Tuukka Järvi

Layer 2 Solutions in Access Provider Networks

Helsinki Metropolia University of Applied Sciences

Master's Degree

Information Technology

Master's Thesis

Date 05-05-2020

Helsinki Metropolia University of Applied Sciences

Author(s) Title Number of Pages Date	Tuukka Järvi Layer 2 Solutions in Access Provider Networks 48 pages + 2 appendices 5 May 2020
Degree	Master of Engineering
Degree Programme	Information Technology
Specialization option	
Instructor(s)	Janne Salonen, Principal Lecturer

The thesis concentrates on Metro Ethernet and Carrier Ethernet solutions in Service Provider and Access Provider networks. Ethernet has been in use in local area networks for more than 30 years. The success of Ethernet is based on its simplicity, ease of deployment, versatility, and low cost. Until the end of the 1900s Ethernet technologies were mainly restricted to LANs, but there were efforts to move from the mainstream LAN technology to metropolitan area network solutions.

The next step in the evolution was to use Ethernet techniques in metropolitan area networks in the beginning of the 2000s. The Metropolitan Ethernet (Metro Ethernet) networks based on previous Ethernet standards are deployed in a metropolitan area. The successor of the Metropolitan Ethernet is Carrier Ethernet. It uses high-bandwidth Ethernet technology to create Internet access and communication between local area networks. Metro Ethernet and Carrier Ethernet can also be used to connect physically multiple locations to a network via an Ethernet Private Line. The driving force in the evolution is a vast increase of sites requiring fast and flexible services. Advantages of these implementations are lower cost of equipment and compatibility with customers' equipment, that are based on Ethernet techniques.

In this project the underlying telecommunications background, including protocols and conventions, is described shortly. Metro Ethernet and Carrier Ethernet technologies are represented in detail, and two real-world cases are introduced, the emphasis being in Access Providers networks. The solutions are compared with legacy implementations, and benefits and limitations are discussed.

Keywords	Metro Ethernet, Carrier Ethernet, L2VPN, VPLS, MPLS

Contents

Acknowledgements

I would first like to thank my thesis advisor Principal Lecturer, Head of Department Janne Salonen of the Information Technology Department at Metropolia University of Applied Sciences.

I also express my warm thanks to Mr. Markus Säkäjärvi for his support and guidance at DNA.

Finally, I must express my very profound gratitude to my parents and to my spouse for providing me with unfailing support and continuous encouragement throughout my years of study and through the process of researching and writing this thesis. This accomplishment would not have been possible without them. Thank you.

Abbreviations

ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
BWP	Bandwidth profile
CBS	Committed Burst Size
CCC	Circuit Cross-Connect
CE	Customer Edge equipment
CE 1.0	Carrier Ethernet 1.0
CE 2.0	Carrier Ethernet 2.0
CEN	Carrier Ethernet Network
CIDR	Classless Inter-Domain Routing
CIR	Committed Information Rate
CoS	Class of Service
CPE	Customer Premises Equipment
CVLAN	C-VLAN, customer VLAN
C-Tag	Customer tag
DEI	Drop Eligibility Indicator
DWDM	Dense Wavelength Division Multiplexing
E-Access	Ethernet Access service type
E-LAN	Ethernet LAN service type
E-Line	Ethernet Line service type
EBS	Excess Burst Size
EIR	Excess Information Rate
ENNI	External Network-to-Network Interface
EoMPLS	Ethernet over MPLS
EPL	Ethernet Private Line service
EP-LAN	Ethernet Private LAN service
EP-Tree	Ethernet Private Tree service
Ethernet	Most widely used local area network technology
E-Tree	Ethernet Tree service type
EVC	Ethernet Virtual Connection
EVPL	Ethernet Virtual Private Line
EVP-LAN	Ethernet Virtual Private LAN service
EVP-Tree	Ethernet Virtual Private Tree service
FPC	Flexible PIC Concentrator
FTTB	Fiber To The Building
G.SHDSL	Symmetric High-Bitrate Digital Subscriber Loop
IANA	Internet Assigned Numbers Authority
IEEE	Institute of Electrical and Electronics Engineers
IEEE 802.1ad	QinQ or Q-in-Q, amendment to IEEE 802.1Q
IEEE 802.1p	Quality of service standard
IEEE 802.1Q	VLAN networking standard
IEEE 802.3	Standard specification for Ethernet
IETF	Internet Engineering Task Force

IPSec	IP Security Architecture
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISO	International Organization for Standardization
ITU-T	International Telecommunication Union Standardization sector
Juniper	Juniper Networks, Inc.
Junos OS	Juniper Network Operating System
Kompella	BGP-based VPLS standard
L2circuit	Layer 2 Circuit
L2VPN	Layer 2 VPN
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
Martini	VPN standard, L2circuit in Junos OS
ME	Metro Ethernet
MEF	Metro Ethernet Forum
MEN	Metro Ethernet Network
MPLS	Multiprotocol Label Switching
MTU	Maximum Transfer Unit
OAM	Operations, Administration and Maintenance
OSI Model	Open Systems Interconnection reference model
OSPF	Open Shortest Path First
OUI	Organization Unique Identifier
OVC	Operator Virtual Connection
PCP	Priority Code Point
PDH	Plesiochronous Digital Hierarchy
PDU	Protocol data unit
PE	Provider Edge router
PIC	Physical Interface Card
Prefix	Network portion of the address
QinQ	IEEE 802.1ad standard
QoS	Quality of Service
RFC	Request for Comments
RSVP	Resource Reservation Protocol
SDH	Synchronous Digital Hierarchy
SLA	Service Level Agreement
SLO	Service Level Objective
SONET	Synchronous Optical Network
SVLAN	S-VLAN, service VLAN identifier
S-TAG	Service tag

TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UNI	User-Network Interface
VLAN	Virtual LAN
VPLS	Virtual Private LAN Service
WAN	Wide Area Network
WDM	Wavelength-Division Multiplexing

1 Introduction

The thesis concentrates on Metro Ethernet and Carrier Ethernet solutions in service provider and access provider networks. Metro Ethernet, Carrier Ethernet and in the background residing communications protocols are introduced, Carrier Ethernet services are described and two cases are represented and analyzed.

1.1 Background

Ethernet has been in use in local area networks (LAN) for more than 30 years. The success of Ethernet is based on its simplicity, ease of deployment, versatility, and low cost. Until the end of the 1900s Ethernet technologies were mainly restricted to LANs, but there were efforts to move from the mainstream LAN technology to metropolitan area network solutions (MENs). From the early 2000s, Metro Ethernet and later Carrier Ethernet began gaining more popularity as a WAN technology. Metro Ethernet Forum, non-profit international industry consortium, started developing technical specifications for Metro Ethernet in 2001 and Carrier Ethernet in 2005. Later both ITU-T and IEEE have been collaborating with the standardisation and capability enhancement for Ethernet.

Carrier Ethernet provides Internet access and communication between local area networks. In the beginning Carrier Ethernet and Metro Ethernet were used as synonyms. Although the functions of Metro Ethernet and Carrier Ethernet are similar, there are several differences. Metro Ethernet is intended for deployment in a metropolitan area and connect multiple locations to a network. Carrier Ethernet is more enhanced and is intended for all network operators. Its main advantages are lower in cost and speed compared with legacy technologies.

1.2 Technology Problem

The theory and protocols of Carrier Ethernet will be expressed to build a solid knowledge base. Practical solutions as well equipment and the configuration of devices will be presented in detail, to help to close the gap between theory and real-world.

1.3 Object and Outcome

In this project Carrier Ethernet solutions and the technical background will be introduced and two real-world cases are presented.

The purpose of the thesis project includes the following:

- Present basic data communications protocols.
- Describe briefly the solutions and architectures used in current networking solutions
- Present the Metro Ethernet and Carrier Ethernet techniques.
- Configure and document two case implementations.
- Discuss the results and evaluate future trends.

1.4 Project Methodology

Firstly, the communications protocols were introduced. The underlying system architectures and technical solutions were represented. There are several legacy technologies used during transition to newer solutions. Some of the technologies were explained in detail.

Secondly, Ethernet-based solutions were described, the time line of different standards was shown, and current solutions were described. Thirdly, Carrier Ethernet protocols and applications were presented in detail. Two real-world cases were described and documented. Fourthly, the results of the work were analyzed.

The steps of the work are:

- The feasibility study for the project: different technologies are explored, and dominant protocols and architectures are presented.
- The system architectures introduction: for this step, the prevailing system architectures are described and the specification acts as a guideline for the next step.
- The protocols focused in this work: for this step Carrier Ethernet protocols and applications are described in detail.
- The solutions introduction and comparison: for this step, the main task is introducing and documenting two case solutions and equipment in Layer 2 operator network interconnection.
- The results: the technical measures, and the data collected in previous steps for this step are drawn together, and are subjected to analysis and synthesis.

1.5 Scope and Structure

The project focuses on at Layer 2 networking systems. The target is to explore, describe and compare prevailing solutions in operator networks and network interconnection.

The thesis contains five sections. In Section 1 a brief introduction about the project is provided. In section 2 the theoretical and technical framework is described. Section 3 contains

detailed description of protocols and system architecture, including Carrier Ethernet technologies. Section 4 describes practical implementations and solutions in selected networks. Section 5 discusses and concludes the achievements and findings of the project.

2 Theoretical and Technical Framework

In this chapter the theoretical and technical details related to the study are presented. It also illustrates the techniques behind the systems and applications used in this project.

2.1 OSI and TCP Models

The OSI model (Open Systems Interconnection) is used to characterize and standardize the communication functions in telecommunications systems. It is independent of the internal structure and technology of underlying systems. The model was presented in 1984 as standard ISO 7498. It was later renamed as standard X.200 by CCITT (ITU-T).

The model contains 7 layers, which are numbered from 1 to 7. Lowest layer is 1, and highest 7. Each layer serves layers above and below it (Figure 1).

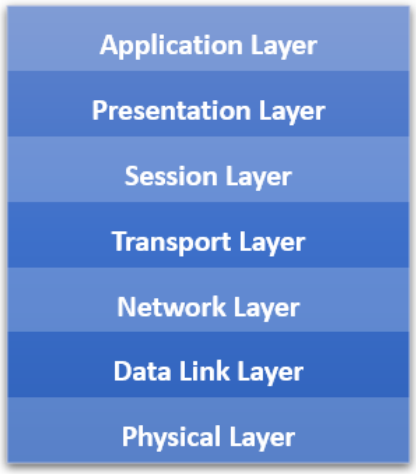

Figure 1. OSI Model. [1.]

The functions of each layer are:

1. Physical layer: Binary transmission of signals and encoding. Layout of pins, voltages, cable specifications and modulation.
2. Data link layer: Transmission of frames between nodes. Physical addressing and access to media are implemented using two sublayers, Logical Link Control (LLC) and Media Access Control (MAC).
3. Network layer: Logical addressing scheme, routing and traffic control, and reporting of delivery errors.
4. Transport layer: Flow control and segmentation/de-segmentation of data. In addition, handling end-to-end connections and reliability is implemented here.
5. Session layer: Establishment and management connections between applications.

6. Presentation layer: An interface for the application layer (MIME encoding, data encryption, conversion, formatting and compression).
7. Application layer: Network services for application processes.

Layers 1 ... 3 are also called Media layers, and layers 4 … 7 Host layers.

Unlike OSI, which is a conceptual model, the TCP/IP model used for establishing a connection and communicating through the network. It contains four layers. [2, 5.]

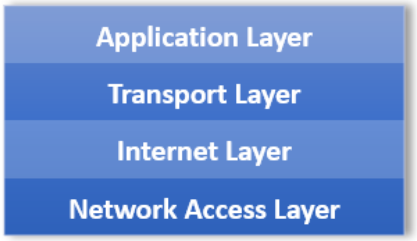

Figure 2. TCP/IP Model. [5.]

The TCP/IP model layers and the OSI layers can be compared as follows:

1. TCP/IP Network Access layer corresponds to OSI Data Link Layer and Physical Layer.
2. TCP/IP Internet layer corresponds to OSI network layer.
3. TCP/IP Transport corresponds to OSI Transport and contains some parts of the Session layer.
4. TCP/IP Application layer includes OSI Application and Presentation layer and contains some parts of the session layer. [2, 5.]

2.2 Ethernet

Ethernet is a networking technique used initially in local area networks (LAN), and later in metropolitan area networks (MAN) and wide area networks (WAN). The first Ethernet standard, DIX 1.0, was developed in 1980-81 by DEC (Digital Equipment Corporation), Intel, and Xerox. Sometimes it is referred as Ethernet I. The next version, the current Ethernet standard, DIX 2.0, was introduced in 1982. The Ethernet standard 802.3 was introduced in 1983 by the Institute of Electrical and Electronics Engineers (IEEE) to standardize the protocol. [3.]

Ethernet resides on the OSI Physical layer and Data Link layer. Ethernet protocol data units, Ethernet frames reside on the Data link layer, and rely on the Physical layer transport mechanisms. At the Physical layer there is a 7-byte preamble and one-byte start frame delimiter

(SFD) in the beginning of the frame. The preamble consists of alternating 1 and 0 bits to provide network devices bit-level synchronization of their receiver clocks. The SFD provides byte-level synchronization and defines the beginning of the frame.

The structure of an Ethernet frame is shown below (Figure 3). The header contains six-octet destination and source addresses, a two-octet Type/Length field and, optionally, a four-octet VLAN tag. The minimum data is 42 octets when a VLAN tag is present and 46 octets otherwise (the optional VLAN tag consumes additional space in the frame. Padding is added at the end, if the actual data is less. The maximum data is 1500 octets in Ethernet II and 1492 octets in IEEE 802.3. In some implementations, e.g. Gigabit Ethernet, larger frames are supported (jumbo frames). At the end of the frame there is a four-octet check sequence (FCS). It is used to detect corrupted data when the frame is received. [3.]

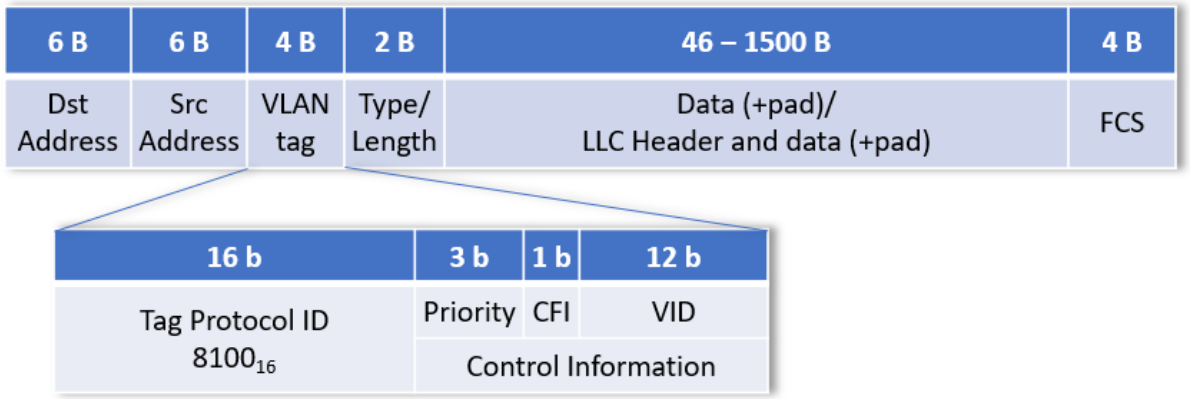

Figure 3. Ethernet II / IEEE 802.3 frame. [3.]

Ethernet II and 802.3 differ from each other in the fields of their Ethernet headers. In Ethernet II the Type field (Ether Type) defines the kind of packet that is in the data field, e.g. IPv4 or IPv6, and it is always at least 1536 (0600_{16}). In the 802.3 the Length field tells the length of the data field, and is followed by the IEEE 802.2 Logical Link Control (LLC). The value in the Length field is always less than 1500 ($05DC_{16}$), which is the maximum frame size for Ethernet. The actual data in the frame is after the LLC, and its length is between 42 and 1496 bytes.

Ethernet II is the most used protocol in local area Ethernet networks. It is simple and the overhead is lower. The Ethernet II and 802.3 systems cannot communicate directly with each other, but can coexist in the same network. Ethernet II systems discard IEEE 802.3 frames as carrying invalid protocol information (the Type/Length field is less than 0600_{16}). On the other hand, IEEE 802.3 systems consider Ethernet II frames to be too long (the Type/Length field is greater than $05DC_{16}$) and discard them.

Network devices contains a unique identifier, a Media Access Control address (MAC address). They are used in communication at OSI Data link layer. A MAC address is 48 bits long (EUI-48). It is divided into two 24-bit parts: organization identifier (OUI) and organization-specified extension identifier.

When the least significant bit of an address's first octet is zero, the address is a unicast address. A unicast frame is transmitted to all nodes within the segment, but only the node with the matching MAC address will accept it. A MAC address consisting of 1-bits is called a broadcast address, and is received and accepted by all nodes in the segment.

2.2.1 VLANs

An Ethernet frame may contain a VLAN tag (IEEE 802.1Q tag), that tells which VLAN the frame belongs to, and also its priority. The 802.1Q standard helps to divide large networks into smaller networks using virtual LANs. On a switch the unicast, multicast and broadcast traffic from one VLAN is transmitted only to the devices, that belong to the same VLAN. Traffic of frames belonging to multiple VLANs is transmitted in trunks in links between devices. [11.]

A 4-byte 802.3Q tag is in the Ethernet header between Source Address and Type/Length fields (see Figure 3). The structure of the VLAN field is as follows:

- Tag Protocol Identifier (TPID): 16-bit field that identifies a tagged frame (value 8100_{16}).
- Priority (User Priority): IEEE 802.1p priority, that can be used to prioritize traffic (8 levels, values 0 through 7).
- Canonical Format Indicator (CFI): Tells whether the MAC Address is in noncanonical format (value 1) or canonical format (value 0). Setting the value of the CFI field to 1 enables Token Ring frames to be transmitted in Ethernet links.
- VLAN Identifier (VID): Identifies the VLAN (12 bits, values 0 through 4095).

Because the length of the 802.1Q tag is 4 bytes, it increases the maximum frame length by four bytes. Thus, the maximum size of the Ethernet frame is 1522 octets. Respectively the minimum size with 802.1Q tagging is 68 octets. When the frame is tagged, the FCS field is recomputed. [11.]

Another protocol for carrying multiple VLANs between devices is ISL. It is a Cisco proprietary protocol and used mainly in Cisco-based environments. ISL encapsulates the original frame

adding its own 30-byte header before sending to the trunk line. The receiving device removes the header before sending the frame to the assigned VLAN. ISL supports 1000 VLANs. [11.]

The IEEE802.1ad (Q-in-Q, QinQ) is an amendment to the 802.1Q standard. It enables adding multiple VLAN tags to a single VLAN header in frames entering the network. Using QinQ the service provider can provide separate services for clients on specific VLANs. In 802.1ad the Drop Eligibility Indicator (DEI) replaces the CFI field.

In figure 4 a second 802.1Q frame is added to an Ethernet frame. On top is the original frame. In the middle an 802.1Q tag with VLAN 100 header is added to it. The tag protocol ID of the first tag (the inner tag, Customer tag, C-TAG) is 8100_{16}. At the bottom another tag with VLAN header 30 is added in front of the first tag (the outer tag, Service tag, S-TAG). The tag protocol ID of the second tag is $88A8_{16}$ (in the old QinQ protocol 9100_{16}). In the figure below also a frame capture of a double-tagged Ethernet frame is shown.

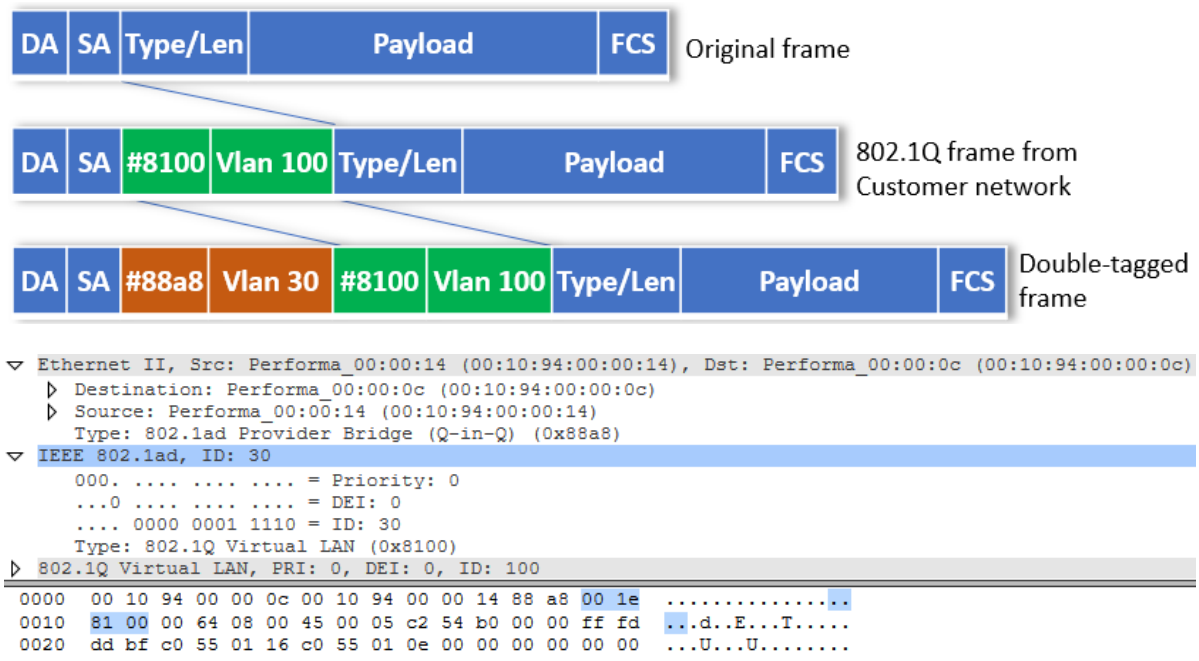

Figure 4. A double-tagged Ethernet frame. [11.]

The innermost tag (closest to the payload) is the C-TAG and all other tags are S-TAGs.

2.3 Internet Protocol

The Internet Protocol (IP) is a connectionless datagram service and was introduced with the first Transmission Control Program in 1974. It is used to deliver OSI Network layer datagrams between hosts. The suit consisting of IP and connection-oriented Transmission Control Protocol (TCP) is called TCP/IP. The older IP version, Internet Protocol version 4 (IPv4), is the

most used protocol of the Internet. The newer version, Internet Protocol version 6 (IPv6) is, however, becoming more and more common. [2.]

The Internet Protocol resides at the OSI Network Layer (TCP/IP Internet Layer). The main functions of IP are logical addressing of hosts and packet routing in networks.

IP encapsulates data segments from the Transport layer into packets. The IP packets consist of an IP header and data. The information in the header is used to deliver the packet to its destination.

IP is a connectionless protocol, and does not guarantee the delivery of packets to the destination, but uses best effort policy. It is the responsibility of upper layer protocols to provide reliable connections. [2.]

2.3.1 Internet Protocol version 4

IPv4 is defined and specified in IETF RFC 791. An IPv4 packet contains a header and encapsulated data. In the header there are of 14 fields. The IPv4 header is shown below (Figure 4). [2.]

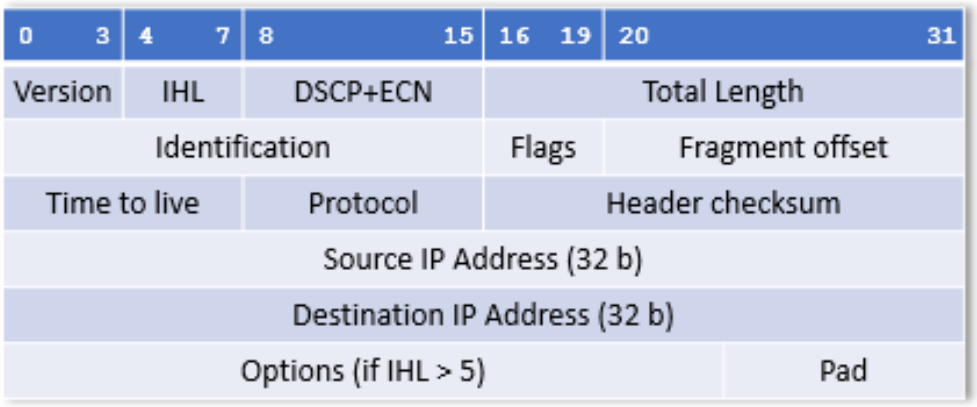

Figure 5. IPv4 header. [2.]

Below is a short description of the functions of each field.

- Version: Internet Protocol version (4 for IPv4).
- IHL, Internet Header Length.
- DSCP, Differentiated Services Code Point (Type of Service).
- ECN, Explicit Congestion Notification. Informs congestion on the route.
- Total Length: IP header and data length.
- Identification: Identifies a group of fragments of an IP packet.

- Flags: Identifies and controls fragments of an IP packet (3 bits, value of bit 0 is always '0').
- Fragment Offset: The offset of a fragment from the beginning of the original IP packet.
- Time to Live (TTL): Used to avoid network looping. Initially TTL contains the number of hops allowed. On each hop, the number is decremented by one, and when it becomes 0, the packet is discarded.
- Protocol: The protocol of the data part of the packet.
- Header Checksum: The header error-checking value. It is recalculated on every router and the packet is discarded if values don't match.
- Source Address: Sending host IP address.
- Destination Address: Receiving host IP address.
- Options: Optional header fields.

The checksum does not include the packet payload. [2.]

Communication between hosts requires them to identify each other on the network. The IPv4 addresses are 32 bits long. The total number of possible addresses is 4 294 967 296 (2^{32}). Special address blocks are reserved for special use (private networking, multicasting and future applications).

The dot-decimal notation is used to show a 32-bit address in a more comfortable format. The address is divided into four decimal-coded octets, that are separated by a period (.).

Classful addressing divides the entire IP address space into classes. Each class defines a range of continuous addresses. The first four bits of the first octet of the address define the class the address belongs to.

There are three host classes, Class A, Class B and Class C, a multicast address class D and an address class for future purposes. Maximum number of Class A, B and C networks is 126, 16 384 and 2 097 152 respectively, and maximum number of hosts in Class A, B and C networks is 16 777 214, 65 534 and 254 respectively.

The addresses are managed by Internet Assigned Numbers Authority (IANA) and regional Internet registries.

A subnet mask is a 32-bit mask that tells the network portion of the IP address. It contains 1-bits in the network portion and 0-bits in the host portion. Using subnet masks in classful networks it is also possible to partition a network into smaller logical subnetworks.

In Classless Inter-Domain Routing (CIDR) addressing the address is interpreted as a 32-bit string of ones and zeroes. The address is followed with its routing prefix. The routing prefix starting with a slash (/) contains count of network portion 1-bits. CIDR is also called supernetting, and it can be used to aggregate multiple Internet addresses of the same class.

The following IP address blocks are reserved for private IP addresses. Unlike public addresses these addresses are not routable in the Internet: 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255 and 192.168.0.0 to 192.168.255.255. Using private IP addresses and networks public IP address space can be saved. Private addresses also hide the local network from the public network. Devices inside private networks can access Internet using network address translation techniques (NAT).

Another private IP address space is defined by IANA: APIPA addresses from 169.254.0.1 to 169.254.255.254 can be used in automatic addressing.

2.3.2 Internet Protocol version 6

The newer Internet Protocol version 6 (IPv6) was introduced by the IETF. The purpose was to upgrade IPv4 protocol, and provide coexistence with IPv4 solutions. The IPv6 protocol makes it possible to add more of hosts to Internet and transfer increasingly amounts of data. The IPv6 header is 40 octets long as shown below (Figure 5). [4.]

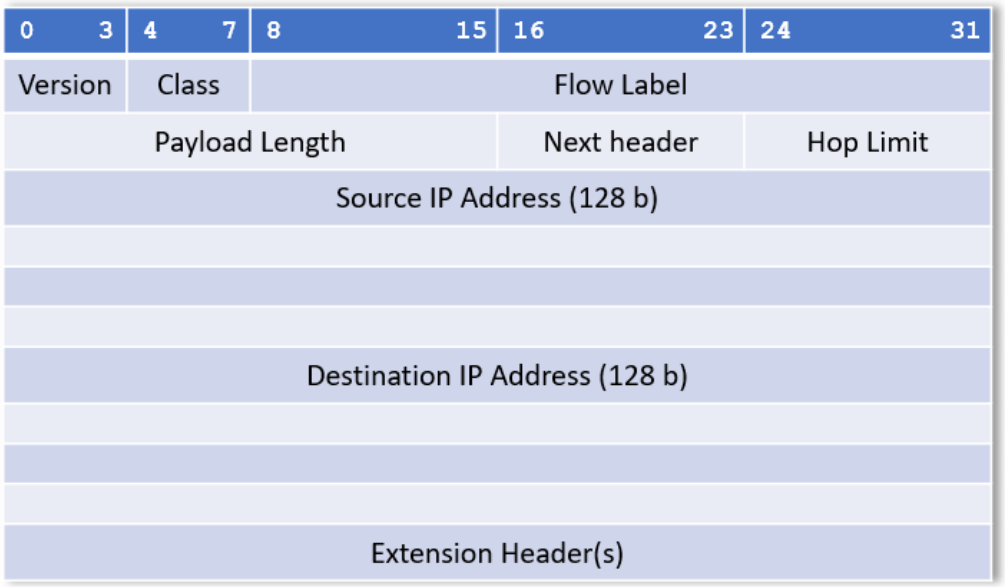

Figure 6. IPv6 header. [4.]

Below is a short description of the functions of each field.

- Version: Internet Protocol version, 6 for IPv6.
- Class: Traffic Class, contains a 6-bit Differentiated Services (DS) portion for classification of packets. The other 2-bit portion is for Explicit Congestion Notification (ECN).
- Flow Label: If the contents of this field are zero, it tells routers and switches to keep the packets on the same path to prevent them to be reordered.
- Payload Length: The payload size in bytes including extension headers.
- Next Header: Next header type.
- Hop Limit: Corresponds to the TTL of IPv4. Even if its value becomes 0, the receiving node should process the packet normally.
- Source Address: Sender's IPv6 address.
- Destination Address: Receiver's IPv6 address.

Extension headers reside between the IPv6 header and the data area (upper-layer protocol header). [4.]

An IPv6 address 128 bits long. The whole address space is thus 2^{128} addresses, or approximately $3{,}40 \cdot 10^{38}$ addresses. The address is expressed in hexadecimal format, in 8 groups of 4 hexadecimal digits separated by colons (:). The leading zeros in every group can be omitted. Consecutive groups of zeros can be replaced with a double colon (::).

The IPv6 address categories are unicast, anycast and multicast addressing. A unicast address pointing to an IPv6 interface is unique in a network segment. Multicast addresses are same as in IPv4. In IPv6 there is no broadcast addressing, but multicasts are used instead. In anycast addressing same IP address is assigned to multiple interfaces.

The lower half (64 bits) of the unicast address is always used for Interface ID. The ID can be autoconfigured from the MAC address by adding a 16-bit value in the middle of the address and complementing the 7^{th} bit of the address (Extended Unique Identifier, EUI-64).

In IPv6 there are three different types of unicast addresses. Global unicast address functions like public IPv4 address. The most significant 48 bits form a global routing prefix, which is assigned to specific autonomous system. The next 16 bits are used to define subnets. The lower half of the address contains Interface ID.

Auto-configured Link-Local addresses are used for communication between IPv6 hosts on a link. They are not routable. The lower half of the address contains Interface ID. The prefix of a Link-Local address is always fe80::/10.

Unique-Local address resemble IPv4 private network addresses. They are globally unique, but intended for local communication. The upper half of the address contains prefix, Local bit, Global ID and Subnet ID. The lower half of the address contains Interface ID. The prefix of a Unique-Local address is fc00::/7.

The prefix of a IPv6 multicast address is ff00::/8. The first 8 bits of the address contain a hexadecimal value $0FF_{16}$. The next 4 bits are allocated for flags and the next 4 bits for Scope. Scope contains the range where multicast packets can be forwarded. The next 112 bits represent the Group ID.

IPv6 anycast addresses use the same address range as global unicast addresses. Each participating device is configured to have the same anycast address.

2.4 TCP and UDP Protocols

The Transport layer protocols are Transmission Control Protocol (TCP, specified in RFC 793), and User Datagram Protocol (UDP, specified in RFC 768).

TCP protocol is a connection-oriented protocol. Data is sent as an unstructured stream of bytes, and the protocol is considered as a reliable transport protocol. TCP header is shown below (Figure 6). [6, 7.]

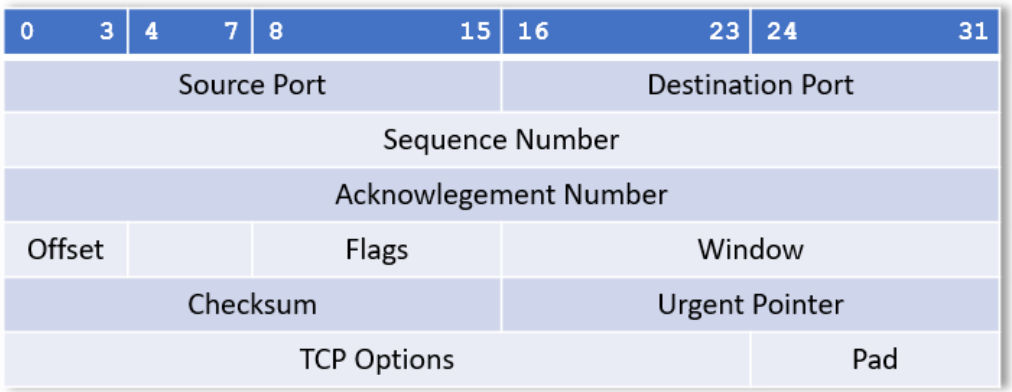

Figure 7. TCP header. [7.]

Below is a short description of the functions of each field.

- Source Port: Source port address (16 bits).

- Destination Port: Destination port address (16 bits).
- Sequence Number: Initial segment number, when the SYN flag is set. Sequence number of the first data octet in the current session, if the SYN bit is not set.
- Acknowledgment Number: Acknowledgement sequence number to inform that the data that has been successfully received.
- Offset: Data offset, total size of a TCP header in 32-bit words. If there are no optional fields, the value is 5. Maximum size is 15.
- Flags: The one-bit flags are:
    - URG: Urgent pointer is set in the header.
    - ACK: Acknowledgment field is valid.
    - PSH: Push the buffered data to the receiver's application.
    - RST: Reset the connection.
    - SYN: Open the connection.
    - FIN: Finish, close the connection in an orderly manner.
- Window: The receive window size in bytes.
- Checksum: Checksum calculated from pseudo header, TCP header and payload.
- Urgent pointer: Marks a segment of data as 'urgent' if the URG flag is set.
- TCP Options: Optional parameters in a TCP header. [7.]

A connectionless protocol UDP provides no reliability, flow-control or error recovery. Only source and destination port numbers, length of the segment, and checksum are in the UDP header. The data follows immediately the header. The maximum length of the segment is 65535 bytes. [6.]

2.5 MPLS

In IP networks the IP header parameters are used in forwarding packets to the next hop. The IP header of every IP packet is examined every time when the packet is sent to the next router in the routing path. The router searches for the best route in its routing table and sends then the packet to the next router. This operation is repeated on every router in the path until the packet reaches its destination. Routing using routing protocols and routing tables on the routers on the network can in some cases be rather complex and even slow down the traffic, because the Border Gateway Protocol (BGP) needs to be configured and running in every router in the network.

Multiprotocol Label Switching (MPLS) is used to avoid complex operations and make the traffic faster. In MPLS networks the BGP is running only in the border routers, and the IP

header is examined only, when the packet arrives at the MPLS network, and leaves the network. The ingress Provider Edge (PE) router examines the packet, and adds to the header a label, that defines the packet's destination. The MPLS label is added between OSI Data Link Layer header and Network Layer header(s) in the incoming frame (see Figure 8). The packet is sent to the first router in the MPLS path, where the label is used for looking up information in the label forwarding table. The old label in the packet is replaced with a new label and the packet is sent to the next router. On the last router (egress PE router) the label is removed from the packet, and the IP packet is sent forward. The information in the IP headers need not to be examined in the MPLS tunnel, which results as enhanced scalability, better performance, and better bandwidth utilization.

Encoding of a single MPLS label and a frame capture example are shown below. The EXP field contains Class of service, S (Bottom of stack) and TTL (Time to Live). In the figure also a frame capture of an MPLS frame is show. [9.]

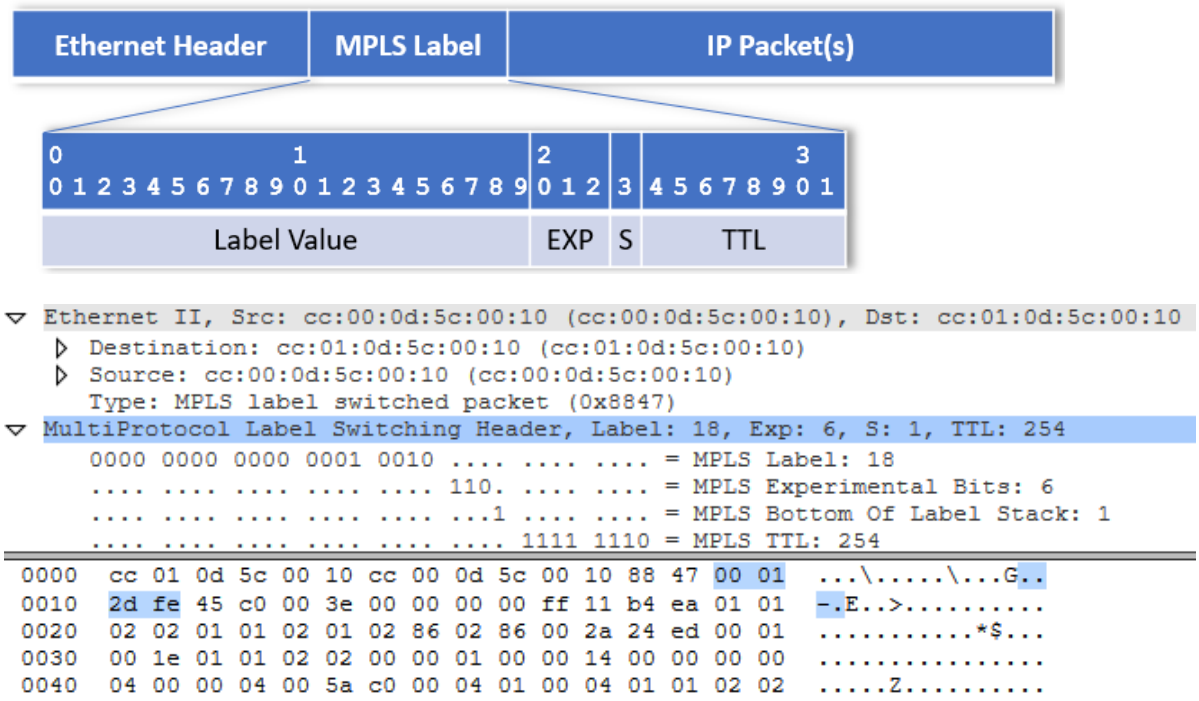

Figure 8. MPLS Label Encoding. [9.]

IP-based routing in the network is required for MPLS operations. The structure of an MPLS network is shown below (Figure 9). Customer's CE router is connected to the ingress PE router (Label Edge Router, LER) on the service provider network. LER determines the path, encapsulates the IP packet, and forwards it to the next router on Label Switched Path (LSP). The Provider routers (P router) on the LSP are called Label Switching Routers (LSR). They

determine next hop on the path according to the packet label, remove the current label, replace it with a new one, and send the packet to the next router. The last router on the path, egress PE, removes the MPLS label, and forwards the packet it to customer's CE router. Label Switched Path (LSP) is a predetermined unidirectional path between two LERs in the MPLS network. In figure 9 there are two LSPs between PE1 and PE2. The MPLS transport LSPs are established using Label Distribution Protocol (LDP), when traffic engineering is not required. LDP establishes LSPs using existing IP routing tables, and suits particularly well to establish a full mesh of LSPs between all routers on the network. [9.]

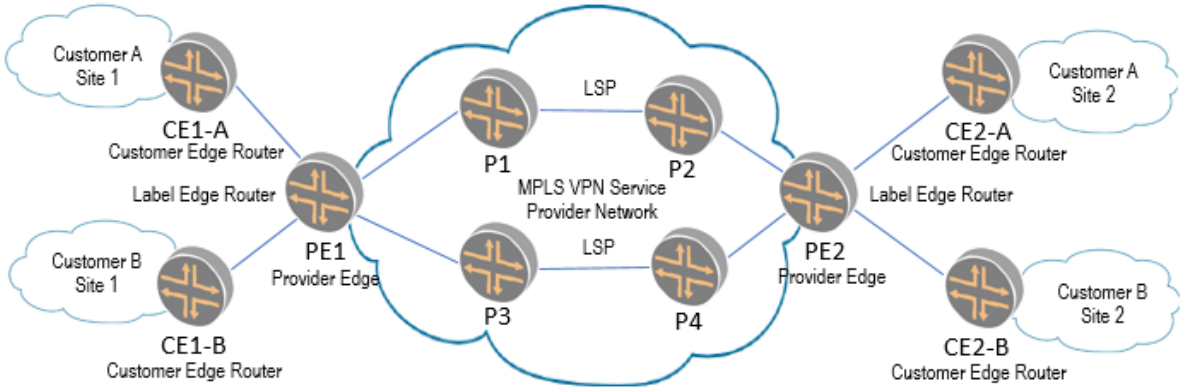

Figure 9. Structure of MPLS network. [10.]

2.6 Metro Ethernet

In the beginning Ethernet techniques were intended for local area networks. In consumer and enterprise environments Ethernet has superseded previous solutions in the IP-based data communication at the end of the 1900s. The service providers and network operators, however, continued using virtual circuits on Frame Relay, ISDN or ATM networks to provide LAN connectivity to their customers. The WAN and Ethernet typically communicated through routers providing OSI Layer-3 services. [8.]

The next step in the evolution was to use Ethernet techniques in metropolitan area networks. The driving force was a vast increase of sites requiring fast and flexible services. The customers wanted also lower start-up costs, faster service delivery and flexible and scalable services. The Metropolitan Area Ethernet (Ethernet MAN, Metro Ethernet) is based on Ethernet standards, and Ethernet networks are deployed in a metropolitan area. Metro Ethernet can also be used to connect physically multiple sites to a network using an Ethernet Private Line (EPL). An advantage of Metro Ethernet implementations is, that the cost of equipment is less than with previous techniques. Another advantage is compatibility with customers' equipment, that are based on Ethernet techniques. [22.]

The growth of Ethernet speeds according the Ethernet Alliance is shown below in figure 10.

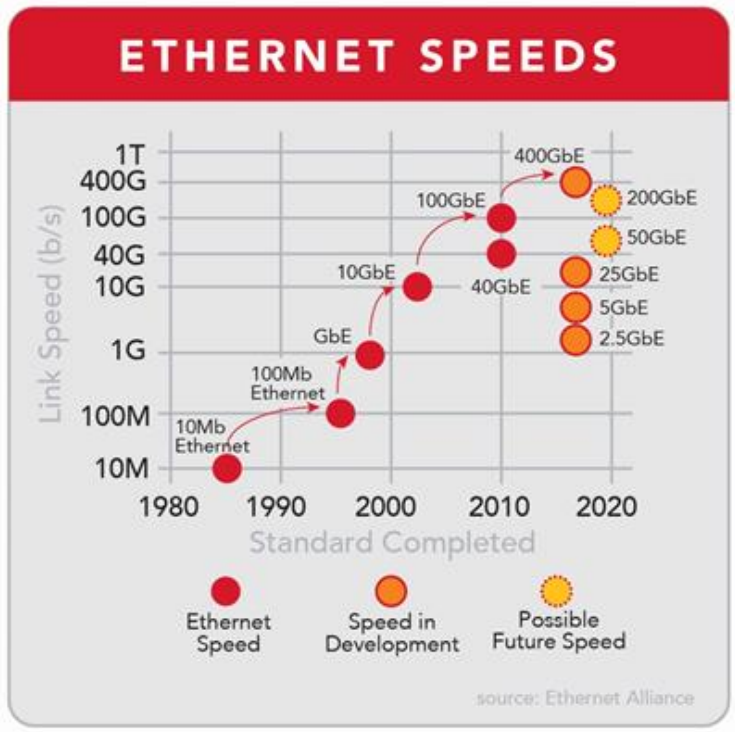

Figure 10. Ethernet speeds 1985-2020. [21.]

As seen in the figure, Ethernet bit speeds grow ten times each time a new rate is defined.

The Metro Ethernet Forum (MEF) is a non-profit international industry consortium, that provides a technical overview of Ethernet services. It comprises of more than 200 global organizations. The primary tasks of the MEF are to define Ethernet services for Metro Ethernet and Carrier Ethernet, and accelerate the worldwide adoption. [8.]

Three main differences between Ethernet LANs and Metro Ethernet are [22.]:

- The whole organization connects to Metro Ethernet through a (single) port at subscriber location.
- The Metro Ethernet network can act as a provider network for many companies.
- The Metro Ethernet resides across a wide area.

Service providers' networks are divided in three hierarchical layers: core, distribution and access. Typically, networks contain switches and routers that are connected with optical fibre or copper lines. The core connects provider's network to another provider's network, and

consists usually of an IP/MPLS backbone. Distribution network connects clients to the service providers. Access equipment resides normally in client's premises. [8.]

The implementation choices of Metro Ethernet are pure Ethernet, Ethernet over SDH (Synchronous Digital Hierarchy), Ethernet over MPLS, or Ethernet over DWDM (Dense Wavelength Division Multiplexing). Metro Ethernet uses Ethernet VLAN tags for creating virtual private lines and virtual private networks. [8.]

Pure Ethernet-based solutions are less expensive, but the disadvantages are lower reliability and lack of scalability. They are suitable only to small scale implementations. If there already exists SDH infrastructure, Ethernet over SDH is a viable solution. One of its disadvantages is weak bandwidth management. [8.]

In Ethernet over MPLS implementations MPLS in the provider's network is often used. Client's equipment has Ethernet interfaces, and Ethernet frames are transmitted over MPLS. The service providers use Ethernet as underlying technique in the MPLS network. The advantages compared to pure Ethernet implementations are scalability, fast resiliency, multiprotocol support, and end-to-end OAM (Operations, Administration and Maintenance). [8.]

2.7 Carrier Ethernet

Metro Ethernet services are also expanding to worldwide services, national and global networks. Legacy technologies fail to provide flexible scalability, because adding bandwidth requires more circuits or upgrading to new technology, which in turn means service disruption.

Carrier Ethernet is based on high-bandwidth Ethernet technology, and provides Internet access and communication between local area networks. In the beginning the terms Carrier Ethernet and Metro Ethernet were used together, but in the 2000s Carrier Ethernet started to include many other Ethernet services. Although the functions of Metro Ethernet and Carrier Ethernet are similar, there are several differences. Firstly, they differ in the scope of usage. Metro Ethernet is intended for deployment in a metropolitan area and connect multiple sites to a network using an EPL. In Carrier Ethernet Metro Ethernet functions can exist, but latter Metro Ethernet does not include Carrier Ethernet. Secondly, Carrier Ethernet relies on high-bandwidth Ethernet technology to create Internet access and communication between LANs. [22.]

The five Carrier Ethernet service key attributes are: Sandardized Services, Scalability, Reliability, Quality of Service and Service Management (Figure 11).

Figure 11. Carrier Ethernet Features. [12.]

The standardized Carrier Ethernet (CE) services are E-Line, E-LAN and E-Tree. They provide solutions to most WAN networks using multiple technology options. Adapting Carrier Ethernet, limitations of legacy technology are avoided. Services scale in granular increments. Bandwidth is easily added through remote provisioning and it is possible for customers to use the same technology in LAN, MAN and WAN connections. The users can build Ethernet MANs and WANs, and service providers can offer Ethernet-based MAN or WAN services. Network scalability makes it possible to expand beyond geographical boundaries. Services scalability means that services can be multiplexed at the same user-network-interface. [12.]

Reliability is enhanced compared to legacy solutions, because the network can detect and recover from incidents without affecting users, with very short recovery times. Quality of Service is included in the services delivering end-to-end performance. Service management contains multiple attributes such as service activation, creation, management, and guaranteed quality. [12.]

Carrier Ethernet 1.0 (CE 1.0) is MEF's first generation standardized carrier-class Ethernet services over one provider's network. It was launched in 2005. The CE 1.0 services are defined in the MEF 6 service definitions. Carrier Ethernet 1.0 services contain point-to-point and multipoint-to-multipoint service connection types E-LINE, E-LAN and E-Tree. Virtual versions are also defined in the standard to enable multiple networks on the same infrastructure. [12.]

Carrier Ethernet 2.0 (CE 2.0) was announced in 2012 as the next generation in the evolution of Ethernet services by Metro Ethernet Forum. CE 2.0 contains a new service type, E-Access. Using E-Access connections can run across the infrastructure of multiple vendors, and multiple classes of service (Multi-CoS) are possible. The E-Tree service is enhanced providing a rooted hub-and-spoke multipoint connection. The CE 2.0 services are defined in the MEF service definitions 6.1, 6.1.1, 7.1, 10.2, 13, 20, 22.1, 23.1, 26.1 and 33. Recommendation ITU-T G.8011/Y.1307 contains a framework of specifications for Ethernet services based on Metro Ethernet Forum (MEF) specifications. [12.]

Carrier Ethernet 1.0 and 2.0 have expanded the scope of LANs. Ethernet bandwidth is growing continually. 100Gbit Ethernet was standardized in 2010 and 2011, and 1Tbit Ethernet is on the way. Cloud services provide Ethernet even wider adoption. [12.]

The third generation Carrier Ethernet specifications, Carrier Ethernet 3.0 (CE 3.0) is already on its way. It contains enhanced subscriber services (E-Line, E-LAN, E-Tree) and operator services (Access E-Line, Access E-LAN, Transit E-Line, and Transit E-LAN). The MEF 3.0 service family also includes dynamic Carrier Ethernet, SD-WAN, Optical Transport, IP, Security-as-a-Service, and other virtualized services. [20.]

3 Carrier Ethernet Networking Architectures

This chapter describes the Carrier Ethernet networking architectures, a part of which are used in this project. Metro Ethernet is used in three major areas: In access networks to connect a shared property and the end user (Fiber To The Building, FTTB), in core networks to replace SDH/SONET in high-speed point-to-point connections (Long-range Ethernet), and in site-to-site services as a replacement of DWDM.

Network operators have three main targets in the future: The clients continue using Ethernet as the dominant network protocol, which requires permanent support. The operators need to find the most cost-effective technologies in their networks to answer to increasing demand of volume and bandwidth. The operators need also replace older non-Ethernet technologies with newer Ethernet-based solutions with better throughput and capacity. The migration to Ethernet-based solutions from traditional technologies is not, however, simple due to limitations of Ethernet: Legacy Ethernet does not support virtual circuits and end-to-end signaling, the OSI Layer-2 addresses or MAC addresses need to be unique, virtual LAN technologies are not scalable, and there is no inherent security architecture.

Carrier Ethernet provides consistent, cost-efficient and high-performance services. With CE transparent migration from legacy networks to new high-speed solutions is achieved. The current services are typically based on the second generation of Carrier Ethernet, Carrier Ethernet 2.0 (CE 2.0). CE 2.0 contains eight port-based and virtual services, and delivers powerful features. The taxonomy of CE 1.0 and CE 2.0 is shown below (Figure 12). [17.]

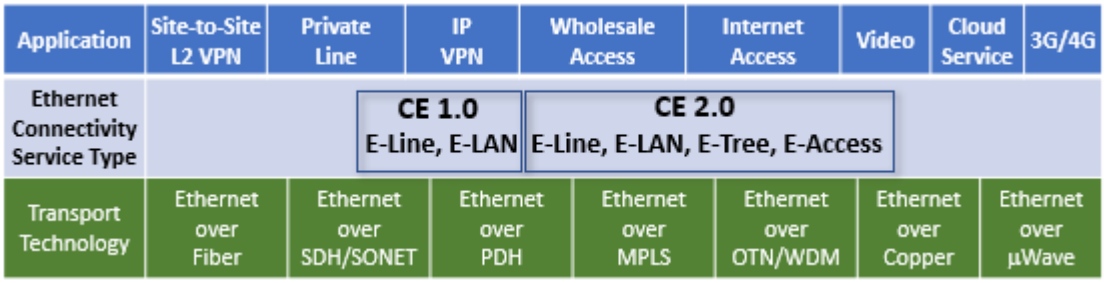

Figure 12. Carrier Ethernet Taxonomy. [12.]

In this work the main emphasis is on transport technologies and the usage in traffic between operators, service providers and end-users. Carrier Ethernet relies on various OSI Layer 1 technologies. The most widely used technologies are listed in the table below (Table 1).

Table 1. Carrier Ethernet Transport types. [12.]

Carrier Ethernet over Layer 1 Transport	Description
Ethernet over Fiber	Ethernet over IEEE 802.3 Ethernet Layer 1 transport
Ethernet over SDH/SONET	Ethernet encapsulated in ITU-T G.8040 GFP over SDH/SONET virtual concatenation groups
Ethernet over PDH	Ethernet encapsulated in ITU-T G.8041 GFP over single or bonded T1, E1, T3 or E3 circuits
Ethernet over MPLS	Ethernet with MPLS shim header used over any Layer 1 transport
Ethernet over OTN	Ethernet encapsulated in ITU-T G.709 digital wrapper
Ethernet over WDM	Ethernet transported over different wavelengths (lambdas)
Ethernet over dry copper pairs	Ethernet encapsulated in ITU-T G.SHDSL
Ethernet over µWave	Ethernet transported over microwave frequency spectrum

Networks based on Ethernet services are called the Carrier Ethernet Networks (CEN). Typical Carrier Ethernet-based applications are explained in table 2.

Table 2. Ethernet-based applications. [12.]

Application	Description
Site-to-site Layer 2 VPNs	High bandwidth and more flexible replacement for the Frame Relay Layer 2 VPNs
EPL	Similar characteristics to a Layer 1 private line but delivered using Ethernet interfaces
Wholesale Ethernet access	First/last mile Ethernet services enabling service providers to reach out-of-franchise customer premises
3G/4G cell site mobile backhaul	Interconnecting 3G/4G base stations at cell sites to their base station controllers at a mobile switching center
Ethernet access to IP services	• Ethernet access to managed IP VPNs • Ethernet dedicated Internet access • Ethernet access to cloud services • Ethernet backhaul of IP video from DSLAM, GePON or CMTS aggregator

Carrier Ethernet uses point-to-point and multipoint-to-multipoint virtual connections. The CEN infrastructure contains OSI Layer 2 networking and optionally access to OSI Layer 3 (IP) services. Ethernet demarcation devices provide separation between two networks. The demarcation types of Carrier Ethernet are Ethernet User Network Interface (UNI) and External Network-to-Network Interface (ENNI or E-NNI). [12.]

The UNI is an Ethernet port used to connect the end-user Customer Equipment (CE) to service provider network. CE can be a router or IEEE 802.1Q bridge. UNI provides a demarcation to the subscriber and provider network. UNI is asymmetric, and always provided by the service provider. It consists of the UNI-C (client's side) and UNI-N (provider's side). [12.]

The provider types type defined by MEF are operator and service provider. The service provider sells Ethernet services to end-users, who are connected to the network through UNI (UNI-to-UNI services). Operators sell Ethernet services to service providers, who connect to the network through ENNI (UNI-ENNI and/or ENNI-ENNI services). [12.]

3.1 Carrier Ethernet 1.0

Carrier Ethernet 1.0 services operate using Ethernet Virtual Circuit (EVC). EVC is an association between UNIs. More than one EVC on one ne UNI can supported using service multiplexing. Data transfer is only possible between sites belonging to the same EVC. The EVC types are Point-to-Point EVC, Multipoint EVC, and Rooted Multipoint EVC. EVCs can be multiplexed at the same UNI. Carrier Ethernet 1.0 is defined in MEF 6, 7, 10 and 15. [12.]

In a Point-to-Point EVC (P2P EVC) there are exactly two UNIs. It supports the Ethernet Private Line (EPL) and Ethernet Virtual Private Line (EVPL) services. The port-based EPL service is used to replace TDM private lines, and is often delivered over SDH. Traffic coming from CE to a UNI is contained in a single EVC. P2P EVC results to a high degree of transparency, because the header and payload of the frames transmitted are identical at the source and destination UNI. [12.]

Using EVPL service multiplexing at the UNI, and multiple virtual connections on a single physical connection to UNI in customer premises are possible. Each customer VLAN uses a separate EVC. Using service multiplexing it is possible to send some frames to one EVC and others to another EVC. Using EVPL it is possible to create point-to-point EVCs between UNIs to interconnect sites. The basic structure of EPL and EVPL service is shown in figures below (Figures 13 and 14). In figure 13 all traffic from a CE to UNI is contained in a single EVC. [12.]

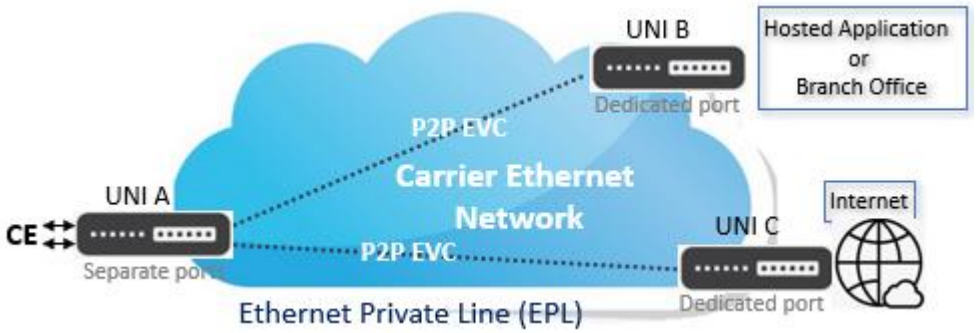

Figure 13. Basic structure of the EPL service. [12.]

In figure 14 each customer VLAN between UNI A and B, and A and C is bound to a separate EVC, and traffic between CE and UNI D is bundled as a single EVC. [12.]

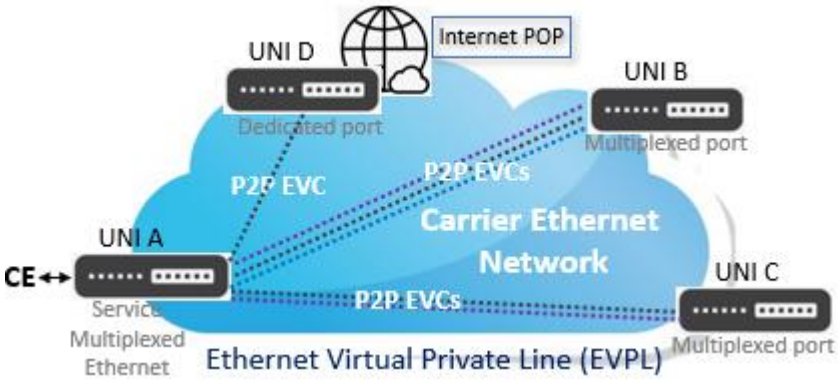

Figure 14. Basic structure of the EVPL service. [12.]

In a Multipoint EVC (MP2MP EVC) there are two or more UNIs. A UNI can be either root or leaf. It provides a full mesh connectivity between sites and carries the following E-LAN services: port-based Ethernet Private LAN (EP-LAN) and VLAN-based Ethernet Virtual Private LAN (EVP-LAN). The EP-LAN is port-based and each UNI is dedicated to the EP-LAN service. It can be used to build a transparent LAN. [12.]

The EVP-LAN is VLAN-aware and service multiplexing is allowed at UNI making it possible to have different EVCs at the same UNI. It can be used to create an Internet access and corporate VPN through one UNI. The basic structure of EP-LAN and EVP-LAN service is shown in figures below (Figures 15 and 16). In figure 15 the customer is spread over three sites. [12.]

Figure 15. Basic structure of the EP-LAN service. [12.]

In figure 16 there is a point-to-point EVC between UNI A and D, and a multipoint-to-multipoint EVC between UNI A, B, and C. [12.]

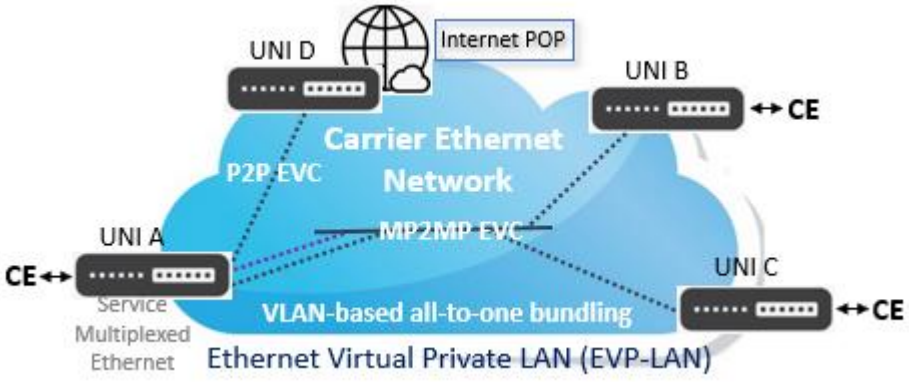

Figure 16. Basic structure of the EVP-LAN service. [12.]

In an E-Tree service (Rooted Multipoint EVC, RMP EVC) each UNI can be either root or leaf. A root UNI communicates with any leaf UNI, but a leaf UNI can communicate only with a root UNI. Rooted Multipoint EVCs carry the following E-Tree services: Ethernet Private Tree (EP-Tree) and Ethernet Virtual Private Tree (EVP-Tree). The basic structure of EP-Tree and EVP-Tree is shown below (Figures 17 and 18). In figure 17 is an example of a port-based E-Tree and in figure 18 VLAN-based multiplexing of an E-Tree and an E-Line. [12.]

Figure 17. Basic structure of the EP-Tree service. [12.]

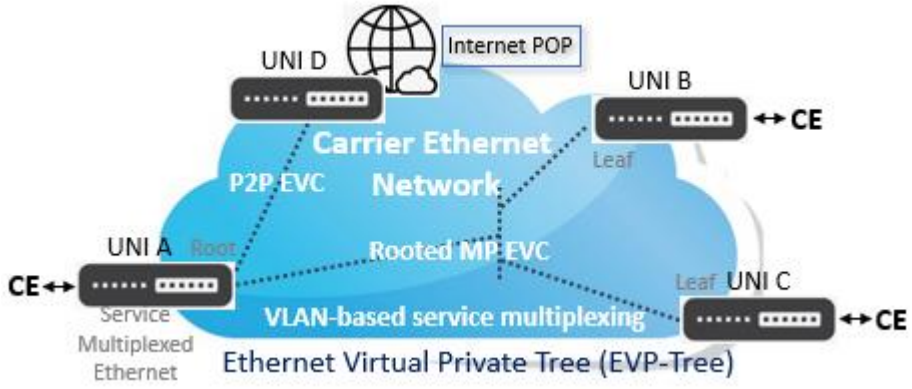

Figure 18. Basic structure of the EVP-Tree service. [12.]

3.2 Carrier Ethernet 2.0

Carrier Ethernet 2.0 enhances CE 1.0 features, and adds new features and services to the previous standard. The CE 2.0 services contain multiple classes of service (Multi-CoS) and management of interconnected provider networks. Class of Service extensions improve quality of service solutions especially in VLAN-based services. Enhanced interconnection services help engineering multiple interconnected networks as a single network. CE 2.0 contains new management services to help in fault management and performance monitoring. [12.]

Carrier Ethernet EVC, defined in CE 1.0, is an association between two or more UNIs. More EVCs can be supported with one UNI with service multiplexing. In CE 2.0 the definition of an Operator Virtual Connection (OVC) is added as an association of external interfaces (UNIs or ENNIs) of a single operator Carrier Ethernet Network. At least one of the external interfaces must be an ENNI. OVC - external interface associations are called an OVC End Points. [12.]

The ENNI is a physical Ethernet interface that is used to connect two service provider networks that belong to separate administrative domains. The service provider is responsible for its service demarcation point towards to the ENNI. ENNI is symmetric, in both sides of the ENNI are a reference points called ENNI-N. The properties of UNI and ENNI are summarized in table 3. [12.]

E-Access is an OVC-based Ethernet service, that associates at least one OVC end point at a UNI and at least one OVC end point at an ENNI. OVCs form a logical association between a UNI and ENNI or two ENNIs. They are used for virtual connections between UNI-ENNI or ENNI-ENNI end points. [12.]

Table 3. UNI and ENNI Comparison. [12.]

Capability	UNI	ENNI
Frame format supported	Untagged or single-tagged (IEEE 802.1Q)	Double-tagged (IEEE 802.1ad/Q-in-Q)
Virtual connectivity type supported	EVC or OVC	OVC
Ethernet interface speeds	All (typically 10/100 Mbps)	1 Gbps or 10 Gbps
EVC/OVC multiplexing	May or may not support (EVC/OVC)	Always supported (OVC)
Maximum transmission unit frame size	1518 bytes minimum	1526 bytes minimum
CoS identification	802.1Q PCP (p bits) or DSCP	802.1ad S-Tag PCP or DSCP
Service demarcation	Between end-user and service provider	Between service providers

The EVC types are Point-to-Point EVC, Multipoint EVC, and Rooted Multipoint EVC. EVCs can be multiplexed at the same UNI.

The OVC service types are Multipoint-to-Multipoint (MP2MP) and Point-to-Point (P2P) OVC, the latter being more popular because of its simplicity. OVC services utilizing a P2P OVC with one UNI endpoint and one ENNI endpoint are port-based Access Ethernet Private Line Service (Access EPL) and VLAN-based Access Ethernet Virtual Private Line (Access EVPL) service. They are typically used for providing EVC-based services to end-user clients. [12.]

In E-Transit all OVC End Points are at ENNIs. The E-Transit services are Transit E-Line (P2P with two ENNIs) and Transit E-LAN service (two or more ENNIs). The Service definitions are based on MEF Technical Specifications MEF 6.1, MEF 10.2, MEF 23.1, MEF 26.1 and MEF 33, and are summarized below (Table 4). [12, 13.]

Table 4. Carrier Ethernet Service Definitions. [13.]

	Service Type	Port-Based (All to One Bundling)	VLAN Based (EVC identified by VLAN ID)
EVC Services	**E-Line** Point-to-Point EVC	Ethernet Private Line (EPL)	Ethernet Virtual Private Line (EVPL)
	E-LAN Multipoint-to-Multipoint EVC	Ethernet Private LAN (EP-LAN)	Ethernet Virtual Private LAN (EVP-LAN)
	E-Tree Rooted multipoint EVC	Ethernet Private Tree (EP-Tree)	Ethernet Virtual Private Tree (EVP-Tree)
OVC Services	**E-Access** OVC	Access Ethernet Private Line (Access EPL)	Access Ethernet Virtual Private Line (Access EVPL)
		Access E-LAN (Multipoint-to-Multipoint OVC with UNI(s) and ENNI)	
	E-Transit OVC	Transit E-Line (Point-to-Point OVC with 2 ENNIs)	
		Transit E-LAN (Multipoint-to-Multipoint OVC with ENNIs)	

The MEF 33 standard-based Ethernet E-Access service consists of an OSI Layer 2 OVC, that associates at least one customer's Ethernet port UNI, and at least one external network-to-network interface ENNI. The services can be port-based with only single OVC instance per UNI, and VLAN-aware services supporting multiple OVC instances per UNI. In multiplexing each service instance is mapped to one of the 4094 S-VLAN IDs in an OVC. [13.]

E-Access is used by a (wholesale) operator as a virtual connection between one or more end user locations on its network, and the retail service provider delivering first-mile access and service provider interconnections. Overview of Access EPL and EVPL service is shown in the below (Figures 19 and 20). [15.]

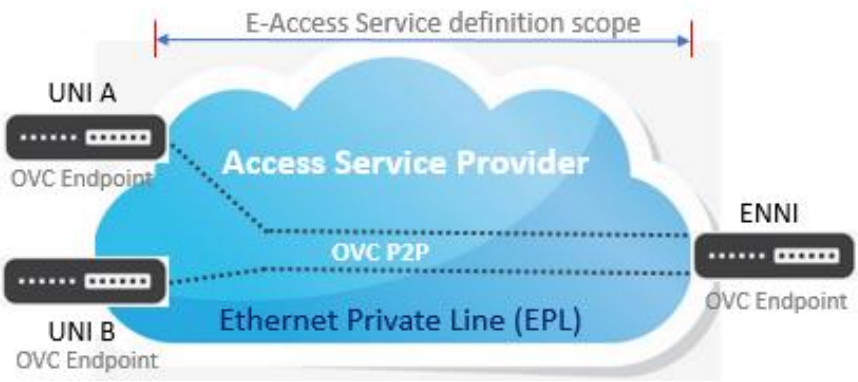

Figure 19. Overview of Access EPL Service. [15.]

In figure 19 all untagged and any C-VLAN frames map to one OVC. There is one UNI per OVC and single CoS per OVC. At ENNI unique S-VLAN ID per Access EPL maps to single OVC End Point. [15.]

In figure 20 at the UNI OVC an end point map must be specified for each OVC. The frames are delivered to ENNI with the addition of an S-VLAN tag. At the ENNI Access EVPL S-VLAN ids map to a single OVC End Point. In figure 20 there is also an EVC that associates UNI A and UNI C. [15.]

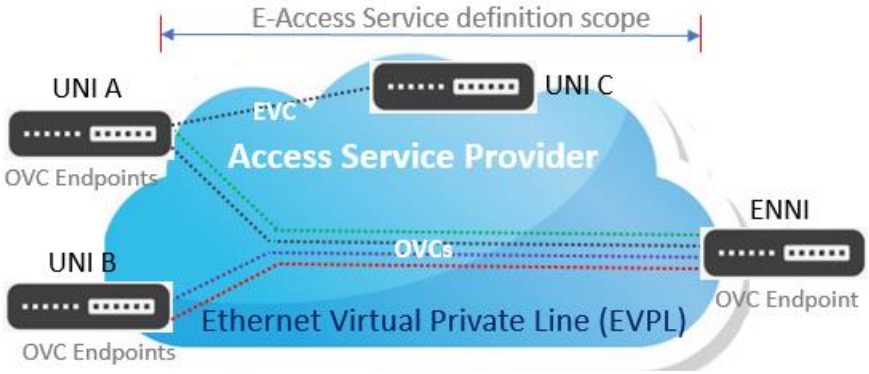

Figure 20. Overview of EVPL Service. [15.]

Port-based Access Ethernet Private Line service (EPL) can also be used to extend EPL as shown below in figure 21. [16.]

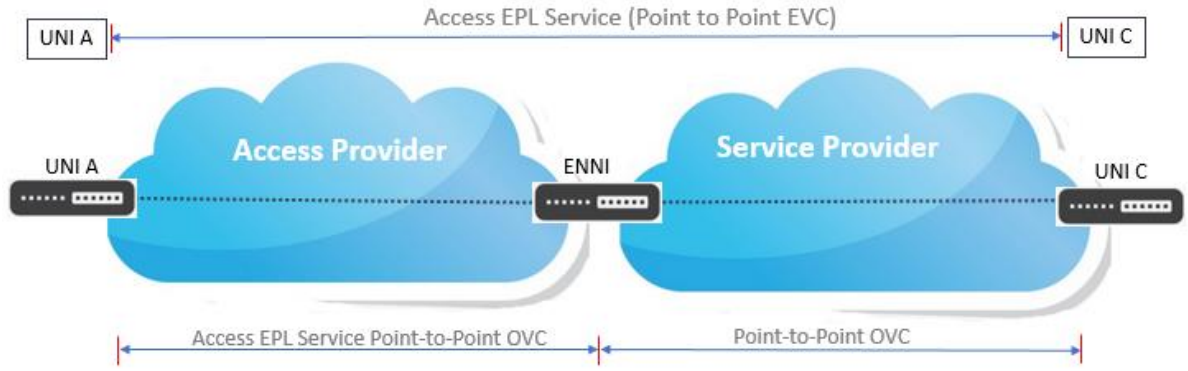

Figure 21. EPL Service across two networks using Access EPL. The subscriber's point of view is shown on top, and the service provider's view below. [15.]

E-LAN is a multipoint-to-multipoint service consisting of Ethernet Private LAN (EP-LAN) and Ethernet Virtual Private LAN (EVP-LAN) with multiplexing of multiple EVCs at each User-to-Network Interface (UNI). Using Ethernet Virtual Private LAN (EVPL) services it is possible to interconnect multiple sites so that they appear to be in the same LAN. [15.]

The EPL service supports also VLAN-based Ethernet Virtual Private Line (EVPL) multiplexed services. The figure 22 shows the subscriber and service provider for an instance of EPL Service offered by the service provider using Access EPL Service in a access provider network. [15.]

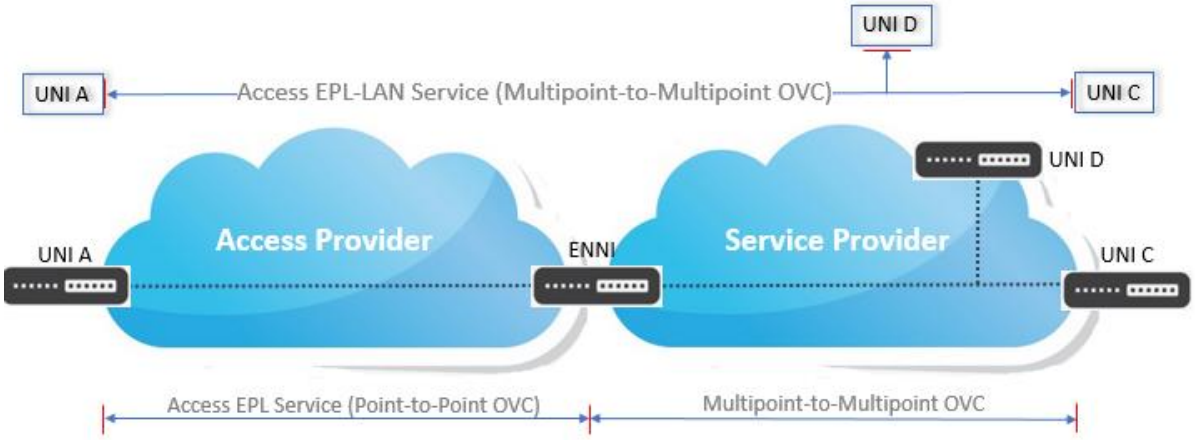

Figure 22. Access EPL-LAN Service. The subscriber's point of view is shown on top, and the service provider's view below. [15.]

It is possible for an Internet service provider to use Access EPL or Access EVPL Service to aggregate customers in access provider footprint (see Figure 23). Only EVCs are supported. [15.]

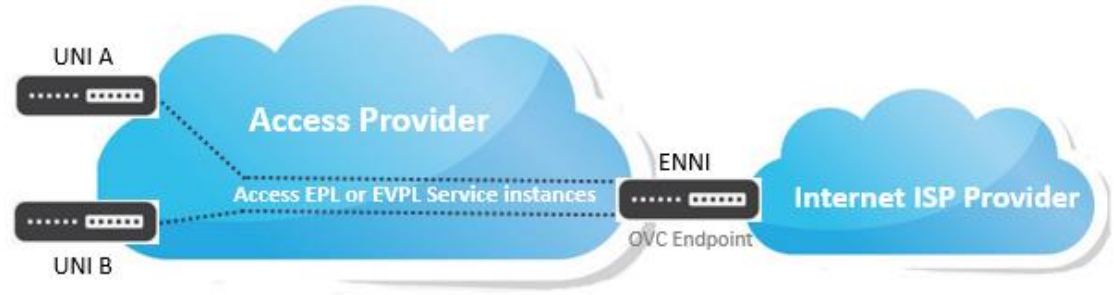

Figure 23. Access aggregation to Layer 3 services using Access EPL or Access EVPL. [15.]

3.3 Service Attributes

Carrier Ethernet specifications (MEF 10.3) contain three sets of generic ingress and egress service attributes, that can be applied at UNI: UNI service attributes, EVC (or OVC) at UNI service attributes, and EVC (or OVC) per COS ID at a UNI service attributes. UNI attributes are applied to all services on the UNI. They define physical capabilities of the interface, service multiplexing capability and C-VLAN bundling capability. [23.]

EVC per UNI service attributes are UNI attributes, but can be different on other UNIs within the EVC. An example is the Ingress Bandwidth Profile attribute, that can be different at each UNI. [23.]

EVC attributes apply to the EVC itself in the whole network. An example is the EVC Connection Type Attribute. The generic attributes are shown in table 5. [23.]

Table 5. Carrier Ethernet Service Attributes [23.]

UNI Service Attributes	EVC per UNI Service Attributes	EVC Service Attributes
UNI Identifier	UNI EVC ID	EVC Type
Physical Medium	CE-VLAN ID / EVC Map	EVC ID
Speed	Ingress Bandwidth Profile per EVC	UNI List
Mode	Ingress Bandwidth Profile per CoS Identifier	Maximum number of UNIs
MAC Layer	Egress Bandwidth Profile per EVC	EVC MTU size
UNI MTU Size	Egress Bandwidth Profile per CoS Identifier	CE-VLAN ID Preservation
Service Multiplexing		CE-VLAN CoS Preservation
Bunding		Unicast Service Frame Relay
All-to-one Bunding		Multicast Service Frame Relay
CE-VLAN ID for untagged and priority tagged Service Frames		Layer 2 Control Protocol Processing (only applies for L2CPs passed to the EVC)
Maximum number of EVCs		EVC Performance
Layer 2 Control Protocols Processing		
Ingress Bandwidth Profile per UNI		
Egress Bandwidth Profile per UNI		

There are two sets of generic ingress and egress service attributes, that can be applied at ENNI: per OVC at ENNI and per OVC per COS ID at an ENNI service attributes. if an OVC has end-points on more than one ENNI, attributes can have different values on each of them. The OVC per ENNI attributes are OVC End Point Identifier, Class of Service ID, and Ingress and Egress Bandwidth Profiles. [12.]

3.4 Quality of Service, Bandwidth profiles and Traffic management

Ethernet is a best-effort technology, and it does not contain any Quality of Service mechanism. In order to make QoS a number of tasks must be done, including traffic marking, traffic conditioning and congestion avoidance. Traffic marking is made in Ethernet by inserting

marks into the CoS field of the VLAN tag. In IP the marks are placed into the IP precedence/ToS field or the DS field. [12.]

Traffic conditioning occurs in UNIs, and consist of shaping and policing. Shaping is the process of delaying frames to make them follow the traffic profile. Policing is passing or discarding frames depending on traffic contract and profile. Congestion avoidance is based on priorization. [12.]

The most important parameter groups that define QoS are Bandwidth profiles and Service parameters. Bandwidth profiles (BWP) define how rate enforcement of Ethernet frames is processed at UNI or ENNI. It is also possible to offer a sub-rate bandwidth, which helps limiting the amount of bandwidth offered. For the subscriber, the bandwidth specifies the average rate of committed and excess frames. [12.]

The bandwidth profile per UNI is applied to entire UNI and the EVCs or OVCs at it. It is used in port-based services utilizing a single EVC or OVC. [12.]

The bandwidth profile per EVC or OVC at a UNI is applied to each EVC or OVC at a UNI. It is used with services with multiple EVCs (or OVCs) at a UNI, e.g. EVPL or Access EVPL. The UNI bandwidth is divided among EVCs or OVCs as shown in figure 24. [12.]

The bandwidth profile per EVC or OVC per CoS at a UNI is applied to frames that belong to each CoS at EVC or OVC at a UNI. It is used to create multiple classes of service. Each CoS is identified by its Priority Code Point (PCP) defined in IEEE 802.1p. Using this attribute, it is possible to partition the EVC bandwidth as shown in figure 24. [12.]

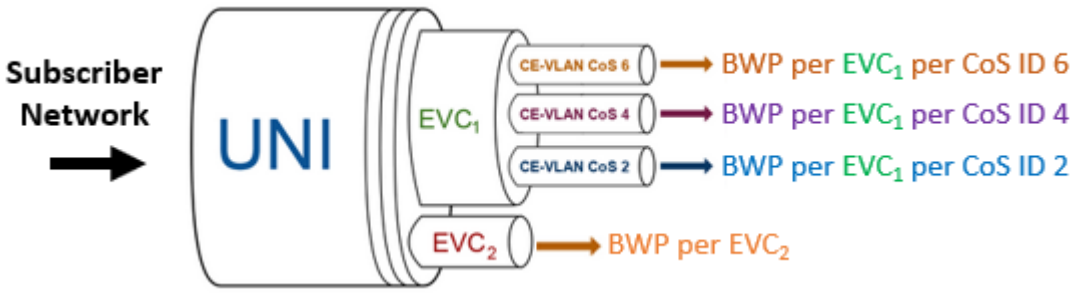

Figure 24. Ingress Bandwidth Profile per EVC per CoS. [12.]

The four bandwidth profile parameters defined by the Metro Ethernet Forum are Committed Information Rate (CIR), Committed Burst Size (CBS), Excess Information Rate (EIR), and Excess Burst Size (EBS). [26.]

CIR is defined as the average rate of frames for a CoS ID of an EVC per Service Level Objective (SLO) defined in the Service Level Agreement (SLA). The SLO is a performance agreement with the service provider contained in SLA. CBS tells the maximum number of bytes that can be sent in a burst without performance objectives. EIR is the average rate up to which the excess frames are allowed without performance objectives, as long as there is no congestion. The excess frames are not delivered per SLO. The frames whose average rate is greater than EIR will be discarded. EBS is the size up to which the traffic is allowed to burst without performance objectives. [26.]

The Color Mode (CM) parameter specifies UNI's operating mode, which can be color-aware or blind. The Color Modes are Green (Forwarded frames, CIR conforming traffic), Yellow (Forward with Best Effort frames, Over CIR, within EIR) and Red (Discarded frames, exceeds EIR). The marking is typically made at ingress. A bandwidth profile graph example is shown in figure 25. [12, 13, 26.]

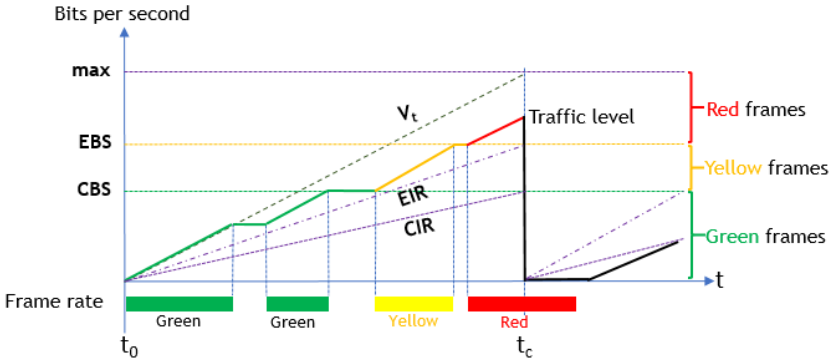

Figure 25. Bandwidth profile graph. [26.]

3.5 Service parameters

The service performance parameters are frame delay, jitter, and frame loss. The delay is a sum of processing delay, serialization delay and propagation delay. Jitter or delay variation is the difference in packet delay. Frame loss is the percentage of frames not delivered to the destination.

3.6 Service OAM

In Carrier Ethernet Networks, Service OAM (SOAM) is used to monitor connectivity and performance for entities. SOAM provides benefits to both the service provider and the subscriber. OAM packets are injected among normal Layer 2 data packets. The end points use them to determine performance, e.g. misconfigurations, data loss and delay, and bit error

rates. SOAM contains two functions, Connectivity Fault Management (CFM) and Performance Monitoring (PM). [14.]

3.7 Ethernet over MPLS

Ethernet frames can be forwarded across an MPLS network embedded in MPLS packets using label stacking (Ethernet over MPLS, EoMPLS). Using EoMPLS it is possible to utilize existing MPLS networks to provide EVPL service or EPLAN service.

4 Carrier Ethernet Example Cases

In this chapter, two cases are presented. They both are implementations of a large Finnish access provider. The first case is a point-to-point Layer 2 connection between an end user and service provider, and the second point-to-multipoint Layer 2 connection between a datacenter and customer's LANs. Ethernet frames are tunneled in Ethernet-over-MPLS tunnels inside MPLS packets, and forwarded through an MPLS-enabled core using label stacking (see chapter 2.5). In an EoMPLS connection all packets received from the local interface are forwarded to the remote interface.

4.1 Case 1. An Ethernet-Based Layer 2 Circuit Connection

In the first case an end user is connected to a service provider over an access provider network. The point-to-point connectivity is defined in the following standards: MEF E-LINE (see chapter 3.2), IETF RFC7432 (Virtual Private Wire Service, VPWS), RFC 2764 (Virtual Leased Line, VLL), and RFC 4665 (Service Requirements for Layer 2 Provider-Provisioned Virtual Private Networks). [27.]

A virtual connection is created to direct traffic between two Customer Edge routers across a network. CEs reside at the customer locations. They may be owned and operated either by the customer or by the service provider. Multiple Layer 2 VPNs or Layer 2 Circuits can be transported using a single LSP tunnel between two PE routers, that are at the edge of the service provider backbone network. Provider Routers inside the backbone network are a part of an LSP path. It is noted, that the connections are point-to-point circuits between two PEs. If multiple sites in the same broadcast are needed, Virtual Private Lan Service (VPLS) can be used instead. [27.]

In Junos OS there are three ways of creating a Layer 2 VPN between two sites. The legacy Circuit Cross-Connect (CCC) was not an option in this project. The other current industry standards are Kompella and Martini. [27.]

Kompella, which is called Layer 2 VPN (L2VPN) in Junos, is the recommended solution for interoperability features. Kompella uses a two-label stack to allow to use the same LSP for multiple circuits. The VC label is signaled via BGP. Virtual Circuits enable the carrier to assign dedicated bandwidth to each organization, as well as offering service level guarantees. Layer 2 VPNs are configured in a routing instance, and require BGP for transport of traffic between PE routers. Kompella is regarded as the best option for large scale deployments, but requires more complex configuration as Martini. [27.]

In Martini, which is called Layer 2 Circuits (L2circuits) in Junos, the same LSP can be used for multiple circuits using a pair of labels is used in front of the Layer 2 frame like in Kompella. Two labels are pushed onto the packet. Outer label is used in transport of the frame from ingress PE to the eggress PE. It is removed through penultimate hop popping before reaching the egress PE. Inner label, VC Label, informs the outgoing sub-interface from receiving PE to CE, where the L2VPN payload should go. It is removed at the egress PE. L2circuits use either LDP or RVSP for MPLS transport, and directed LDP for signaling the VC service label between the PE devices. L2circuits require less configuration than Layer 2 VPNs.

In the first case the configuration of devices is performed using L2circuits.In Junos the paths that emulate a Layer 2 point-to-point connection over a packet-switched network are called pseudowires. L2circuits are configured between two peers. They must use the same interior gateway protocol (IGP). They must have a symmetrical Layer 2 configuration and belong to the same routing domain or autonomous system. L2circuit uses Virtual Circuits to build a point-to-point Layer 2 connection over MPLS. Multiple VCs can be transported over a single LSP tunnel between PEs. [28.]

In figure 26 an end user CE2 is connected to a service provider edge PE0 over an access provider network.

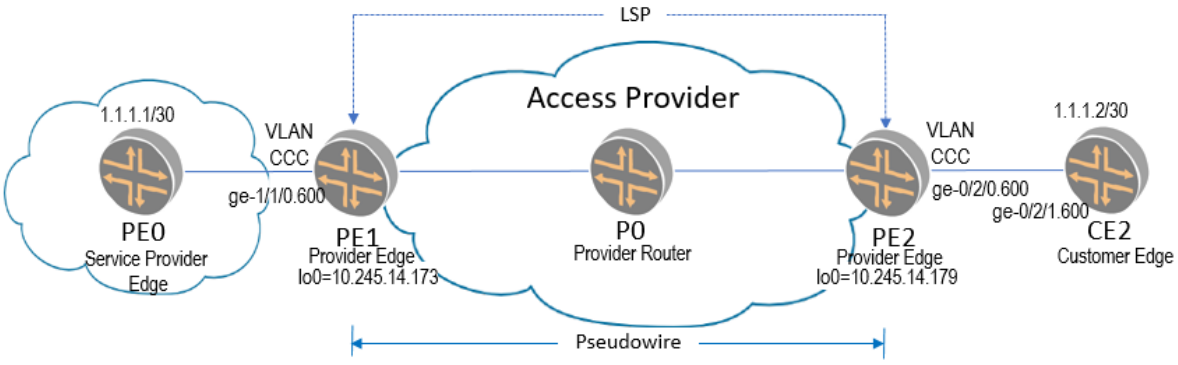

Figure 26. Ethernet-Based Layer 2 Circuit Configuration. [28.]

The PE routers maintain VPN forwarding tables, and exchange them with other PE routers. The MPLS provider router(s) on the LDP path is P0. The Provider routers have no awareness of VPNs. The Junos OS does not allow the same VLAN ID to be configured on more than one logical interface under the same pseudowire client physical interface. This restriction is bypassed using `vlan-ccc` encapsulation on the transport interface of the provider PEs,

which makes it possible to configure the same VLAN ID on more than one logical interface. VLAN CCC encapsulation supports Tag Protocol ID 0x8100 only. [28.]

The symbols and naming conventions used in the figure follow the guidelines of Juniper Inc. Network interfaces in Junos OS are specified by the media type, the interface location, the physical interface card (PIC) port, and logical unit number: `type-fpc/pic/port.logical`. In the notation `type` is the network device media type, `fpc` is the number of the slot in which the interface card is installed, `pic` identifies the number of the physical interface on the interface card, and `port` identifies a specific port. The `logical` unit part of the interface, separated by a period, corresponds to the logical unit number. In the figure type `xe-` stands for TenGigabit Ethernet interface, `ge-` stands for Gigabit Ethernet interface, `fe-` stands for Fast Ethernet interface, `vt-` for virtual loopback tunnel interface, and `lo-` for loopback interface. [30.]

CE2 uses an Ethernet-based interface to connect VLAN 600 to PE2. The IP addresses are allocated and configured by service provider. In most cases the CE2 equipment is provided by access provider.

In PE2 there is a Gigabit Ethernet interface `ge-0/2/0`, and loopback address `lo0=10.245.14.179`. PE1 has a Gigabit Ethernet interface `ge-1/1/0`, and loopback address `lo0=10.245.14.173`.

4.1.1 Equipment and interfaces

The hardware and software components used in this configuration in the access provider network consist of:

- Junos OS Release 9.3 or later
- 2 MX Series 5G Universal Routing Platforms

4.1.2 Configuring the L2circuit

No configuration is needed by the access provider on local CE (CE2). The Gigabit Ethernet interfaces are configured to handle VLAN traffic. The VLAN ID (600) must be same on PE0 and PE1. Junos OS CLI commands are organized under various hierarchies. Commands that perform a similar function are grouped together under the same level of the hierarchy. [28.]

The configuration of routers PE0 and CE2 is only partly shown in this report, in order to clarify general environment. To configure vlan tagging of VLAN 600 in PE1 and PE2, the `vlan-tagging` and `unit` statements are used at the `[edit interfaces ethernet-interface-fpc/pic/port]` hierarchy level. CLI configuration commands and corresponding configuration file on PE1 and PE2 using Junos OS CLI are shown below [28.]

```
set interfaces fe-1/1/2 vlan-tagging
set interfaces fe-1/1/2 unit 600 vlan-id 600
set interfaces fe-1/1/2 unit 600 family inet address 10.1.1.1/24
```

```
[edit]
interfaces {
  fe-1/1/2 {
    vlan-tagging;
    unit 600 {
      vlan-id 600;
      family inet {
        address 10.1.1.1/24;
      }
    }
  }
}
```

On PE1 and PE2, the Ethernet interface is configured with the CCC encapsulation type. The VLAN CCC is selected by including the `vlan-tagging` statement at the `[edit interfaces ethernet-interface-fpc/pic/port]` hierarchy level. The `encapsulation vlan-ccc` statement is included at both the `[edit interfaces ethernet-interface-fpc/pic/port]` and `[edit interfaces ethernet-interface-fpc/pic/port unit unit-number]` hierarchy levels.

The L2circuit is configured with the `l2circuit` statement at the `[edit protocols]` hierarchy level. The configuration in PE1 consists of the loopback address of PE2, the local PE0-facing interface and virtual circuit ID. The `ignore-mtu-mismatch` statement may be used to allow the connection, even though the MTUs on PEs do not match. On PE2 the configuration is similar. [28.]

```
[edit]
protocols {
  l2circuit {
    neighbor 10.245.14.179 {
      interface fe-1/1/0.600 {
        virtual-circuit-id 5;
      }
    }
  }
}
```

In addition to L2circuit configuration on, MPLS, LDP, and OSPF are configured at the `[edit protocols]` hierarchy level to enable signaling. On PE2, the L2circuit, MPLS, LDP, and OSPF are configured in the same way as on PE1.

The provider core P0 router only requires MPLS and LDP on the appropriate interfaces to enable labels to be shared between PE1 and PE2. [28.]

Complete configuration scripts are shown in appendix 1.

4.1.3 Verifying the configuration

The checking of Layer 2 circuit operations and status is performed using `show` and `ping` commands:

- `show l2circuit connections`
- `ping mpls l2circuit interface` *`interface-name`*
- `ping mpls l2circuit virtual-circuit virtual-circuit-id` *`neighbor ip-address`*
- `show ldp database`
- Change PE2 interface to Layer 3 and `ping` *`CE2 wan address`* (this requires the knowledge of the IP address used in CE2 from the service provider).

In the beginning the L2circuit status was tested using `show l2circuit connections` command on PE1. The command displays status information about Layer 2 virtual circuits from the PE to its neighbors. The output showed that the connection status (St) is Up.

The operability of the MPLS Layer 2 circuit connections was tested using `ping mpls l2circuit virtual-circuit 5 neighbor 192.168.245.16/30 detail.`

All entries in the LDP database were displayed using `show ldp database` command.

4.1.4 L2circuit connection experience and benefits

As seen in the case, the L2circuit connection is simple to configure and operate. Because L2circuit uses the LDP protocol instead of BGP, a simpler environment is accomplished, but each neighbor must be configured explicitly and, as a consequence, the scalability is lost.

The existing network design and operation can be utilised, and only the transport technology has changed from legacy to Carrier Ethernet, which results as increased efficiency at lower costs and reduced cost per data bit.

Additional benefits of adapting L2circuit are ease of change, flexibility, scalability and reliability. The solution can be applied for multiple applications via EVCs, allowing the management of VLAN traffic.

Checking the status is straightforward using native Junos commands. In addition to the commands shown in 4.1.3, the routing tables could be checked with `show route table` commands.

4.2 Case 2. Point-to-Multipoint Layer 2 VPLS

The second case consists of Ethernet-based point-to-multipoint Layer 2 VPN connection. Using BGP-based Virtual Private LAN Service it is possible for a service provider to connect geographically spread LAN networks to each other over an MPLS core. The LANs seem to be in the same LAN even though traffic is transmitted over service provider network. QoS is achieved using the services of the MPLS network. VPLS customers see the service provider network is a switch, that connects transparently all customer sites together. The difference compared with L2circuit connections, which functions as a point-to-point fashion, is that packets from one CE can be sent to all PE routers in a VPLS instance. The VPLS paths carrying VPLS traffic between PE routers are pseudowires. In VPLS configurations the CE device needs not necessarily to be a router, but the PE routers can be linked directly to Ethernet switches. This practice is not, however, advisable in all the circumstances. [29.]

In VPLS a full mesh connectivity is required, which can be established using BGP or LDP. In Juniper equipment BGP is used as a signaling protocol to discover Label Edge Routers and pseudowires. With BGP, PEs can signal VPLS membership and exchange the routing information required to setup VPLS connections. It, also, allows for auto discovery of new sites. [29.]

RSVP and LDP can be used to signal MPLS LSPs. LDP distributes MPLS labels in non-traffic engineering MPLS applications. RSVP provides support for dynamic signaling of MPLS LSP, and it also provides support for traffic engineering. [29.]

PE creates a separate MAC table for each VPLS. The MAC table is built by examining the addresses of received frames, that can origin from other PEs or from local CEs. Frames with unknown destination MAC addresses are flooded across VPLS. [29.]

The VPLS connectivity is defined in the following standards: MEF E-LAN, IETF RFC 4761 (Virtual Private LAN Service, VPLS, Using BGP for Auto-Discovery and Signaling), and RFC 4762 (Virtual Private LAN Service, VPLS, Using Label Distribution Protocol, LDP, Signaling). [29.]

In figure 27 a simple VPLS topology is configured between three user sites connected by CE1, CE2 and CE3. VPLS is enabled between PE routers. Packets from customer network are sent first to a customer CE, from where they are sent to a PE in service provider network. Before sending PE verifies the destination address of the VPLS packet is found in the routing table. If so, it sends the packet to the PE or CE. If not, it sends the packet to all other PEs and CEs, that belong to the same VPLS routing instance. The packets traverse across an MPLS label-switched path. When a PE receives a packet from another PE, it verifies that the address of it is the destination is found in its routing table. If so and if the destination is a local CE device, PE forwards the packet to it. Otherwise the packet is discarded. If PE cannot determine the destination of the VPLS packet, it floods the packet to all attached CEs. Traffic received from remote PE routers is never forwarded to other PE routers, which helps prevent loops in the core network. [29.]

CE routers are connected to their local PE router with Ethernet interfaces. The PE routers are connected to other routers by LSPs using service provider backbone running MPLS, BGP, RSVP, and OSPF. [29.]

CE1, CE2, and CE3 have local Gigabit Ethernet interfaces. In a VPLS routing instance, e.g. named `green`, PE1 has a local Gigabit Ethernet interface `ge-0/1/0`, and a loopback address `lo0=10.254.14.218`. PE2 has a local Gigabit Ethernet interface `ge-0/1/0`, and a loopback address `lo0=10.254.14.219` in the same `green` instance, and PE3 has a local Gigabit Ethernet interface `ge-0/1/0`, and a loopback address `lo0=10.254.14.220`. As a result, routers CE1, CE2, and CE3 send Ethernet traffic to one another as if they were physically connected to each other on the same LAN. [28.]

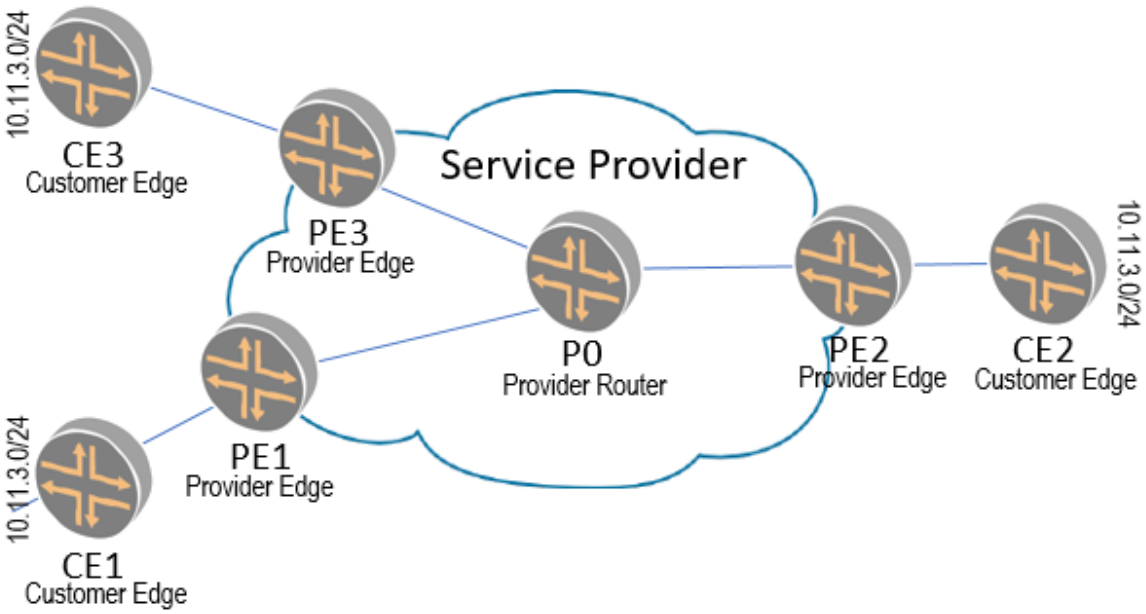

Figure 27. VPLS Topology Diagram.

Layer 2 information (MAC addresses and interface ports) is gathered by PEs and put in the VPLS instance tables. The router allows remote traffic for a VPLS instance to be delivered across an LSP and arrive on a virtual port. Traffic can be learned, forwarded, or flooded to the virtual port in the same way as the way traffic is sent to a local port. [28.]

4.2.1 Equipment and interfaces

The hardware and software components used in this configuration in the access provider network consist of:

- Junos OS Release 9.3 or later
- 3 MX Series 5G Universal Routing Platforms

4.2.2 Configuring the Layer 2 VPLS

Before configuring VPLS, configure the network so that the MPLS in the core is configured so that a label switched path exists between the PE routers. [28.]

The CEs, equipment in the customer network, are configured as if they were connected to a single bridge. No special configuration is required. The Fast Ethernet interfaces are configured to handle VLAN traffic. The VLAN ID (600) must be same on CE1m CE2, and CE3. On CE1 vlan tagging of VLAN 600 is configured at the `[edit interfaces ethernet-interface-fpc/pic/port]` hierarchy level. The configuration on CE2 and CE3 is similar. [28.]

On PE1, the Ethernet-based interface to CE1 is configured with the `vlan-tagging`. The VLAN VPLS encapsulation is included at both the physical and logical interface levels using `vlan-tagging` statement at the `[edit interfaces ethernet-interface-fpc/pic/port]` hierarchy level. The `encapsulation vlan-vpls` statement is included at both the `[edit interfaces ethernet-interface-fpc/pic/port]` and `[edit interfaces ethernet-interface-fpc/pic/port unit` *`unit-number`*`]` hierarchy levels. The VLAN ID is specifies at `[edit interfaces ethernet-interface-fpc/pic/port unit` *`unit-number`*`]` hierarchy level. [28.]

At the `[edit protocols]` hierarchy level the RSVP, MPLS, BGP and OSPF protocols are configured, the Fast Ethernet interface is added into a VPLS routing instance, and the site range, site ID number, and site name are specified. PE2 is configured in the same way as PE1. [28.]

The provider core P0 router requires BGP, MPLS, OSPF and RSVP need to be configured. [28.]

Complete configuration scripts are shown in appendix 2.

4.2.3 Verifying the configuration

The operation of VPLS is performed using `show` commands:

- `clear vpls mac-address instance` *`instance-name`*
- `show interfaces terse`
- `show route forwarding-table family mpls`
- `show route forwarding-table family vpls (destination | extensive | matching | table)`
- `show route instance (detail)`
- `show system statistics vpls`
- `show vpls connections`
- `show vpls statistics`

4.2.4 VPLS connection experience and benefits

VPLS provides offers an efficient way to interconnect multiple sites in a LAN type of configuration. The purpose of this case was to a put VPLS service in production for testing on a real scenario. Its behaviour in a real production network was analysed in order to research the benefits and usability. Using VPLS it is possible to connect hosts located in different geographic locations as if they were in the same LAN. VPLS uses client's Ethernet interfaces, which makes service provisioning rapid and flexible. The configuration and management of

the VPLS connection is, however, more complicated than the point-to-point L2circuit configuration in case 1.

The benefits of VPLS compared with legacy solutions are enhanced control over business, because all the remote sites behave together as if the were on the same LAN, no need for management of traffic on leased connections, because the connections use shared infrastructure, and efficient use of bandwidth with low round-trip latencies and jitter. In addition, less equipment is needed which lowers the costs of deployment, and all traffic can be delivered over a single Ethernet interface. MAC addresses are used to switch traffic between sites, and MPLS labels are used in the core, multipoint setup makes the management simpler than in earlier Ethernet solutions.

The limitations of VPLS are complexity of network management, because VPLS architectures need the support of many control protocols for VPLS management. Other limitations are limited scalability and granularity, lack of attack mitigation, and challenges with MAC address management.

5 Discussion and Conclusions

Although Ethernet being most widely used technology in LANs for more than 30 years, wide area networks were based on legacy techniques, like ISDN, Frame Relay, ATM, and MPLS up to the 2000s. In the beginning of this century, efforts to adapt Ethernet technology in metropolitan area networks started, and Metro Ethernet standards and solutions were introduced. Soon after that the next generation, Carrier Ethernet, was published, and Ethernet started gaining more popularity as a WAN technology. The success of Ethernet is based on its relative simplicity, ease of deployment, versatility, speed and low cost. Enterprise and network operators can also achieve savings by using same technology in corporate and carrier networks.

This project involves a theoretical background of Metro Ethernet and Carrier Ethernet services and applications, and a detailed presentation of two cases in access provider network utilising Carrier Ethernet. In the beginning of the thesis communications techniques, protocols, and conventions are introduced. The Metro Ethernet and Carrier Ethernet standards and topologies are then described in detail. Solutions using Carrier Ethernet as an alternative technology for current WAN connection services are discussed.

Two cases from a large national operator are represented. The architectural solutions, protocols, interfaces, equipment and configurations are shown. The networks are implemented and tested using physical equipment in a real scenario.

The first case consists of an L2circuit point-to-point connection over access provider MPLS network using Juniper equipment. The purpose was to use L2circuit between two sites, to connect the same subnet between two different geographic locations over an MPLS cloud. Configuring the connection is easy and straightforward, and the service provides rapid and flexible service provisioning. The connection was verified using native Junos commands. One of the most important benefit adapting L2circuit is, that existing network design and operation are used, and only the transport technology has changed from legacy to Carrier Ethernet, which results as increased efficiency at lower costs and reduced cost per data bit.

In the second case an Ethernet-based point-to-multipoint Layer 2 VPN connection was established to connect LAN networks over an MPLS core. A service provider can connect geographically spread LAN networks to each other using BGP-based Virtual Private LAN Service. The networks appear to be in the same LAN, even though the traffic is transmitted over the service provider's network. For VPLS customers the service provider network is shown

as a switch, that connects transparently all customer sites together. The difference compared with case 1's L2circuit connections, which functions as a point-to-point fashion, is that packets originating from one CE may be broadcast to all PE routers in a VPLS instance.

Because VPLS uses customer's Ethernet interfaces, service provisioning is rapid and flexible. In CE there are no requirements to map the logical connection to the remote site, they seem to be connected to a single bridge.

The MEF Layer 2 approach provides the best egression over legacy private line and packet services, because of its simplicity and possibility to run different applications over the same infrastructure and even over the same circuit. Layer 2 point-to-point is a flexible and cost-effective alternative to fast leased lines. Virtual Private LAN, on the other hand, is a simple and robust solution for delivering Ethernet services. Providers can utilize existing equipment. Label stacking allows multiple services over a single LSP, and there are no scalability problems with numerous VPN routes. For subscribers the main benefits are easy migration from existing Layer 2 environment, and ability to outsource WAN infrastructure.

References

1. Day J D, Zimmermann H. The OSI reference model. Proceedings of the IEEE 1983;71(12):1334-1340.
2. Stevens W R. TCP/IP illustrated. Volume 1, The protocols. Reading (MA): Addison-Wesley. 1994. ISBN 978-9332535954.
3. Jaakonhuhta H. Lähiverkot – Ethernet. IT Press 2005. ISBN 951-826-787-1.
4. Deering S, Hinden R. Internet Protocol, Version 6 (IPv6) Specification. ACM Digital Library. 1998. 10.17487/RFC2460.
5. Goralski W. The Illustrated Network: How TCP/IP Works in a Modern Network. Morgan Kaufmann. ISBN 978-0123745415.
6. Stevens W R, Wright G R. TCP/IP Illustrated, Volume 2: The Implementation. Addison-Wesley. 1995. ISBN 978-0201633542.
7. Huston G. TCP Performance. [ONLINE]. Available: https://www.cisco.com/c/en/us/about/press/Internet-protocol-journal/back-issues/table-contents-5/ipj-archive/article09186a00800c8417.html [Accessed December 2, 2018].
8. Halabi, S. Metro Ethernet. Cisco Press 2003. ISBN 1-58705-096-X.
9. De Ghein L. MPLS Fundamentals. Cisco Press. 2006. ISBN 978-1-58705-197-5.
10. Lakshman U, Lobo L. MPLS Configuration on Cisco IOS Software. Cisco Press. 2005. ISBN 978-1-58705-199-9.
11. Cisco Networking Academy's Introduction to VLANs [ONLINE]. Available: http://www.ciscopress.com/articles/article.asp?p=2181837&seqNum=5. [Accessed January 2, 2019].
12. Carrier Ethernet Essentials. Fujitsu. [ONLINE]. Available: https://www.fujitsu.com/us/Images/CarrierEthernetEssentials.pdf. [Accessed January 2, 2019].
13. Juniper Networks. Metro Ethernet Design Guide. [ONLINE]. Available: https://www.juniper.net/documentation/en_US/release.../metro-Ethernet-dg.pdf. [Accessed January 20, 2019].
14. Dicko H. Understanding Ethernet OAM. White paper 038. Exfo Inc. 2014.
15. Technical Specification MEF 33 Ethernet Access Services Definition. The MEF Forum 2012.
16. CE 2.0 Ethernet Access Services. MEF Informational and Technical Paper. October, 2013.
17. Elisa Carrier Ethernet Services. [ONLINE]. [Accessed February 18, 2019.]

18. Metro Ethernet palvelukuvaus - DNA Minun palveluni. [ONLINE]. [Accessed February 22, 2019.]
19. Telia Carrier. [ONLINE]. Available: https://www.teliacarrier.com/our-services/connectivity/ethernet.html?title=Ethernet%20Services. [Accessed February 19, 2019.]
20. MEF 3.0 Carrier Ethernet. [ONLINE]. Available: http://www.mef.net/mef-3-0-carrier-ethernet-mef-3-0-ce. [Accessed February 18, 2019.]
21. Carrier Ethernet 101: Speeds, Standards and Services. [ONLINE]. Available: https://www.ciena.com/insights/articles/Carrier-Ethernet-Speeds-Standards-and-Services.html?campaign=X827517. [Accessed February 18, 2019.]
22. Hawkins J.,Follis E. Carrier Ethernet. Ciena, Hanover, MD. 2016.
23. MEF. Technical Specification 10.3. [ONLINE]. Available: www.mef.net/PDF_Documents/technical.../MEF10.3.pdf. [Accessed February 19, 2019.]
24. MEF. Understanding Bandwidth Profiles in MEF 6.2 Service Definitions. [ONLINE]. Available: https//mef.net/Assets/White_Papers/Understanding_MEF_6.2_Bandwidth_Profiles_FINAL.pdf&usg=AOvVaw3rSH6OU4MAL-VuU2ymZ2Jh. [Accessed February 20, 2019.]
25. Juniper Networks Metro Ethernet Design Guide. Juniper Networks, Inc Sunnyvale, California. 2016.
26. Santitoro R. Bandwidth Profiles for Ethernet Services. [ONLINE]. Available: https//www.MetroEthernetForum.com. [Accessed February 20, 2019.]
27. MPLS Applications Feature Guide. [ONLINE]. Available: https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/config-guide-mpls-applications/config-guide-mpls-applications.html. [Accessed February 26, 2019.]
28. Juniper Networks. TechLibrary. [ONLINE]. Available: https://www.juniper.net/documentation/. [Accessed February 28, 2019.]
29. Juniper Networks. Layer 2 VPNs and VPLS Feature Guide for Routing Devices. [ONLINE]. Available: https://www.juniper.net/documentation/. [Accessed March 21, 2019.]
30. Juniper Networks. Interface Naming Overview. [ONLINE]. Available: https://www.juniper.net/documentation/en_US/junos/topics/concept/interfaces-interface-naming-overview.html/. [Accessed March 21, 2019.]

Ethernet-Based Layer 2 Circuit Configuration

Router Configurations

This page is left blank intentionally because of confidential company details.

Point-to-Multipoint Layer 2 VPLS

Router Configurations

This page is left blank intentionally because of confidential company details.