB-TE architecture

1. **Network Elements:**

A typical PBB-TE network is composed of two main network elements:

- **PBT Edge Bridge:** The edge bridge is the interface between the customer network and the service provider network. Edge bridges map frames to and from an I-SID and perform the MAC header encapsulation and de-encapsulation functions of customer's Ethernet frames. I-SID is used by Backbone Edge Bridges to multiplex and de-multiplex customer services inside Backbone VLANs.
  Frames in PBB-TE network will be switched based on the backbone destination MAC address (B-DA) and the backbone VLAN ID (B-VID).
- **PBT Core Bridge:** The core or backbone bridge is responsible for the forwarding of frames within the PBB-TE network using predefined routes according to the B-VID. These act as transit nodes, the packets are forwarded based on outer VLAN ID (B-VID) and Destination MAC address (B-DA). They achieve the usual learning of B-SA (backbone SA) addresses and build forwarding tables free of customer MAC addresses.

2. **Ethernet Switched Path**

An Ethernet Switched Path (ESP) is a provisioned traffic engineered unidirectional connectivity path within a PBB-TE network. An Ethernet Switched Path is point-to-point or point-to-multipoint.

- **Point-to-point:** There is one unidirectional connectivity path, supported by two point-to-point ESPs where the ESPs' endpoints have the same Backbone MAC addresses.
- **Point-to-multipoint:** There is a set of unidirectional connectivity paths, supported by a set of ESPs that comprises one point-to-multipoint ESP from root source to n leaf destination and a point-to-point ESP from each of the leaves to the root.

3. **Frame Forwarding**

In PBB-TE, switches don't perform spanning tree and flooding function to discover neighboring switches, hence no dynamic forwarding routes are created. Here switches are

configured with static routes by the network operator, confirming that frames take predetermined paths in the network.
The user configures all the core switches in the forwarding table using external management operation. Frames with unknown destination MAC addresses in the switch table will be dropped. In PBB-TE networks broadcast frames are not supported, so they will also be dropped by the backbone switches.

4. Network Resiliency

In PBB-TE the spanning tree mechanism is disabled and routes are configured by the network operators. In this configuration, there are two paths: working path and backup path. Backup path is enabled when and if there is a failure within working path currently carrying traffic on a PBB-TE network.
Path assignment is based on the B-VID assigned to the frames during their encapsulation at the edge switch. Network operator determines the working and Backup VLANs as well as configures the routes that each VLAN must take on the network. In case when a backbone bridge does not receive a CFM (Connectivity Fault Management) message after a definite interval of time, link failure is expected. Frames are then automatically forwarded using the backup path within 50 ms.

5.4 PBB-TE Frame Format

PBB-TE extends the functions of PBB by addition of T-DA, T-SA and T-IID fields to existing PBB frame format. T-SA and T-DA is TE-Service addresses that identify the Traffic Engineering endpoints. T-IID is Service Instance identifier and part of TE service Instance Tag.

T-DA	T-SA	T-IID	B-DA	B-SA	B-VID	I-SID	DA	SA	S-VID	C-VID	Payload

Figure 4: 802.1 Qay (PBB-TE) Frame Structure

There are following fields in PBB-TE Frame structure:

SA: Source Address
DA: Destination Address
T-DA: TE-Service DA
T-SA: TE-Service SA
T-IID: TE-Service Instance Identifier
B-DA: Backbone DA
B-SA: Backbone SA
B-VID: Backbone VLAN ID

I-SID: 24-bit Service ID
S-VID: Service VLAN ID
C-VID: Customer VLAN ID

PBB-TE uses a 60-bit label composed of B-VID + B-DA to forward on the B-VLANs allocated for PPB-TE. B-DA, B-SA and B-VID fields are used for forwarding the frames in the backbone network. B-VID identifies a specific path through the network, in combination with the B-DA address. A service is identified by an I-SID and by controlling the mapping of I-SID to different B-VID, allows the service provider to separate the topologies used by different customers.

5.5 PBB-TE QoS

In PBB-TE networks, all QoS techniques that are developed for Ethernet are appropriate. PBB TE enhances support to PBB for deterministic paths and offers the feature set desirable for providing bandwidth guarantees, resilience and QoS. Bandwidth guarantee is handled by the external control plane and its efficiency depends on different dealer methodologies. PBB-TE technology discards the STP technology and source address learning mechanism. It sets up a QoS-guaranteed Ethernet switched path (ESP) for transport services that should be established through the network management system or manually according to the user's service requirements. PBB-TE is connection-oriented with every ESP having certain Traffic Engineering attributes and QoS assurance.

Traffic flows are allocated a unique I-Tag (Instance Tag) that allows carrier to identify QoS levels and define a unique customer identifier (I-SID). The Service Instance ID (I-SID) identifies every service, when it is combined with the Backbone MAC Address and Backbone V-LAN ID it shows which service is being provided to particular customer at specific time, they can be anywhere in the network. The deterministic paths of PBB-TE make the admission control procedure of QoS.

PBB-TE delivers several features required for QOS:

- PBB-TE frame is self-identifying, that is it can be extracted from anywhere in the network and by viewing at different fields, one can exactly know about:

1. From where frame is coming
2. Where that frame is going
3. Path it is taking
4. Action or service it is delivering

- PBB-TE can separate customer and service provider domains.
- Its deterministic nature makes the traffic more predictable and QOS mechanisms are more competent.
- I-Tag is assigned per customer and QoS can be performed per customer instead of per VLAN.

5.6 PBB-TE OAM

OAM has remained the main concern from long time for the service providers those were looking at Ethernet as a carrier technology. PBB-TE defines mechanisms for protection switching of bidirectional Ethernet connections. It can provide carrier-class OAM without support from other layers by using a Connectivity Fault Management (CFM) OAM mechanism. CFM is an essential component of the PBB TE protection mechanism, CCM messages should be triggered for both primary and backup tunnels. The speed of PBB TE protection switching is determined by the frequency of CCM messages. The PBB-TE packets are self-describe and it is ideal for in band OAM, traces and flow monitoring.

5.6.1 OAM Functionality

OAM tool facilitates path discovery, fault detection, fault verification, fault notification, and fault recovery.

- **Continuity Check (CC)**
    1. Fast detection of loss of connectivity and misconnections
    2. Continuity check messages (CCMs) are used over each path for fault-detection-triggering notification.
- **Loopback – Connectivity Check (unicast & multicast)**
    1. Unicast bi-directional request/response
    2. Used for Fault verification and to check reachability to different points
- **Traceroute (Link trace)**
    1. Usage for Fault Isolation
- **Alarm Indication Signal (AIS)**
    1. Fault localization
    2. Alarm suppression
- **Performance Monitoring**
    1. Frame Delay
    2. Frame Loss
- **Remote Defect Indication (RDI)**
    1. Indicator for Fault Detection

5.6.2 Connectivity Fault Management

CFM is an end-to-end per service instance OAM protocol that checks the liveliness of Ethernet networks including the connectivity monitoring and fault verification. PBB-TE uses CFM as the main failure detection mechanism. CFM continuity check messages are received at particular intervals, In the event that a core device does not obtain a CFM message after a particular interval, a failure in the link is expected. Frames are then automatically forwarded using the

protection path within 50 ms. Different organizational domains implement CFM functions to detect, isolate, and correct connectivity faults with minimum access to other equipment. PBB-TE CFM functions are as follows:

- **PBB-TE path continuity fault detection:** Between two end-points of PBB-TE path, Administrator uses continuity check protocol to detect continuity break.
- **PBB-TE path continuity fault verification**: Loopback messages and traceroute protocol are used to verify connectivity between two end-points of PBB-TE path.
- **PBB-TE path continuity fault localization:** Isolate fault location when connectivity fault after the fault is detected.
- **PBB-TE path continuity fault notification:** End point prompts spontaneous fault notification when it detects connectivity fault in the maintenance association.
- **PBB-TE path continuity fault recovery:** Connectivity faults can be recovered by administrator's activities.

5.7 Traffic Protection and Restoration

PBB-TE supports complete path backup, and provides good protection and traffic engineering. It supports a protection path switching capability similar to MPLS path protection to provide resilient connections. PBB-TE path fault analysis and protection triggering are all completed on the data plane and corresponding sub-50ms switchover takes place.

PBB-TE provides end-to-end linear protection for point-to-point and point-to-multipoint ESP with 1:1 path protection. It not only allows the service provider to provision a point-to-point Ethernet tunnel, but too provisions an additional backup tunnel to provide resiliency.

The PBB-TE path protection mechanism uses two deterministic paths working and backup. Traffic is automatically switched from working to a backup path when the failure of a primary path is detected. Protection switching requires that both the working and protection tunnels are monitored and this is accomplished with CCM. Continuity Check messages are sent over both the Working and backup paths, these messages are used to determine failure events and cause protection switching. PBB-TE networks results in very scalable with guaranteed paths and ability to provide guaranteed bandwidth for customer traffic.

5.8 PBB-TE meets the Carrier Ethernet attributes defined by MEF

- **Standardised Services:**

1. The PBB-TE standard is based on Nortel technology known as PBT (Provider Backbone Transport).
2. The IEEE standardizes PBB-TE in 2009 by ratifying the 802.1Qay specification.

3. PBB-TE enhances the Provider Bridge (PB) and Provider Backbone Bridges (PBB) with support for traffic engineered paths called Ethernet switched paths (ESPs) and support for 1:1 protection switching.
4. Its pre-determined paths guarantee service performance and QOS mechanisms are more competent.
5. Traffic flows are allocated a unique I-Tag (Instance Tag) that allows carrier to identify QoS levels and define a unique customer identifier (I-SID).

- **Scalability:**

1. PBB-TE supports up to 16 million customer services.
2. Separates the provider core switches from customer VIDs and customer MAC addresses.
3. There is no customer MAC learning as the Destination MAC is based on a Provider MAC address.
4. Reuses the existing Ethernet forwarding plane
5. Combination of destination MAC + VLAN identifies uniquely the PBB-TE circuit.
6. PBB-TE has good manageability as it supports the newest Ethernet OAM functionality.
7. Maximum utilization of core network with engineered paths.
8. No undesirable broadcast functionality that creates MAC flooding and limits the size of the network as MAC learning feature is disabled.
9. Independent of service and transport layer, the services inside the tunnel could be Ethernet, IP, MPLS pseudo-wires, or VPLS.

- **Reliability:**
    1. Allows carriers to engineer and provision deterministic, protected and secured connection-oriented tunnels and services within the Ethernet networks.
    2. Provides 50ms protection switching.
    3. Fast notification of end-to-end connectivity failure.
    4. PBB-TE provisions backup tunnels.
    5. Self-identifying frame leads to easier fault management
    6. PBB-TE separates customer and service provider domains.
    7. No learning of customer MAC address at the provider backbone bridges
    8. Customer’s separation is provided by unique PBB I-SID, no customer can interrupt the privacy of other customer.

- **Quality of Service:**
    1. I-Tag is assigned per customer and QoS can be performed per customer instead of per VLAN.
    2. Service providers can define and uphold a clear service level agreement (SLA) for each customer flow, in a consistent manner.

3. PBT tunnels reserve suitable bandwidth and support the provisioned QoS metrics that guarantee SLAs.
4. Provider networks depends on path routing so that traffic engineering can be used to allocate bandwidth and select path performance as required by service level agreements.

- **Service Management:**
  1. Enables more effective alarm correlation, service-fault management and service-performance correlation.
  2. PBB-TE packets are self-describe and it is ideal for in band OAM, traces and flow monitoring.
  3. Strong service management when combined with Traffic Engineering & Service Assurance.
  4. PBB-TE uses Connectivity Fault Management (CFM) as the main failure detection mechanism.
  5. Comprehensive Performance Monitoring allow simple to achieve SLAs.

5.9 Applications of PBB-TE

PBB-TE has definite benefits over classical Ethernet inter router links because of its resilience, manageability and TE functionality. Protection capability supports the applicability of PBB-TE networks in different Services:

1. **Business Services :** E-Line services, Backhaul to L3 VPN
2. **Wholesale Services :** Wireless backhaul, High bandwidth backhaul including WiMAX
3. **Residential Services :** Internet Access, Voice over IP (VoIP), Broadcast Video
4. **Mobile backhaul:** Present mode of operation, Ethernet Access and Backhaul
5. **Core Transport :** Core Point-to-Point Connections
6. Frame based expansion and replacement of TDM/SONET
7. Interworking to other Point to point services
8. Low cost edge aggregation with resiliency
9. Adding traffic engineering to PBB networks
10. Targeted to support mission-critical and latency sensitive practices
11. Native end-to-end transport of layer 2 services
12. Backhauling of mobile and Data center
13. PBB-TE is a major replacement of TDM-based solutions for mobile operator’s backhaul as it provides deterministic paths with several classes of service and bandwidth guarantees that are important for transferring delay-sensitive voice traffic.
14. It offers a cheap and effective way to connect base stations to a central station

5.10 Advantages of PBB-TE

There are several characteristics of PBB-TE that make it attractive to many vendors and providers:

1. PBB-TE technology brings the highly required cost-effectiveness and simplicity of the technology to core carrier networks. Architecture is simple to manage and provision protected virtual circuits.
2. Provides carriers with the scalability, reliability and granularity of service they require while taking advantage of the wide acceptance and low operating costs of Ethernet.
3. PBB-TE requires no changes to the data plane frame forwarding behavior defined for a PBB, this makes PBB-TE attractive to bridge vendors.
4. Delivers guaranteed bandwidth and deterministic performance in aggregation with end-to-end timing protocol.
5. PBB-TE enable carriers to reduce the cost of metro transport networks by replacing IP/MPLS with lower cost Ethernet.
6. Use simpler network tools based on Layer 2 network equipment which makes it less expensive than MPLS.
7. Single-ended Provisioning in which only the end-nodes are provisioned
8. Service Level Agreement capable Ethernet connections
9. PBB-TE have simple control plane as compared to the complicated IP/MPLS protocols.
10. Low cost edge aggregation with resiliency
11. Customer Separation & Service Scalability – PBB provides 16 million unique service identifiers, apart from providing 2 transport tunnels.
12. There are CAPEX Savings and OPEX Savings up to 40-65%

5.11 Limitations of PBB-TE

1. PBB-TE only supports point-to-point Ethernet services (P2P and MP2P); it is short of meeting significant packet transport requirements multiservice support and MP2MP connectivity. This results in inefficient management of the bandwidth in triple play networks.
2. VPLS services over PBB-TE tunnels cannot work as it disables the MAC learning function.
3. All the resource reservation functions required to be controlled by the network administration. Thus, the NMS requires high scalability or the network needs to use signaling in the control plane.
4. It adds complexity to the network by using PBB in the core and also, it has difficulties with scalability and STP restoration in the edge.

6 Optical Transport Network (OTN)

The optical transport network (OTN) was standardized in 2001 by the ITU-T (as specified in G.709). It was designed with the purpose of combining the benefits of SONET/SDH with the

bandwidth expanding capabilities of dense wavelength division multiplexing (DWDM). OTN was created to be a carrier technology and importance was given to enhance transparency, scalability and monitoring of signals carried over large distances over several domains. Transport of Ethernet frames over OTN is highly transparent. Optical Transport Network (OTN) ITU-T standards are:

1. Architecture of Optical Transport Network (G.872)
2. Interfaces for the Optical Transport Network (G.709)
3. Characteristics of OTN hierarchy equipment functional blocks (G.798)
4. Linear protection switching (G.873)
5. Management aspects of Optical Transport Network element (G.874)
6. Control of Jitter and Wander within the OTN (G.8251)

OTN improves transport network performance, bit rate efficiency and resiliency at high capacity. It offers innovative optical communication technologies such as optical paths and forward error correction (FEC). The FEC helps reduce the number of transmission errors on unreliable channels, extending the transmission of traffic for longer distances.

6.1 Introduction

There is continuous progress in traffic resulting from the shift from voice traffic to data traffic, to support this WDM systems based on the OTN are now being deployed. OTN offers many features that will help enable the transparent transport of growing packet traffic and support services such as wavelength services that require strong service level agreements.

The ITU-T defines OTN as follows: “An Optical Transport Network (OTN) is composed of a set of Optical Network Elements (ONE) connected by optical fiber links, able to provide functionality of transport, multiplexing, routing, management, supervision and survivability of optical channels carrying client signals.”

ITU-T Recommendation G.709 defines rates and formats chosen for the OTN that describes a means of communicating data over an optical network. Different issues of G.709 were released

- Issue 1 of G.709 (Released in 2001): With the goal of providing a set of references that covered all aspects of optical networking including rates and formats, and optical WDM. Its clients were STM-N, ATM, IP and Ethernet.
- Issue 2 of G.709 (Released in2003): OTN has been enhanced to keep pace as there have been various changes in the networking world with time. It define different features that are ODU0 (optical channel data unit) and TTT (timing transparent transcoding).
- Issue 3 of G.709 (Released in2010): With the increased demand, development, and deployment of OTN technologies there have been several improvements to fulfill the desire to have greater packet client related features. It defines several new features that include ODUflex (CBR), ODUflex (GFP), OTU/ODU/OPU4, delay measurements capability and Multistage Multiplexing.

OTN is also commonly called digital wrapper as it multiplex data streams from several sources into optical light paths. It provides a common way of managing different client signals into a single entity that is managed through a lesser amount of overhead in a multi-wavelength system. It provides improved reliability than the previously dominant architecture SONET/SDH, and provides the ability to build a carrier's carrier network. ITU has worked a lot to define standardized methods for transporting various Ethernet rates over the OTN. These include 2G Ethernet, 10G Ethernet, 40G Ethernet and 100G Ethernet. It has capabilities essential to monitor, manage, and control each client signal transported in the network.

6.2 Features of OTN

- Combines the benefits of SONET/SDH with DWDM bandwidth-expanding capabilities.
- Eliminates traditional TDM transport complexity and related costs.
- Adds operations, administration and maintenance (OAM) and provisioning capabilities to optical carriers.
- Interconnection of different administrative areas and ability to perform multiplexing at very high data rates.
- Transparent transport of different Ethernet frames over OTN
- No MAC learning, forwarding or filtering is performed.
- FEC improves error performance and extends the transmission of traffic for longer distances.
- First transmission technology in which each stakeholder gets its own Optical data unit connection monitoring.
- Performance monitoring and alarm supervision
- Provides a service independent, network-to-network interface for transiting the multiple transport domains among multiple providers.
- Higher rates specification such as 2GbE, 10GbE, 40GbE, and 100GbE.
- It provides a mechanism to separate client and network optics, providing both capital cost and operational cost efficiency.
- Offers simplified fault isolation and improved troubleshooting.
- Improved vendor interoperability and intelligent on-demand provisioning.
- Simplifies end-customer network management
- Enables network scalability as well as support for dedicated Ethernet services.
- To use wavelengths efficiently OTN allows service providers to efficiently prepare client traffic into higher rate containers such as OTU1, OTU2, OTU3 and OTU4.

6.3 OTN Architecture

Optical transport network (OTN) architecture has been defined by ITU –T G.872 based on OTN frames that define techniques for mapping client signals onto the Optical Channel via layers.

OTN consists of the following layers:

- Optical Channel (OCh)
- Optical Multiplex Section (OMS)
- Optical Transport Section (OTS)
- Optical Channel Payload Unit (OPU)
- Optical Data Unit (ODU)
- Optical Transport Unit (OTU)

Each of these layers and their functions are distributed along the network and activated when they reach their termination points. These Layers within an OTN are illustrated in Figure 1 below.

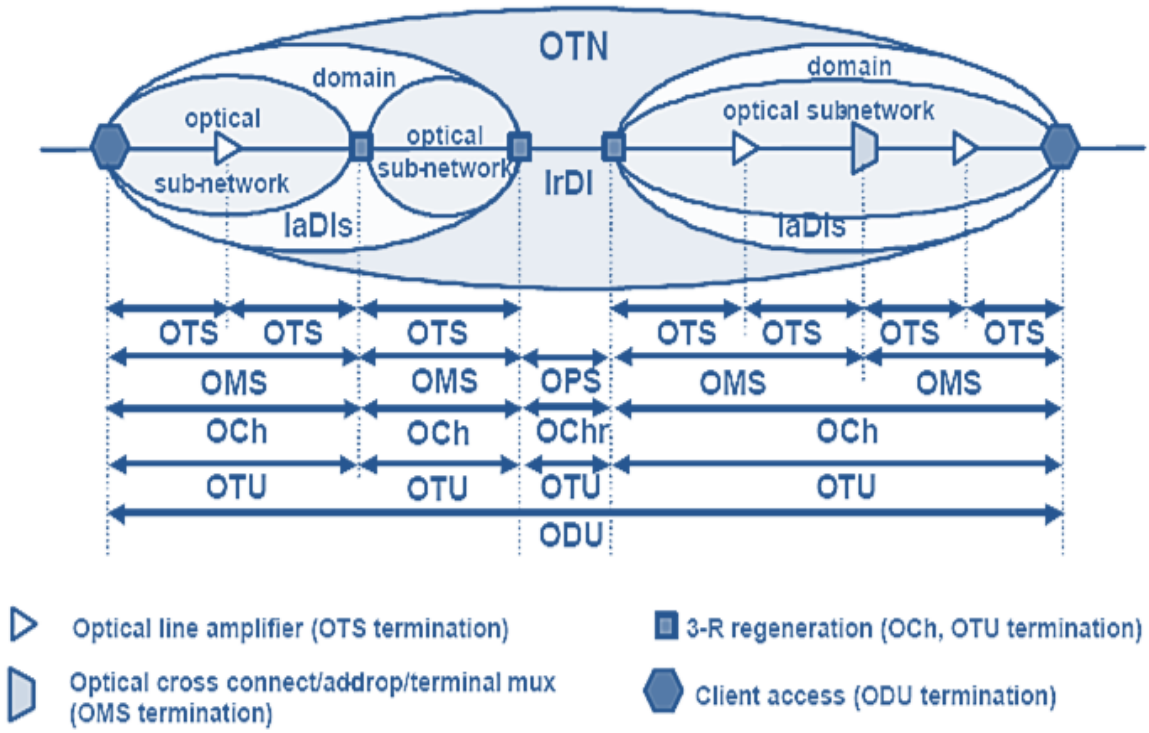

Figure 5: OTN Network Layers [20], p.19

Optical Transport Hierarchy (OTH) contains two distinct Domains:

- Optical Domain
- Digital Domain

- **Optical Domain:** It is based on the network architecture defined in different recommendations G.872 on architecture and G.709 on frames and formats. OTH includes the roles and interactions of the Optical Transport Network unit layers end to end.

1. **Optical Channel (OCh):** OCh represents end to end optical network connection between two nodes. It carries core traffic and terminates at the edge nodes; also it performs the electrical to optical signal conversion.
2. **Optical Multiplex Section (OMS):** OMS is the section between optical multiplexors and de-multiplexors. It is intended to support the connection monitoring and assist service providers in troubleshooting and fault isolation. It multiplexes several wavelengths, each carrying one OCh into one fibre.
3. **Optical Transport Section (OTS):** OTS is the optical section in between optical line devices and any network elements in the OTN, including amplifiers. It allows the network operator to perform monitoring and maintenance tasks between Network Elements.

- **Digital domain:** It is also known as the digital wrapper and it offers specific overhead to manage the OTN's digital functions. The digital OTN layered structure is comprised of:
  1. **Optical Channel Payload Unit (OPU):** OPU is transparent client data transport and contain a header describing the type of data. It encapsulates the client signal asynchronously into the OTN frame, and adjusts the client signal rate to the OPU rate if needed.
  2. **Optical Data Unit (ODU):** ODU consists of the OPU and the ODU overhead. It provides multiplexing, optical path level monitoring, alarm indication signals, maintenance signals protection switching, end-to-end path supervision and tandem connection monitoring.
  3. **Optical Transport Unit (OTU):** OTU is the highest multiplexing level in the digital domain. It adds Forward Error Correction and performance monitoring. By adding FEC to the network elements OTN allows operators to reduce the number of required regenerators used in the network leading to reduced network costs.

6.4 OTN Frame Structure and Overhead

When data is transmitted in an optical transport system, the receiving equipment must be able to identify its block boundaries. In every frame, frame bytes are transmitted that helps to identify the starting point in the OTN.

The OTU framing is divided into two portions:

1. **Frame alignment signal (FAS):** It is 6-byte signal and are transmitted unscrambled. It is used to provide framing for the entire signal.
2. **Multiframe alignment signal (MFAS):** It is used to extend command and management functions over several frames. MFAS is continuously incremented frame after frame from 0 to 255. Some overhead signals span multiple frames and use this signal to lock to a common multi-frame.

- **OTN Frame Structure:** OTN frame structure is structured in a block frame structure with four rows and 4080 columns. Each portion of the frame has its own specific overhead functions. These overhead bytes provide path and section performance monitoring, alarm indication, monitoring end-to end signal quality and protection switching capabilities. There are three overhead areas in an OTN frame they are described below:

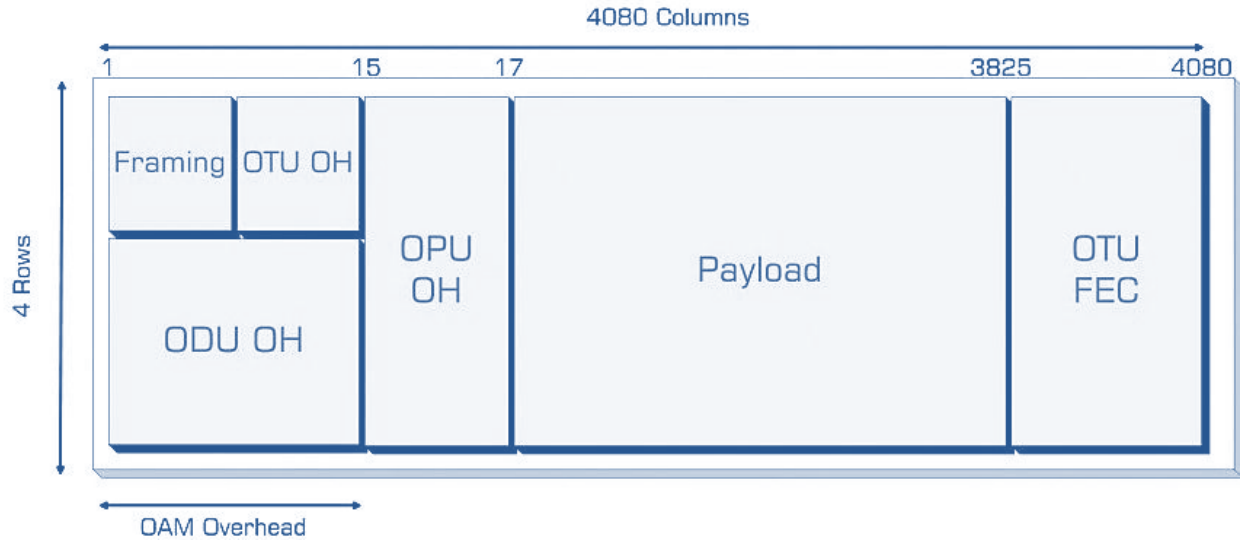

Figure 6: OTN Frame Structure [18], p.1

1. **Optical Transport Unit (OTU) Overhead:** The OTU overhead provides FEC and supervisory functions. Also, it conditions the signal for transport between 3R (re-timing, reshaping and regeneration) optical channel termination points. The OTU overhead is comprised of the SM, GCC0 and RES bytes.
    - **Section monitoring (SM):** It consists of 3 bytes that are used for the trail trace identifier (TTI), Error detection code (BIP-8) and the backward error indication (BEI).
    - **General communication channel 0 (GCC0):** It is two byte communication between section end points. This clear channel used for transmission of information between OTU termination points.
    - **Reserved bytes (RES):** These are the two bytes reserved for future use.

2. **Optical Data Unit (ODU) Overhead:** The ODU overhead provides end path supervision and supports tandem connection monitoring. It is broken into several fields:
    - Reserved Bytes (RES)
    - Path Monitoring (PM)
    - Tandem connection monitoring (TCMi)
    - Tandem connection monitoring activation/deactivation (TCM ACT)
    - Fault type and fault location reporting communication channel (FTFL)

- Experimental field (EXP)
- General communication channels 1 and 2 (GCC1/GCC2)
- Automatic protection switching and protection communication channel (APS/ PCC)

3. **Optical Payload Unit (OPU) Overhead:** OPU overhead is added to support the adaptation of the various client signals for transport over an optical channel. The OPU overhead consists of the following fields:
   - **Payload Structure Identifier (PSI):** PSI is a primary overhead field defined to transport a 256-byte message aligned with MFAS.
   - **Payload Type (PT):** It contains the PT identifier that reports the type of payload being carried in the OPU payload to the receiving equipment.
   - **Multiplex Structure Identifier (MSI):** This field is located in the mapping-specific area of the PSI signal and it is used to encode the ODU multiplex structure in the OPU.
   - **Justification Control (JC):** The justification overhead bytes are used to make the justification decision in the mapping/demapping process of the client signal to protect against error.

4. **Forward Error Correction (FEC):** The ITU G.709 standard supports forward error correction (FEC) in the OTU frame. FEC uses the Reed-Solomon RS (255,239) coding technique. FEC provides a method to reduce the number of transmitted errors due to noise. It has been proven to be effective in systems limited by optical signal-to-noise ratio and dispersion. The FEC improves the Optical Signal-to-Noise Ratio (OSNR) by 4 to 6 dB, resulting in longer spans and fewer regeneration requirements.
   FEC is most utilised to improve the resiliency of point to point wavelength services and for burst errors where up to 128 consecutive bytes can be corrected per OTU frame. FEC can correct up to eight byte errors and detect up to 16 byte errors in the code.

6.5 OTN Interfaces and Rates

The ITU-T G.709 standard defines interfaces and rates. OTN data rates were constructed so that they could transfer SONET/SDH signal efficiently.

G.709 Interface	OTU rates	ODU rates	OPU rates
0		1.24 Gb/s	1.24 Gb/s
1	2.66 Gb/s	2.48 Gb/s	2.48 Gb/s
2	10.71 Gb/s	10.03 Gb/s	9.95 Gb/s
3	43.01 Gb/s	40.31 Gb/s	39.81 Gb/s
4	111.80 Gb/s	104.79 Gb/s	104.79 Gb/s

Table 6.1 OTN Interfaces and Rates [20], p.20

6.6 OTN QoS

Quality of Service allows TDM network utilisation and traffic monitoring that is engaged in end-to-end traffic engineering. In OTN Tandem Connection Monitoring (TCM) is used to monitor end to end and various domains QoS. Transport capacity and traffic statistics are important to QoS that are defined in traffic contract and agreed between user and network.
The OAM&P overhead added by G.709 supplements the QoS of WDM and DWDM equipment. ODU switching and multi stage ODUk mapping offer more flexible and integrated way to perform circuit switching in a large-scale, cross-domain and IP-over-DWDM network. It makes it possible to deliver dedicated capacity with a high level of Quality of Service (QoS) to the user. To offer end-to-end traffic engineering, the following capabilities are included in the layer network:

- **Optical channel supervisory functions:** for supporting network level operations and management functions, such as connection provisioning and quality of service network survivability.
- **OTN multiplexing and switching capabilities:** offer the desirable granularity for delivery of packet based dynamic services with very specific requirements for Quality of Service (QoS).

6.7 OTN OAM

OTN adds operations, administration, maintenance, and provisioning (OAM&P) functionality to optical carriers, especially in a multi-wavelength system such as dense wavelength division multiplexing (DWDM). As a result it improves the performance of WDM networks in network administration. OTN provides rich overhead resources and allows management and control plane interaction with the optical layer.
OAM features of OTN are similar to SONET/SDH allowing end-to-end service monitoring across multiple domains. In addition, some advanced fault management and performance monitoring mechanisms are added into OTN to provide carrier-class QoS guarantee. It certainly understands the industry looked for networking capacity of building multiple-ring, mesh or star topology networks.
OTN has several important OAM features:

1. **Forward Error Correction (FEC):** FEC enables the detection and correction of bit errors caused by impairments in the transmission medium. FEC considerably increases the maximum span and signal resilience of the link in optical domain, an optical path can cross more transparent optical network elements.. It allows an OTN receiver to correct errors in the received OCh signal, which in turn allows an optical path to be resilient to

defects. It decreases the number of retransmits due to transmission errors and improves overall network efficiency.

2. **Connectivity Verification:** It provides a method to identify misconnections, with procedure based on emitting a Trace Trail Identifier (TTI) that is known by both endpoints. The TTI is included for each connection and then receiver node compares the received TTI with the expected value and decides if a misconnection happened.
3. **Continuity Check:** It provides methods for monitoring the status of the service connection.
4. **Tandem Connection Monitoring (TCM):** TCM allows the user and its signal carriers to monitor the quality of the traffic that is transported through several administrative domains. In a multi domain scenario where the originating domain can't ensure performance or unable to monitor the signal when it passes to another domain, TCM add a performance monitoring layer between line and path monitoring allowing each network to be monitored, therefore reducing the complexity of troubleshooting.
5. SONET/SDH allowed a single level of TCM to be configured, while ITU G.709 allows six levels of independent TCM to be configured. TCM layer is used for Connectivity Verification, Performance Monitoring and Protection/Restoration triggers.
6. **Maintenance Signals:** These signals are used in OTN for fault isolation and alarm suppression, and can avoid repeated alarms. Management and Alarm information is used to locate and diagnose the fault, to trace paths, and monitor tandem connections.
7. **Path Monitoring:** OTN enables path monitoring at multiple layers and user-defined endpoints, allowing carriers to guarantee customer Service Level Agreements (SLAs). In OTN TCM bytes provide path monitoring function. There are up to six different levels of TCM bytes available in the OTN overhead, these bytes allow carriers to define their own path layers. TCM layer Used for Connectivity Verification, Path Monitoring, Protection/Restoration triggers.
8. **Q Factor:** Q factor reproduces the quality of optical communications signal. It is mainly used measurement technique for measuring coding gain. Q factor compares the good quality received signal with the total received power, channel input Signal to Noise Ratio (SNR/OSNR). It has fast measurement time and helps in improving the performance monitoring of optical channel.

6.8 Traffic Protection and Restoration

OTN protection schemes are similar to those defined by SONET and SDH networks. OTN Protection occurs on the service level that makes it possible to apply different measures to traffic with different QoS. OTN technology provisions the complete variety of protection methods to prevent failures and speed up recovery times. OTN switching moreover supports practices such as hold-off timers to avoid the triggering of several protection actions and wait-to restore timers that automatically restores the original traffic configuration when estimated.

Protection Switching components detect a loss of optical signal and automatically switch from the working path to the protection path. Protection paths are constructed in the network using ring topology and dual nodes. Protected OTN traffic switched over a packet recover from failure conditions within 50ms.
ITU Recommendation G.873.1 defines the Automatic Protection Switching protocol (APS) and Protection Communication Channel (PCC) for the linear protection schemes for the Optical Transport Network at the Optical Channel Data Unit (ODUk) level.

Protection Schemes in OTN:

- **Linear Protection:** Protection switching occurs only at end nodes (head end and tail end) of a protected subnetwork connection. Head end is capable of performing bridge function, sending a copy of the traffic signal along the protection path. Tail end does a selector function that selects traffic signal either from working entity or from a protection entity. Linear protection is mostly used for low density of population.
- **Ring Protection:** In ring protection every node of the ring performs a protection activity. OTN ring protection is currently being developed in the ITU draft G.873.2. Ring protection is mostly used for medium density of population.
- **Shared Mesh protection:** Shared mesh protection allows a number of customer circuits among a specific start point and specific end point to grow in real-time. It dynamically adjusts capacity of a protection circuit based on the number of customer circuits. They offer greater spatial diversity, shorter routing and eliminate the rigidity of the ring topologies. Shared Mesh protection is used mostly for high density of population.

Automatic Protection Switching (APS) is a capability of carrier grade transport networks that provides the fault tolerance and high reliability which is needed to support various services.
Functions of APS include:

- Detection of signal failures on a working channel
- Switching traffic to a protection channel
- Once the failure is repaired then returning back to the working channel

APS is a general term for three different protection switching architectures:

- **1+1:** Every single traffic channel is protected by a single protection channel. Head end Bridge is permanent and sends data on both channels. Tail end chooses the channel to use.
- **1: N:** N numbers of working channels are protected by a single protection channel where the bridge at the head end is not permanent. When there is failure on the primary channel, both source and destination switches to the alternate channel.
- **M: N:** In this M protection channels are established to protect N different working channels.

6.9 OTN meets the Carrier Ethernet attributes defined by MEF

- **Standardised Services:**
  1. OTN was developed by the ITU's Telecommunication Standardization Sector (ITU-T) as a way of enhancing traffic efficiently whereas at the same time coping with a new traffic combination.
  2. OTN offers a solution to the converged transparent transport of TDM, packet and broadband services.
  3. It goes beyond point-to-point wavelength services by applying a more flexible architecture based on Optical Channel Data Units (ODU).
  4. OTN (G.872) has standardized a Digital Wrapper solution for its optical payload unit (OPU) hierarchy to report wavelength related issues.

- **Scalability:**
  1. OTN technology provides efficiency and scalability for a wide range of service and client types.
  2. It has extreme scalability and flexibility to adopt new service types protects investments.
  3. OTN is designed to carry a payload of larger bulk, its granularity is coarser and the multiplexing structure is less complicated.
  4. Offers customers full end-to-end transparency
  5. OTN assigns a dedicated amount of bandwidth to each application and each application has its own layer with guaranteed bandwidth.
  6. Transparent switching of DWDM line capacity
  7. Provides a service independent, network-to-network interface for transiting the multiple transport domains among multiple providers.

- **Reliability:**
  1. OTN has mesh and ring structure that guarantees a supreme degree of reliability because if one node fail then the other node take over immediately, thus keeping the whole network working.
  2. Enhanced OAM for wavelengths
  3. OTN technology provisions the complete variety of protection methods to prevent failures and speed up recovery times.
  4. OTN nodes offers redundancy of the main components such as power supplies, common logic cards and optical modules.

- **Quality of Service:**
  1. Tandem Connection Monitoring (TCM) is used to monitor end to end and various domains QoS.
  2. Simplifies end-customer network management
  3. Through use of OTN Control Plane mesh it has New Service Level Agreement options.

- **Service Management:**
  1. FEC that is provided in the OTU frame allows detection and correction of line bit errors.
  2. Fast provisioning via end to end OTN
  3. OTN Network Management System (OMS) controls the network and reduces the risk of errors.
  4. Trail Trace Identifier (TTL) supports provisioning of transmitted and anticipated values and allows retrieval of accepted value.
  5. Adds operations, administration and maintenance (OAM) and provisioning capabilities to optical carriers.

6.10 Applications of OTN

1. OTN offers large amount of bandwidth that make it perfectly suited for video applications.
2. OTN is designed to be much more suited to hybrid networking and various Ethernet, TDM, and DWDM network infrastructures.
3. Transport data packets such as Ethernet, MPLS, IP or SDH/SONET over OTN using Generic Framing Procedure (GFP).
4. Multi-protocol and multi-service Ethernet services are offered over public transport networks.
5. OTN is used in Long-Haul DWDM and Point of presence scenarios.
6. In OTN each application has guaranteed bandwidth therefore CCTV, telephony and other applications run smoothly on the OTN, without interfering with each other.

6.11 Advantages of OTN

OTN offers networks with more powerful switching, mapping and survivability functionality in the digital area compared to SDH. OTN offers the following advantages that make it attractive:

1. Performs multiplexing for best possible capacity utilization, thus improving network efficiency.
2. More levels of Tandem Connection Monitoring (TCM) that allows a major improvement in performance monitoring signals and enhanced maintenance for signals transported through several operator networks.
3. Assigns dedicated amount of bandwidth to each application.
4. OTN provides digital wrapper, a common way of managing different client signals into a single entity that is managed through a lesser amount of overhead in a multi-wavelength system.
5. OTN provides a stronger FEC code than the one existing with SONET/SDH, allowing improvement of the Signal-to-Noise Ratio (SNR) by 6.2 dB. This allows improved bit error rate and link reliability in long span amplified links.

6. End to end optical transport transparency of signals encapsulating all client-management information protects the network against uncertain service grouping.
7. Better switching scalability as granularity is coarser and the multiplexing structure is less complicated.
8. When joint with intelligent control plane it supports automated mesh connectivity and 50ms traffic restoration for different clients like Ethernet, OTN, SONET and SDH.
9. OTN reduces CAPEX through common transport framework and also reduces OPEX through network simplification and integration.
10. OTN adds operations, administration and maintenance and provisioning (OAM&P) capability and troubleshooting functionality to optical carriers.
11. Support for dedicated Ethernet services with higher rates specification such as 2GbE, 10GbE, 40GbE, and 100GbE.
12. It has all the capabilities required for reliable service provisioning and to monitor, manage, and control each client signal transported in the network.
13. Universal high rate containers such as OTU1, OTU2, OTU3 and OTU4 supporting any service type.
14. Low latency and low jitter

6.12 Limitations of OTN

OTN has the some limitations:

1. Requires new hardware and management system.
2. OTN networks can't be oversubscribed — that is total capacity of offered circuits cannot exceed that of the link, thus the efficiency gains that come with influencing oversubscription are vanished.
3. OTN need Layer 2 provision at the edges to pack the ODU0s.

7. Comparison and Contrast between different Carrier Ethernet Technologies

In this segment there is Comparison and Contrast between different Carrier Ethernet Technologies described in the project. The question then arises: Which is the better Technology for services delivery? It depends upon different carrier-class functions and flexibility to support different situations like infrastructure, architecture, technology, and so on. This segment will exhibit key features of different types of technologies based on following measures:

- Standardisation
- Carrier Ethernet Services
- Scalability
- Connectivity

- OAM
- QoS/ Traffic engineering
- CAPEX and OPEX
- Reliability
- Manageability
- Comparing Data plane and Control plane

7.1 Standardisation

EoMPLS	MPLS-TP	PBB-TE	OTN
EoMPLS is an IETF standard-track protocol based on the Martini draft. IETF standardise MPLS, pseudowires, and VPLS (VPLS-LDP and VPLS-BGP) to guarantee that service providers can develop practical equipment that offers EoMPLS services.	Firstly, the ITU-T started to enhance MPLS for transport networks under the name T-MPLS. Due to concerns about T-MPLS not being compatible with existing MPLS, ITU-T terminates further work on T-MPLS. MPLS-TP standardisation is outcome of a joint effort between the IETF and the ITU-T. There is still work in progress regarding extensions to the LDP to configure and control proactive OAM functions, suitable for dynamic Single-Segment Pseudowire (SS-PW) and Multi-Segment Pseudowire (MS-PW).	The PBB-TE standard is based on Nortel technology known as PBT (Provider Backbone Transport). The IEEE standardizes PBB-TE in 2009 by ratifying the 802.1Qay specification.	OTN was standardized in 2001 by the ITU-T (as specified in G.709). It was designed with the purpose of combining the benefits of SONET/SDH with the bandwidth expanding capabilities of DWDM.

Table 7.1 Standardisation

7.2 Carrier Ethernet Services

Feature	EoMPLS	MPLS-TP	PBB-TE	OTN
Clients	Ethernet, ATM, Frame Relay, PPP and TDM across a common IP/MPLS networks.	Ethernet, ATM, Frame Relay, PPP and TDM across a common IP/MPLS networks.	Ethernet, IP and VPLS.	Ethernet, SDH/SONET, ATM, IP and Fibre Channel.
Network Services	Multiservice IP, L2 Carrier Ethernet and L3 VPNs Services	Transport-level Carrier Ethernet Services.	Carrier Ethernet Services Over PBB Networks.	
Support for MEF Services	E-LINE, E-TREE, E-LAN	E-LINE, E-TREE, E-LAN	E-LINE and E-TREE	E-LINE, E-TREE and E-LAN

Table 7.2 Carrier Ethernet Services

7.3 Scalability

EoMPLS	MPLS-TP	PBB-TE	OTN
• It supports huge number of services in every network by layering different services onto each MPLS Label Switched Paths and distributed network architecture. • Highly scalable based on number of VLAN supported by the platform, it can scale to thousands/Ten thousands of VLANs per framework.	• MPLS-TP scales well with increase in end-points, number of services and bandwidth. • MPLS-TP interoperates with existing MPLS and PWE3 networks. It helps to extend IP/MPLS networks beyond their geographical limits to deliver end-to-end services. • MPLS-TP is a multi-	• PBB-TE supports up to 16 million customer services. • Reuses the existing Ethernet forwarding plane. • Separates the provider core switches from customer VIDs and customer MAC addresses. • There is no customer MAC learning as the	• It has extreme scalability and flexibility to adopt new service types. • OTN assigns a dedicated amount of bandwidth to each application and each application has its own layer with guaranteed bandwidth. • Provides a service independent, network-to-network interface for

• Large number of customers over a common infrastructure. • Rapid bandwidth scaling without equipment changes for ample flexibility and scalability.	client technology that supports different technology types such as Ethernet, SDH and ATM.	Destination MAC is based on a Provider MAC address.	transiting the multiple transport domains among multiple providers.

Table 7.3 Scalability

7.4 Connectivity

Features	EoMPLS	MPLS-TP	PBB-TE	OTN
Point-to-point connections	Yes	Yes	Yes	Yes
Point-to-multipoint connections	Yes	Yes	Yes	No
Multipoint-to-multipoint connections	No	No	No	No

Table 7.4 Connectivity

7.5 Operations, Administration and Maintenance (OAM)

Managing Carrier Ethernet services enforces significant challenges. There are many entities and service-level agreement issues to manage, and new mechanisms for OAM required.

Features	EoMPLS	MPLS-TP	PBB-TE	OTN
Link Monitoring	BFD protocol is designed to detect faults where the router fails to detect loss of the physical layer and also applied end-to-end on MPLS LSPs to detect LSP failure.	• Continuity Check • Remote Defect Indication • Alarm Indication Signal • Lock Reporting • Loopback messages There is still work in progress regarding extensions to the LDP to configure and control proactive OAM.	• Continuity Check • Continuity check messages • Loopback Connectivity Check • Traceroute (Link trace) • Alarm Indication Signal	• Forward Error Correction • Tandem Connection Monitoring • Maintenance Signals • Q Factor
Troubleshooting tools	• LSP ping mode can be used to ping a LSP periodically to verify connectivity. • LSP Traceroute mode is used if the ping fails and to diagnose the location of the fault.	• For MPLS-TP, new extensions for LSP ping and PW have been standardized to support the use of the GACH. • LSP Ping and Traceroute provide the on-demand connectivity verification and path tracing functions.	• CFM Loopback mechanism • CFM Continuity Check mechanism • CFM Link trace mechanism	• Link Trace • Trail Trace Identifier (TTI) messages • Path Monitoring • Section Monitoring • TCM

Performance monitoring	Work in progress to standardise mechanism for performance monitoring	• Delay Measurement • Loss Measurement • Client Fault Indication	• Frame Delay • Frame Loss • Remote Defect Indication	• TCM • Alarm indication signal • Q Factor • BER

Table 7.5 Operations, Administration and Maintenance (OAM)

7.6 QoS / Traffic Engineering

QoS is the set of techniques to manage network resources. Networks must provide secure, measurable and SLA guaranteed services and these can be achieved by managing different parameters like delay, jitter, bandwidth, and packet loss.

Features	EoMPLS	MPLS-TP	PBB-TE	OTN
QoS Mechanisms	• E-LSP model offers scalable Soft QoS (characterised by the IETF DiffServ architecture) suitable for most services • L-LSP model offers the Hard QoS (characterised by the IETF IntServ architecture) that guarantee performance under all	• Supports DiffServ QoS with Traffic Engineering capabilities • Two modes supported by MPLS-TP for multi-layer QoS management: 1. Pipe mode 2. Short pipe mode	• It set up a QoS guaranteed Ethernet switched path (ESP) for transport services • Deterministic paths of PBB-TE make the admission control procedure of QoS. • I-Tag is assigned per customer and QoS can be	• Tandem Connection Monitoring (TCM) is used to monitor end to end and various domains QoS. • Restoration through GMPLS • The OAM&P overhead added by G.709 supplements the QoS of

	network conditions		performed per customer instead of per VLAN.	WDM and DWDM equipment.
Traffic Handling Mechanisms	Supports establishment of Traffic Engineering paths in different ways: • Control plane based • Network Management System based • Manually configured	MPLS-TP establish TE paths by means of GMPLS	PBB TE adds support to PBB for deterministic paths and thus provides the feature set needed for providing bandwidth guarantees, resilience and robust QoS.	To offer end-to-end traffic engineering, the following capabilities are included in the layer network: • Optical channel supervisory functions • OTN multiplexing and switching capabilities

Table 7.6 QoS / Traffic Engineering

7.7 CAPEX and OPEX

Features	EoMPLS	MPLS-TP	PBB-TE	OTN
CAPEX and OPEX	EoMPLS reduces CAPEX and OPEX and helps operators to construct real networks: • Service providers make use of common infrastructure and cheaply-available Ethernet	MPLS-TP is cost-efficient technology: • Makes use of existing infrastructure. • In MPLS-TP network an operator can distinguish between different traffic	PBB-TE is a more cost effective approach to building the Ethernet network for these reasons: • PBB-TE switching system enhances	• Reduces OPEX through network simplification by making use of technology that offers simple fault isolation and improved

	interfaces for delivering the services. • Knowledge and maturity of Ethernet reduces the training costs needed for operating EoMPLS network. • Keeps it simple with MPLS Layer 2 capability. • It eliminates the requirement for service providers to build separate networks for different types of services. All services are shared in the same backbone infrastructure.	types and adjust its CAPEX spending accordingly. • An MPLS-TP operator experiences less OPEX than other services as it has significantly fewer ports to operate and maintain. • MPLS-TP enables an operator to separate traffic bandwidth and capacity provisioning that is the main factors that affect cost.	existing Ethernet switching technology with a lower cost structure than IP/MPLS switching and routing hardware. • Ethernet platforms have a cost advantage over IP/MPLS as it have Simple control plane compare to complicated IP/MPLS protocols. • Architecture is simpler and less expensive to manage and provision.	trouble-shooting. • OTN switching eliminates the need for multiple limited functionality NE, resulting in up to 65% CAPEX and 70% OPEX savings. • Reduces CAPEX by lowering the cost-per-bit via technology simplification and transport commonality.

Table 7.7 CAPEX and OPEX

7.8 Reliability

Carrier Ethernet services are projected to support mission-critical applications and ability to quick fault detection, isolation and recovery of any failures that may arise in the physical infrastructure. Protection switching and connection restoration are very important features of any transport technology for uninterrupted customer connections.

Features	EoMPLS	MPLS-TP	PBB-TE	OTN
Protection and Restoration	Supports following protection mechanisms (fast-reroute): • Path protection • Node protection • Link protection	There are different protection topologies: • Linear Protection schemes are 1+1, 1: n and 1:1. • Ring Protection schemes are Facility bypass ring protection and Detours ring protection. • Mesh protection	End-to-end linear protection for point-to-point and point-to-multipoint ESP with 1:1 path protection.	Protection Schemes in OTN: • Linear Protection • Ring Protection • Shared Mesh protection
Reliability	• The Fast Reroute (FRR) structure is used for providing network protection and recovery from failures that occurs in less than 50 milliseconds. • Capability to rapidly detect and recover from different failures meets the most demanding quality requirements for the delivery of high-quality	• Protection State Coordination (PSC) protocol to coordinate the both ends on protection state and commands. • Enhances the resiliency mechanism of MPLS by adding provision for OAM-triggered protection and enhancing protection in ring topologies.	• Provides 50ms protection switching. • Fast notification of end-to-end connectivity failure. • Provisions backup tunnels. • No learning of customer MAC address at the provider backbone bridges	• OTN technology provisions the complete variety of protection methods to prevent failures and speed up recovery times.

	voice and video services.			

Table 7.8 Reliability

7.9 Manageability

Managing a large number of customers extended over a wider geographical area requires Service Providers to have a sophisticated capability for installing, troubleshooting, and upgrading Carrier Ethernet services. To ensure the manageability of a provider network and to make services stable and robust the provider and customer networks can be separated.

Features	EoMPLS	MPLS-TP	PBB-TE	OTN
Service Management	EoMPLS manages tunnels and services that can benefit from user friendly provisioning service and management: • NMS-based service provisioning • Combined NMS and MPLS signaling	• It provides static provisioning with NMS and dynamic provisioning with GMPLS. • OAM and data packets are carried on the same path, it allows simpler and faster monitoring of the PW and LSP layers.	• PBB-TE packets are self-describe and it is ideal for in band OAM, traces and flow monitoring.	• Simplifies end-customer network management. • Fast provisioning via end to end OTN.
Provider-customer network separation	• Service-provider network is separate from the customer network, the service provider can upgrade to	Full separation for core nodes.	• Customer network is completely separate from provider network enabling the customer	OTN is a transparent transport service and designed for full separation.

	EoMPLS without disruption of service to the customer. • The customers assume that they are using a traditional Layer 2 backbone.		Ethernet frames to be transparently transported in the carrier Ethernet frames. • Separates the provider core switches from customer VIDs and customer MAC addresses.	
Customer-customer network separation	Logical separation by means of pseudowires.	Logical separation by means of pseudowires.	Logical separation by means of virtual connections.	OTN is a transparent transport service and designed for full separation.

Table 7.9 Manageability

7.10 Comparing Data plane and Control plane

Features	EoMPLS	MPLS-TP	PBB-TE	OTN
Data Plane	• Forwarding decisions are made based on the MPLS label value in the MPLS encapsulation header.	• MPLS-TP data plane operate and configure without any IP forwarding capability in the MPLS-TP data plane. • Data plane only operates on the MPLS label.	• Uses B-VID + D-MAC (60 bits) to switch packet to egress node • Uses I-SID (24 bits) to identify service at egress node.	• Tributary Port Number (TPN) • GMPLS

Control Plane	• Path calculation is done based on OSPF-TE and IS-IS TE.	• IETF defined GMPLS as a MPLS-TP control plane protocol to be applied to packet switched networks. • GMPLS control plane supports connection management functions as well as protection and restoration techniques making MPLS-TP more dependable transport protocol.	• Employs a MAC-in-MAC forwarding scheme from PBB and distributes the bridging tables using the control plane.	• GMPLS

Table 7.10 Comparing Data plane and Control plane

8. Conclusion

The purpose of this project report is to provide detailed analysis of different transport network technologies on basis of Carrier Ethernet's five different attributes that are Standardized services, Scalability, Reliability, Quality of Service and Service management. Some of these solutions are more useful than others in specific framework.

Section 1 of this report definite different characteristic of Carrier Ethernet that are used to classify the transport technology, including Attributes, Services, Components, Benefits and Applications. Section 2 summarize about different Carrier Ethernet Technologies that these technologies can be implemented over many different types of transport network technologies to support both existing and emerging services. There are multiple solutions that can be used to deliver Carrier Ethernet over Service Provider networks, each with its own specific standard and goal, and accordingly, different in how the Carrier Ethernet solution is offered.

Section 3 to Section 7 describes about each of the Carrier Ethernet technologies:

- Ethernet over Internet Protocol/Multi-protocol Label switching(EoMPLS)
- Multiprotocol Label Switching Transport Profile (MPLS-TP)
- Provider Backbone Bridge –Traffic Engineering (PBB-TE)
- Optical Transport Network (OTN)

All of the Ethernet-based technologies described in this project report are seeing rapid adoption globally. This report does not select any technology as best or better technology for services delivery instead it describes about all of them. Some of these technologies are more useful than others in specific framework. To find out that which technology is best depends upon different carrier-class functions and flexibility to support different situations like infrastructure, architecture, technology, and so on.

References

1. *Carrier_Grade_Ethernet_WP_00.pdf*. (n.d.). Retrieved from http://www.brocade.com: http://www.brocade.com/downloads/documents/white_papers/Carrier_Grade_Ethernet_WP_00.pdf

2. *Carrier Ethernet services* from MEF 6.1 Ethernet Services Definitions - Phase 2

3. *Ethernet service components* available from Metro Ethernet Services – A Technical Overview, Ralph Santitoro /Metro Ethernet Forum

4. *Carrier_Ethernet.pdf*. (n.d.). Retrieved from http://www.geant.net: http://www.geant.net/Media_Centre/Media_Library/Media%20Library/Carrier%20Ethernet.pdf

5. Metroethernetforum.org http://metroethernetforum.org/PDF_Documents/Access_WG_Whitepaper_FINALv3.pdf

6. *Carrier Ethernet Technologies and E- access* retrieved from MEF 33 Ethernet Access Services Definition carrierethernetstudyguide.org

7. *Emerging Carrier Ethernet Technologies* http://www.ja.net/documents/development/EmergingCarrierEthernettechnologiesv.1.3.pdf

8. *CarrierEthernetEssentials.pdf*. (n.d.). Retrieved from http://www.fujitsu.com: http://www.fujitsu.com/downloads/TEL/fnc/whitepapers/CarrierEthernetEssentials.pdf

9. Kasim, A. Delivering Carrier Ethernet: Extending Ethernet Beyond the LAN . In A. Kasim, *Delivering Carrier Ethernet: Extending Ethernet Beyond the LAN.*

10. *VPWS* available from Designing and Implementing IP/MPLS-Based Ethernet Layer 2 VPN Services: An Advanced Guide for VPLS and VLL

11. *Virtual Private Multicast Service* from draft-ietf-l2vpn-vpms-frmwk-requirements

12. Xu, Z. (. (2010). In Z. (. Xu, *Designing and Implementating IP/MPLS Based Ethernet Layer 2 VPN Services.* Wiley Publishing Inc.

13. *MPLS-TP* available from RFC 5317 "Joint Working Team (JWT) Report on MPLS Architectural Considerations for a Transport Profile"

http://tools.ietf.org/html/rfc5317

14. *Bidirectional Forwarding Detection* from RFC 5880 "Bidirectional Forwarding Detection (BFD)"
    http://tools.ietf.org/html/rfc5880

15. *MPLS-TP QOS* available from RFC 3270 "Multi-Protocol Label Switching (MPLS) Support of Differentiated Services"
    http://www.ietf.org/rfc/rfc3270.txt

16. *MPLS-TP* Ring protection draft-yang-mpls-tp-ring-protection-analysis-01
    MPLS vs MPLS-TP from Brocade's "WHAT'S GOING ON WITH ETHERNET?"
    http://www.nanog.org/meetings/nanog50/presentations/Tuesday/NANOG50.Talk40.Hankins-Talk40.whats-going-on-with-ethernet-nanog.pdf

17. *PBB-TE QOS* Retrieved from
    http://www.lightreading.com/document.asp?doc_id=146364&page_number=8

18. *OTN* introduction from http://www.networkworld.com/details/4521.html?def
    OTN frame structure from "Aliathon Technology"
    http://www.aliathon.com/our_products/otn/fec/

19. *OTN* Features available at http://www.slideshare.net/udunuwara/optical-transport-network.

20. *OTN architecture and Layers within an OTN* retrieved from T. Walker's tutorial, ITU-T, “Optical Transport Network”
    http://www.itu.int/ITU-T/studygroups/com15/otn/OTNtutorial.pdf

21. *OAM Architecture* from draft-ietf-mpls-tp-oam-framework-11.txt

Glossary

AIS	Alarm Indication Signal
APS	Automatic Protection Switching
ATM	Asynchronous Transfer Mode
B-DA	Backbone DA
BFD	Bi-directional Forwarding Detection
BGP	Border Gateway Protocol
B-SA	Backbone SA
B-VID	Backbone VLAN ID
CAPEX	Capital Expenditure
CBR	Constant Bit Rate
CC	Continuity Check
CC & CV	Continuity Check and Connectivity Verification
CCM	Continuity Check Message
CE	Customer Edge
CFM	Connectivity Fault Management
CIR	Committed Information Rate
CSPF	Constrained Shortest Path First
C-Tag	Customer Tag
C-VID	Customer VLAN ID
DA	Destination Address
DiffServ	Differentiated Services

DSCP	DiffServ Code Point
DWDM	Dense Wavelength Division Multiplexing
EIR	Excess Information Rate
E-LAN	Ethernet LAN
E-LSP	EXP-derived Label-Switched Path
ENNI	External Network-to-Network Interface
EoMPLS	Ethernet over Multi-Protocol Label Switching
ESP	Ethernet Switched Path
E-Tree	Ethernet Tree
EVC	Ethernet Virtual Connection
EVPL	Ethernet Virtual Private Line
EXP	Experimental
FAS	Frame Alignment Signal
FEC	Forwarding Equivalence Class
FR	Frame Relay
FRR	Fast Rerouting
G-ACh	Generic Associated Channel
GAL	G-ACh Label
GCC	General Communication Channel
GFP	Generic Framing Procedure
GMPLS	Generalised Multi-Protocol Label Switching
IEEE	Institute of Electrical and Electronics Engineers

IETF	Internet Engineering Task Force
IGP	Interior Gateway Protocol
IP	Internet Protocol
IP/MPLS	Internet Protocol/Multiprotocol Label Switching
IPTV	Internet Protocol Television
I-SID	Service Identifier
IS-IS-TE	Intermediate System to Intermediate System – Traffic Engineering
ISO	International Standards Organisation
ITU-T	International Telecommunication Union – Telecommunication Standardisation Sector
I-Tag	Instance Tag
JC	Justification Control
L2VPN	Layer 2 Virtual Private Network
LAN	Local Area Network
LDP	Label Distribution Protocol
LER	Label Edge Router
LSP	Label Switched Path
LSR	Label Switching Router
MAC	Media Access Control
MAN	Metropolitan Area Network
ME	Maintenance Entity
MEF	Metro Ethernet Forum

MEG	Maintenance Entity Group
MEN	Metro Ethernet Network
MEP	Maintenance End Point
MFAS	Multi-Frame Alignment Signal
MIP	Maintenance Intermediate Point
MP2P	Multipoint to Point
MPLS	Multi-Protocol Label Switching
MPLS-TP	Multi-Protocol Label Switching – Transport Profile
MP2MP	Multipoint to Multipoint
MSI	Multiplex Structure Identifier
MS-PW	Multi-Segment Pseudowire
NE	Network Element
NMS	Network Management System
OAM	Operations, Administration and Maintenance
OAM&P	Operations, Administration, Maintenance and Provisioning
OCh	Optical Channel
ODU	Optical Data Unit
ODUk	Optical Data Unit-k
OH	Overhead
OMS	Optical Multiplex Section
OMS	OTN Network Management System
OPEX	Operating Expense

OPU	Optical Channel Payload Unit
OPUk	Optical Channel Payload Unit-k
OSI	Open Systems Interconnection
OSPF-TE	Open Shortest Path First – Traffic Engineering
OSNR	Optical Signal-to-Noise Ratio
OTH	Optical Transport Hierarchy
OTM	Optical Transport Module
OTN	Optical Transport Network
OTS	Optical Transmission Section
OTS-OH	Optical Transmission Section Overhead
OTU	Optical Channel Transport Unit
OTUk	Optical Channel Transport Unit-k
OVC	Operator Virtual Connection
P2MP	Point to Multipoint
P2P	Point to Point
PB	Provider Bridge
PBB	Provider Backbone Bridge
PBB-TE	Provider Backbone Bridge Traffic Engineering
PBT	Provider Backbone Transport
PCC	Protection Communication Channel
PDU	Protocol Data Unit
PDH	Plesiochronous Digital Hierarchy

PE	Provider Edge
PM	Path Monitoring
POTN	Packet Optical Transport Network
PON	Passive Optical Networks
PPP	Point-to-Point Protocol
PM	Path Monitoring
PSI	Payload Structure Identifier
PT	Payload Type
PW	Pseudowire
PWE	Pseudowire Emulation
PWE3	Pseudowire Emulation Edge to Edge
QoS	Quality of Service
RDI	Remote Defect Indication
RES	Reserved for future use
RPR	Resilient Packet Ring
RSVP-TE	Resource Reservation Protocol – Traffic Engineering
SA	Source Address
SDH	Synchronous digital hierarchy
SLA	Service Level Agreement
SM	Section Monitoring
SONET	Synchronous Optical Networking
SS-PW	Single Segment Pseudowire

S-Tag	Service provider's VLAN tag
STP	Spanning Tree Protocol
S-VID	Service VLAN ID
TC	Tandem Connection
TC	Traffic Class
TCM	Tandem Connection Monitoring
T-DA	TE-Service DA
TDM	Time-Division Multiplexing
TE	Traffic Engineering
T-IID	TE-Service Instance Identifier
T-LDP	Targeted Label Distribution Protocol
T-MPLS	Transport Multi-Protocol Label Switching
TTI	Trail Trace Identifier
TTL	Time to Live
TTT	Timing Transparent Transcoding
T-SA	TE-Service SA
UDP	User Datagram Protocol
UNI	User-to-Network Interface
VC	Virtual Connection
VID	VLAN ID
VLAN	Virtual Local Area Network
VLAN ID	Virtual LAN Identifier

VLL	Virtual Leased Line
VoIP	Voice over IP
VPLS	Virtual Private LAN Service
VPMS	Virtual Private Multicast Service
VPN	Virtual Private Network
VPWS	Virtual Private Wire Service
WAN	Wide Area Network
WDM	Wavelength Division Multiplexing