“Architecting Fiber Access for LTE backhaul with EPL in Access and IP Layer 3 in Core backbone.”

By

Mir Nawsif Arman

A report submitted in partial fulfillment of the Capstone Project for the degree of

Master of Science

In

Internetworking

Department of Electrical and Computer Engineering

University of Alberta

Abstract

This report is intended for my Capstone project, "**Architecting Fiber Access for LTE backhaul with EPL in Access and IP Layer 3 in Core backbone**" under the supervision of Juned Noonari. This report will discuss some of the legacy cellular technologies and how it has evolved over time. It will in details explain the current and future 'Long Term Evolution' technology and its components. The Mobile Backhaul properties required for supporting the current and future traffic load along with its operation will also be discussed. For the Access portion of this MBH, various transmission mediums (wireless and wireline) along with their capabilities such as rate and topologies will be considered keeping sustainability and scalability needs in mind. Carrier Ethernet Service with emphasis on EPL access will be detailed and how it can be implemented to better support this MBH. This network discussion will then be extended to the core backbone technologies running on IP and how it will work in conjunction with the CE® services to better utilize and benefit from it. A lab implementation is done to mock this network architecture from the access to the core and correlated to how EPL in access and IP/MPLS in the core will behave to better understand the prospects of this report.

Acknowledgements

I would like to express my sincere gratitude to **Juned Noonari** for his constant support and guidance throughout the duration of this Capstone Project. I have gained knowledge in various aspects of the telecom and networking technologies while completing this project. I would also like to thank the MINT Department for offering this unique program and also providing us with a great LAB to do the hands-on implementation.

Table of Contents

List of Tables

List of Figures

List of Abbreviations

3GPP	3rd Generation Partnership Project
ABR	Area Border Router
ADSL	Asymmetric Digital Subscriber Line
AS	Autonomous System
ASBR	Autonomous System Boundary Router
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
BS	Base station
BSC	Base Station Controller
BSS	Base Station System
BTS	Base Transceiver System
CDMA	Code Division Multiple Access
CE	Customer Equipment
CE®	Carrier Ethernet
CS	Circuit Switched
DSL	Digital Subscriber Line
EDGE	Enhanced Data rates for Global Evolution
eNodeB	Evolved-eNodeB
EPC	Evolved Packet Core
EPL	Ethernet Private Line
EPON	Ethernet Passive Optical Network
E-UTRAN	Evolved-UTRAN
EVC	Ethernet Virtual Connection
FDMA	Frequency Division Multiple Access
FEC	Forwarding Equivalence Class
FTP	Foiled Twisted Pair
GbE	Gigabit Ethernet
GBR	Guaranteed Bit Rate

GPON	Gigabit Passive Optical Network
GPRS	General Packet Radio Service
GSM	Global System for Mobile communication
IBGP	Interior Border Gateway Protocol
IEEE	Institute of Electrical and Electronics Engineers
IGP	Interior Gateway Protocol
IS-IS	Intermediate System to Intermediate System
ITU	International Telecommunications Union
LAPD	Link Access Procedure , Channel D
LER	Label Edge Router
LSP	Label Switched Path
LSR	Label Switch Router
LTE	Long Term Evolution
MBH	Mobile Backhaul
MEF	Metro Ethernet Forum
MIMO	Multiple Input Multiple Output
MMS	Multimedia Messaging Service
MPLS	Multi-Protocol Label Switching
MSC	Mobile Switching Center
MW	Microwave
NNI/ENNI	Network to Network Interface
OFDMA	Orthogonal Frequency Division Multiple Access
OLT	Optical Line Terminal
OSPF	Open Shortest Path First
OVC	Operator Virtual Connection
P2P	Point-to-Point
PDH	Plesiochronous Digital Hierarchy
PDN	Packet Data Network
PE	Provider Edge
PGW	PDN Gateway

PON	Passive Optical Network
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RAN	Radio Access Network
RSVP	Resource ReserVation Protocol
SDH	Synchronous Digital Hierarchy
SGSN	Serving GPRS Support Node
SGW	Serving Gateway
SONET	Synchronous Optical Network
STM	Synchronous transport module
STP	Shielded Twisted Pair
TCP	Transmission Control Protocol
TDM	Time Division Multiplexed
TDMA	Time Division Multiple Access
UDP	User Datagram Protocol
UE	User Equipment
UMTS	Universal Mobile Telecommunications Service
UNI	User Network Interface
UTP	Unshielded Twisted Pair
UTRAN	Universal Terrestrial Radio Access Network
VDSL	Very high bit rate digital subscriber line
VoIP	Voice over IP
VPN	Virtual Private Network
WAP	Wireless Access Protocol
WCDMA	Wideband CDMA
WDM	Wavelength Division Multiplexing

--------------------------Blank-Page---------------------------

1.0 Introduction

With the drastic increase in mobile subscribers along with the increasing traffic generated, it has become crucial to provide infrastructure, design, and solutions that can not only support the current needs but also support future demands and prerequisites. Long Term Evolution (LTE) being the ‘must implement’ mobile technology for current needs, it has become essential to discuss the advancements necessary to keep LTE sustaining and prepare for more. This paper will discuss various legacy network technologies along with LTE from the Radio Access Network (RAN) to the Evolved Packet Core (EPC); also known at the Mobile Backhaul (MBH). The wireless and wireline transport mediums will be discussed along with their capabilities, limitations and future prospects. This will then be presented with possible access network topologies. Carrier Ethernet will be discussed in details including its services and how they operate plus its advantages. Further discussion will be done where we will discuss the possibility of implementing Access Ethernet Private Line (EPL) in the Access network of the MBH and how it can be advantageous. The Layer 3 core network will be discussed and how it plays a significant role in LTE MBH. The later part of the report will include a design of a network to provide an example how MBH performs from the access network to the EPC. This will include the proposed idea, its setup, configuration and testing.

1.1 What is Backhaul?

Backhaul in general means getting information from a core network to the edge network and vice versa. The portion of the cellular network which links the mobile network to the transport network is called Cellular Backhaul or Mobile Backhaul (MBH). In this case, MBH becomes the transporting medium for all data that has to travel to/from the Core Network and Radio Access Network (RAN), often known as base stations. MBH was introduced because there are a significant number of mobile network base stations spread around a geographical area and they all must somehow be connected to fewer or single mobile network, and this is where MBH comes in. It is responsible for aggregating all traffic from the base stations and transporting them to and from the core network. A cell site refers to a single Base Station (BS) or a collection of BS within a designated area and is connected to the Aggregation network.

1.2 Why is MBH important?

MBH is one of the key elements of the whole wireless industry mainly because it is responsible for efficient transportation of all data through it though it is not responsible for any data processing. As the mobile network technologies advance through time (2G>3G>4G….), MBH technologies also have to keep up to accommodate this increase in rates, increase in bandwidth, better Quality of Service (QoS) and more efficient. This is mainly because MBH plays a major role in the end-to-end performance and quality of the mobile network and without this, the advancements of Radio technology is almost useless as this acts as the backbone to the Mobile Network. For our discussion, we will separate the MBH in two parts, the Access Network, and the Aggregation network. The MBH design and architecture is primarily based on the radio access technology, location of cell sites, traffic flow patterns, QoS and BW.

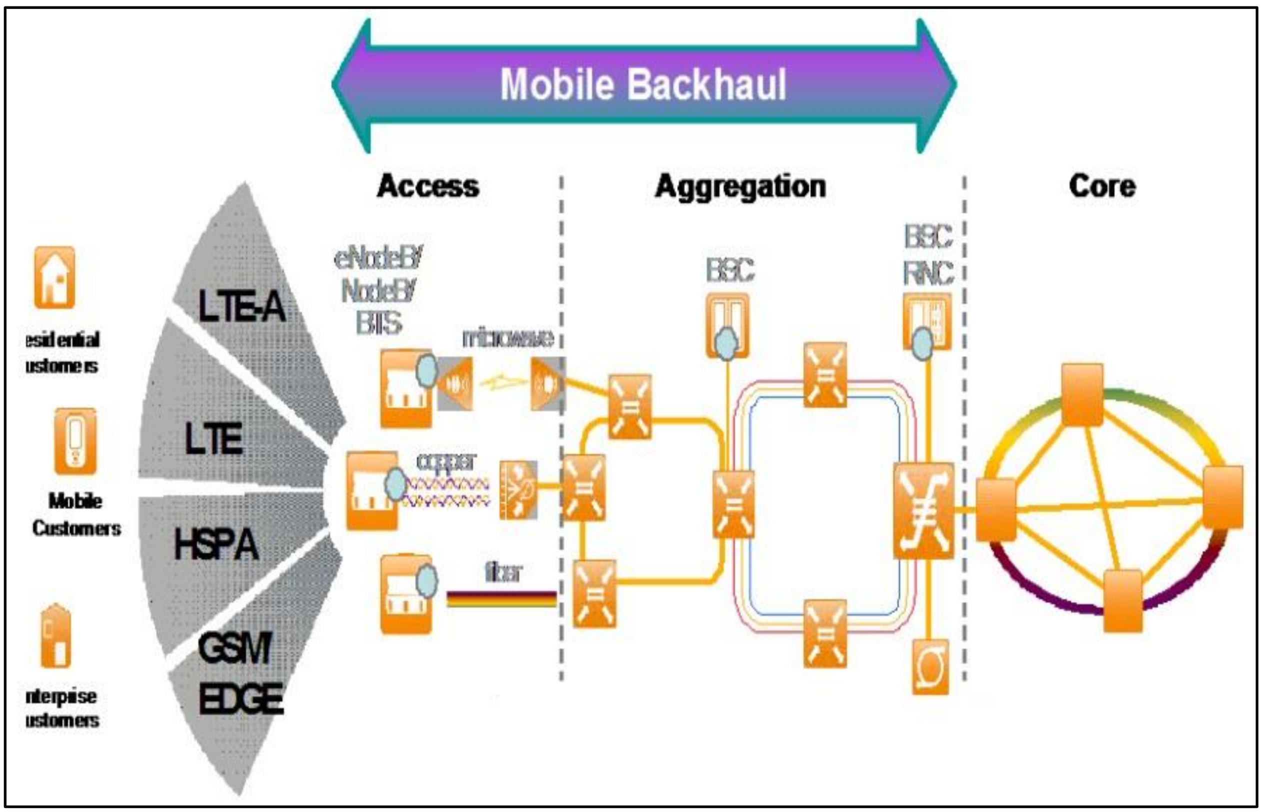


Figure 1: Mobile Backhaul [1]

2.0 Legacy 2G Backhaul

The initial target of 2nd Generation (2G) network was to provide voice services using digital communication as compared to the legacy 1G analog network. This change also allowed the implementation of Short Message System (SMS) for the first time. 2G standardized Time Division Multiple Access (TDMA) and Code Division Multiple Access (CDMA) as their radio access technology. The initial and most popular 2G network was Global System for Mobile communication (GSM) which was based on TDMA. For our purpose, we will discuss the architecture of GSM to give an idea of what 2G backhaul consist of.

For 2G GSM, the MBH access network starts from the Base Transceiver System (BTS) which is the radio access point for the Customer Equipment. Multiple of these BTS are connected to a Base Station Controller (BSC). Multiple BTS that serve a designated area and become part of a common network connect to this single BSC. BSC can be briefly described as the brain of all BTS and it responsible of how and what the BTS can or should do. This is often known as Base Station System (BSS). Multiple BSC then connects to a Mobile Switching Center (MSC) which resides in the Core Mobile Network. The communication between the BTS and MSC is considered as the backhaul for 2G GSM.

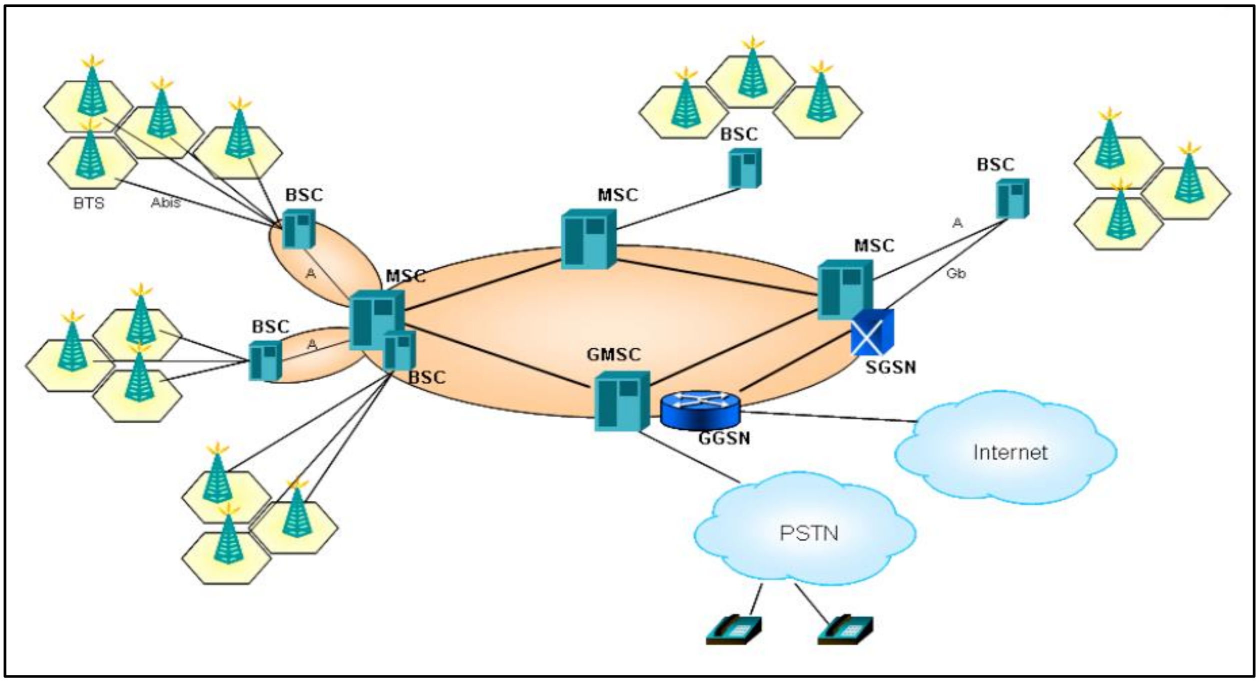


Figure 2: Typical GSM Network [2]

The standardized interface between BTS and BSC is known as *Abis* interface whereas the interface between BSC and the MSC is known as the *A* interface. The user plane responsible for carrying voice traffic in 2G backhaul is Circuit Switched and is Time Division Multiplexed (TDM). The BTS consists of transceivers(s) (TRX) and a switching device which can be linked to BSC by either individual or grouped format using *Abis* interface. The control plane between the BTS and BSC uses Link Access Procedure , Channel D (LAPD) as its control plane protocol also using the *Abis* interface. The traffic channels in *Abis* interface can carry encoded speech in full rate (TCH/F) or half rate (TCH/H) or Circuit Switched (CS) data. The full rate is considered as 12.2kbit/s and half rate as 5.6kbit/s. Therefore, traffic channel (SDC) capacities are 8, 16 or 64 kbit/s with the ability to combine multiple channels and the signaling channel (SCH) capacities are 16, 32 or 64 kbit/s. [3] The signaling system between MSC and BSS happens in the A interface using signaling system No.7(SS7) which is a reliable transport mechanism.

The standard for all the GSM interface and physical layer specifications were set by 3rd Generation Partnership Project (3GPP) and the Intermediate System to Intermediate System (ITU). As per 3GPP, "*Layer 1 shall utilize digital transmission at a rate of 2 048 kbit/s with a frame structure of 32 x 64 kbit/s time slots, as specified in ITU-T Recommendation G.705 clause 3 or at a rate of 64 kbit/s.*"[3]. Following this standard, the most commonly used was T1/E1. E1 having the capability of 32 time slots of each 64 kbit/s. These time slots have sub-timeslot of 8 or 16 kbit/s.

The next advancement to 2G is also known as 2.5+G where packet switched data services were introduced and standardized along with capabilities for Internet access, Wireless Access Protocol (WAP), and Multimedia Messaging Service (MMS). These technologies include the General Packet Radio Service (GPRS) and Enhanced Data rates for Global Evolution (EDGE). This included the introduction of Gb interface between the Serving GPRS Support Node (SGSN) at MSC and BSC. Edge used a more sophisticated modulation technique (8PSK) to increase the network capacity.

When 2G was first introduced, microwave or one to three T1/E1 was sufficient for the physical layer to carry the required bandwidth. But, as the number of customers increased along with the introduction of data services, it would soon require more bandwidth.

3.0 Legacy 3G Backhaul

The Third Generation Mobile (3G) technology was developed to support more multimedia data services along with increased data rates. There were various technologies in the 3G period by the IMT such as Universal Mobile Telecommunications Service (UMTS) and CDMA2000. For our purpose, we will discuss the Universal Mobile Telecommunication System (UMTS) for comparison. The standards for UMTS are set by the 3GPP body. This generation of mobile network tried to deliver requested data rates, smoother functionality, various application support and provide multi-level of QoS for different user traffic. The main backhaul components of 3G backhaul are:

- Base station (BS)
- Radio Network Controller (RNC)
- Mobile Switching Network (MSC)
- Serving GPRS Support Node (SGSN)

In comparison to 2G, the BTS is now named as NodeB, and the RNC can be compared to the BSC. The MSC and SGSN are parts of the CN. The backhaul for 3G can be considered from the NodeB to the CN. The 3G backhaul was designed to carry Circuit Switched traffic, Packed Switched traffic and/or both in order to comply with legacy 2G networks as well as cope with the increased demand for data traffic and services.

The NodeB uses Wideband CDMA (WCDMA) as the air interface for the radio access technology. Since WCDMA uses a higher frequency, more bandwidth, and more concurrent users, more NodeBs are required to support the cell coverage. Each NodeBs in a particular area have direct links to a single RNC and that RNC acts as the resource controller and management for multiple NodeBs' within that designated area. The interface between the NodeB and RNC is called the IuB. The NodeB can theoretically handle downlink up to 168 Mbit/s with eight carriers aggregated [3].

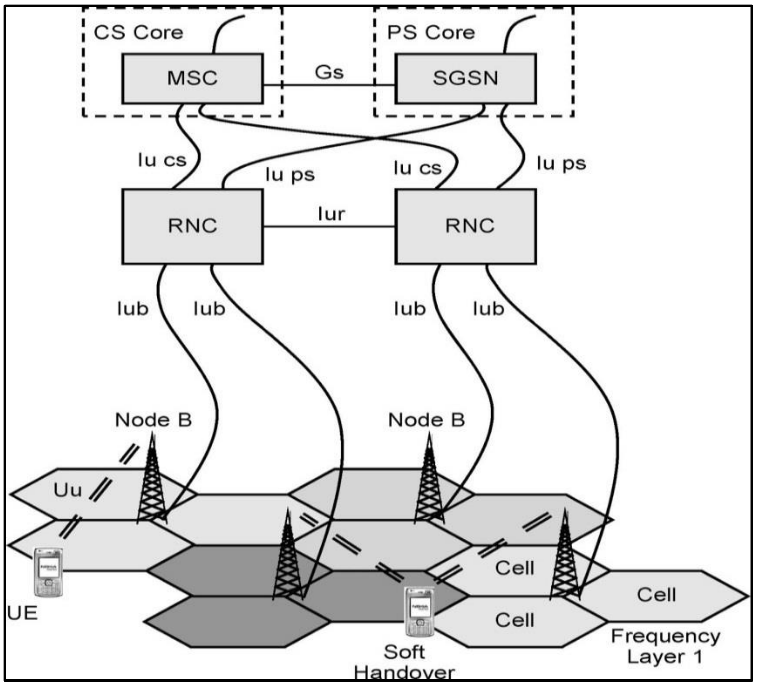


Figure 3: 3G Backhaul Architecture [4]

Then, multiple RNC that covers a whole metropolitan city communicates between each other through the IuR interface which allows them to implement Soft Handovers of the User Equipment (UE) without consulting with the CN. The RNC communicates with the CN using Iu interface. This interface is further divided into Iu-ps for packet switched traffic and Iu-cs for circuit switched traffic. The Circuit Switching is used primarily on real-time data such as voice and is connected to the Public Switched Telephone Network (PSTN) whereas packet switched is used for the rest types such as data and is linked to the Internet through the SGSN.

The 3G backhaul is primarily based on Asynchronous Transfer Mode (ATM) transport technology which was eventually moved to IP-based as 3GPP kept updating their specifications. 3GPPs initial Rel-99 defines the ATM standard for the IuB link. The traffic was separated using VCCs for a different kind of traffic characterization. This link can use multiple physical methods such as ATM over narrowband TDM E1/T1, Synchronous Optical Network (SONET)/ Synchronous Digital Hierarchy (SDH), and Microwave. This was same for the IuR interface and Iu interfaces. This was then moved to complete IP based with the release of 3GPP Rel-5. This meant that CS was no longer required for 3G as Voice over IP (VoIP) (standardized in Rel-7) was possible unless legacy support was required. [3]

4.0 LTE

4.1 What is LTE?

LTE stands for Long Term Evolution and is the Fourth Generation (4G) network. From the 3G UMTS, this network was heavily modified and overhauled mainly due to the excessive growth and demand for mobile networks to provide more traffic and lower cost. The initial requirements for 4G networks were set by ITU and 3GPP standardized the mobile network known as LTE. There was considerable change in both the air interface and the backhaul networks. The radio access was standardized for OFDMA, Orthogonal Frequency Domain Multiple Access for downlink, and SC-FDMA, Single Carrier FDMA for uplink. This means that the air interface combines frequency, time and coding methods to increase the bandwidth, speed and efficiency. High throughput, low latency and better optimization of battery life were enabled by the use of Multiple Input- Multiple Output (MIMO) in the UE.

The backhaul section went through a bigger change, and it was the implementation of the complete IP-based system and simplified flat network architecture with one core responsible for both voice and data. This network was completely based on packet-switching eliminating the concept of circuit-switching in the network. Circuit Switched data now had to be run over IP. This provided end-to-end IP connectivity between the end-user and the LTE provider. Unlike ATM –based backhaul, this IP-based transport system resulted in improved implementation and lower cost. There has been an extreme increase in the bandwidth it can carry, much higher data rates and lower latency.

4.2 Components and Properties of LTE.

When speaking of LTE backhaul, the first thing that comes is the Base Station. In LTE, the BS is called the Evolved-eNodeB (eNodeB). This was the first standard, which allowed the intercommunication of BSs without the need of any controlling element. In short, elements such as BSC and RNC were completely eliminated. The eNodeB is now responsible for all radio management, similar to 3G RNC thus making the network flatter, faster and simpler. Though, there are options to communicate with other eNodeBs when there is no communication link between them. The eNodeB now directly connects to the core network. This section of the backhaul is termed as the E-UTRAN (Evolved Universal Terrestrial Radio Access Network)

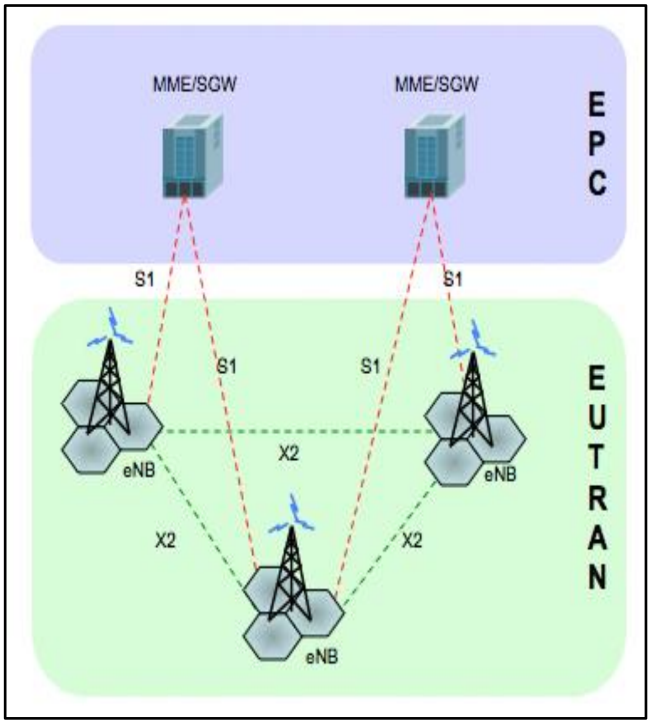


Figure 4: Basic LTE Architecture [5]

The CN primarily consists of the MME and P/S-GW. Since the core network is flat and is pure IP based, it's known as the Evolved Packet Core, EPC. The EPC is responsible for building and tearing bearers to the UE for the transfer of IP traffic through the E-UTRAN. The MME, Mobility Management Entity which has direct communication to all eNodeB is responsible for the key-control of the LTE Access Network. This includes functions such as Authentication, Authorization, and Accounting. The role of MME control plane can be compared to 3G SGSN control plane and is responsible for managing the bearers, authenticating the UEs, and managing mobility [3]. This control plane entity for LTE system connects to the eNodeBs using S1-C interface.

Then we have the S-GW, Serving Gateway and P-GW, Packet Data Network Gateway which behaves as the user plane entity. This two are often referred to as the Serving and Packet data network gateway, SP-GW. The eNodeB connects to this portion of the CN using the S1-U user plane. The S-GW, comparable to SGSN data plane, is responsible for inter-mobile-system management such as inter-eNodeB mobility (in the case when there is no communication between the eNodeBs) and for hand-overs towards 2G and 3G systems. The P-GW acts as the interface between UE's and the external network (i.e., the Internet).

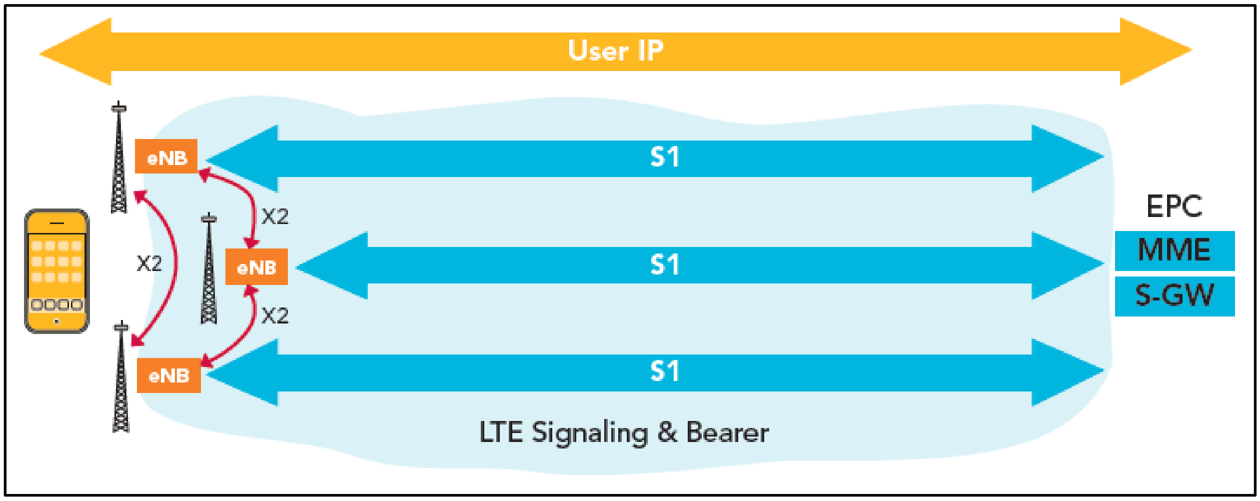


Figure 5: LTE Logical Architecture [14]

The eNodeBs are far more intelligent and capable of performing tasks that were previously done by intermediate nodes in the network. The eNodeBs can now perform tasks such as radio related functions and controller functions. They can communicate with each other in a peer to peer technique using the X2 logical interface.

X2 Interface

The X2 interface is designed for communications between neighboring eNodeBs and allows them to carry out handovers without going to any other network elements in the access/backhaul. Here, the eNodeBs communicate with each other directly on certain tasks. This optimizes the handover process making area/coverage change seamless, better resource management, lower setup time, reduced loss and lower cost. Even though this interface has both control and data plane, it does not need to have a significant volume requirement since it will only deal with handovers and not a continuous transmission. This will result in data plane traffic of X2 to be an in the lower ranges of the S1 data plane. At an average, the bandwidth will be a maximum of

2%-5% of the S1 traffic and the bandwidth for the signaling plane is considered negligible since it is in the kbps range. [25]

In comparison to legacy technologies, the resource management and handover process was carried out by the RNC. In this new LTE flatter architecture, it is done by the more intelligent eNodeBs. This X2 interface is a logical link which can be set up over the existing transport network with the option of point-to-point physical links. Regardless, it is this interface that allows the elimination on intermediate nodes as shown in the following figure:

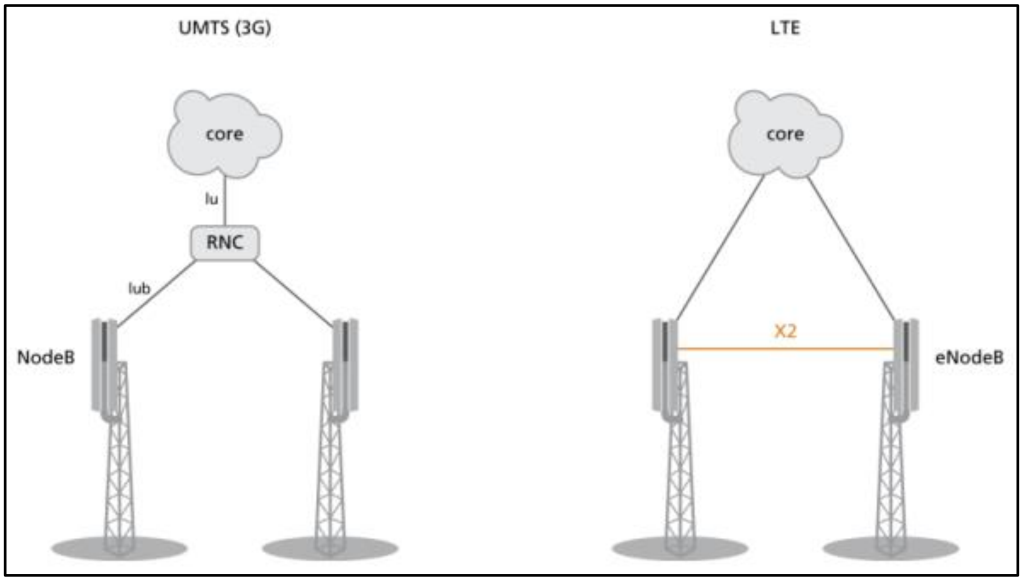


Figure 6: Legacy handover VS X2 interface handover in LTE [25]

X2 interface is primarily configured between neighboring nodes where there are areas of overlapping cell coverage and to facilitate a smooth handover for a moving UE or interface coordination is necessary.

There are multiple reasons why the carriers and LTE providers implement the X2 interface even when it is optional. In addition to the handover advantages mentioned above, it can do various other network related functions which make the overall QoS and resource management more efficient by keeping some basic processes local between neighboring eNodeBs. The functions that are supported by the X2 interface are as below:-[25]

- Handovers
- Load Management
- CoMP: Coordinated Multi-Point transmission or reception
- Network Optimization
- eNodeB configuration and updates
- Mobility Optimization
- General Management

The majority of X2 interface task is carried out in its control plane, but the data plane is also used for a brief period of time when the actual handover is taking place to pass on the user data until the handover is complete. The X2 interface communication is standardized so that there is interoperability between multiple vendors.

X2 interface based handovers in the LTE architecture is termed as 'hard handover'. In comparison to legacy architectures, where soft-handovers was used, which is made before make to make sure that the connectivity is maintained. Whereas in LTE, fast break before making is used over this interface. The following figure illustrates the overview:

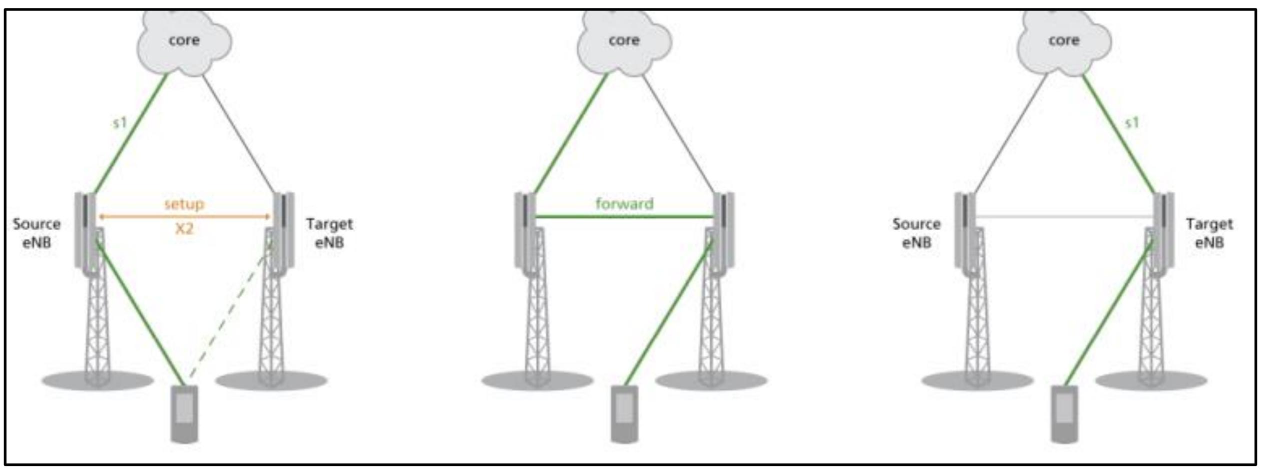


Figure 7: X2 assisted handover [25]

In reference to the figure above, the moving UE detects signals from the approaching eNodeB. This is then reported to the serving eNodeB which at some point decides that the other eNodeB can serve the UE better or is going out of reach. This is when the handover requests are sent over the X2 interface. On receiving the request, the target eNodeB does its own management calculations such as resource availability, admission control, etc. and when the request is accepted, the acceptance is sent to the serving eNodeB. The serving eNodeB then passes the connectivity details to connect to the target eNodeB. Once the UE connects to the target eNodeB, the X2 data plane is used to transmit the user data to the target eNodeB until the information is updated at the EPC. Once EPC has updated it send the user traffic directly to the target eNodeB. The following sequence diagram will give an over view:

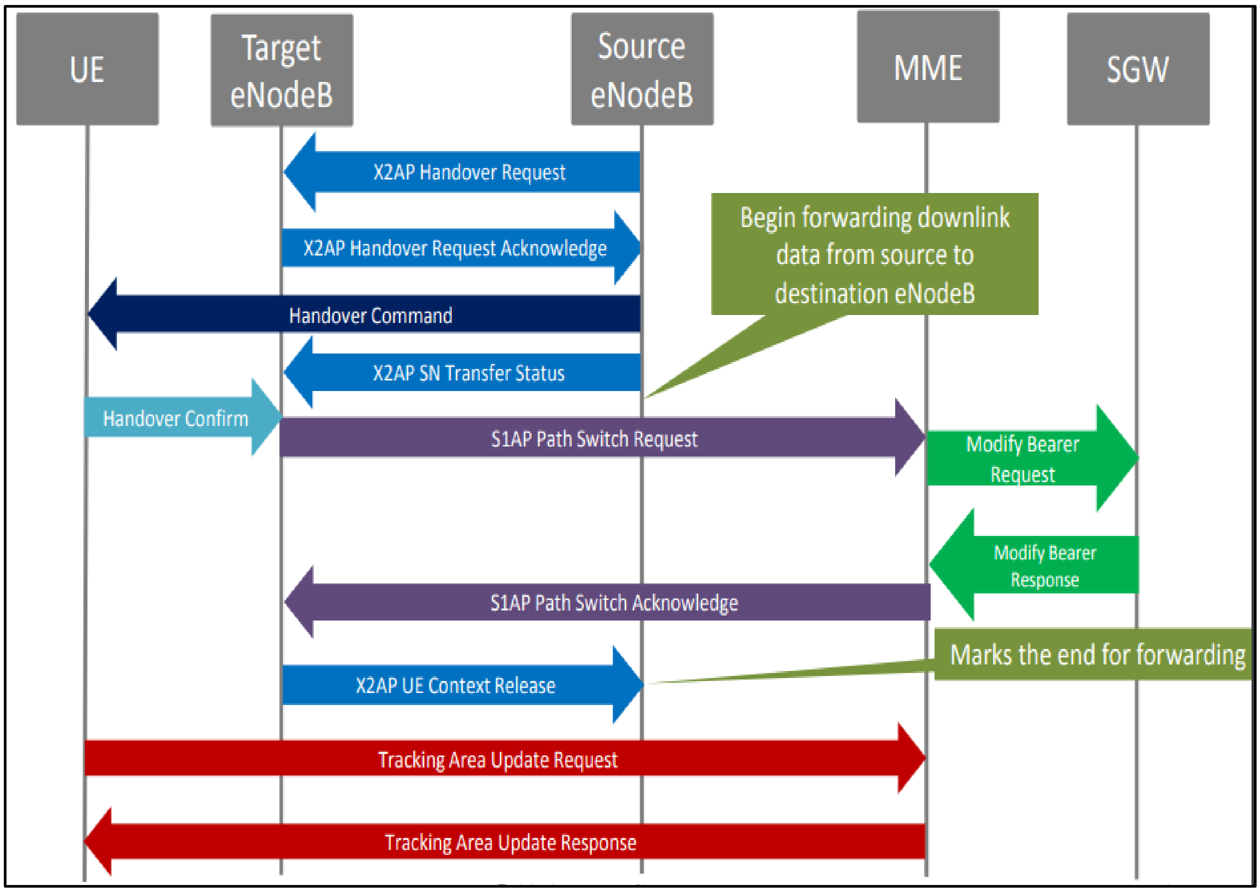


Figure 8: X2 Handover sequence diagram [26]

As per NGMN, the end to end delay in a standard LTE communication should be less than 10ms. This standard is even applicable when X2 is tasked with user data forwarding. Ideally, the combined delay of S1 delay and X2 delay should be less than 10ms. This interface design has to be considered when the backhaul is being designed to make sure that intercommunication between the eNodeB is efficient and standards are maintained. In theory, up to 32 neighboring eNodeBs can be connected to a single eNodeB via the X2 interface, but in real deployments, this number is less than 10. [27] Since X2 is a logical interface as mentioned above, there are multiple backhaul architecting options when designing the backhaul. The interface can be over direct physical links between the eNodeBs, It can be via the starting or ending Aggregation Node. This solely depends on the design and standard requirements. The following diagram gives an example:

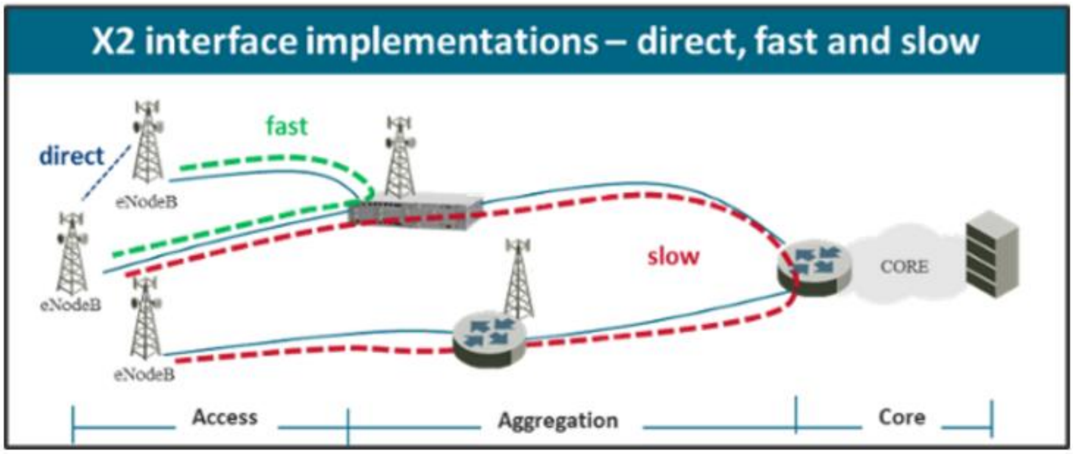


Figure 9: Physical Link possibilities for X2 logical interface [28]

The IP layer is not standardized like 3G (i.e. ATM), thus making it possible to use various protocols such as Ethernet or Point-to-Point Protocols. LTE enabled high-speed, low latency mobile backhaul by providing simplified system architecture by removing intermediate network elements and having an all IP-based network. The following figure gives a bird's eye view of LTE backhaul components and functionalities: -

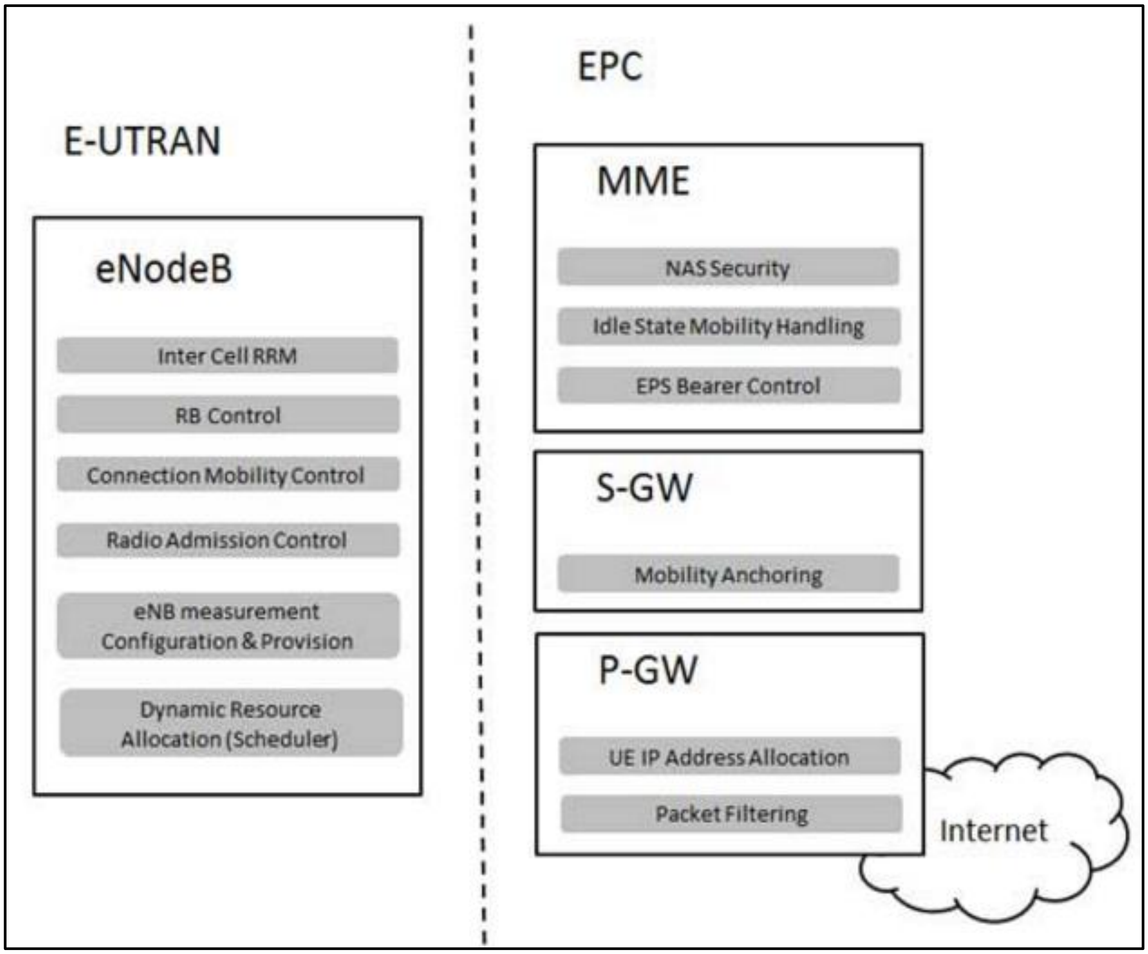


Figure 10: LTE Network Element Functionalities [6]

In LTE architecture, when a UE is making a call, the EPC creates a bearer between the IP targeted UE and the Packet Data Network (PDN) having a certain/specific QoS to carry the VoIP traffic. If the user wishes to use the internet at the same time, the EPC will create a new bearer for the data service with a different required QoS. Two kinds of bearers are defined, Guaranteed Bit Rate (GBR) and non-GBR. GBR provides guaranteed bit rate, and this is for the services that need some kind of minimum resources to meet the service standard such as VoIP. On the other hand, non-GBR is used for application in which are not time sensitive, and best-effort delivery is sufficient such as web browsing.

QoS

In LTE architecture, the initial QoS mapping is done at the bearer level. For different QoS, separate bearers are required along with the default bearer that supports any IP service connectivity. This QoS architecture is responsible for scheduling and queue management policy, RLC configurations and a shaping policy which indicated in the by the Quality of Service Class Indicator (QCI). Then we have the Traffic Flow Template which decides which bearer should be used by which user. This is enforced at the UE for uplink transmission and at the EPC/PDN GW for downlink transmissions. In the core network, we have the Service Data Flow (SDF) which is concerned with the Policing and Charging Control (PCC). [3]

As discussed in the previously, a bearer is set up between the UE and the PGW in the EPC. Before establishing this bearer, PCC rules are required to detect the SDFs and will set the QoS parameters. Multiple bearers are required for different types of service and for different QoS classes. It is important to note that the QoS specified all nodes in-between the UE and the EPC must have the resources to accommodate the required QoS. 3GPP has set the standards for QoS aspects. Firstly, many types of applications are involved in LTE transmission. 3GPP has defined them into four classes as shown below:

Traffic class	**Fundamental characteristics**	**Example of the application**
Conversational Real-time	- Preserve time relation (variation) between information entities of the stream. Conversational pattern (stringent and low delay)	-Voice (VoIP)
Streaming Real-time	- Preserve time relation (variation) between information entities of the stream	- Streaming video
Interactive best-effort	- Request response pattern - Preserve payload content	- Web browsing
Background best-effort	- Destination is not expecting the data within a certain time - Preserve payload content	-Background downloads, non realtime

Figure 11: 3GPP defined traffic classes for LTE [33]

Also, as discussed above, the bearers are divided into two categories, GBR and non-GBR. This is indicated by the QCI. QCI is further divided into nine classes as shown below:-

QCI	Resource Type	Priority	Packet Delay Budget	Packet Error Loss Rate	Services
1	GBR	2	100 ms	1e-2	Conversational Voice (VoIP)
2		4	150 ms	1e-3	Conversational Video (Live streaming, Video call)
3		3	50 ms	1e-3	Real Time Gaming
4		5	300 ms	1e-6	Non-Conversational Video (Buffered Streaming)
5	Non-GBR	1	100 ms	1e-6	IMS Signaling
6		6	300 ms	1e-6	Video (Buffered Streaming) TCP Based (www,email,ftp, p2p filesharing etc…)
7		7	100 ms	1e-3	Voice, Video (Live Streaming), Interactive Gaming
8		8	300 ms	le-6	Video Buffered Streaming) TCP Based (www,email,ftp, p2p filesharing etc…)
9		9			

Figure 12: 3GPP standardized UCI classes [33]

4.3 Summary of Mobile Technologies

Table 1: RAN of Mobile Technologies [18]

MOBILE TECHNOLOGY GENERATION	TYPE OF TECHNOLOGY	RAN COMPONENTS	EXAMPLE OF ROLE
Generation			
2G	GSM	BTS BSC MSC	• Communication between air interface and BSC • Controls multiple BS • Handles voice calls and SMS
2.5G	GPRS	BTS SGSN GGSN BSC + PCU	• Communication between air interface and BSC • Mobility management, data delivery to and from mobile user devices • Gateway to external data network • Controls multiple BS and processes data packets
3G	EVDO	BTS RNC PDSN	• Communication between air interface and RNC • Call processing and handoffs, communication with PDSN • Gateway to external network
	UTRAN	NodeB RNC MSC	• Performs functions similar to BTS • Performs functions similar to BSC • Handles voice calls and SMS
4G	LTE	eNodeB SGW (Serving Gateway) MME (Mobility Management Entity) PDN Gateway	• Performs functions similar to BTS and radio resource management • Routing and forwarding of user data, mobility anchoring • Tracking idle user devices, handoff management • Gateway to external data network

Table 2: MBH Technology Comparison

Generation	Technology	Base Station Interface	Base Station Support	Backhaul Network Support
2/2.5G	GPRS/TDMA/CDMA	Abis	Channelized TDM	PDH/SDH
3G (Rel99)	UMTS	Iub	ATM	ATM
3G/4G	EVDO, UMTS (Rel5), WiMAX , LTE	Iub/Abis	Ethernet/IP	IP/MPLS/Ethernet

5.0 Physical Access Network in MBH:

Packet-based mobile backhaul relies on IP connectivity between peer network nodes. This mean, the MBH can run on either Layer2 or Layer3 services. The MBH carries the data packets from the eNodeBs, encapsulate them in transport bearers and transport them to the CN. 3GPP mandates the use of IP in the logical interface and underlying protocol can be any depending on implementation and network requirements. The MBH also has to account for the network control and management traffic along with user traffic. When we design a backhaul it is primarily based on what radio access technology is being used (i.e., 2G, 3G, LTE...) and what services are required by the user. The MBH should at least be able to:

- Transport aggregated user traffic from required radio access nodes to CN
- Minimum Delay
- Maximum BW efficiency

In the MBH access network, the physical connectivity is considered as the base. This is where all services will be built, the cost will be decided, and network capacities will be determined. Often referred to as the first stationary/physical connectivity in the MBH, this access transport can be any technology that can fulfill the basic requirements stated above. In this paper, we will discuss the following access technologies:

- Wireless:
    - Microwave
- Wireline:
    - Copper
    - Fiber

All the physical mediums have the capability to support Ethernet technologies. It is also possible to combine multiple physical links in the MBH network based on requirements. The decision often depends on the requirements, available resources (e.g., spectrum and spectral efficiency for Microwave) and costs.

5.1 Wireless: Microwave

The most common wireless technology used for MBH access between the BS and the Aggregation Network is Microwave. When talking about Microwave, we have to understand that has to be a point-to-point radio link. These radio links transmission depends primarily on the frequency used. Over 55% of all MBH physical connections worldwide are in the microwave, and a total of 64% of MBH equipment revenue in 2010 was from TDM, dual TDM/Ethernet and packet microwave [3]. The unparalleled advantage of using Microwave is that no need to physically place, install and maintain cables which are not always possible or even required. One major disadvantage of the microwave is the reliability of radio propagations. Several factors such as attenuation, obstruction, bending, diffraction, and fading make implementation of microwave design very difficult. One key requirement of microwave implementation is that the transmitter and receiver have to be in the 'line of sight' for any kind of transmission.

Wireless Transmissions

The usability of spectrum and frequency to be used must first be determined. There are permission, regulations, and costs required for certain frequency use. The various microwave technologies are:-

- TDM MW:
    - The most commonly used Microwave technology. Based on Plesiochronous Digital Hierarchy (PDH)/SDH, multiplexes voice and low data rate to 56/64 kbps channels for the T1/E1 facility. Oldest Microwave technology and mainly optimized for voice.
- Packet MW:
    - This technology maps Ethernet packets directly onto radio airframe with no encapsulation required. Supports Layer 2 switching.
- E-Band:
    - This microwave technology uses radio frequencies between 60 and 90 GHz. ITU-R recommends using 71-76 GHz and 81-86 GHz, divided into

19 channels each 250 MHz wide. Huge spectrum and thus capacities can easily range from 2.5 Gbps to 5 Gbps.

Data rates required

Modulation plays a major role when designing the data rates required. Wider the signal BW allows higher modulation scheme, that is, more bits can be transmitted per symbol. The following graph illustrates the data rate achievable for various channel width in comparison to modulation used and acceptable attenuation.

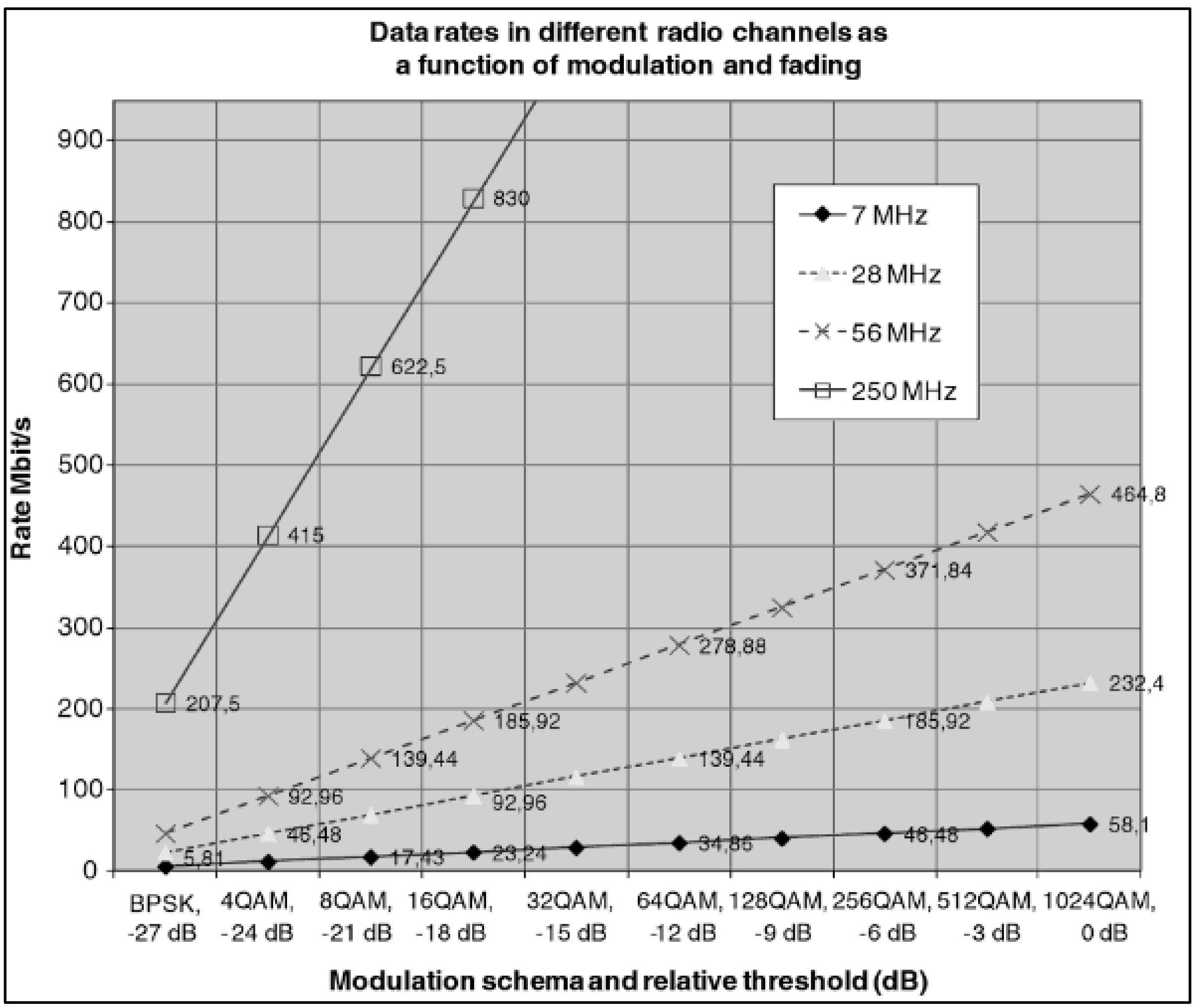


Figure 13: Possible Microwave Data rates [3]

Microwave topologies can work on various radio link topologies depending on area and design. They can be a point to point, point to multipoint or multipoint to multipoint. Currently, the most commonly used link establishment method used is the point to point and this then combined to form various topologies depending on requirements. Topologies such as chain, tree, ring and star and are possible depending on requirements (discussed further in Section 7).

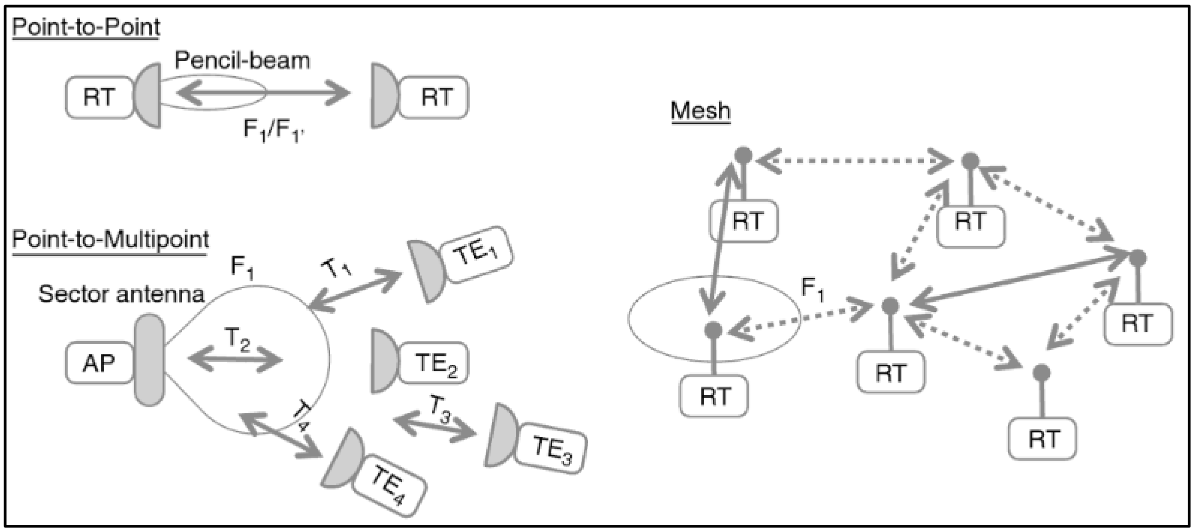


Figure 14: Examples of wireless network topologies: [3]

5.2 Wire-Line

Copper

When we talk about copper wire transmission, we talk about Digital Subscriber Line (DSL) () and/or Ethernet.

In the access, we mainly make use of xDSL which is a descendant of DSL [12]. This uses the transmission lines on twisted pairs that were set out for the POTS. This was then modified to Asymmetric Digital Subscriber Line (ADSL)/ADSL+ which had the asymmetric capacity for downlink and uplink along with the capability to carry both voice and data at the same time. Currently, the fastest and the most deployed DSL technology is called the Very high bit rate digital subscriber line (VDSL). This technology can be used to backhaul between lightly used eNodeBs and CN because it can support speeds up to 200Mbits/s.

Advantages of DSL:

- Infrastructure is either already in place/or cheap to install
- Equipments are simple and affordable

Dis-Advantages of DSL:

- Not enough capacity to deal with current traffic, especially for urban areas.
- Error Prone (Noise, Interference Delay…)
- Rate decreases drastically as length increases

Table 3: Properties of DSL Techniques using Twisted Pair Copper Wire [3]

Name	Reference standard	Maximum speed down/up	Symm/ Asymm	Loop length	Pairs	Bonding
ADSL	ANSI T1.413 Issue 2 ITU G.992.1 Annex A	8.0/1.0 Mbit/s 12.0/1.3 Mbit/s	A	. . .5 km	1	Yes
ADSL2+	ITU G.992.5 Annex M	24.0/3.5 Mbit/s	A	. . . 9 km	1. . .	32
SHDSL	ITU G.991.2	2.3/2.3 Mbit/s	S	. . . 3 km	2	4
VDSL	ITU G.993.1	52/16 Mbit/s	A	. . . 1200 m	1	
VDSL2	ITU G.993.2	250 . . . 4 Mbit/s	S + A	50 m . . . 5 km		

The other flavor of DSL which is just emerging is known as the G.Fast. Similar to VDLS2, this also runs over the existing copper infrastructure but has a wider frequency spectrum to for transmission. VDSL2 has a spectrum of up to 17MHz whereas G.Fast widens this spectrum to 106MHz which allows it to reach speeds of up to 1Gbps. As opposed to FDD duplexing in VDSL2, G.Fast uses TDD. The limitation of this technology is the distance. To achieve 1Gbps, the distance has to be less than 100m. In the case of longer distance, the speed keeps deteriorating. The following diagram will give an idea of G.Fast and VDSL2 comparison:

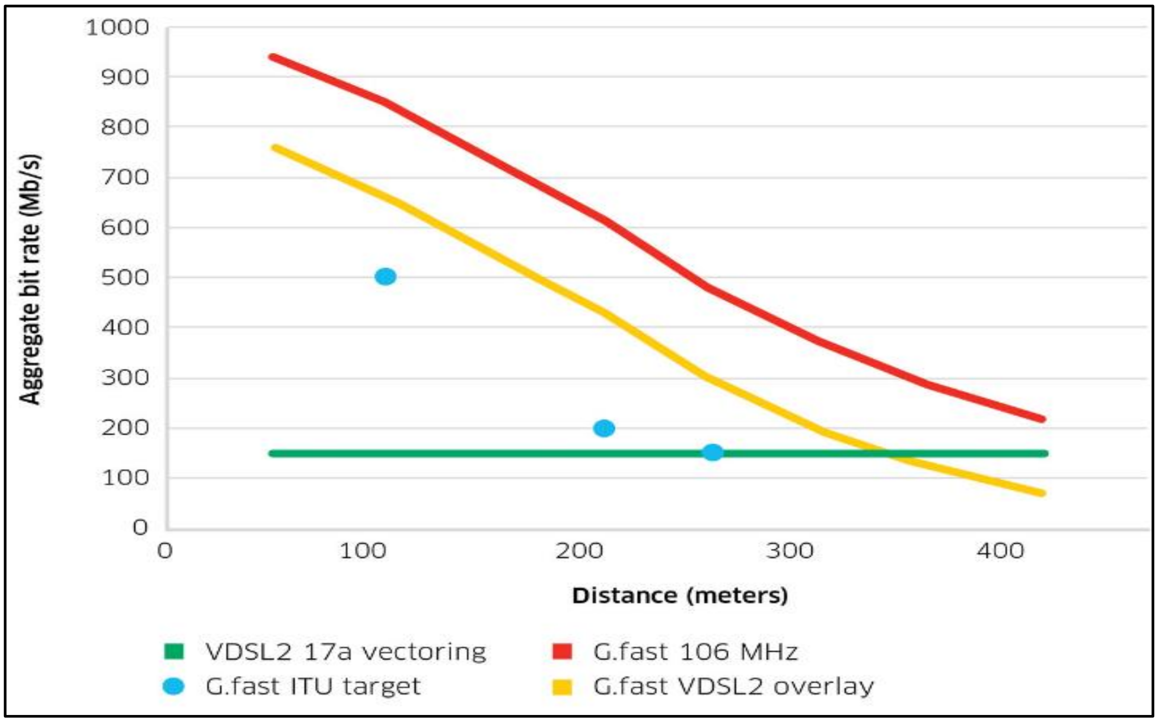


Figure 15: G.Fast (red) vs. VDSL2 (green)

G.Fast is very viable and cost effective way of delivering fiber-like speeds at a shorter distance. This reduces the initial implementation cost of Fiber layout for the last-file if very high BW is required by making use of the existing copper infrastructure. This technology can be used in conjunction to Fiber deployments. For example, Fiber would run till the FTTC/ONT. Usually from there, the distance to the Building, eNodeB or Home is comparatively less, so this technology can be used to deliver high speeds without extra cost.

Ethernet, being the most commonly used physical medium in houses and small offices spaces, has the potential to be used in MBH Access Network. There are multiple types of copper Ethernet cables with various properties and advancements. Due to their degrading properties, they often need repeaters in the case of long distance transmissions. All of them use twisted pair cabling method to cancel out the electromagnetic interference and reduce crosstalk. Ethernet of twisted pair copper is grouped into several categories from CAT 3 to CAT 8 depending on their frequency and capacity. This type of twisted pair is often characterized into Unshielded Twisted Pair (UTP), Foiled Twisted Pair (FTP), and Shielded Twisted Pair (STP). It can range from 1Mbps to 10Gbps depending on category and type. The following table will give an overview:

Table4: Ethernet Physical Properties

Name	Distance(m)	Speed(Mbps)	Cable Type	Standard
10BASE-T	100	10	CAT 3	802.3i
100BASE-TX	100	100	CAT 5 (2 pairs)	802.3u
1000BASE-T	100	1000	CAT 5e, CAT 6	802.3ab
2.5GBASE-T	100	2500	CAT 5e, CAT 6	802.3bz
5GBASE-T	100	5000	CAT 6	802.3bz

<u>Advantages of Copper Ethernet:</u>

- Cables are cheap
- Easy to handle and install
- Reliable and Fast transmission

<u>Dis-Advantages of Copper Ethernet:</u>

- Only short distances per segment. Might slightly increase cost for repeaters.
- Interference can be an issue

Fiber

When we talk about Fiber transmission, there are two kinds of optical fibers, single mode, and multimode fiber. Single mode fibers have longer distance capability, cheaper fiber cost, lower attenuation but the cost of optical transceivers are comparatively higher.. Multimode fibers have higher BW, lower distance capability due to higher attenuation, higher fiber cost and comparatively cheaper optical transceivers cost.. Fiber transmission usually occurs at selected wavelengths that have lower attenuation and reach higher distance. Various Wavelength Division Multiplexing (WDM) schemes can be used to transport multiple wavelengths and increasing BW. In legacy MBH, where data rates were not in the Gigabit range, Synchronous transport module (STM)-1 to STM-16 was very common in a ring topology.

PON, Passive Optical Network is a point to multipoint access technology for optical networks. Here, multiple fibers are combined/split to one central node called Optical Line Terminal (OLT). Typically the fibers are combined transmission from multiple nodes (at different locations) and passed to the OLT. Two main types of PON:

- GPON: Gigabit PON
  Uses Generic Encapsulation Method
- EPON: Ethernet PON
  Uses Ethernet Frames

Table 5: Comparison of PON technologies [3]

	EPON	GPON	10G-PON	WDM-PON
Standard	IEEE 802.3ah	ITU G.984	ITU G.987 IEEE 802.3av	No
Users/PON	32768 max	128 max		32 typical
System BW	1 Gbit/s symmetric	2.5 Gbit/s down, 1,25 Gbit/s up	100 Gbit/s down, 10/1 Gbit/s up	<1 Tbit/s
Average user BW	67 Mbit/s	120 Mbit/s	250 Mbit/s	1 Gbit/s
Frame type	Ethernet	GPON Encapsulation	Ethernet	Agnostic

Ethernet interface being the most common and saleable interface option, it is very much desirable to have Ethernet access in the first mile. It then comes down to the physical transport medium to carry the traffic and distance it can travel. The following table gives a rough idea of Ethernet First Mile options set by the Institute of Electrical and Electronics Engineers (IEEE) standard 802.3ah - 2004:

Abbreviation	Medium	Reach up to	Description
2BASE-TL	Copper, POTS	2.7 km	Up to 5.696 Mb/s (varying) over POTS wires at distances in the order of 2.7 km based on SHDSL
10PASS-TS	Copper, POTS	100 m	Up to 10 Mb/s (varying) over POTS at distances in the order of 750 m based on VDSL
1000BASE-LX10	Fiber, Pair SM	10 km	Single wavelength 1270…1355 nm, high-quality cabling
1000BASE-PX10	Fiber, SM	10 km	Ethernet passive optical network (EPON) between up to 16 users.
1000BASE-PX20		20 km	Ethernet passive optical network (EPON) between up to 16 users.

Table 6: Ethernet in First Mile [3]

When using fiber as the physical transport medium, the common ones are:

- Point to Point Fiber:
    - This is where a cell site directly connects to the aggregation point with one physical link (i.e., fiber in our case) often termed as Metro Ethernet. Switches/Routers at both ends have Gigabit ports/interface. This can be a direct fiber line from the CO/Aggregation Point to the eNodeB without any other splitting and/sharing as shown in the diagram below. This means lower latency, higher performance, and reliability but much costlier and under-utilized since a single fiber has the capacity to support multiple eNodeBs because of its high BW capability.

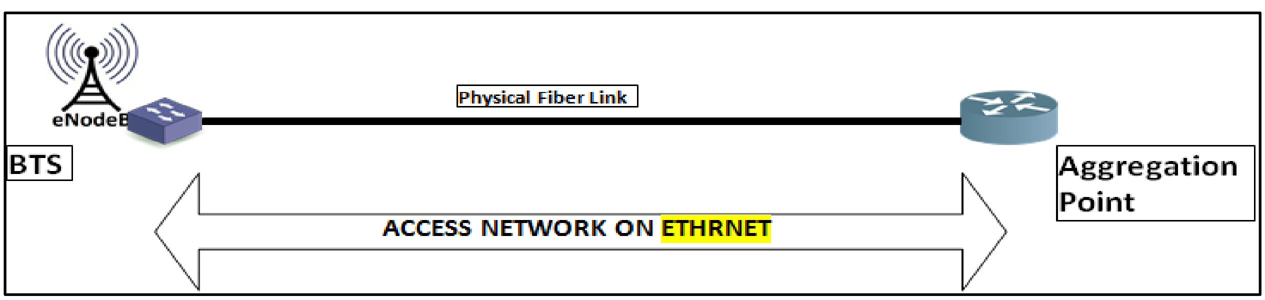


Figure 16: Point to Point Metro Ethernet to eNodeB from CO

- GPON/EPON (Point to Multipoint):
    - This is where multiple sites (each with their ONUs) are combined together and conned at the other end via one link. (The scope of GPON and EPON functionalities are out of the scope of this report). The following diagram will give an overview of GPON FTTx:

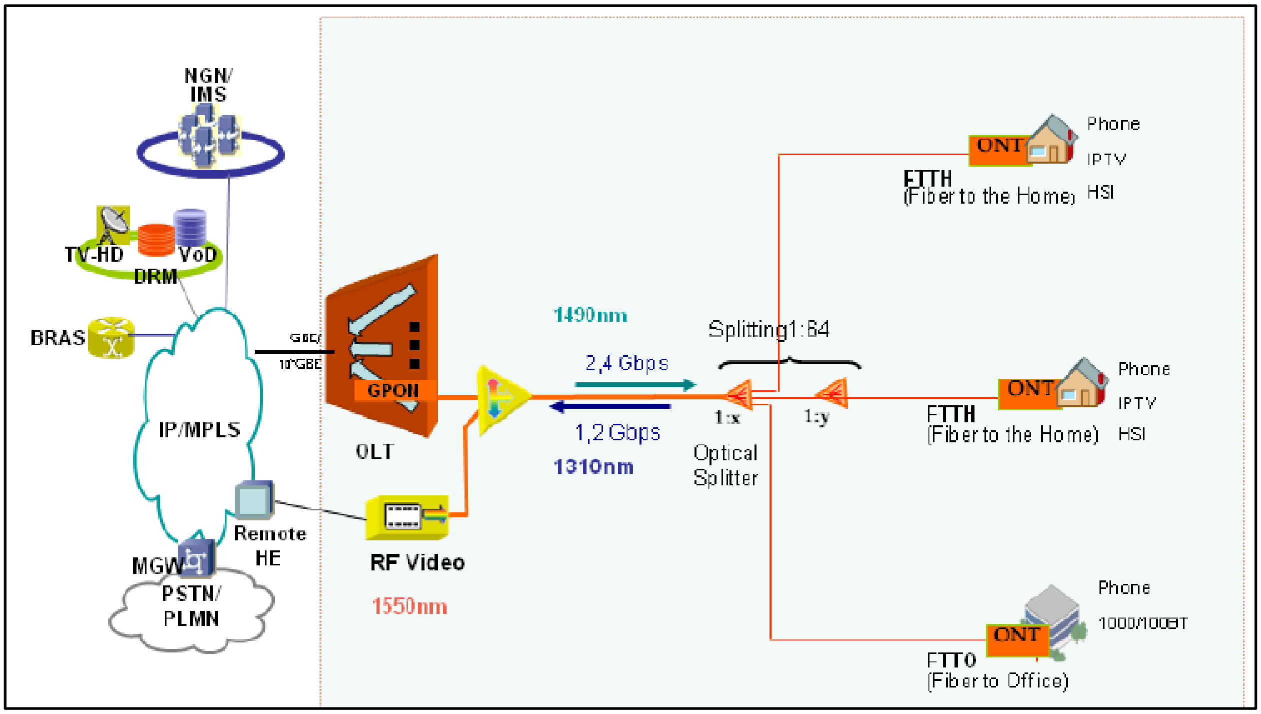


Figure 17: Typical GPON network [29]

Previously, the mobile operators leased TDM lines from the telecom companies to provide for their MBH connection. These leased line services are now moving to Ethernet Services since Ethernet is now being deployed commonly by service providers. Often it is not necessary to lease a dedicated line because Ethernet capacities are very high and options for sharing needed to be developed. IEEE 802.3 states the specifications of Ethernet Service implementation over various physical medium, including copper and fiber. This opens up the options to implement Ethernet Services like Ethernet E-line, E-LAN, and E-Access. These services are explained in details in later sections.

6.0 Access-Aggregation-Core

As discussed, MBH is separated into the access, aggregation, and core. This intermediate transportation between the eNodeBs and the EPC can be done in L2, L3 or a combination of both. Given all-packet based communication, Ethernet and/or IP/Multi-Protocol Label Switching (MPLS) protocols can be implemented, but each stand-alone/combination has its own advantages and disadvantages. This section will discuss the various combinations in each section and their effectiveness. The following diagram will give an overview of the whole LTE MBH network.

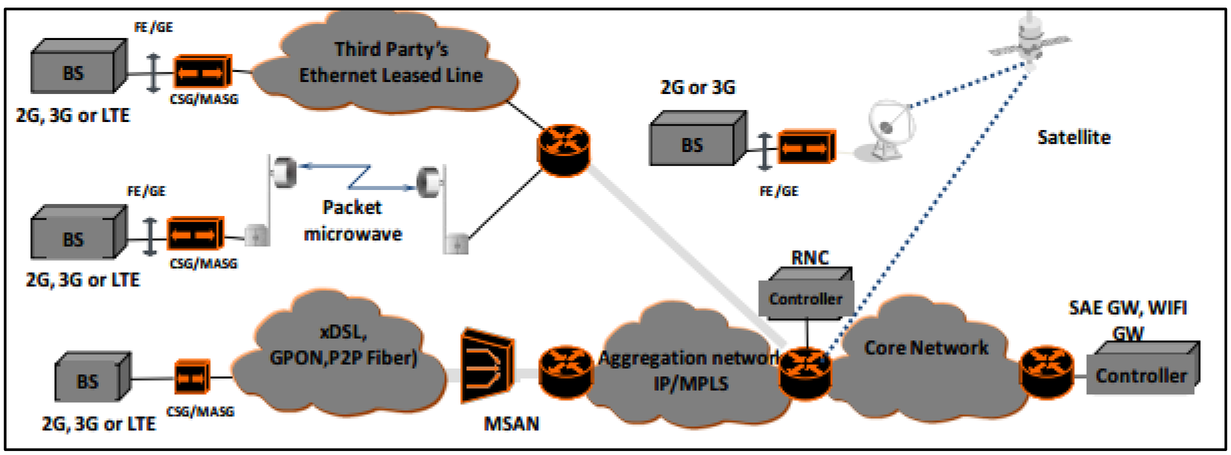


Figure 18: LTE MBH network [24]

6.1 Access-Aggregation Network

Access-Aggregation Network is defined between the eNodeB cell sites to the aggregation point. Implementing Layer 2 Ethernet provides multiple advantages. When Ethernet is used in this network, the cost of the hardware's needed for this protocol is greatly reduced. Given the high throughput needed for LTE cell sites, Ethernet switching devices can easily support 1GbE, 10GbE and soon 40GbE with lower operating cost. This also allows flexibility in controlling/leasing the required speed for each cell site depending on the customers supported in that area by that eNodeB. Sometimes, an increase in BW will only need a change to the port to something higher given that physical link can support which if Fiber is used, gives a huge scope for scalability. The leasing of Carrier Ethernet (CE®) services is also lower than that of leasing IP services which also is a significant plus and CE® services also provides very detailed manipulation of QoS and service separation. Since LTE is IP-based, CE in the access backhaul provides transparency to the IP layer. With overall services available in CE, the easiness of installment, managing and decreased need of troubleshooting makes it the ‘to go’ option for reduced cost and increased uptime.

6.2 Aggregation-Core Network

In reference to the access network discussed in the previous section, eNodeBs connect to the PE node of this aggregation network. The aggregation network combines all traffic and connects to the EPC. In reference to our report, this portion is from the Aggregation point to the EPC. MBH backbone has shifted to the IP-based network since the legacy ATM and TDM networks. This network consists of the links, switches, and routers, and is responsible for various and all traffic that is generated from numerous access networks route it to and from its destination. Often this network is shared by multiple Service operators and multiple sources as the infrastructure of a backbone network is huge and immense.

For our purpose, we will emphasize on the use of MPLS networks. So when running MPLS on IP backbone network, we refer to it as the IP/MPLS backbone. IETF has exampled the use of MPLS in the user plane with IP control plane. This transport technology makes use of labels for each packet for a certain route. When the packets travel through the network, the MPLS labels are used to determine where it has to travel next instead of overburdening the Router to look into each packet to determine its next hop. This also gives the flexibility to use different services for different customers as required. Backbone networks are very busy with multiple packets going through them. It is necessary to speed up the network flow to keep up with the heavy traffic this is coming in and out of this network. In this network, give the heavy-duty it has to perform, the devices used are capable of extremely high bandwidth along with a network that is very redundant and fail-safe. Often they are all interconnected using fiber and also in a semi/full mesh design so that there are always backup routes available. MPLS technology also has a variety of Traffic Engineering options which allow the flexibility to route traffic in the most efficient and organized manner.

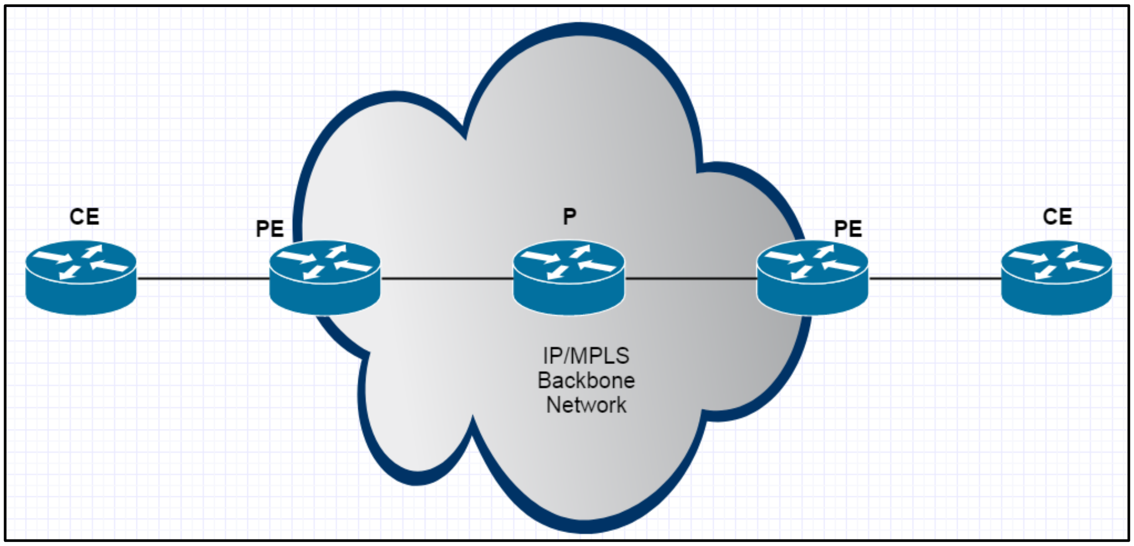


Figure 19: IP/MPLS backbone network in MBH

This network can be implemented using L2 or L3 MPLS services. Since both will serve the purpose, we will explain and compare which one is preferred. Since IP layer 3 will be in the backbone, we will be using IP/MPLS, Layer 3 Virtual Private Network (VPN) technology from the Aggregation to Backbone network. MPLS VPN can be used to connect different customer sites through other networks. This MPLS L3 VPN provides IP connectivity between the nodes by using multiple VRF instances. Each VRF instance is used to store the routing data, and IP address is used to map the traffic. [3] In LTE MBH, from the eNodeB, S1-U connects to S-GW and S1-C to the MME using IP addressing. The VRFs permit the separation of each type of traffic from each eNodeB allowing the better scope of troubleshooting, tracking, and security. L3 MPLS VPN is further discussed in Chapter 10.4.

Since this technology runs over IP layer 3, it makes the addition of eNodeBs much easier and thus making the expansion of customer network easier. Security is also a major advantage of this technology as it will only route traffic if the destination is known as per IP address or else it is dropped. Whereas, in L2 MPLS VPN, since it is based on MAC learning using flooding, it can become a security issue and resource issue with all the MAC address learning. This also increases the chances of endless loops within the aggregation network. L2 MPLS VPN is also more difficult to manage and scale.

6.3 Synchronization

In order to support smooth handover, better voice quality and low call drops within the LTE RAN technology; it is important that the end to end nodes are synched with each other. Unlike TDM, where the traffic is transferred over the medium through all intermediate nodes in a specific time slot and synchronized manner, packet switched is a little different. In a packet switched or IP-based network like the one required for LTE MBH, it is necessary to implement a separate synchronization method to meet service SLAs, avoid service disruption and greater QoS. This is mainly because circuit-switched is synchronous and IP/packet based is asynchronous.

Compared to legacy transport technology such as SDH and PDH, the synchronization is done on the physical layer where often a PRC is used as the central synchronizing node. With packet-based networks, often where, IP runs on top of Ethernet, issues such has a varying delay, jitter and packet loss make it difficult to implement synchronization mechanism. Synchronization mechanisms can be both/or time and frequency synchronized. Depending on the Radio Access technology used, the compatible synchronization methods should be used to meet the standards outlined in Table 7.Some of the mechanisms and protocols available for the clock synchronization in MBH are as follows: [18]

- Using GPS or a legacy TDM network that is external to the IP-packet-based network
- Packet-based dedicated streams (IEEE1588- or NTP-based)
- Using Synchronous Ethernet over the physical layer
- Adaptive clocking
- DSL clocking

Since this paper is based on MBH and CE®, following Metro Ethernet Forum, MEF 22 and 3GPP standards, we will further discuss some of the recommended methods mentioned above. As per wireless standards, timing requirements are as follows for legacy and LTE technology:

Table 7: Legacy and LTE Frequency and Timing Synchronization Requirements [20]

Wireless Standards	Requirement on Frequency Synchronization Precision	Requirement on Time Synchronization Precision
GSM	0.05 ppm	NA
WCDMA	0.05 ppm	NA
TD-SCDMA	0.05 ppm	+/–1.5 µs
CDMA2000	0.05 ppm	+/–3 µs
WiMAX FDD	0.05 ppm	NA
WiMAX TDD	0.05 ppm	+/–0.5 µs
LTE FDD	0.05 ppm	NA (except for MB-SFN < +/–1 µs, LBS)
LTE TDD	0.05 ppm	+/–1.5 µs

IEEE 1588v2 – Precision Time Protocol (PTP)

In this timing distribution method, the information is exchanged in packet form in the same network as data/voice traffic without the need for any timing hardware upgrade to elements in the Ethernet network (unlike SyncE). Timing information is exchanged between the Master and Slave(s) clocks using existing Ethernet network using User Datagram Protocol (UDP) over IP. The Master Clock is where all the downstream slave clocks receive their timing information from. Often multiple Master Clocks are configured for redundancy with varying priority to avoid conflicts.

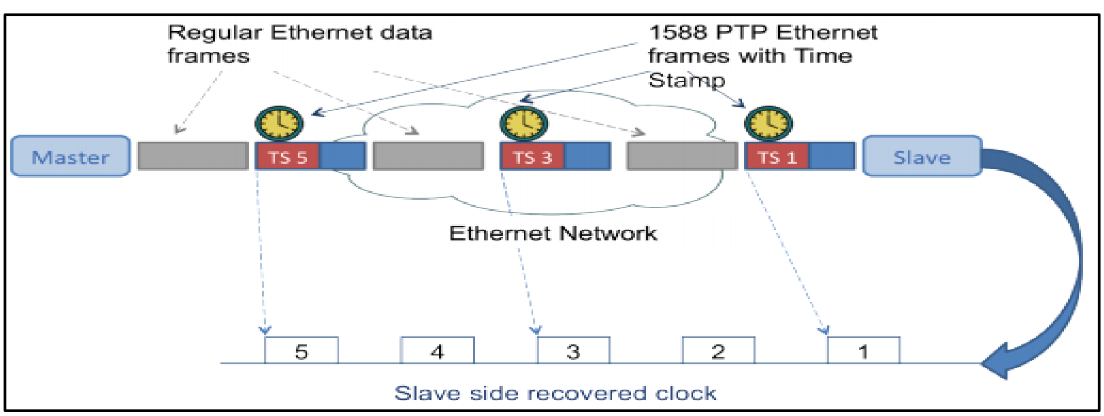


Figure 20: Clocking in 1588v2 [21]

In this protocol, the slave clock devices are aligned with the Master clock device by utilizing the time stamps in the synch messages exchanged between them. The slave clock also has the ability to compensate for the propagation delay between them. For both time-frequency and phase synchronization, four time stamps are required whereas for only frequency on two timestamps are required. Here the clock signal is injected through the MBH and till the last mile (i.e., eNodeB) adhering to the acceptable time synchronization precision in nanoseconds. This protocol has multiple advantages such as high precision (nanosecond-level), low-cost (no additional hardware required) and smooth compatibility with packet networks.

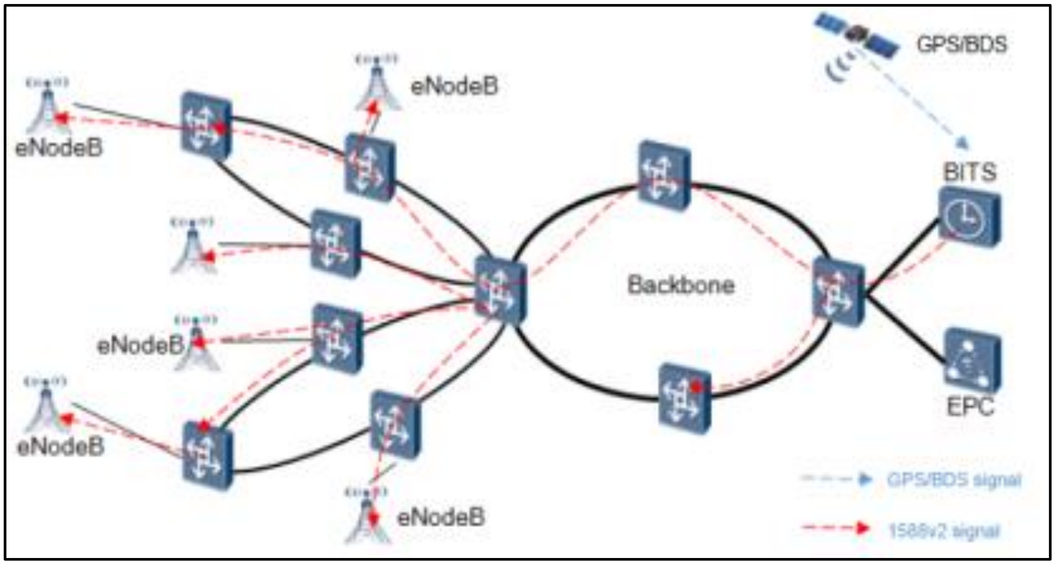


Figure 21: MBH using 1588v2

Synchronous Ethernet (SyncE)

This protocol of synchronization allows a very effective way of synchronizing devices within the MBH that is running on Ethernet on the physical layer. This protocol is standardized by ITU-T and is designed to be implemented in the physical layer of a packet based network. SyncE allows the synchronization of frequency and is suitable for wireless standards that require frequency synchronization. In similarity to the legacy TDM and SONET, SyncE allows time synchronization on a node by node basis. This also implies that all the interfaces along the synchronization path, from the BS to the EPC, have to support SyncE to be able to transfer the clock (i.e., frequency). This is supported by both wireline and wireless services, so it is a very desirable protocol to be used in the MBH networks.

This protocol requires the interface of any Ethernet devices to have at least two external reference clocks as well as capability to create own synchronization signals. In this protocol, the device does not follow a free running clock. Instead, it gets an input reference clock from a primary clock reference. As per standard, this input reference has to have an accuracy of ±100 ppm. ITU-T G.8261, G.8262, and G.8264 set the standards for SyncE in packet-based networks detailing requirements for clock accuracy, holdover performance, and noise transfer, tolerance and generation. It is important to note that the clock signal in SyncE needs to be filtered and regenerated before being fed again to remove the jitter and also other functions as outlined by ITU-T. The following diagram gives a high-level example of how SyncE will work in MBH:

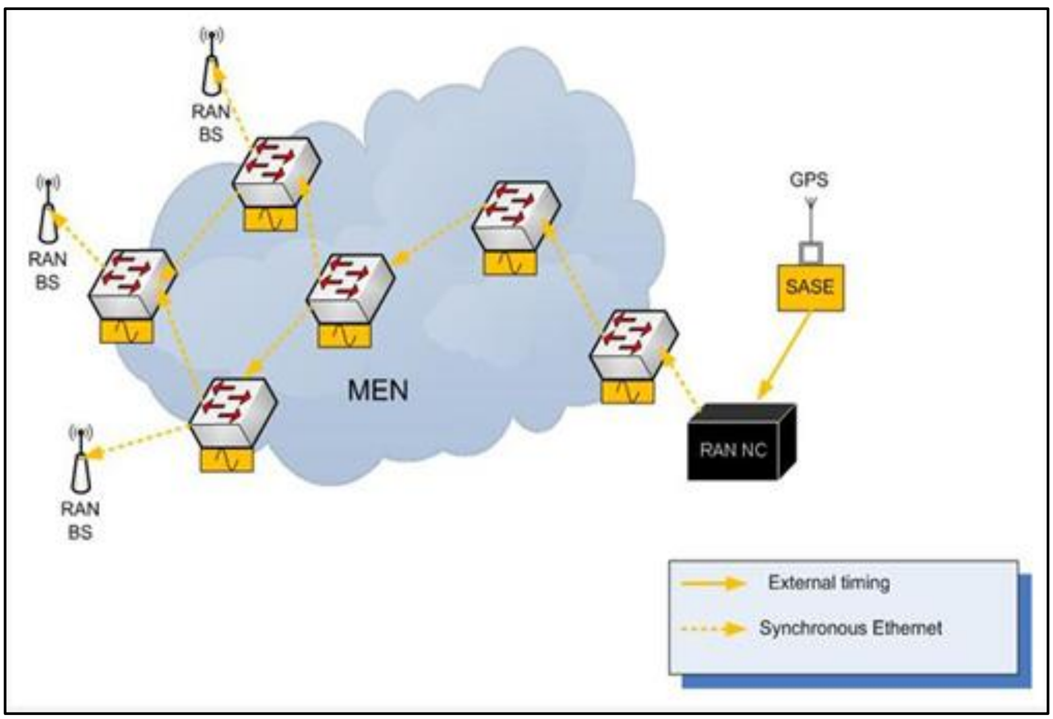


Figure 22: SyncE in MBH [19]

6.4 Bandwidth and Physical Medium

This section will emphasize on the required BW properties of the physical Access technologies discussed in Chapter 5. This portion of the network in the MBH should be able to carry all data from the eNodeBs serving that area. To determine which physical transport can/should be used depends on the estimated capacity of data that is going to travel. The physical transport bandwidths of Microwave, Copper, and Fiber are also discussed in Chapter 5.0. In legacy 2G backhaul networks, it was primarily based on TDM. When 3G was introduced along with packet switched network, ATM was mandated by the 3GPP. Technologies that used copper or microwave as their transport medium was enough to handle the aggregated traffic from the BTS to the aggregation point. With the growth in mobile users and their need for more bandwidth, fiber is the next alternative that can deal with the aggregated traffic in the backhaul. As a matter of fact, data rate per user has increased from few kbps to about 25Mbps [12]. To more accurately determine which of these is best suitable for our LTE backhaul need, we have to discuss the BW from each cell site and the backhaul. The following table is an example to cell site BW between legacy and LTE variations:

Table 8: Cell Site BWs [6]

Wireless Capacity Requirements								
	Voice Spectrum (MHz)	Data Spectrum (MHz)	Voice Spectral Efficiency (bit/s/Hz)	Data Efficiency (bit/s/Hz)	# Sectors	Traffic Eng % Peak	Total Bandwidth (Mbps)	# T1s
GSM 2G	1.2		0.52		3	70%	1.3	1
GSM / Edge 2.75G	1.2	2.3	0.52	1	3	70%	6.1	4
HSDPA 3G		5	0	2	3	70%	21.0	14
LTE 4G		5	0	3.8	3	70%	**39.9**	**n/a**
LTE 4G		10	0	3.8	3	70%	**79.8**	**n/a**

Along with the above data, we also have to consider the deployment area of the cell site. This will determine a more precise BW requirement for that area of eNodeB. The following table gives an example of comparison between various LTE BW channels used in radio access and the type of area it is serving. It also considers the effect of MIMO types, since the capacity of TX/RX practically doubles with every 2X2 MIMO upgrade playing a major role in the overall BW produced.

Table 9: LTE MBH requirements [15]

Scenarios	Deployment	UL/DL	The Eengineering Peak Throughput (on air, Mbps)	The Engineering Average Throughput (on air, Mbps)	ROHC not support on air interface		ROHC support on air interface	
					Backhaul Peak throughput (Mbps)	Backhaul Average Throughput (Mbps)	Backhaul Peak Throughput (Mbps)	Backhaul Average Throughput (Mbps)
HDU/DU Macro	20MHz, 3 Sectors DL 2X2 MIMO	UL	72.67	24.22	107.85	35.95	150.50	50.17
		DL	247.15	82.38	366.77	122.26	511.83	170.61
Sub Ubran Macro	10MHz, 3 Sectors no MIMO	UL	36.34	12.11	53.92	17.97	75.25	25.08
		DL	61.79	20.60	91.69	30.56	127.96	42.65
Rural Macro	5MHz, 3 Sectors no MIMO	UL	18.17	6.06	26.96	8.99	37.63	12.54
		DL	30.89	10.30	45.85	15.28	63.98	21.33
In-building Pico	20MHz, 1 Sector DL 2X2 MIMO	UL	24.22	8.07	35.95	11.98	50.17	16.72
		DL	82.38	27.46	122.26	40.75	170.61	56.87
In-building Femto	20MHz, 1 Sector DL 2X2 MIMO	UL	24.22	8.07	35.95	11.98	50.17	16.72
		DL	82.38	27.46	122.26	40.75	170.61	56.87

Give the above requirements; we can use few physical medium options. We will compare and contrast some of the available physical medium and show how fiber is the ideal solution:

Table 10: Physical Medium Option for LTE MBH

	Reference Name	Speed Mbps (Up/Down)	Use	Primary Advantage	Primary Disadvantage
Copper	VDSL	52/16	Short Distance Lightly used BTS	Infrastructure already in place	Not expandable
Copper	VDSL2	250…4	Short Distances	Infrastructure already in place	Not expandable
Microwave	E-Band	1000-3000	Point-to-Point short distance	Cheap installation	Has to be line of sight
Fiber	G/E/x-PON	1000++	Long distance Practically no limit	Expensive	Meets current and future needs

Fiber physical medium not only is capable of meeting the current needs, but it is also ready to take on traffic generated for future generations. Upgrades will be based on current fiber infrastructure with only few hardware changes. Fiber might be the most expensive one to install at this moment, but it is the most future-proof.

Reusing some of copper and microwave technology might be an option for short-term solution assuming it meets the minimum BW requirements for services. Given the fact that the loss and attenuation are lower of copper at shorter distances, it is possible to combine both fiber and copper in the same access network to provide optimal speed and lower cost. Same can be done for Microwave technologies. Example:

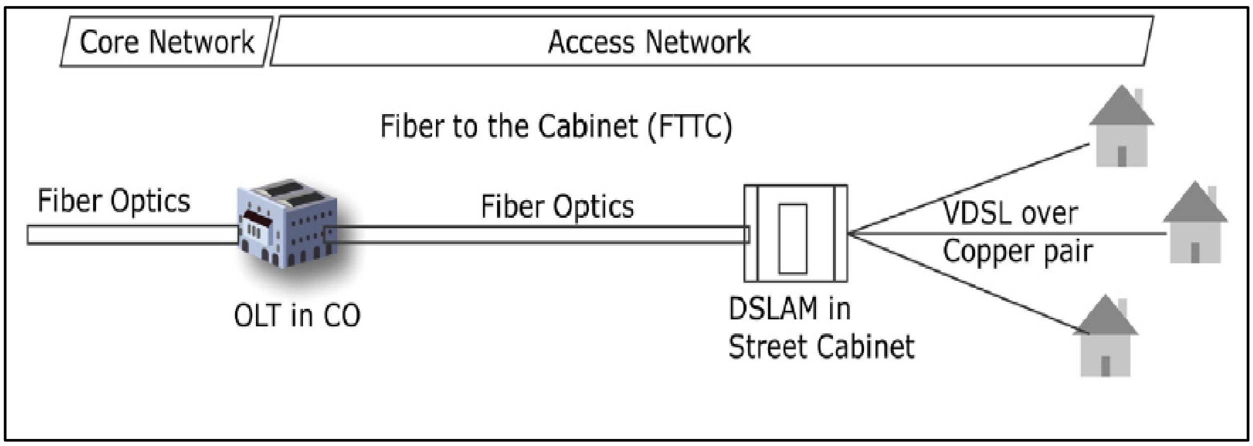


Figure 23: Comparison of VDSL and GPON-based Access [12]

7.0 MBH Access Topologies:

The access portion of the network is considered from the eNodeBs to the Aggregation point. The design of such networks primarily depends on the physical transport medium that will be used to connect to the aggregation point. Access topology is the physical arrangement eNodeBs in such a manner that they are connected to each other (in the case of LTE BS to BS handover) and to the Aggregation network in the most efficient and the least point of failure design. In addition, area coverage, protection required, link capacities and complexity also matters. Each cell-site/eNodeBs BW must be pre-determined/estimated to ensure proper topology is implemented. The physical medium used also plays a major role in designing the Access topology. Overall, few of the major topologies are discussed below:

- **BUS Topology**

  This is where multiple eNodeBs are connected Point-to-Point (P2P) to a primary transport medium (often known as backbone link) going to the Aggregation PE. Traffic from each node travel to all other nodes. This topology can be implemented using physical copper mediums. Primary link has to be very high capacity to carry all aggregated data.

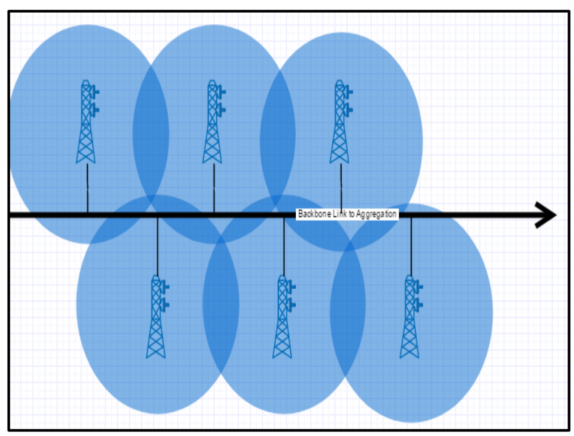


Figure 24: Bus Topology

  Advantage:

  - Easy to implement and expand
  - Lower link cost for each node

  Disadvantage:

  - Single point of failure at the bus
  - Unwanted traffic, interference and same collision domain

  Physical Medium:

  - Coax Cable using BNC T-Connectors (10BASE-2 and 10BASE-5)

This topology is **not** feasible for LTE MBH Access network because this wireline copper (Coax – maximum 10Mbps)) technology cannot support the high BW required.

- **Star Topology:**

This topology also includes P2P connectivity of multiple eNodeBs to connect to a central/hub eNodeB/switch which is then linked to the aggregation point. All the data transmission has to go through the central node. The hub to aggregation point has to be high capacity, enough to carry traffic of combined nodes.

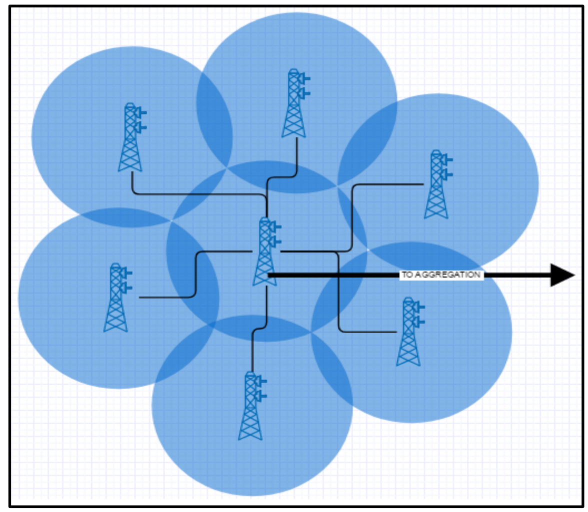


Figure 25: Star Topology

Advantage:

- P2P links thus no sharing of links to the hub.
- Easy addition/modification in case of changes
- One link failure does not affect other nodes
- Easy identification and troubleshooting for node failures

Disadvantage:

- Hub failure can bring the entire network down

Physical Medium:

- Node to Central P2P: Can be dedicated CAT6, Fiber or Microwave depending capacity and distance
- Central to Aggregation P2P: Dedicated Fiber

The hub can be placed in the aggregation point, in which it would seem as if there are **direct links to aggregation**

- **Chain Topology (Linear):**

This is a line of eNodeBs connected together one after another. Each node's traffic crosses all the nodes till the aggregation point. The closer you get to the aggregation point, the thicker the links should be to be able to carry combined traffic.

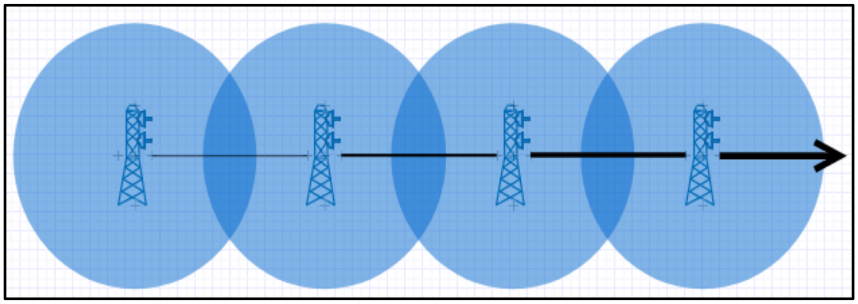


Figure 26: Chain Topology

Advantage:

- On specific architecture, it is easy to implement and extend
- Shorter links required

Disadvantage:

- One node/link down will bring down all previous nodes

Physical Medium:

- Node to Node P2P: Can be dedicated CAT6, Fiber or Microwave depending on capacity and distance

▪ **Tree Topology:**

The network starts with multiple eNodeB sites and gradually shrinking the network down to one node in a hierarchy fashion that connects to the aggregation point. The starting node is called the root with levels of following hierarchy. The closer you get to aggregation point, the thicker the links should be to be able to carry combined traffic

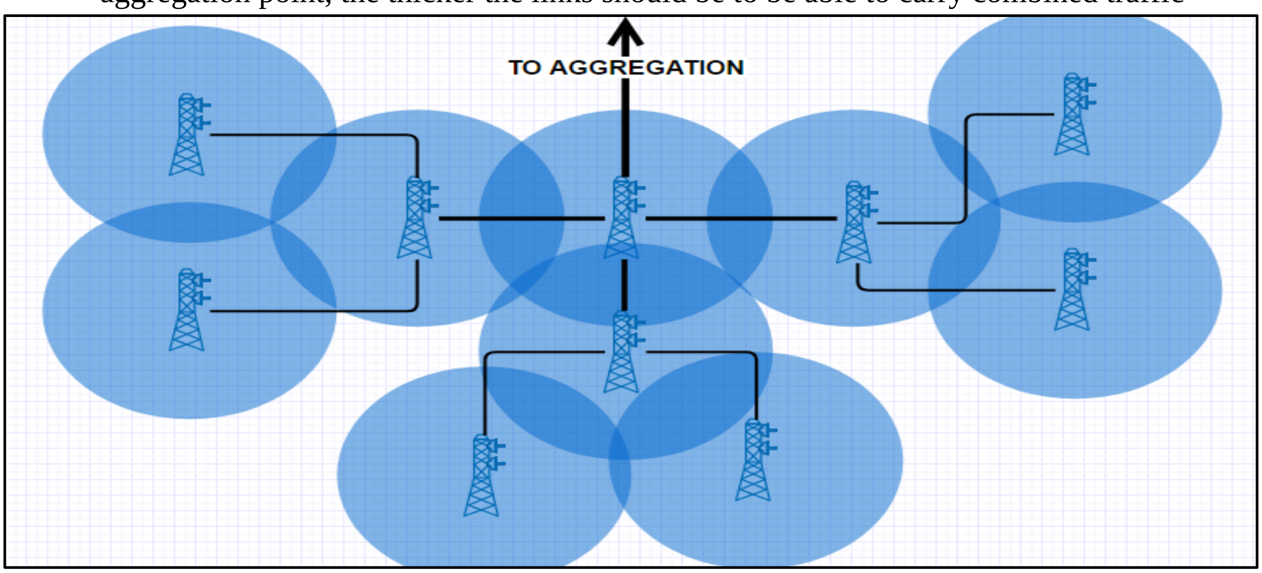


Figure 27: Star Topology

Advantage:

- Easy network expanding and wider coverage
- Nodes can be grouped in other topologies

Disadvantage:

- Root node/link goes, the network goes down

Physical Medium Possibilities:

- Can be dedicated CAT6, Fiber, GPON/EPON or Microwave depending on hierarchical capacity and distance

- **Ring Topology:**

All eNodeBs are connected to in a ring format, and all traffic has to go through other nodes before reaching the Aggregation point. It can be signed to support data flow in both directions

Advantage:

- Shorter links
- Resilient to single node/link failure, traffic can reach the hub in the other direction

Disadvantage:

- The hub node is a single point of failure
- Larger the ring, more the delay

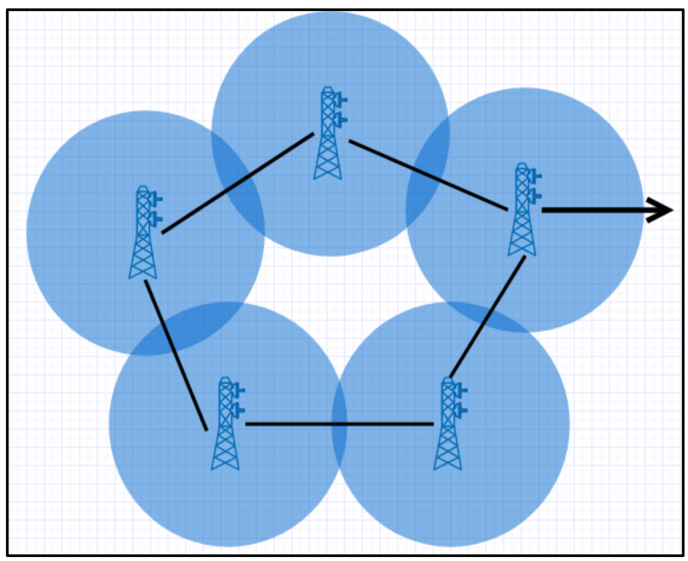


Figure 28: Ring Topology

Physical Medium Applications:

- Node to Node P2P: Can be dedicated CAT6, Fiber or Microwave depending on capacity and distance.

- **Mesh/Combination**

  This is where multiple nodes are connected to each other to build a single network. Each node is linked to every other node in the network.

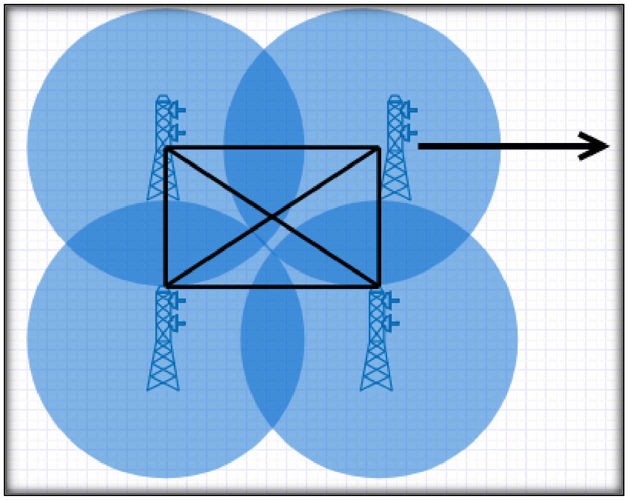


Figure 29: Mesh Topology

Advantage:

- Network can be build based on requirements
- Robust and most reliable

Disadvantage:

- Expensive and complex to implement

Physical Medium Applications:

- Node to Node P2P: Can be dedicated CAT6, Fiber or Microwave depending on capacity and distance.

NGMN – Next Generation Mobile Networks group focuses heavily on research and provide a recommendation to a wide range of future mobile networks. As per a white paper under their 'Backhaul Evolution' project, they have suggested the following wire-line and wireless access backhaul topology. This example is based on Small Cell BTS and Macro Cell:

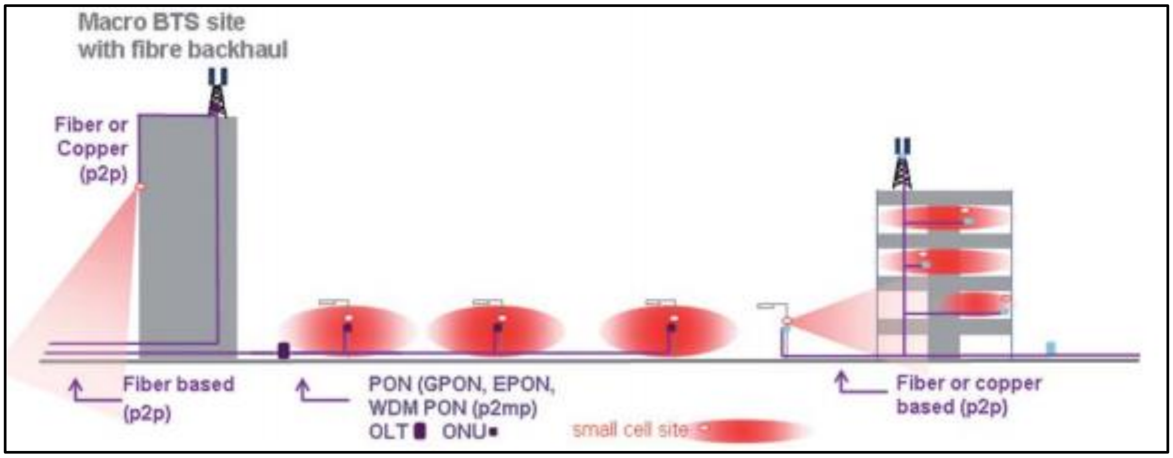


Figure 30: NGMN recommendation of Wireline Access Backhaul Topology [13]

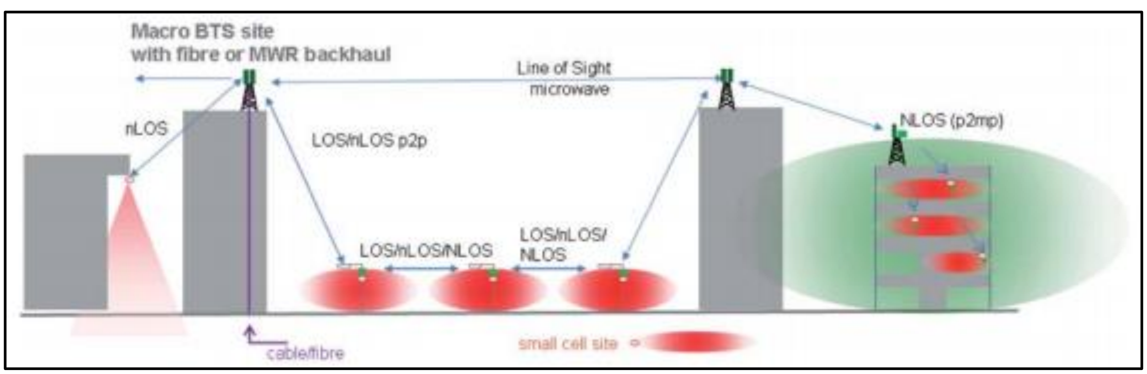


Figure 31: NGMN recommendation of Wireless Access Backhaul Topology [13]

8.0 Carrier Ethernet

With legacy technologies soon reaching their throughput peak, the next best alternative for an upgrade is Ethernet into the wide-area and metro networks which are termed as the Carrier Ethernet. Ethernet is capable of running on different transport mediums such as Copper, Fiber and Wireless and technologies such as MPLS, Plesiochronous Digital Hierarchy (PDH), Microwave, and SONET. These standards are defined in Metro Ethernet Forum 6.X, 9 and 33. Bringing CE into the metro means that their BW can be scaled up to 1/10/40/100 Gb/s (200Gb/s and 400Gb/s on its way [8]); mostly all of which runs over Fiber physical connection. This advancement of Ethernet into Metro area means:-

- More Flexible BW: BW can be controlled by remote provisioning up to the port speed
- Lower cost: Cheaper equipment, fewer infrastructure changes once built, lower cost per bit, lower operational and maintenance expense
- Easier usability: Older well know technology just with new implementation technique and standard.

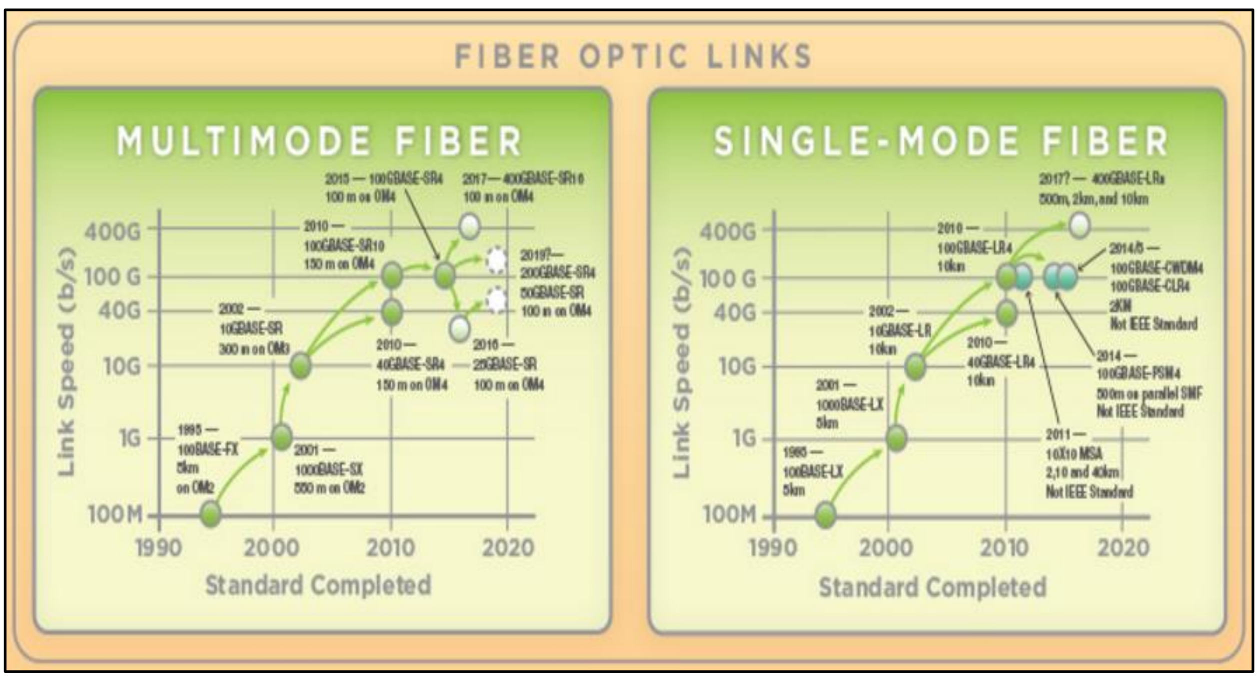


Figure 32: Ethernet Speed advancements [9]

CE® Services

Along with CE® implementation standards, MEF also set standards for various CE® services. CE® services add additional capabilities within the metro area network, and the standard allows the interoperability between different network providers. MEF defines the service framework, attributes and parameters for available CE® services. CE adds capabilities such as:

- Multiple services definition to address different design requirements
- Standardized CoS, Interconnect, and Manageability
- High rates, Low Latency, Low Cost
- Defined QoS
- Optimal Resource Allocation

For this report, we will discuss CE® services such as E-Line, E-LAN, E-Tree, and E-Access as defined by MEF. Few definitions required before proceeding are:

User Network Interface (UNI) – User to Network Interface: This is the physical interface (port) between the service provider network and customer/endpoints, and it realizes the demarcation between the customer and service provider. [3] The UNI in a Carrier Ethernet Network is a physical Ethernet Interface at operating speeds 10Mbs, 100Mbps, 1Gbps, 10Gbps ++[MEF CE Service]. This is where the CE® services are terminated. UNI standards are defined in details in MEF 6.1.

Network to Network Interface (NNI/ENNI) – Ethernet Network to Network Interface: This is the interfaces that join/peers two different networks of service providers. This realizes the demarcation between two network providers. Standards are defined in details in MEF 26.

Ethernet Virtual Connection (EVC) – Ethernet Virtual Connection: is an association of two or more UNIs. EVCs are logical service containers connecting the customer sites (UNIs) [3]. This virtual connection ensures that the traffic only flows between two UNIs within the same EVC. EVCs can be point-to-point, multipoint-to-multipoint and/or rooted multipoint. The specifications are well defined in MEF 10.2. Standards are defined in details in MEF 6.1.

Operator Virtual Connection (OVC) – Operator Virtual Connection: is an association of two or more NNIs or between UNI and NNI. OVCs are logical service containers connecting the customer sites-network or network-network and that the traffic only flows between them. Multiple OVCs can be created within one EVC. As per MEF, OVC can be point-to-point or rooted multipoint. Multiple OVCs within an EVC come into play when there is an interconnection between multiple Carrier Ethernet Networks. Standards are defined in details in MEF 26.

MEN – Metro Ethernet Network: This describes a metropolitan/access network that is running on Ethernet transport.

8.1 E-Line

This is a point-to-point Ethernet Virtual Connection between two UNIs. It emulates a P2P Ethernet service. The two types are discussed below:

Ethernet Private Line Service – EPL

This is a port based point-to-point service between two UNI. Separate interface/port is required at each UNI for individual EVCs and provides a site to site connectivity. This service has a high degree of transparency for Service Frames between the connected UNIs. The major advantage of having this service is that there is a low frame delay, loss, variation, and simplicity. This can be considered as a replacement to TDM private line. Service multiplexing is not available.

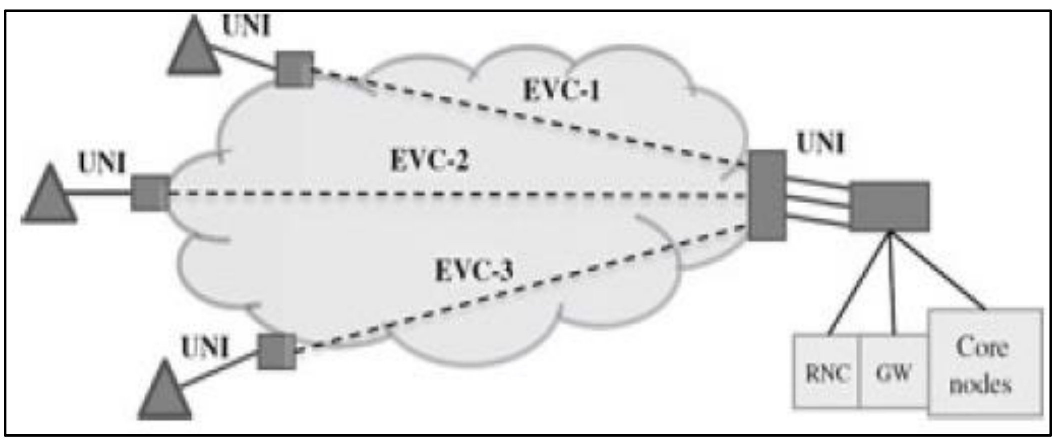


Figure 33: EPL [3]

Ethernet Virtual Private Line Service – EVPL

EVPL is similar to a virtual line and thus allows service multiplexing at the ports reducing the number of ports needed at the provider's edge. Since multiplexing can be used, it can support multiple EVCs at the UNI hub end allowing implementation of various services. As compared to EPL, frame distinguishing is required for different EVCs. This can be considered a replacement to frame relay or ATM L2 VPN.

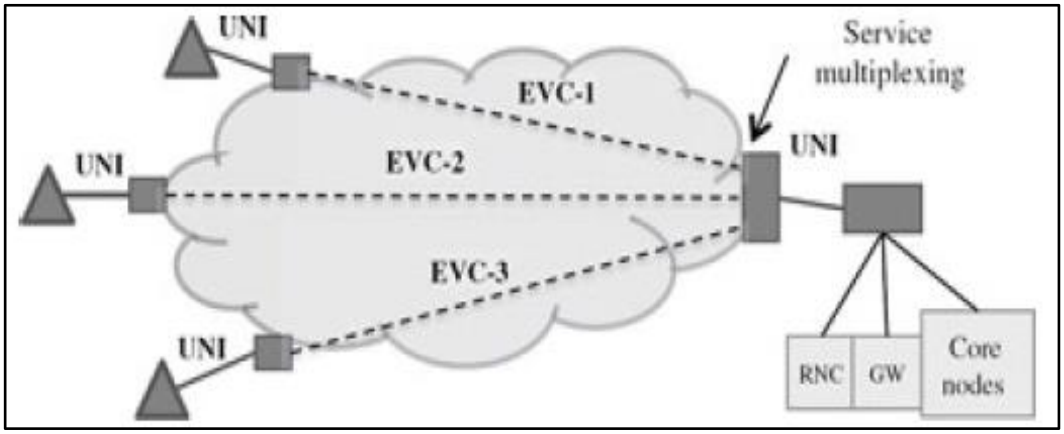


Figure 34: EVPL [3]

8.2 E-LAN:

This is a multipoint-to-multipoint Ethernet Virtual Connection between multiple UNIs. This provides services between all the UNIs in the EVC such that it emulates a LAN service. The two types are discussed below:

Ethernet Private LAN Service:

EP-LAN is a port based multipoint to multipoint local area network service. Each EVC can have two or more UNIs connected, but it does not support service multiplexing. Thus each EVC has to have separate ports on the UNIs.

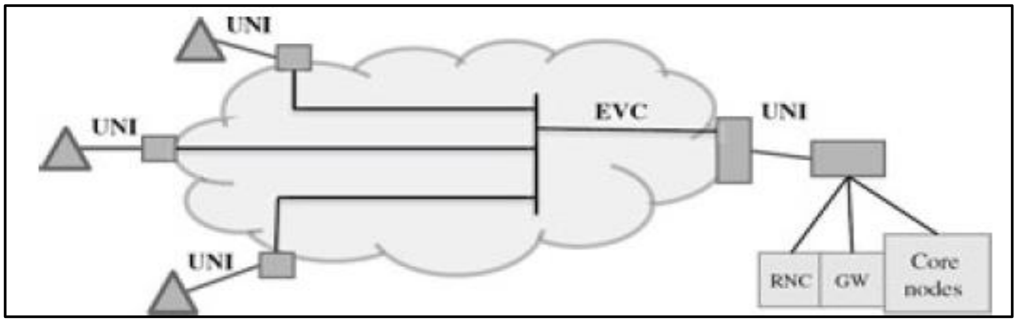


Figure 35: EP-LAN [3]

Ethernet Virtual Private LAN Service:

EVP-LAN is a VLAN based multipoint to multipoint local area network service. Each EVC can have two or more UNIs connected, and it does support service multiplexing. Thus fewer ports are required.

8.3 E-Tree:

Ethernet Private Tree Service:

In EP-Tree, there is one root UNI and multiple leaf UNIs. This is a port based point to multipoint service and does not support service multiplexing thus multiple ports are required for each EVC.

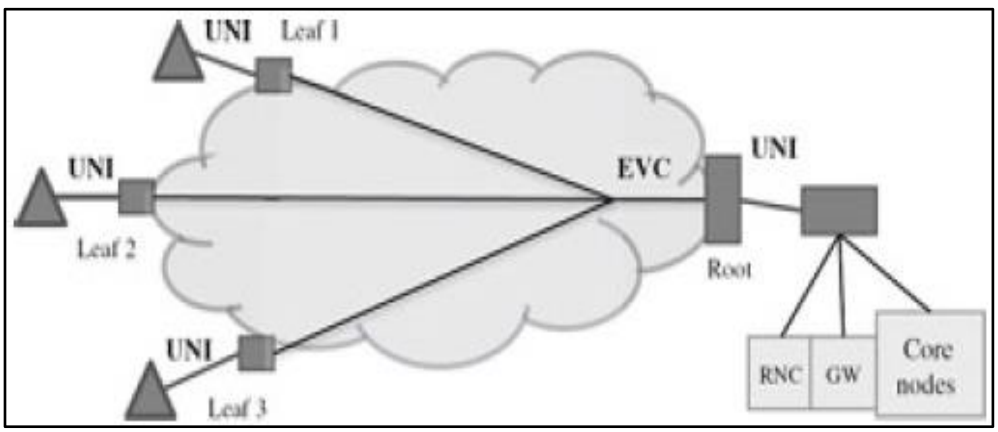


Figure 36: EP-Tree [3]

Ethernet Virtual Private Tree Service:

In EVP-Tree, there is one root UNI and multiple leaf UNIs. This is a VLAN based point to multipoint service and does support service multiplexing thus fewer ports are required for each EVC. The following table gives a summary of the Ethernet Service.

Service Type	Port-Based (All-to-One Bundling)	VLAN-Based (Service Multiplexed)
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)

Table 11: Ethernet Services [3]

8.4 E-Access

This is a point-to-point Operator Virtual Connection between a UNI and an NNI. It emulates a P2P Ethernet service within an Ethernet Access Network. This was introduced to allow the integration of other end-to-end CE® services even when there are foreign networks between customer sites. The two types are discussed below:

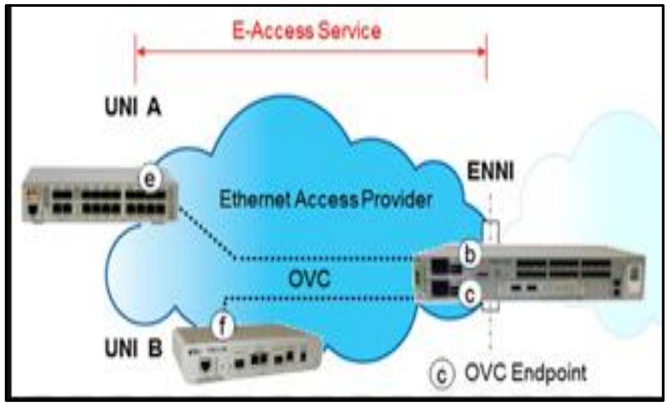


Figure 37: E-Access [10]

Access EPL

This is a port based point-to-point service between a UNI and an NNI in a single OVC. Separate interface/port is required at each end for individual OVCs and provides a site to site connectivity. In this service, only one service instance can be mapped to a single OVC in the UNI end. This service has a high degree of transparency for Service Frames between the connected UNI and NNI. The major advantage of having this service is that there is a low frame delay, loss, variation, and simplicity. This can be considered as a replacement to TDM private line. Service multiplexing is not available.

Access EVPL

This is a VLAN based point-to-point service between a UNI and an NNI in a single OVC. Multiplexing at the UNI end of multiple OVCs is possible. This allows the implementation of EVPL and EVP-LAN.

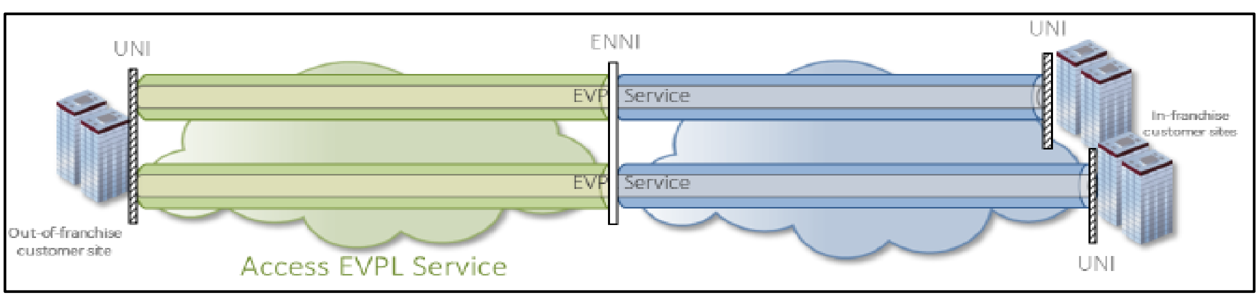


Figure 38: Access EVPL [13]

9.0 Access EPL Explained

Access EPL allows the interconnection of foreign networks to carry the service provider's traffic in a guaranteed QoS because CE's high standardized policies. This was first standardized by the MEF CE 2.0. Services such as end-to-end EPL and EP-LAN can be implemented on top of Access EPL. In reference and addition to Section 7.4 Access EPL, this section will in detail describe and outline the functionalities. The overview for Access EPL:

- Carrier Ethernet Network
- Point-to-Point OVC
- Port-based at UNI and NNI
- UNI at one end of OVC
- NNI at another end of OVC

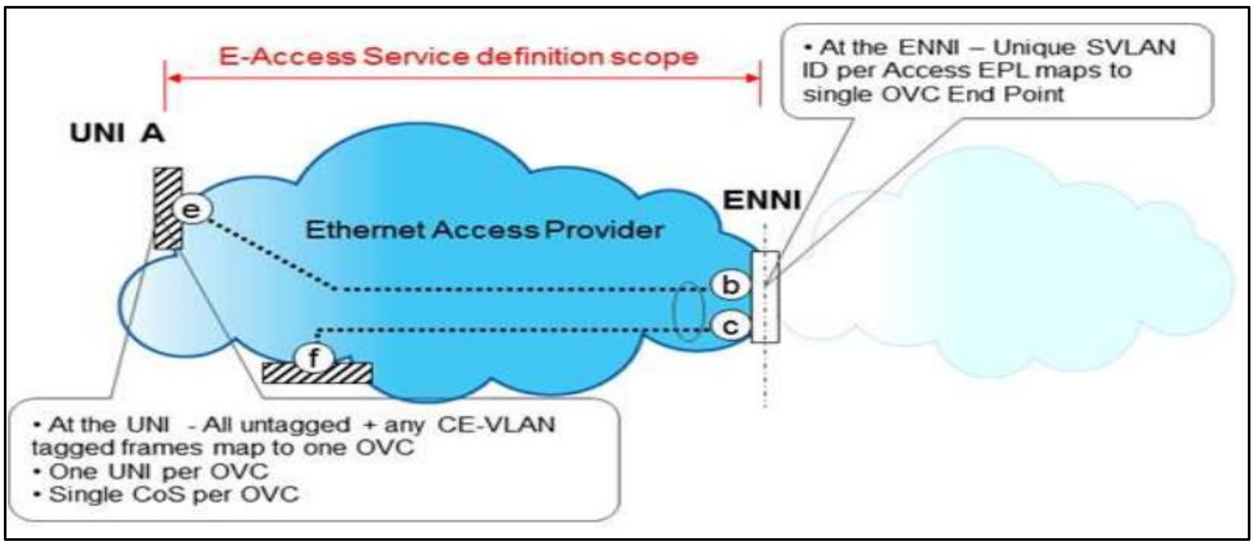


Figure 39: Access EPL [11]

UNI A is one end of the OVC through which any and every service frames are passed on to the other end of the OVC which is at the ENNI. This service complete has nothing to do whether the CE data is tagged or untagged. It transfers the frame as it is to the NNI with the only addition of an S-VLAN tag. This S-VLAN tag is used for the identifying the OVC and is internal to the Access Network.

9.1 Access EPL Attributes:

When implementing the above CES, the attributes and parameters of Ethernet need to be set as outlined by MEF 10.2 and 33. The UNI, NNI and OVC service attributes for enabling these types of services include

- BW profiles: Bandwidth can be allocated per service instance allowing greater flexibility with the BW allocation to the customer and/or type of data. Additionally, NNI can have a color mode in BW profiles which allows even deeper profiling before entering the foreign network.
- CoS: This increases the granularity in providing more flexible Quality of Service.

MEF also specifies the performance attributes for each which includes frame delay, inter-frame delay variation, frame loss ratio, and availability. The specifications of UNI service attributes are also specified such as physical interface capabilities, service multiplexing capabilities and Customer-VLAN bundling capability. BW Profiles can be enforced depending on required SLA/QoS on the ingress/egress of UNI ports, OVC or NNI ports. For the following diagrams, OVC and EVC are interchangeable.

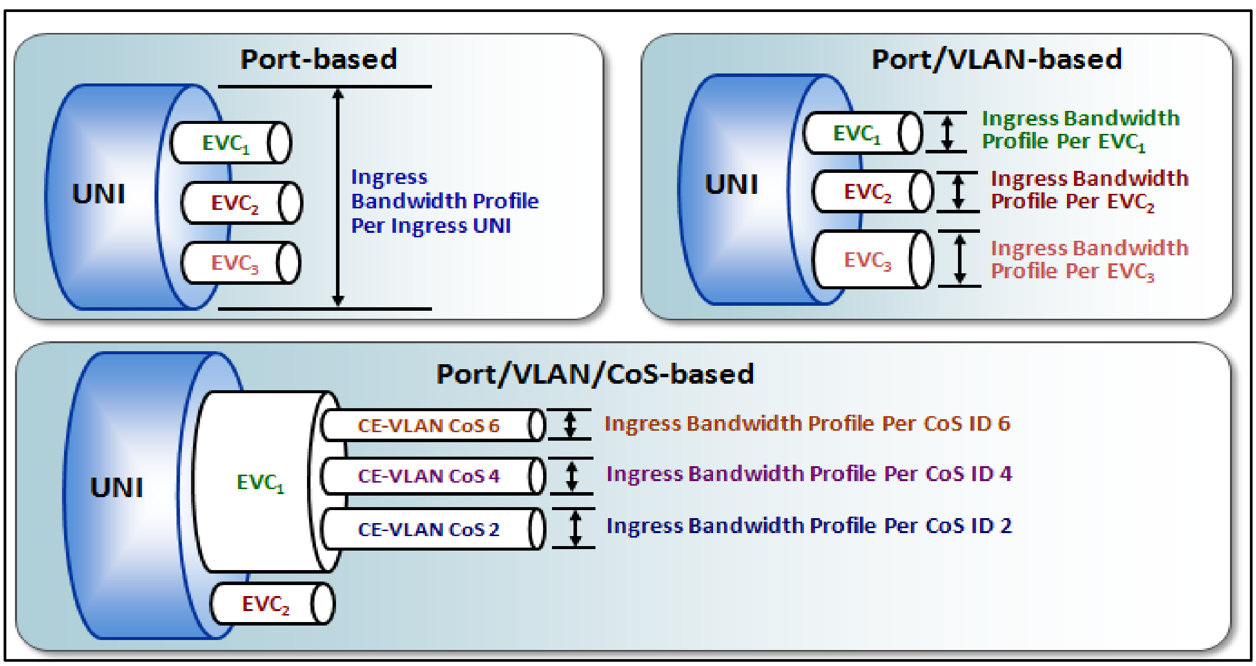


Figure 40: BW Profile example [7]

The following figure will summarize the basic implementation of Access EPL as per MEF 2.0 standards:

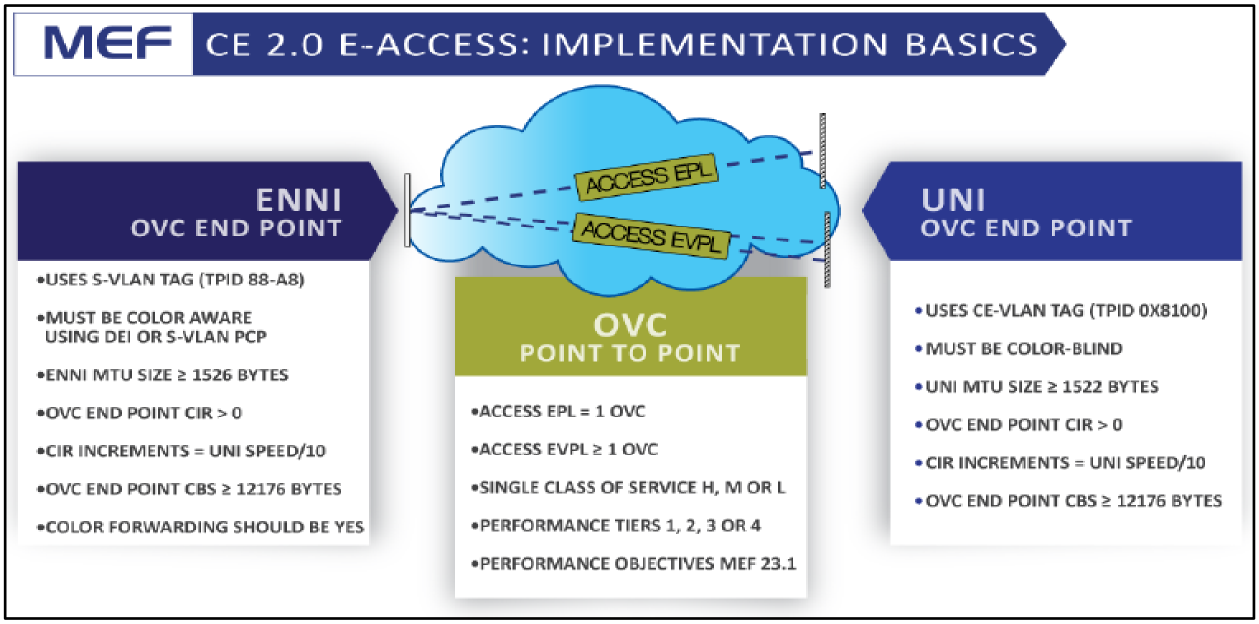


Figure 41: EPL basics [13]

9.2 Access EPL in LTE Access-Aggregation Network

In the scope of this Capstone Project, we will implement Access EPL in the access network of LTE Mobile Backhaul. This solution is intended for Ethernet metro network and a core consisting of Layer 3 IP/MPLS backbone. Out project will be similar to the diagram below:

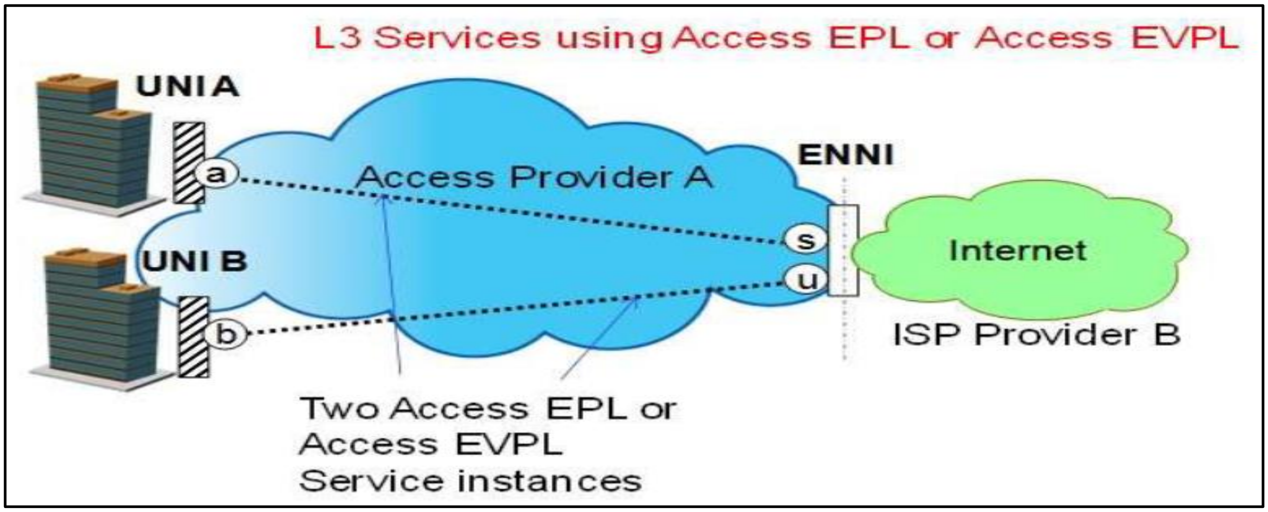


Figure 42: EPL in Access Network [10]

10.0 IP core/Backbone

This portion of the MBH is what connects the Access Network to the EPC. The core network interconnects all the end nodes of various access networks and provides the gateway to other networks. This portion of the network has to be of very high capacity as it will transport all traffic from multiple access networks and end nodes. Legacy core networks were primary build on TDM circuits but with the increase in demand, technological advancements and the need for improvements in the overall all core network technology, IP Core is now in place. This IP core gives has multiple advantages such as unbroken multi-service support, flexibility and better scalability. This paper will discuss the use of MPLS over IP core. The next chapter details the MPLS protocol.

This core network has to be capable of carrying the aggregated traffic and also be able to respond to failures in such manner that services are not disrupted. Traffic that flows through the core are often unpredicted and have unknown characteristics. Thus this network has to build to withstand the current force and future needs. In the physical layer, given the continuous increase in traffic volume, Fiber links with DWDM is used. This fulfills the demand of high-speed transport mechanism needed for high volume traffic. This network consists of internal routers which do routing within the core, and there are edge routers which connect the external networks, and these routers are often termed as the PE. The traffic coming in will be routed hop by hop using the destination IP address.

10.1 Interior Gateway Protocol (IGP)

Within the core, routing can be either static or dynamic. Given that core networks are large in size, combining multiple routers within and that it has to be scalable; dynamic routing protocols should be used. It can be either Open Shortest Path First (OSPF) or ISIS. OSPF and Intermediate System to Intermediate System (IS-IS) are dynamic IGP routing protocols that determine the forwarding path for traffic movement within the network. Both IS-IS and OSPF are link state routing algorithm that uses replicated distributed database. All the routers store this database, and it contains the whole internal network topology with the cost information to each node. The forwarding decision is based on the end-end BW metric without any hop limitations. Though it is difficult to implement and has high overhead, it is capable of very fast convergence and supports traffic engineering; which is very important in the core networks. For our purpose, we will use OSPF as our IGP within the core network.

OSPF uses IP datagrams and is identified by protocol number 89. The routers need to exchange multiple routing information messages before it can build the database. The messages exchanged are as follows:

- Hello
- Database Description
- Link State Request
- Link State Updates
- Link State Acknowledgement

The first step to run OSPF, the routers exchange Hello packets. This creates adjacencies between the neighbors. Then one of the routers sets itself as the root and sends their database description packet which includes a brief list of links states. Then the neighboring routers compare this database with its local OSPF database, and if any new or updated link is found, it sends the Link state request packets to the root neighbor. As a response to this request, the root router sends the link state update to the requesting node. This node then acknowledges the message by replying with a link state acknowledgment message. Once this is completed, the shortest path to each node is calculated and updated into the forwarding table. In the case of any change within the network, triggered updates are sent, and the calculation is done again.

In the case of large core networks, OSPF can be separated into multiple areas to provide more scalability and avoiding large databases. This allows the flexibility in hardware resource management and lowers convergence time by using a separate database for each area. In the case of multi-area OSPF, there has to be one area that acts as the backbone area, and there are three kinds of router configurations:

- Autonomous System Boundary Router (ASBR): Often known as the PE/edge router connecting to other networks
- Area Border Router (ABR): Router that connects multiple areas to the backbone area
- Internal Router: Routers within one area only

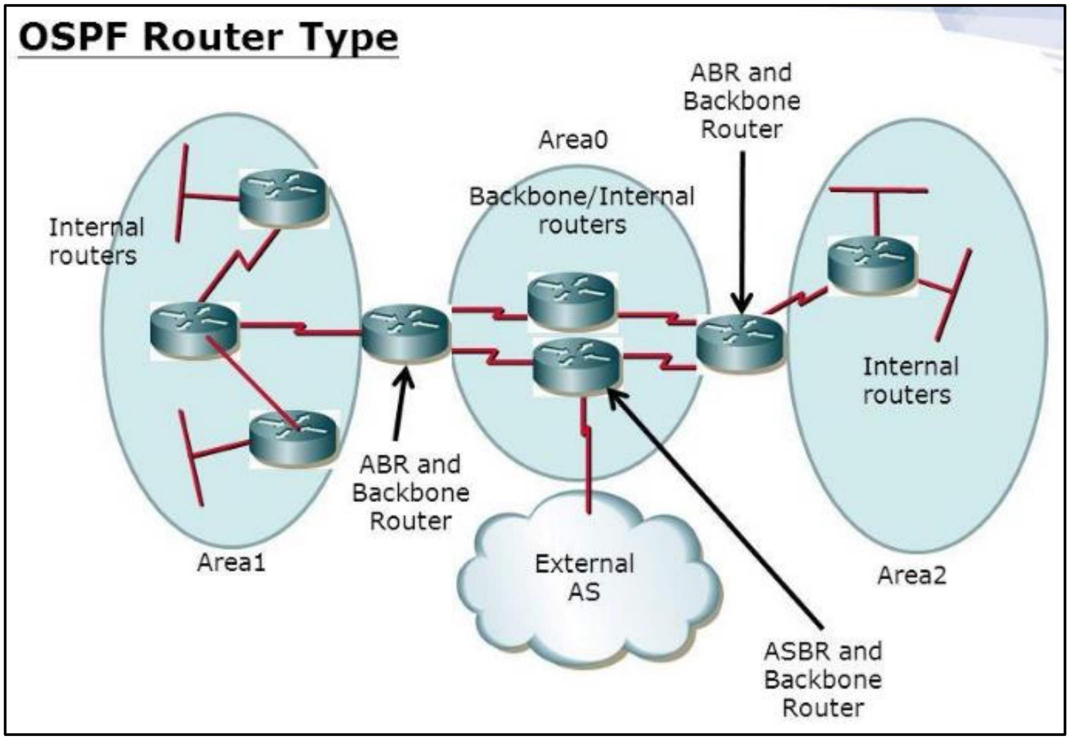


Figure 43: OSPF Router Types in Multiple Areas [16]

10.2 Border Gateway Protocol (BGP)

BGP can be termed as one of the most important exterior routing protocol in use. This is also how traffic flows over the internet throughout the world. BGP runs on top of IP using Transmission Control Protocol (TCP) port number 179, and it is primarily used to interconnect AS and or different networks using path-vector protocol for routing decisions. This is known as eBGP. When traffic needs to pass multiple AS/networks, BGP decides which AS and or path to take so that the traffic crosses the least number of AS to reach its destination. In this protocol, there is no peer discovery. The neighboring AS router running BGP has to be directly connected and explicitly configured. eBGP is configured on edge routers of an AS which directly connects to edge router of another AS.

BGP can also be used for routing within an AS. This is referred to as the Interior Border Gateway Protocol (iBGP). Here all the routers have to be in either full-mesh network or use Route Reflectors (explained later) to avoid loops and since advertisement of learned prefixes is not allowed within iBGP peers. If the network is in full-mesh configuration, then in case large AS with multiple routers, it becomes very resource intensive and difficult to manage, and this is where RR becomes very useful. iBGP can be effectively used when an AS is transiting foreign traffic, and it has to redirect it to exit in a controlled path within the AS.

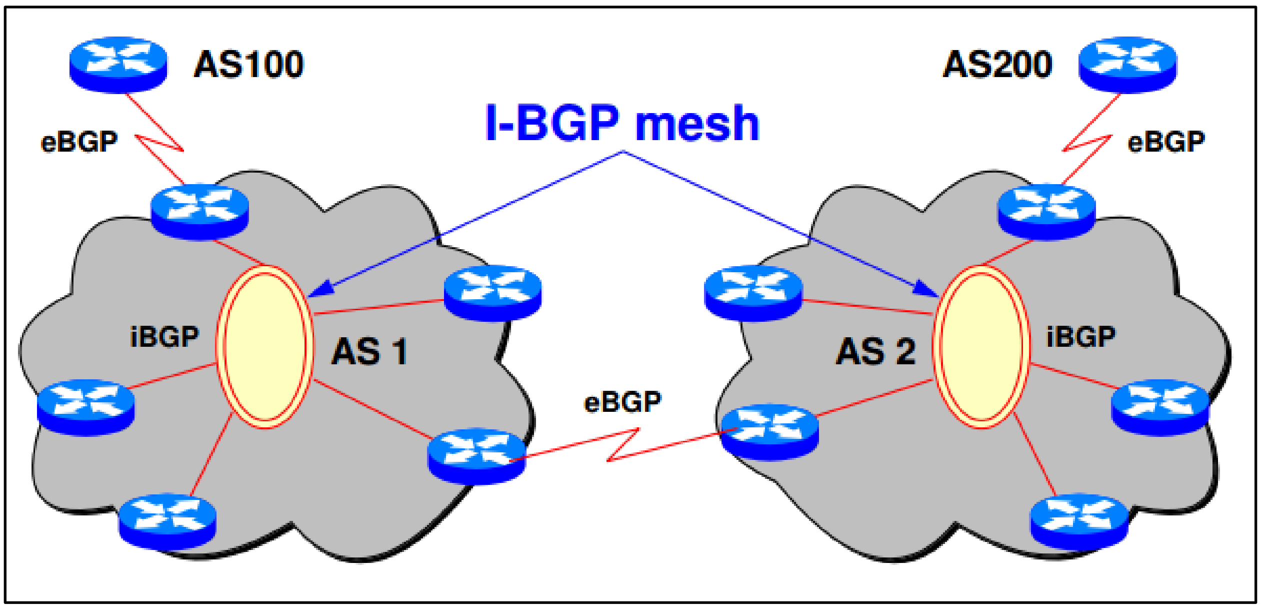


Figure 44: eBGP and iBGP[17]

10.3 MPLS

In continuation to Section 6.2, this section will discuss the transport technology MPLS and how it works. When a packet enters an IP/MPLS-enabled network, a 32-bit MPLS header is added between the L2 header and the L3 header. This header includes the Label, TC (Traffic Class), S (Stacking) and TTL (Time to Live) as shown in the diagram below:-

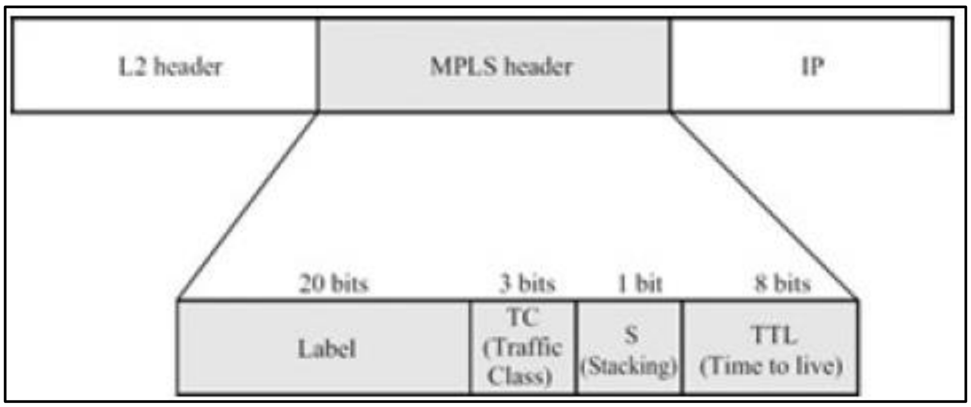


Figure 45: MPLS header

Few major advantages of MPLS are:

- Routers don't have to dig deeper into the stack for IP address saving ample of resource and increasing performance. Here the Router's forwarding decisions are made by looking into the MPLS header field.
- TC allows the use of QoS to better serve the traffic flow as per requirements
- Traffic Engineering and better network scalability. Its dynamic control plane allows fast recovery and routing mechanism. It can scale to thousands of nodes with the seamless recovery of L1, L2, and L3 failures.

The MPLS labels are based on the Forwarding Equivalence Class (FECs). The FEC has pre-configured Label Switched Path (LSP) for each kind of traffic based on the IP address. This is done at the Label Edge Router (LER), where L3/IP look up is performed when a packet first enters an MPLS network. Based on the FEC, a label is inserted into the packet. This is then forwarded to the next router, known as Label Switch Router (LSR), which only looks at the

MPLS headers and switches it according to what the next hop is. This eventually comes to the LER from where the packet will leave. This whole path from one ingress LER to another egress LER is called the LSP. When the packet leaves the MPLS network, the egress LER removes the MPLS header, does the IP look up again, if required to forward the packet. This can be compared to a tunnel, and the type of traffic that it is transporting is not a concern to the MPLS network.

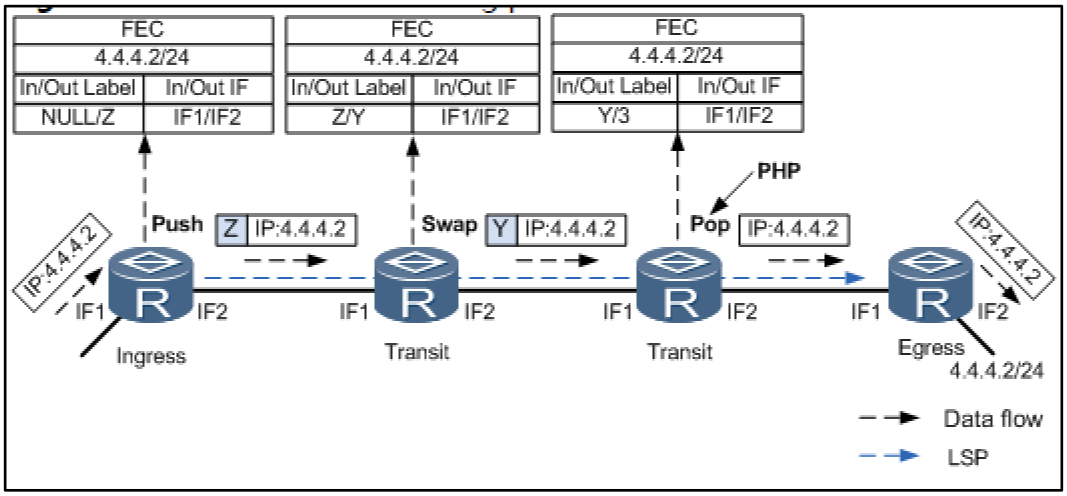


Figure 46: Label Switching in MPLS [22]

The S field in the MPLS header identifies if there are more MPLS label to look for in a packet. This scenario arises when using L3 VPN or L2 VPN. When such services are used over MPLS, the multiple labels help to distinguish between the services that the packet belongs to. The routers within the MPLS network have an MPLS forwarding table from which they decide the values/labels to be pushed, swapped or popped. These labels can be determined and distributed within the network by using LDP or Resource ReserVation Protocol (RSVP).

LDP

LDP is used for exchanging the labels that will be used between the routers in the MPLS Network. It uses UDP to discover its neighbors and uses TCP for its underlying transport protocol to negotiate the peer-peer session parameters. LDP relies on an IGP for network discovery such as OSPF.

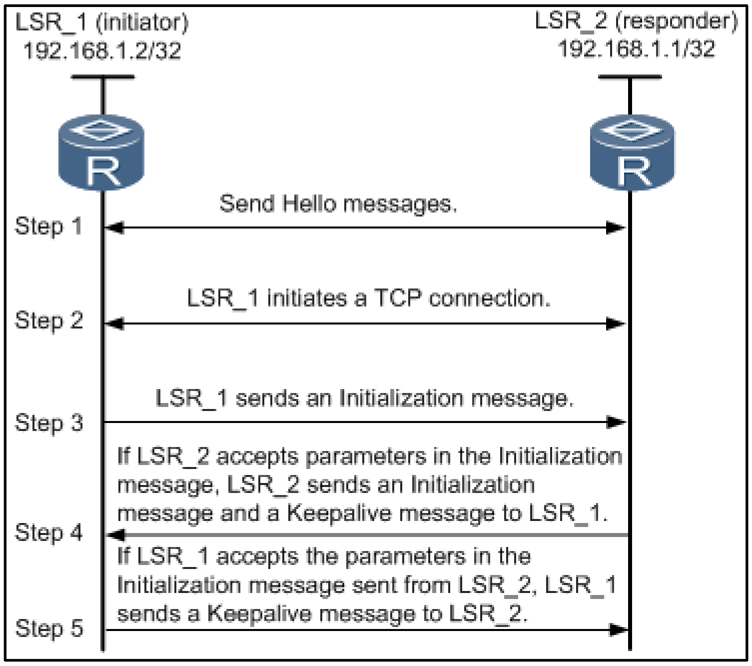


Figure 47: LDP Session [22]

RSVP

This is an alternative method for label distribution with more granularities present. RSVP allows the allocation of the specified path to be used along with bandwidth reservation mechanism. An LSP can be set from the head (ingress to MPLS network) to the end (egress of MPLS network) with the specification of which path to used or which nodes to forward to. This can be configured to not to follow the OSPF shortest path method thus allowing a more efficient use of links, nodes, and bandwidth. This limitation of using RSVP is that it is limited to the number of LSP sessions it can keep at a given point. RSVP uses refresh messages between the neighboring nodes to keep the specific LSP alive. RSVP also makes uses of hello messages to confirm that link is up. This allows failure detection and fast convergence for an alternative route creation.

In comparison, we use LDP when the network is huge with numerous of LER because creating a fully meshed network with RSVP LSP is just not possible due to the limited hardware resource.

10.4 IP/L3 MPLS VPN

VPN in general means a logical connection between two private networks over a public network. This allows the traffic from one customer site to another site that belongs to the same customer where the customer does not worry about the routing or infrastructure between the two sites. VPN can be both point to point and point to multipoint.

L3 MPLS VPN uses IP tunnels to pass customer traffic, and the public network is not visible to the customer. Customers peer with the PE of the service provider and same from the other end, making it look like the customers are peered together, and their traffic is flowing within its own network. In the case of multiple PE or any cases, BGP is responsible for creating VPN tunnels to each customer site and differentiating between them. In the case of multiple customers with the same IP block, they are differentiated using VRFs. Multiple VRFs are maintained where each VRF corresponds to the routing table of one customer allowing the use of same IP block of multiple customers. A 12 byte RD is used to uniquely identify a VPN route within the BGP network. This is done by the source PE to the target PE. This is included in the VPNIPv4 address family along with the 4byte IPv4 address [3].

Since the BGP is only between the PEs, implementing MPLS tunnels in the core network is very much preferable as it has nothing to do with the target PE IP address. Internal routing will be done using MPLS labels, and PE-PE routing will be done by BGP by LSPs already in place between all customer sites. Two labels are used in the MPLS core, the first one is intended for label switching and forwarding within the LSP of the MPLS network and the second one is to map the packet the correct VPN.

Route Reflectors can be used when the core network is very large. This is to avoid the full mesh requirement of MP-BGP between all the PEs. Instead, the PE maintains one session with an RR and this where all the routing information of all the PEs are stored. This kind of MBH is very much suitable as multiple sites can be included and all sites can have connectivity between them. The following diagram gives an example:

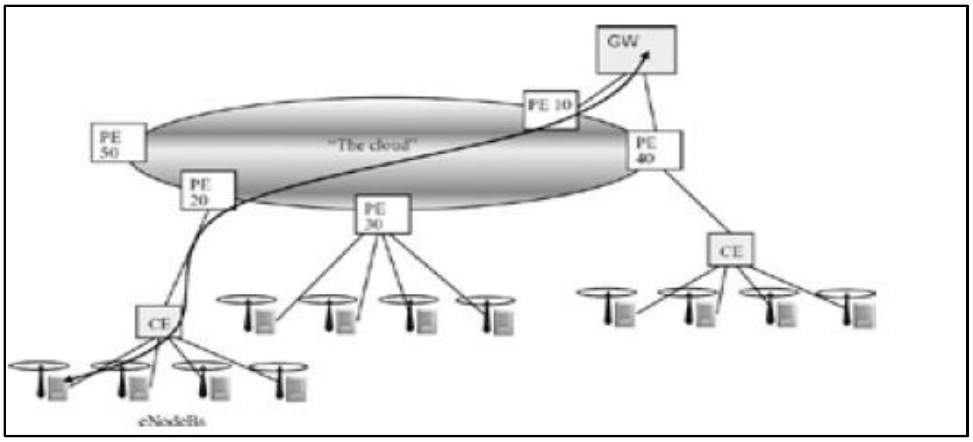


Figure 48: Layer 3 VMP in BMH [3]

Advantages of IP MPLS VPN [3]

- Reliability, QoS, Security, and Synchronization
- Flexible Configurable IP Layer Connectivity
- Scalable and Support for IPv4 and IPv6
- Support for node and link failure detection with fast convergence and traffic engineering

10.5 L2 MPLS VPN – VPLS

This is a method to implement multipoint virtual logical connectivity between multiple customer sites and can be compared to a LAN service. AN SVI instance is required at the PE to emulate Ethernet Bridging function. Since this is an L2 service, there is no concept of IP connectivity. This method, since similar to LAN, has the concept of MAC learning, unicast, broadcast, and flooding. In comparison to the IP MPLS VPN, the inner MPLS label is used to identify the Virtual Channel which is the pseudowire connecting the two ends. PE-PE forwarding is done via MAC-learning with packets encapsulated within Ethernet frames and transported by MPLS in the core network. Overall, L2 MPLS VPN-VPLS is not needed in the MBH as there is no need for L2 connectivity explicitly because LTE technology is based out of IP connectivity end to end. Though it is possible, it can increase the burden of security issues with unnecessary broadcasting along with the increased failure and misconfiguration possibilities.

11.0 Implementation Design

In this section, we will implement a network emulating the MBH. The implementation will be done using platforms available in the MINT Lab available for students. This section will in detail show and describe all steps taken to implement and test this proposed network. The implementation was done using EVE-NG, an emulated networking platform running on ESXi hypervisor using a server from the MINT LAB. The overall proposed network is shown below, and the next page will describe each platform in details:

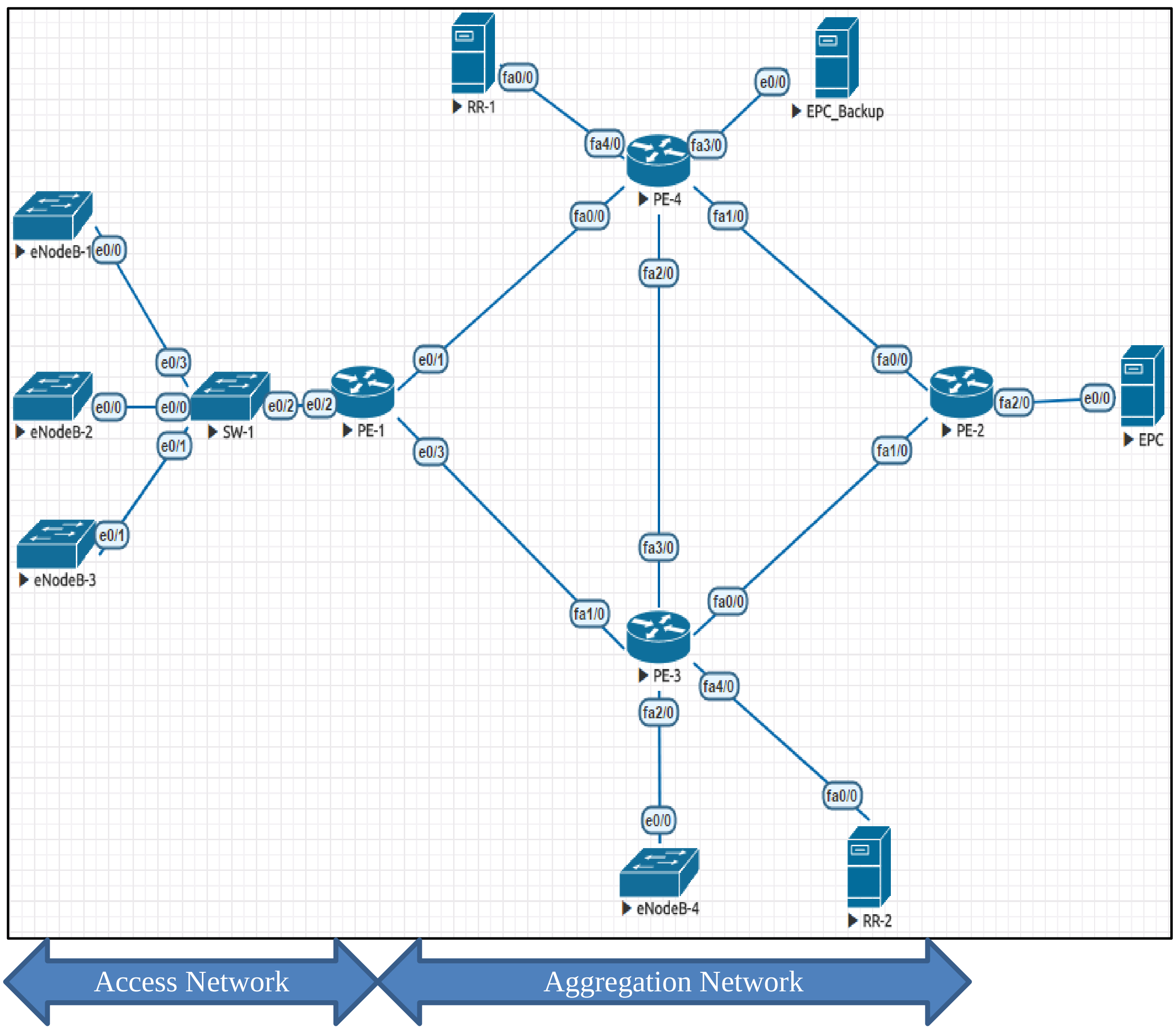


Figure 49: Overall Network

Table 12: Implementation devices

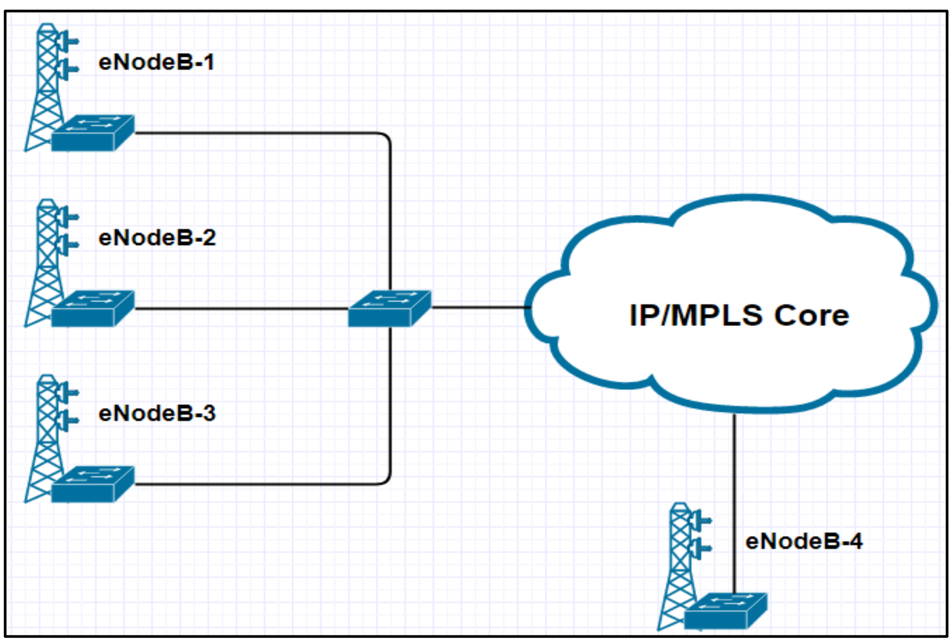
PLATFORM AS PER FIGURE 29	FUNCTION / ACTING AS	DEVICE AND OS USED	IMPLEMENTATION NETWORK ADDRESSING / INTERFACE	NETWORK LAYER
eNodeB-1	Switch	EVE, l2-adventerprise-15.1	E0/0 - Trunk (VLAN 10) 172.16.3.2/24	Access (Site X)
eNodeB-2	Switch	EVE, l2-adventerprise-15.1	E0/0 - Trunk (VLAN 10) 172.16.3.3/24	Access (Site X)
eNodeB-3	Switch	EVE, l2-adventerprise-15.1	E0/0 - Trunk (VLAN 10) 172.16.3.4/24	Access (Site X)
eNodeB-4	Switch	EVE, l2-adventerprise-15.1	E0/0 - Trunk (VLAN 10) 172.16.2.2/24	Access (Site Y)
SW-1	Aggregation Switch	EVE, l2-adventerprise-15.1	N/A	Access (Site X)
PE-1	Router	EVE, l2-adventerprise-15.1	Loopback0 – 192.168.255.1 E0/2 – Trunk (VLAN 10) E0/2.10 – 172.16.3.1/24 (Sub) E0/1 – 192.168.1.1/30 E0/3 – 192.168.1.5/30	Aggregation
PE-2	Router	EVE, 7200, Version 15.2(4)S6	Loopback0 – 192.168.255.2 E0/0 – 192.168.1.18/30 E0/1 – 192.168.1.14/30 E0/2 – Trunk (VLAN 10) E0/2.10 – 172.16.1.1/24	Aggregation

			(Sub)	
PE-3	Router	EVE, 7200, Version 15.2(4)S6	Loopback0 – 192.168.255.3 E0/0 – 192.168.1.13/30 E0/1 – 192.168.1.6/30 E0/2 – Trunk (VLAN 10) E0/2.10 – 172.16.2.1/24 (Sub) E0/3 – 192.168.1.9/30 E0/4 – 192.168.1.25/30	Aggregation
PE-4	Router	EVE, 7200, Version 15.2(4)S6	Loopback0 – 192.168.255.4 E0/0 – 192.168.1.2/30 E0/1 – 192.168.1.17/30 E0/2 – 192.168.1.10/30 E0/3 – Trunk (VLAN 10) E0/3.10 – 172.16.1.1/24 (Sub) E0/4 – 192.168.1.21/30	Aggregation
EPC	Primary EPC Server (MME/SGW /PGW)	EVE, l2-adventerprise-15.1	E0/0 - Trunk (VLAN 10) 172.16.1.2/24	LTE Core
EPC_Backup	Secondary/Backup EPC Server (MME/SGW /PGW)	EVE, l2-adventerprise-15.1	E0/0 - Trunk (VLAN 10) 172.16.1.2/24	Backup LTE Core

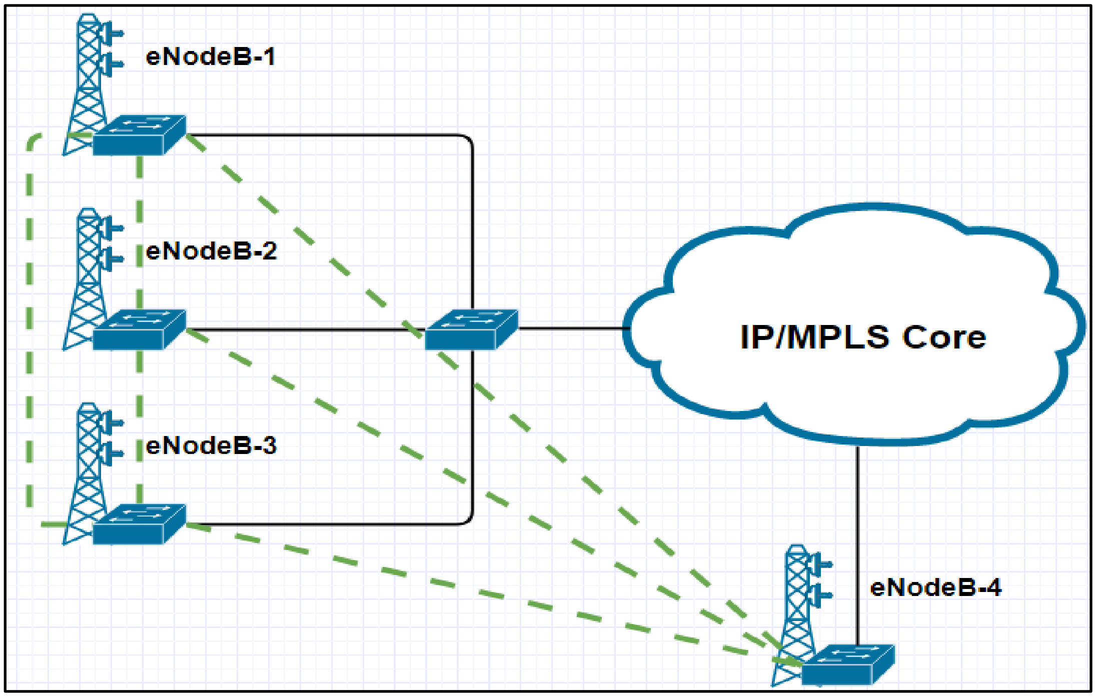
RR-1	VPNv4 Route Reflector	EVE, 7200, Version 15.2(4)S6	E0/0 – 192.168.1.22/30 Loopback0 – 192.168.255.11	Aggregation
RR-1	VPNv4 Route Reflector	EVE, 7200, Version 15.2(4)S6	E0/0 – 192.168.1.22/30 Loopback0 – 192.168.255.22	Aggregation

11.1 Access Network Design

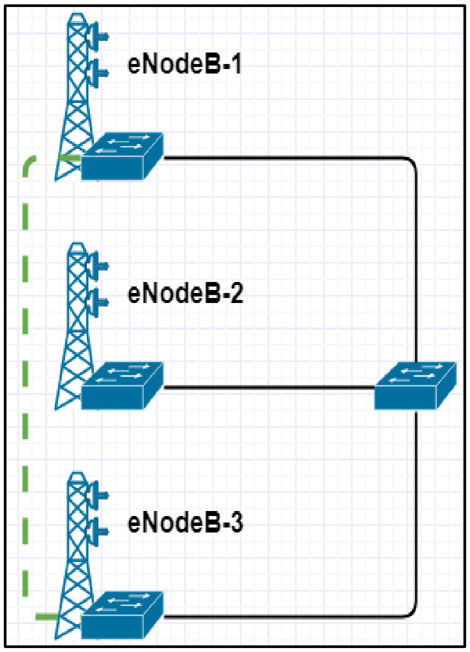
e-NodeBs: This is where the BTS is positioned. In our lab implementation, we have positioned them at two different sites. Site X which includes eNodeB-1, eNodeB-2 and eNodeB-3. This site also has a switch which interconnects links from all the eNodeBs and connects to the Aggregation Router (PE-X) with a single link. Site Y has a single eNodeB-4. The following diagram gives a simplified view of the access network and eNodeBs. Each black straight line represents a physical connection.

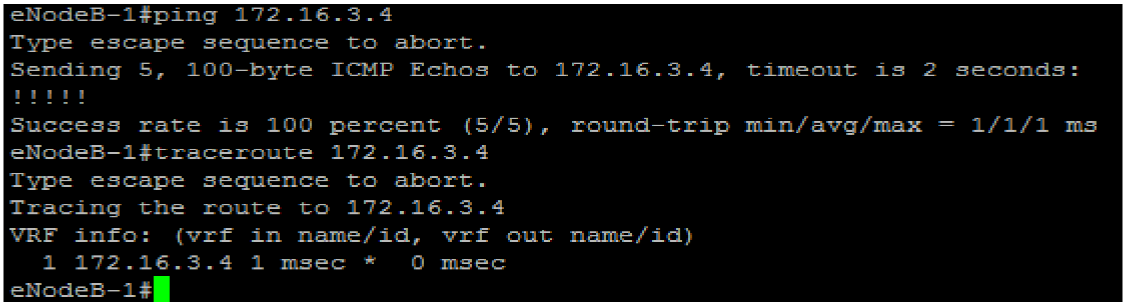


This portion, from the eNodeBs to the Aggregation (PE-X), is the Access network and it is implemented by using Layer 2 Trunks and VLANs. This will emulate the Access EPL. All the eNBs are using the VLAN10 for all traffic with subnet 172.16.X.X which belongs to the LTE service provider. They link to the Aggregation router (PE-X) using Trunk interface with the dot1q encapsulation method. All the traffic from these nodes is default routed to their gateway. The following diagram shows the logical links between the eNodeBs since they are all under the same VLAN:

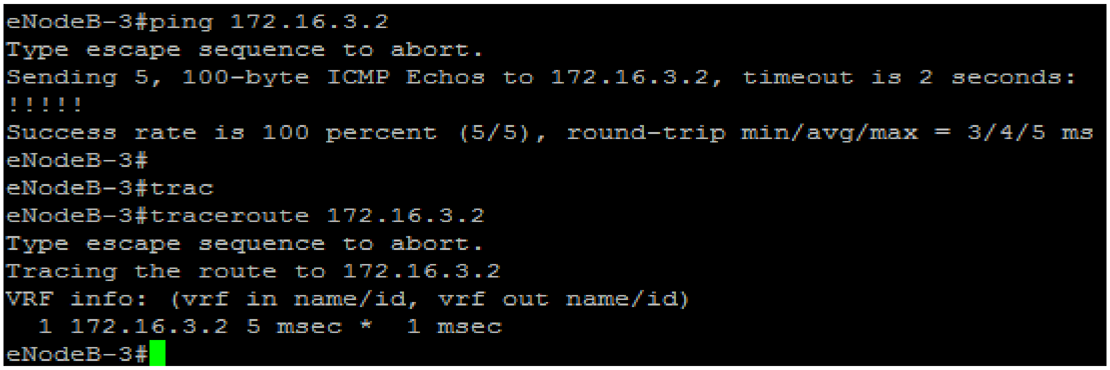


In real-life deployment, the above 'green' dotted lines would represent the X2 interface between the eNodeBs. An Example of communication between eNodeB-1 and eNodeB-3 is illustrated below where the green dotted lines are the logical link, and the black line is the physical link. A screen shot of the ping test (bidirectional) is also included which shows that this communication does not go through any other intermediate nodes and is a representation of the X2 interface.



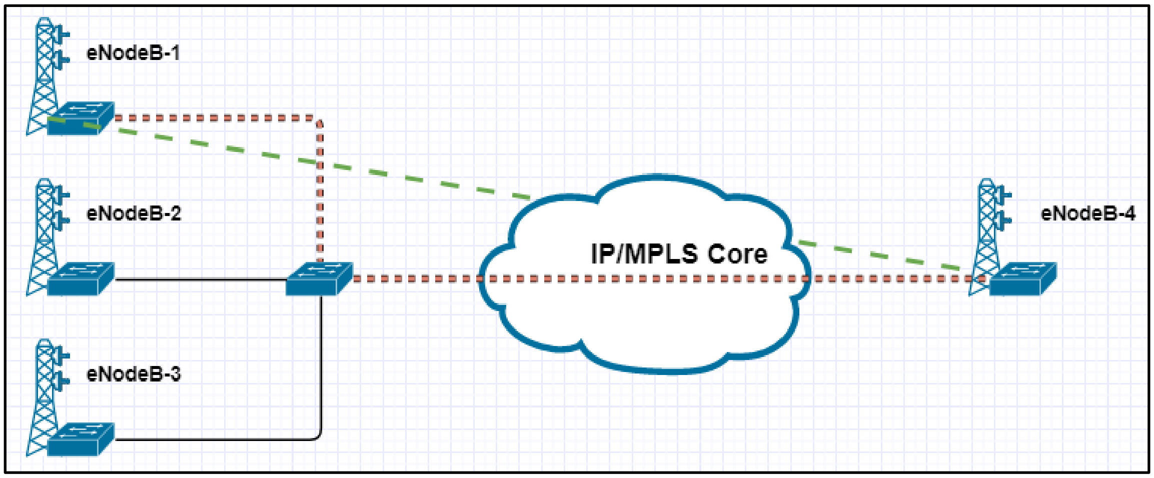


```
eNodeB-1#ping 172.16.3.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.3.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
eNodeB-1#traceroute 172.16.3.4
Type escape sequence to abort.
Tracing the route to 172.16.3.4
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.3.4 1 msec *  0 msec
eNodeB-1#
```



```
eNodeB-3#ping 172.16.3.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.3.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/4/5 ms
eNodeB-3#
eNodeB-3#trac
eNodeB-3#traceroute 172.16.3.2
Type escape sequence to abort.
Tracing the route to 172.16.3.2
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.3.2 5 msec *  1 msec
eNodeB-3#
```

All of the eNodeBs have connectivity with the EPC. The EPC is also under the same VLAN as the eNodeBs. The logical link between the each eNodeB (e.g. eNodeB-1) and the EPC is as shown below in green dotted line and the traffic flow is shown in red dotted line:



There are also two separate EPCs which connect to the Aggregation network for redundancy; though only one is serving the network at a time. Both EPCs are using the same subnet, and they have been assigned the same IP address because the eNodeBs can use the same address to reach either of them. Furthermore, only one EPC can be seen by the eNodeBs. This is achieved by assigning a higher metric for the EPC-Backup.

This design is compared to one QOS class traffic using point to point OVC in the actual CE® implemented Access Network of real life scenario. We can implement multiple VLAN emulating multiple QOS to provide a comparison to MEFs CE® Services.

11.2 Aggregation Network Design

This portion of the network uses OSPF as the interior routing protocol. Even though the default OSPF network type is a broadcast, we changed it to point to point for fast convergence. MPLS and LDP are used as the transport protocol. The PE-1, PE-2, PE-3, and PE-4 are edge routers which use an M-BGP routing protocol to exchange VPNv4 prefixes. This network design includes two Route Reflectors for redundancy and to eliminate the need for full-mesh requirement between the PEs.

L3VPN is been used to provide reachability among eNodeBs and ECP, all eNodeBs and ECPs are using the same Route-Target import and export to learn and install the prefixes inside their VRFs. The VRF details are shown below for each PE:

Table 13: VRfs

Point of Presence (POP)	VRF name	Route Distinguisher	Route-Target Import	Route-Target Export
PE-1	eNodeB-1-3	10:10	10:10	10:10
PE-2	EPC	10:10	10:10	10:10
PE-3	eNodeB-4	10:10	10:10	10:10
PE-4	EPC_Backup	10:10	10:10	10:10

Please refer to 11.3-Traffic Flow Diagrams, Ping and Trace Route sections for more figures and descriptive diagrams.

11.3 Configuration

All configuration files for each node are included in the Appendix A. This subsection will discuss some of the necessary configurations performed and why:

- To enable trunk interface on the eNodeBs and access side of PEs with dot1q encapsulation and allowing VLAN 10:

```
interface Ethernet X
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10
 switchport mode trunk
```

- Configuring Access port for eNodeB:

```
Interface Ethernet X
        switchport mode access
        switchport access vlan 10
```

- Enabling OSPF at the Aggregation network routers:

```
router ospf X
        router-id X.X.X.X
        passive-interface LoopbackX
        network X.X.X.X Y.Y.Y.Y area X
interface EthernetX
        ip ospf network point-to-point
```

- Enabling BGP at the PEs:

```
router bgp XXX
        no bgp default ipv4-unicast
        neighbor X.X.X.X remote-as XXX
        neighbor X.X.X.X update-source LoopbackX
        address-family vpnv4
                neighbor X.X.X.X activate
                neighbor X.X.X.X send-community extended
        address-family ipv4 vrf X
                redistribute connected
```

- Enabling LDP and MPLS:

```
mpls label range X X
mpls label protocol ldp
mpls ldp router-id LoopbackX
interface EthernetX
        mpls label protocol ldp
        mpls ip
```

- Configuring VRF parameters:

```
ip vrf X
        rd 10:10
        route-target export 10:10
        route-target import 10:10
```

- Assigning VRF to an interface:

```
interface EthernetX.10
        ip vrf forwarding X
        ip address X.X.X.X 255.255.255.0
```

- Configuring Route Reflectors clients:

```
router bgp XXX
        bgp log-neighbor-changes
        no bgp default ipv4-unicast
        neighbor IBGP peer-group
        neighbor IBGP remote-as XXX
        neighbor IBGP update-source Loopback0
        neighbor X.X.X.X peer-group IBGP
        address-family vpnv4
                neighbor IBGP send-community extended
                neighbor IBGP route-reflector-client
                neighbor X.X.X.X activate
```

Screenshots of Configuration Testing:

Interface details of all nodes:

```
eNodeB-1>show ip interface brief | exclude unassigned
Interface              IP-Address      OK? Method Status                Protocol
Vlan10                 172.16.3.2      YES TFTP   up                    up
eNodeB-1#show interfaces status | exclude disabled

Port      Name               Status       Vlan       Duplex  Speed Type
Et0/0     eNodeB-1_to_SW-1   connected    trunk        auto   auto unknown
```

```
eNodeB-2>show ip interface brief | exclude unassigned
Interface              IP-Address      OK? Method Status                Protocol
Vlan10                 172.16.3.3      YES TFTP   up                    up
eNodeB-2#show interfaces status | exclude disabled

Port      Name               Status       Vlan       Duplex  Speed Type
Et0/0     eNodeB-2_to_SW-1   connected    trunk        auto   auto unknown
```

```
eNodeB-3>show ip interface brief | exclude unassigned
Interface              IP-Address      OK? Method Status                Protocol
Vlan10                 172.16.3.4      YES TFTP   up                    up
eNodeB-3#show interfaces status | exclude disabled

Port      Name               Status       Vlan       Duplex  Speed Type
Et0/1     eNodeB-3_to_SW-1   connected    trunk        auto   auto unknown
```

```
eNodeB-4>show ip in br | exclude unassigned
Interface              IP-Address      OK? Method Status                Protocol
Vlan10                 172.16.2.2      YES TFTP   up                    up
eNodeB-4#show interfaces status | exclude disabled

Port      Name               Status       Vlan       Duplex  Speed Type
Et0/0     eNodeB-4_to_PE-3   connected    trunk        auto   auto unknown
```

```
EPC#sho ip inter br | exclude unassigned
Interface              IP-Address      OK? Method Status                Protocol
Vlan10                 172.16.1.2      YES TFTP   up                    up
EPC#show interfaces status | exclude disabled

Port      Name               Status       Vlan       Duplex  Speed Type
Et0/0     EPC_to_PE-2        connected    trunk        auto   auto unknown
```

```
EPC_Backup#show ip interface brief | exclude unassigned
Interface              IP-Address      OK? Method Status                Protocol
Vlan10                 172.16.1.2      YES TFTP   up                    up
EPC_Backup#show interfaces status | exclude disabled

Port      Name               Status       Vlan       Duplex  Speed Type
Et0/0     EPC_Backup_to_PE-4 connected    trunk        auto   auto unknown
```

```
PE-1#show ip interface brief | exclude unassigned
Interface              IP-Address      OK? Method Status                Protocol
Ethernet0/1            192.168.1.1     YES TFTP   up                    up
Ethernet0/2.10         172.16.3.1      YES TFTP   up                    up
Ethernet0/3            192.168.1.5     YES TFTP   up                    up
Loopback0              192.168.255.1   YES TFTP   up                    up
PE-1#show interfaces status | exclude disabled

Port      Name               Status       Vlan       Duplex  Speed Type
Et0/1     PE-1_to_PE-4       connected    routed       auto   auto unknown
Et0/2     PE-1_to_SW-1       connected    routed       auto   auto unknown
Et0/3     PE-1_to_PE-3       connected    routed       auto   auto unknown
```

```
PE-2#show ip int brief | exclude unassigned
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        192.168.1.18    YES NVRAM  up                    up
FastEthernet1/0        192.168.1.14    YES NVRAM  up                    up
FastEthernet2/0.10     172.16.1.1      YES NVRAM  up                    up
Loopback0              192.168.255.2   YES NVRAM  up                    up
```

```
PE-3#show ip int brief | exclude unassigned
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        192.168.1.13    YES NVRAM  up                    up
FastEthernet1/0        192.168.1.6     YES NVRAM  up                    up
FastEthernet2/0.10     172.16.2.1      YES NVRAM  up                    up
FastEthernet3/0        192.168.1.9     YES NVRAM  up                    up
FastEthernet4/0        192.168.1.25    YES NVRAM  up                    up
Loopback0              192.168.255.3   YES NVRAM  up                    up
```

```
PE-4#sho ip interface brief | exclude unassigned
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        192.168.1.2     YES NVRAM  up                    up
FastEthernet1/0        192.168.1.17    YES NVRAM  up                    up
FastEthernet2/0        192.168.1.10    YES NVRAM  up                    up
FastEthernet3/0.10     172.16.1.1      YES NVRAM  up                    up
FastEthernet4/0        192.168.1.21    YES NVRAM  up                    up
Loopback0              192.168.255.4   YES NVRAM  up                    up
```

```
RR-1#show ip interface brief | exclude unassigned
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        192.168.1.22    YES NVRAM  up                    up
Loopback0              192.168.255.11  YES NVRAM  up                    up
```

```
RR-2#show ip interface brief | exclude unassigned
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        192.168.1.26    YES NVRAM  up                    up
Loopback0              192.168.255.22  YES NVRAM  up                    up
```

VRF of the Aggregation Network:

```
PE-1#show ip vrf detail
VRF eNodeB-1-3 (VRF Id = 1); default RD 10:10; default VPNID <not set>
  Interfaces:
    Et0/2.10
VRF Table ID = 1
  Export VPN route-target communities
    RT:10:10
  Import VPN route-target communities
    RT:10:10
```

```
PE-2#show ip vrf detail
VRF EPC (VRF Id = 1); default RD 10:10; default VPNID <not set>
  Interfaces:
    Fa2/0.10
VRF Table ID = 1
  Export VPN route-target communities
    RT:10:10
  Import VPN route-target communities
    RT:10:10
```

```
PE-3#show ip vrf detail
VRF eNodeB-4 (VRF Id = 1); default RD 10:10; default VPNID <not set>
  Interfaces:
    Fa2/0.10
VRF Table ID = 1
  Export VPN route-target communities
    RT:10:10
  Import VPN route-target communities
    RT:10:10
```

```
PE-4#show ip vrf detail
VRF EPC-Backup (VRF Id = 1); default RD 10:10; default VPNID <not set>
  Interfaces:
    Fa3/0.10
VRF Table ID = 1
  Export VPN route-target communities
    RT:10:10
  Import VPN route-target communities
    RT:10:10
  No import route-map
  No global export route-map
  No export route-map
  VRF label distribution protocol: not configured
  VRF label allocation mode: per-prefix
```

OSPF Running:

```
PE-1#show ip ospf interface brief
Interface    PID   Area            IP Address/Mask    Cost  State Nbrs F/C
Lo0          1     0               192.168.255.1/32   1     P2P   0/0
Et0/3        1     0               192.168.1.5/30     10    P2P   1/1
Et0/1        1     0               192.168.1.1/30     1     P2P   1/1
PE-1#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.255.3     0   FULL/  -        00:00:36    192.168.1.6     Ethernet0/3
192.168.255.4     0   FULL/  -        00:00:38    192.168.1.2     Ethernet0/1
```

```
PE-2#show ip ospf interface brief
Interface    PID   Area            IP Address/Mask    Cost  State Nbrs F/C
Lo0          1     0               192.168.255.2/32   1     P2P   0/0
Fa0/0        1     0               192.168.1.18/30    1     P2P   1/1
Fa1/0        1     0               192.168.1.14/30    1     P2P   1/1
PE-2#
PE-2#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.255.4     0   FULL/  -        00:00:37    192.168.1.17    FastEthernet0/0
192.168.255.3     0   FULL/  -        00:00:35    192.168.1.13    FastEthernet1/0
```

```
PE-3#show ip ospf interface brief
Interface    PID   Area            IP Address/Mask    Cost  State Nbrs F/C
Lo0          1     0               192.168.255.3/32   1     P2P   0/0
Fa4/0        1     0               192.168.1.25/30    1     P2P   1/1
Fa3/0        1     0               192.168.1.9/30     1     P2P   1/1
Fa1/0        1     0               192.168.1.6/30     10    P2P   1/1
Fa0/0        1     0               192.168.1.13/30    1     P2P   1/1
PE-3#
PE-3#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.255.22    0   FULL/  -        00:00:36    192.168.1.26    FastEthernet4/0
192.168.255.4     0   FULL/  -        00:00:31    192.168.1.10    FastEthernet3/0
192.168.255.1     0   FULL/  -        00:00:33    192.168.1.5     FastEthernet1/0
192.168.255.2     0   FULL/  -        00:00:34    192.168.1.14    FastEthernet0/0
```

```
PE-4#show ip ospf interface brief
Interface    PID   Area            IP Address/Mask    Cost  State Nbrs F/C
Lo0          1     0               192.168.255.4/32   1     P2P   0/0
Fa4/0        1     0               192.168.1.21/30    1     P2P   1/1
Fa2/0        1     0               192.168.1.10/30    1     P2P   1/1
Fa1/0        1     0               192.168.1.17/30    1     P2P   1/1
Fa0/0        1     0               192.168.1.2/30     1     P2P   1/1
PE-4#
PE-4#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.255.11    0   FULL/  -        00:00:36    192.168.1.22    FastEthernet4/0
192.168.255.3     0   FULL/  -        00:00:32    192.168.1.9     FastEthernet2/0
192.168.255.2     0   FULL/  -        00:00:36    192.168.1.18    FastEthernet1/0
192.168.255.1     0   FULL/  -        00:00:37    192.168.1.1     FastEthernet0/0
```

```
RR-1#show ip ospf interface brief
Interface    PID   Area            IP Address/Mask    Cost  State Nbrs F/C
Lo0          1     0               192.168.255.11/32  1     P2P   0/0
Fa0/0        1     0               192.168.1.22/30    1     P2P   1/1
RR-1#
RR-1#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.255.4     0   FULL/  -        00:00:37    192.168.1.21    FastEthernet0/0
```

```
RR-2#show ip ospf interface brief
Interface    PID   Area            IP Address/Mask    Cost  State Nbrs F/C
Lo0          1     0               192.168.255.22/32  1     P2P   0/0
Fa0/0        1     0               192.168.1.26/30    1     P2P   1/1
RR-2#
RR-2#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.255.3     0   FULL/  -        00:00:35    192.168.1.25    FastEthernet0/0
```

MPLS/LDP

```
PE-1#show mpls label range
Downstream Generic label region: Min/Max label: 100/199

PE-1#show mpls ldp neighbor
    Peer LDP Ident: 192.168.255.3:0; Local LDP Ident 192.168.255.1:0
        TCP connection: 192.168.255.3.43381 - 192.168.255.1.646
        State: Oper; Msgs sent/rcvd: 179/181; Downstream
        Up time: 02:23:25
        LDP discovery sources:
          Ethernet0/3, Src IP addr: 192.168.1.6
        Addresses bound to peer LDP Ident:
          192.168.1.13    192.168.255.3   192.168.1.6     192.168.1.9
          192.168.1.25
    Peer LDP Ident: 192.168.255.4:0; Local LDP Ident 192.168.255.1:0
        TCP connection: 192.168.255.4.22378 - 192.168.255.1.646
        State: Oper; Msgs sent/rcvd: 179/179; Downstream
        Up time: 02:23:25
        LDP discovery sources:
          Ethernet0/1, Src IP addr: 192.168.1.2
        Addresses bound to peer LDP Ident:
          192.168.1.2     192.168.255.4   192.168.1.17    192.168.1.10
          192.168.1.21
```

```
PE-2#show mpls label range
Downstream Generic label region: Min/Max label: 200/299

PE-2#
PE-2#show mpls ldp neighbor
    Peer LDP Ident: 192.168.255.4:0; Local LDP Ident 192.168.255.2:0
        TCP connection: 192.168.255.4.18443 - 192.168.255.2.646
        State: Oper; Msgs sent/rcvd: 181/181; Downstream
        Up time: 02:24:22
        LDP discovery sources:
          FastEthernet0/0, Src IP addr: 192.168.1.17
        Addresses bound to peer LDP Ident:
          192.168.1.2     192.168.255.4   192.168.1.17    192.168.1.10
          192.168.1.21
    Peer LDP Ident: 192.168.255.3:0; Local LDP Ident 192.168.255.2:0
        TCP connection: 192.168.255.3.20310 - 192.168.255.2.646
        State: Oper; Msgs sent/rcvd: 180/182; Downstream
        Up time: 02:24:21
        LDP discovery sources:
          FastEthernet1/0, Src IP addr: 192.168.1.13
        Addresses bound to peer LDP Ident:
          192.168.1.13    192.168.255.3   192.168.1.6     192.168.1.9
          192.168.1.25
```

```
PE-3#show mpls label range
Downstream Generic label region: Min/Max label: 300/399

PE-3#
PE-3#show mpls ldp neighbor
    Peer LDP Ident: 192.168.255.1:0; Local LDP Ident 192.168.255.3:0
        TCP connection: 192.168.255.1.646 - 192.168.255.3.43381
        State: Oper; Msgs sent/rcvd: 182/180; Downstream
        Up time: 02:24:45
        LDP discovery sources:
          FastEthernet1/0, Src IP addr: 192.168.1.5
        Addresses bound to peer LDP Ident:
          192.168.1.1     192.168.255.1   192.168.1.5
    Peer LDP Ident: 192.168.255.2:0; Local LDP Ident 192.168.255.3:0
        TCP connection: 192.168.255.2.646 - 192.168.255.3.20310
        State: Oper; Msgs sent/rcvd: 182/180; Downstream
        Up time: 02:24:39
        LDP discovery sources:
          FastEthernet0/0, Src IP addr: 192.168.1.14
        Addresses bound to peer LDP Ident:
          192.168.1.18    192.168.255.2   192.168.1.14
    Peer LDP Ident: 192.168.255.4:0; Local LDP Ident 192.168.255.3:0
        TCP connection: 192.168.255.4.46667 - 192.168.255.3.646
        State: Oper; Msgs sent/rcvd: 180/180; Downstream
        Up time: 02:24:34
        LDP discovery sources:
          FastEthernet3/0, Src IP addr: 192.168.1.10
        Addresses bound to peer LDP Ident:
          192.168.1.2     192.168.255.4   192.168.1.17    192.168.1.10
          192.168.1.21
```

```
PE-4#show mpls label range
Downstream Generic label region: Min/Max label: 400/499

PE-4#
PE-4#show mpls ldp neighbor
    Peer LDP Ident: 192.168.255.1:0; Local LDP Ident 192.168.255.4:0
        TCP connection: 192.168.255.1.646 - 192.168.255.4.22378
        State: Oper; Msgs sent/rcvd: 181/180; Downstream
        Up time: 02:25:03
        LDP discovery sources:
          FastEthernet0/0, Src IP addr: 192.168.1.1
        Addresses bound to peer LDP Ident:
          192.168.1.1     192.168.255.1   192.168.1.5
    Peer LDP Ident: 192.168.255.2:0; Local LDP Ident 192.168.255.4:0
        TCP connection: 192.168.255.2.646 - 192.168.255.4.18443
        State: Oper; Msgs sent/rcvd: 182/182; Downstream
        Up time: 02:24:59
        LDP discovery sources:
          FastEthernet1/0, Src IP addr: 192.168.1.18
        Addresses bound to peer LDP Ident:
          192.168.1.18    192.168.255.2   192.168.1.14
    Peer LDP Ident: 192.168.255.3:0; Local LDP Ident 192.168.255.4:0
        TCP connection: 192.168.255.3.646 - 192.168.255.4.46667
        State: Oper; Msgs sent/rcvd: 180/180; Downstream
        Up time: 02:24:53
        LDP discovery sources:
          FastEthernet2/0, Src IP addr: 192.168.1.9
        Addresses bound to peer LDP Ident:
          192.168.1.13    192.168.255.3   192.168.1.6     192.168.1.9
          192.168.1.25
```

BGP

```
PE-1#show ip bgp vpnv4 all summary
BGP router identifier 192.168.255.1, local AS number 65000
BGP table version is 6, main routing table version 6
3 network entries using 456 bytes of memory
5 path entries using 380 bytes of memory
2/2 BGP path/bestpath attribute entries using 288 bytes of memory
4 BGP rrinfo entries using 96 bytes of memory
1 BGP extended community entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 1244 total bytes of memory
BGP activity 3/0 prefixes, 5/0 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.255.11  4        65000     175     174        6    0    0 02:34:35        2
192.168.255.22  4        65000     177     173        6    0    0 02:34:40        2
PE-1#
PE-1#show ip bgp vpnv4 vrf eNodeB-1-3
BGP table version is 6, local router ID is 192.168.255.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 10:10 (default for vrf eNodeB-1-3)
 * i 172.16.1.0/24    192.168.255.2            0    100      0 ?
 *>i                  192.168.255.2            0    100      0 ?
 * i 172.16.2.0/24    192.168.255.3            0    100      0 ?
 *>i                  192.168.255.3            0    100      0 ?
 *>  172.16.3.0/24    0.0.0.0                  0         32768 ?
```

```
PE-2#show ip bgp vpnv4 all summary
BGP router identifier 192.168.255.2, local AS number 65000
BGP table version is 6, main routing table version 6
3 network entries using 468 bytes of memory
5 path entries using 400 bytes of memory
2/2 BGP path/bestpath attribute entries using 288 bytes of memory
4 BGP rrinfo entries using 96 bytes of memory
1 BGP extended community entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 1276 total bytes of memory
BGP activity 3/0 prefixes, 5/0 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.255.11  4        65000     176     175        6    0    0 02:36:53        2
192.168.255.22  4        65000     179     175        6    0    0 02:36:56        2
PE-2#
PE-2#
PE-2#show ip bgp vpnv4 vrf EPC
BGP table version is 6, local router ID is 192.168.255.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 10:10 (default for vrf EPC)
 *>  172.16.1.0/24    0.0.0.0                  0         32768 ?
 * i 172.16.2.0/24    192.168.255.3            0    100      0 ?
 *>i                  192.168.255.3            0    100      0 ?
 * i 172.16.3.0/24    192.168.255.1            0    100      0 ?
 *>i                  192.168.255.1            0    100      0 ?
```

```
PE-3#show ip bgp vpnv4 all summary
BGP router identifier 192.168.255.3, local AS number 65000
BGP table version is 6, main routing table version 6
3 network entries using 468 bytes of memory
5 path entries using 400 bytes of memory
2/2 BGP path/bestpath attribute entries using 288 bytes of memory
4 BGP rrinfo entries using 96 bytes of memory
1 BGP extended community entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 1276 total bytes of memory
BGP activity 3/0 prefixes, 5/0 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.255.11  4        65000     178     175        6    0    0 02:37:42        2
192.168.255.22  4        65000     179     176        6    0    0 02:37:51        2
PE-3#
PE-3#
PE-3#show ip bgp vpnv4 vrf eNodeB-4
BGP table version is 6, local router ID is 192.168.255.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 10:10 (default for vrf eNodeB-4)
 * i 172.16.1.0/24    192.168.255.2            0    100      0 ?
 *>i                  192.168.255.2            0    100      0 ?
 *>  172.16.2.0/24    0.0.0.0                  0         32768 ?
 * i 172.16.3.0/24    192.168.255.1            0    100      0 ?
 *>i                  192.168.255.1            0    100      0 ?
```

```
PE-4#show ip bgp vpnv4 all summary
BGP router identifier 192.168.255.4, local AS number 65000
BGP table version is 6, main routing table version 6
3 network entries using 468 bytes of memory
7 path entries using 560 bytes of memory
2/2 BGP path/bestpath attribute entries using 288 bytes of memory
6 BGP rrinfo entries using 144 bytes of memory
1 BGP extended community entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 1484 total bytes of memory
BGP activity 3/0 prefixes, 7/0 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.255.11  4        65000     180     177        6    0    0 02:38:25        3
192.168.255.22  4        65000     180     178        6    0    0 02:38:33        3
PE-4#
PE-4#
PE-4#show ip bgp vpnv4 vrf EPC-Backup
BGP table version is 6, local router ID is 192.168.255.4
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 10:10 (default for vrf EPC-Backup)
 * i 172.16.1.0/24    192.168.255.2            0    100      0 ?
 * i                  192.168.255.2            0    100      0 ?
 *>                   0.0.0.0             100000         32768 ?
 * i 172.16.2.0/24    192.168.255.3            0    100      0 ?
 *>i                  192.168.255.3            0    100      0 ?
 * i 172.16.3.0/24    192.168.255.1            0    100      0 ?
 *>i                  192.168.255.1            0    100      0 ?
```

End-to-End Routes:

```
eNodeB-1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 172.16.3.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 172.16.3.1
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.3.0/24 is directly connected, Vlan10
L        172.16.3.2/32 is directly connected, Vlan10
eNodeB-1#
```

```
eNodeB-2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 172.16.3.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 172.16.3.1
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.3.0/24 is directly connected, Vlan10
L        172.16.3.3/32 is directly connected, Vlan10
eNodeB-2#
```

```
eNodeB-3#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 172.16.3.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 172.16.3.1
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.3.0/24 is directly connected, Vlan10
L        172.16.3.4/32 is directly connected, Vlan10
eNodeB-3#
```

```
eNodeB-4#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 172.16.2.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 172.16.2.1
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.2.0/24 is directly connected, Vlan10
L        172.16.2.2/32 is directly connected, Vlan10
eNodeB-4#
```

```
EPC#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 172.16.1.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 172.16.1.1
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.1.0/24 is directly connected, Vlan10
L        172.16.1.2/32 is directly connected, Vlan10
EPC#
```

```
EPC_Backup#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 172.16.1.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 172.16.1.1
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.1.0/24 is directly connected, Vlan10
L        172.16.1.2/32 is directly connected, Vlan10
EPC_Backup#
```

```
RR-1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      192.168.1.0/24 is variably subnetted, 8 subnets, 2 masks
O        192.168.1.0/30 [110/2] via 192.168.1.21, 22:04:23, FastEthernet0/0
O        192.168.1.4/30 [110/12] via 192.168.1.21, 22:04:23, FastEthernet0/0
O        192.168.1.8/30 [110/2] via 192.168.1.21, 22:04:23, FastEthernet0/0
O        192.168.1.12/30 [110/3] via 192.168.1.21, 22:04:23, FastEthernet0/0
O        192.168.1.16/30 [110/2] via 192.168.1.21, 22:04:23, FastEthernet0/0
C        192.168.1.20/30 is directly connected, FastEthernet0/0
L        192.168.1.22/32 is directly connected, FastEthernet0/0
O        192.168.1.24/30 [110/3] via 192.168.1.21, 22:04:23, FastEthernet0/0
      192.168.255.0/32 is subnetted, 6 subnets
O        192.168.255.1 [110/3] via 192.168.1.21, 22:04:23, FastEthernet0/0
O        192.168.255.2 [110/3] via 192.168.1.21, 22:04:23, FastEthernet0/0
O        192.168.255.3 [110/3] via 192.168.1.21, 22:04:23, FastEthernet0/0
O        192.168.255.4 [110/2] via 192.168.1.21, 22:04:23, FastEthernet0/0
C        192.168.255.11 is directly connected, Loopback0
O        192.168.255.22 [110/4] via 192.168.1.21, 22:04:23, FastEthernet0/0
RR-1#
```

```
RR-2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      192.168.1.0/24 is variably subnetted, 8 subnets, 2 masks
O        192.168.1.0/30 [110/3] via 192.168.1.25, 22:02:39, FastEthernet0/0
O        192.168.1.4/30 [110/11] via 192.168.1.25, 22:02:49, FastEthernet0/0
O        192.168.1.8/30 [110/2] via 192.168.1.25, 22:02:49, FastEthernet0/0
O        192.168.1.12/30 [110/2] via 192.168.1.25, 22:02:49, FastEthernet0/0
O        192.168.1.16/30 [110/3] via 192.168.1.25, 22:02:39, FastEthernet0/0
O        192.168.1.20/30 [110/3] via 192.168.1.25, 22:02:39, FastEthernet0/0
C        192.168.1.24/30 is directly connected, FastEthernet0/0
L        192.168.1.26/32 is directly connected, FastEthernet0/0
      192.168.255.0/32 is subnetted, 6 subnets
O        192.168.255.1 [110/4] via 192.168.1.25, 22:02:39, FastEthernet0/0
O        192.168.255.2 [110/3] via 192.168.1.25, 22:02:39, FastEthernet0/0
O        192.168.255.3 [110/2] via 192.168.1.25, 22:02:49, FastEthernet0/0
O        192.168.255.4 [110/3] via 192.168.1.25, 22:02:39, FastEthernet0/0
O        192.168.255.11 [110/4] via 192.168.1.25, 22:02:39, FastEthernet0/0
C        192.168.255.22 is directly connected, Loopback0
RR-2#
```

Aggregation Network Route/OSPF/MPLS/VRFS

```
PE-1#show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      192.168.1.0/24 is variably subnetted, 9 subnets, 2 masks
O        192.168.1.8/30 [110/2] via 192.168.1.2, 22:09:49, Ethernet0/1
O        192.168.1.12/30 [110/3] via 192.168.1.2, 22:09:39, Ethernet0/1
O        192.168.1.16/30 [110/2] via 192.168.1.2, 22:09:49, Ethernet0/1
O        192.168.1.20/30 [110/2] via 192.168.1.2, 22:09:49, Ethernet0/1
O        192.168.1.24/30 [110/3] via 192.168.1.2, 22:09:39, Ethernet0/1
      192.168.255.0/32 is subnetted, 6 subnets
O        192.168.255.2 [110/3] via 192.168.1.2, 22:09:39, Ethernet0/1
O        192.168.255.3 [110/3] via 192.168.1.2, 22:09:39, Ethernet0/1
O        192.168.255.4 [110/2] via 192.168.1.2, 22:09:49, Ethernet0/1
O        192.168.255.11 [110/3] via 192.168.1.2, 22:09:39, Ethernet0/1
O        192.168.255.22 [110/4] via 192.168.1.2, 22:09:39, Ethernet0/1
PE-1#show ip route vrf eNodeB-1-3

Routing Table: eNodeB-1-3
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
B        172.16.1.0/24 [200/0] via 192.168.255.2, 22:08:39
B        172.16.2.0/24 [200/0] via 192.168.255.3, 22:08:39
C        172.16.3.0/24 is directly connected, Ethernet0/2.10
L        172.16.3.1/32 is directly connected, Ethernet0/2.10
PE-1#
```

```
PE-1#show mpls forwarding-table
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
100        400        192.168.255.22/32   \
                                       0             Et0/1      192.168.1.2
101        Pop Label  192.168.255.4/32 0             Et0/1      192.168.1.2
102        401        192.168.255.3/32 0             Et0/1      192.168.1.2
103        403        192.168.1.24/30  0             Et0/1      192.168.1.2
104        Pop Label  192.168.1.20/30  0             Et0/1      192.168.1.2
105        Pop Label  192.168.1.16/30  0             Et0/1      192.168.1.2
106        404        192.168.1.12/30  0             Et0/1      192.168.1.2
107        Pop Label  192.168.1.8/30   0             Et0/1      192.168.1.2
108        406        192.168.255.11/32   \
                                       0             Et0/1      192.168.1.2
109        407        192.168.255.2/32 0             Et0/1      192.168.1.2
110        No Label   172.16.3.0/24[V] 0             aggregate/eNodeB-1-3
PE-1#
PE-1#show mpls forwarding-table vrf eNodeB-1-3 172.16.1.0 detail
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
None       210        172.16.1.0/24[V] 0             Et0/1      192.168.1.2
        MAC/Encaps=14/22, MRU=1496, Label Stack{407 210}
        CA024FF40000AABBCC0040108847 00197000000D2000
        VPN route: eNodeB-1-3
        No output feature configured
PE-1#
```

```
PE-2#show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      192.168.1.0/24 is variably subnetted, 9 subnets, 2 masks
O        192.168.1.0/30 [110/2] via 192.168.1.17, 22:17:58, FastEthernet0/0
O        192.168.1.4/30 [110/11] via 192.168.1.13, 22:17:58, FastEthernet1/0
O        192.168.1.8/30 [110/2] via 192.168.1.17, 22:17:58, FastEthernet0/0
                        [110/2] via 192.168.1.13, 22:17:58, FastEthernet1/0
O        192.168.1.20/30 [110/2] via 192.168.1.17, 22:17:58, FastEthernet0/0
O        192.168.1.24/30 [110/2] via 192.168.1.13, 22:17:58, FastEthernet1/0
      192.168.255.0/32 is subnetted, 6 subnets
O        192.168.255.1 [110/3] via 192.168.1.17, 22:17:58, FastEthernet0/0
O        192.168.255.3 [110/2] via 192.168.1.13, 22:17:58, FastEthernet1/0
O        192.168.255.4 [110/2] via 192.168.1.17, 22:17:58, FastEthernet0/0
O        192.168.255.11 [110/3] via 192.168.1.17, 22:17:58, FastEthernet0/0
O        192.168.255.22 [110/3] via 192.168.1.13, 22:17:58, FastEthernet1/0
PE-2#
```

```
PE-2#show ip route vrf EPC

Routing Table: EPC
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
C        172.16.1.0/24 is directly connected, FastEthernet2/0.10
L        172.16.1.1/32 is directly connected, FastEthernet2/0.10
B        172.16.2.0/24 [200/0] via 192.168.255.3, 22:18:45
B        172.16.3.0/24 [200/0] via 192.168.255.1, 22:18:45
PE-2#
PE-2#show mpls forwarding-table
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
200        300        192.168.255.22/32   \
                                       0             Fa1/0      192.168.1.13
201        406        192.168.255.11/32   \
                                       0             Fa0/0      192.168.1.17
202        Pop Label  192.168.255.4/32 0             Fa0/0      192.168.1.17
203        Pop Label  192.168.255.3/32 0             Fa1/0      192.168.1.13
204        402        192.168.255.1/32 0             Fa0/0      192.168.1.17
205        Pop Label  192.168.1.24/30  0             Fa1/0      192.168.1.13
206        Pop Label  192.168.1.20/30  0             Fa0/0      192.168.1.17
207        Pop Label  192.168.1.8/30   0             Fa1/0      192.168.1.13
           Pop Label  192.168.1.8/30   0             Fa0/0      192.168.1.17
208        Pop Label  192.168.1.4/30   0             Fa1/0      192.168.1.13
209        Pop Label  192.168.1.0/30   0             Fa0/0      192.168.1.17
210        No Label   172.16.1.0/24[V] 0             aggregate/EPC
PE-2#
```

```
PE-2#show mpls forwarding-table vrf EPC 172.16.3.0 detail
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
None       110        172.16.3.0/24[V] 0             Fa0/0      192.168.1.17
        MAC/Encaps=14/22, MRU=1496, Label Stack{402 110}
        CA024FF4001CCA0151CF00008847 001920000006E000
        VPN route: EPC
        No output feature configured
PE-2#
```

```
PE-2#show mpls forwarding-table vrf EPC 172.16.2.0 detail
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
None       308        172.16.2.0/24[V] 0             Fa1/0      192.168.1.13
        MAC/Encaps=14/18, MRU=1500, Label Stack{308}
        CA034DF70000CA0151CF001C8847 00134000
        VPN route: EPC
        No output feature configured
```

```
PE-3#show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      192.168.1.0/24 is variably subnetted, 11 subnets, 2 masks
O        192.168.1.0/30 [110/2] via 192.168.1.10, 22:22:43, FastEthernet3/0
O        192.168.1.16/30 [110/2] via 192.168.1.14, 22:22:43, FastEthernet0/0
                         [110/2] via 192.168.1.10, 22:22:43, FastEthernet3/0
O        192.168.1.20/30 [110/2] via 192.168.1.10, 22:22:43, FastEthernet3/0
      192.168.255.0/32 is subnetted, 6 subnets
O        192.168.255.1 [110/3] via 192.168.1.10, 22:22:43, FastEthernet3/0
O        192.168.255.2 [110/2] via 192.168.1.14, 22:22:43, FastEthernet0/0
O        192.168.255.4 [110/2] via 192.168.1.10, 22:22:43, FastEthernet3/0
O        192.168.255.11 [110/3] via 192.168.1.10, 22:22:43, FastEthernet3/0
O        192.168.255.22 [110/2] via 192.168.1.26, 22:22:53, FastEthernet4/0
PE-3#
PE-3#show ip route vrf eNodeB-4

Routing Table: eNodeB-4
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
B        172.16.1.0/24 [200/0] via 192.168.255.2, 22:21:47
C        172.16.2.0/24 is directly connected, FastEthernet2/0.10
L        172.16.2.1/32 is directly connected, FastEthernet2/0.10
B        172.16.3.0/24 [200/0] via 192.168.255.1, 22:21:46
PE-3#
```

```
PE-3#show mpls forwarding-table
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
300        No Label   192.168.255.22/32   \
                                       563711        Fa4/0      192.168.1.26
301        402        192.168.255.1/32 0             Fa3/0      192.168.1.10
302        Pop Label  192.168.1.0/30   0             Fa3/0      192.168.1.10
303        406        192.168.255.11/32   \
                                       0             Fa3/0      192.168.1.10
304        Pop Label  192.168.255.4/32 0             Fa3/0      192.168.1.10
305        Pop Label  192.168.255.2/32 0             Fa0/0      192.168.1.14
306        Pop Label  192.168.1.20/30  0             Fa3/0      192.168.1.10
307        Pop Label  192.168.1.16/30  0             Fa3/0      192.168.1.10
           Pop Label  192.168.1.16/30  0             Fa0/0      192.168.1.14
308        No Label   172.16.2.0/24[V] 0             aggregate/eNodeB-4
PE-3#
PE-3#show mpls forwarding-table vrf eNodeB-4 172.16.1.0 detail
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
None       210        172.16.1.0/24[V] 0             Fa0/0      192.168.1.14
        MAC/Encaps=14/18, MRU=1500, Label Stack{210}
        CA0151CF001CCA034DF700008847 000D2000
        VPN route: eNodeB-4
        No output feature configured
```

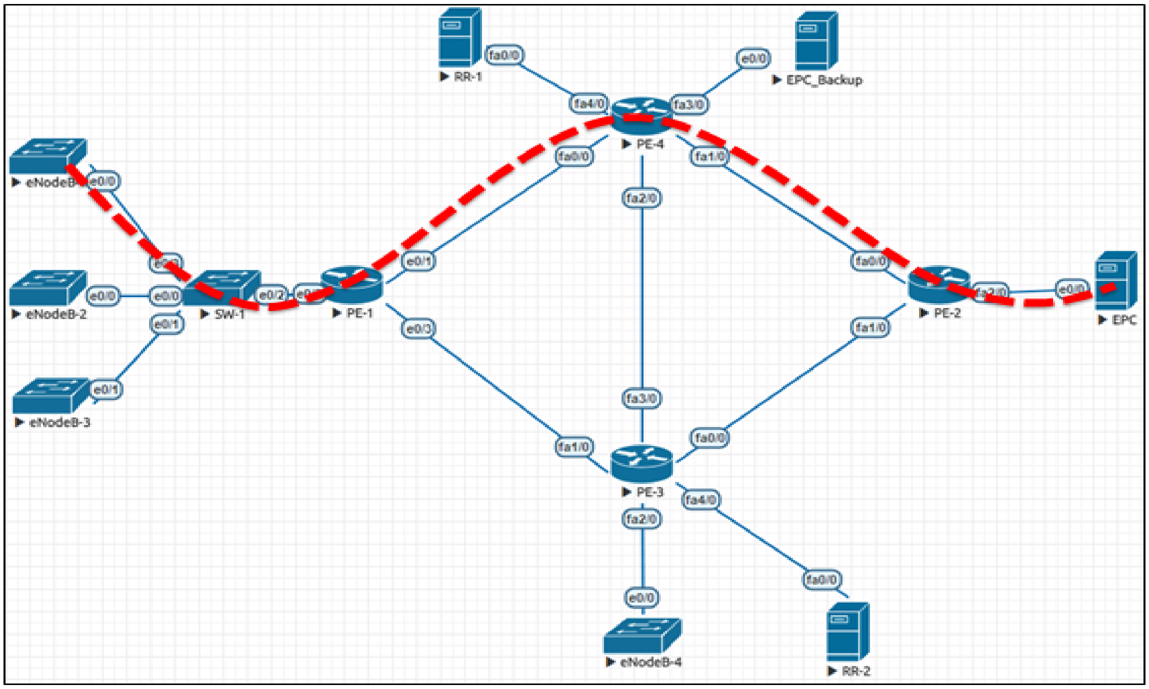
```
PE-4#show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      192.168.1.0/24 is variably subnetted, 11 subnets, 2 masks
O        192.168.1.4/30 [110/11] via 192.168.1.9, 22:25:52, FastEthernet2/0
                        [110/11] via 192.168.1.1, 22:26:02, FastEthernet0/0
O        192.168.1.12/30 [110/2] via 192.168.1.18, 22:25:52, FastEthernet1/0
                         [110/2] via 192.168.1.9, 22:25:52, FastEthernet2/0
O        192.168.1.24/30 [110/2] via 192.168.1.9, 22:25:52, FastEthernet2/0
      192.168.255.0/32 is subnetted, 6 subnets
O        192.168.255.1 [110/2] via 192.168.1.1, 22:26:02, FastEthernet0/0
O        192.168.255.2 [110/2] via 192.168.1.18, 22:25:52, FastEthernet1/0
O        192.168.255.3 [110/2] via 192.168.1.9, 22:25:52, FastEthernet2/0
O        192.168.255.11 [110/2] via 192.168.1.22, 22:25:52, FastEthernet4/0
O        192.168.255.22 [110/3] via 192.168.1.9, 22:25:52, FastEthernet2/0
```

```
PE-4#show ip route vrf EPC-Backup

Routing Table: EPC-Backup
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
C        172.16.1.0/24 is directly connected, FastEthernet3/0.10
L        172.16.1.1/32 is directly connected, FastEthernet3/0.10
B        172.16.2.0/24 [200/0] via 192.168.255.3, 22:24:53
B        172.16.3.0/24 [200/0] via 192.168.255.1, 22:24:53
PE-4#
```

```
PE-4#show mpls forwarding-table vrf EPC-Backup 172.16.2.0 detail
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
None       308        172.16.2.0/24[V] 0             Fa2/0      192.168.1.9
        MAC/Encaps=14/18, MRU=1500, Label Stack{308}
        CA034DF70054CA024FF400388847 00134000
        VPN route: EPC-Backup
        No output feature configured
PE-4#show mpls forwarding-table vrf EPC-Backup 172.16.3.0 detail
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
None       110        172.16.3.0/24[V] 0             Fa0/0      192.168.1.1
        MAC/Encaps=14/18, MRU=1500, Label Stack{110}
        AABBCC004010CA024FF400008847 0006E000
        VPN route: EPC-Backup
        No output feature configured
PE-4#
```

Traffic Flow Diagrams, Ping and Trace Route Results:

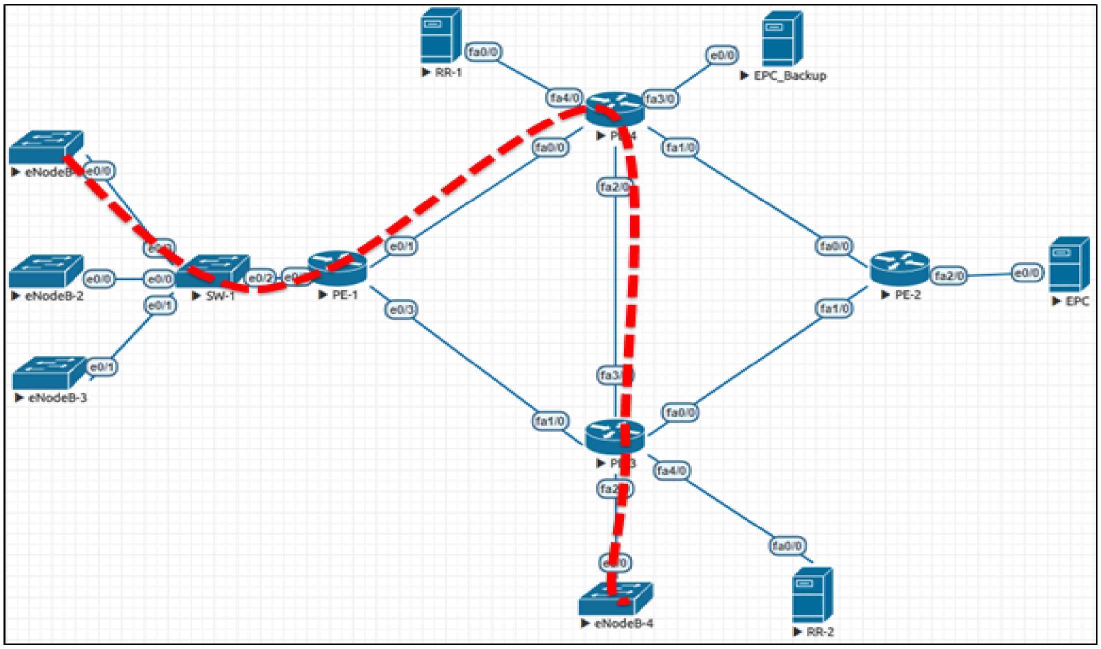
eNodeB-1 to EPC and vice-versa:




```
eNodeB-1#ping 172.16.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 30/30/32 ms
eNodeB-1#trace
eNodeB-1#traceroute 172.16.1.2
Type escape sequence to abort.
Tracing the route to 172.16.1.2
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.3.1 1 msec 0 msec 1 msec
  2 192.168.1.2 [MPLS: Labels 407/210 Exp 0] 18 msec 21 msec 20 msec
  3 172.16.1.1 20 msec 20 msec 20 msec
  4 172.16.1.2 31 msec *  26 msec
eNodeB-1#
```

```
EPC#ping 172.16.3.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.3.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 27/29/30 ms
EPC#
EPC#traceroute 172.16.3.2
Type escape sequence to abort.
Tracing the route to 172.16.3.2
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.1.1 8 msec 10 msec 10 msec
  2 192.168.1.17 [MPLS: Labels 402/110 Exp 0] 31 msec 30 msec 30 msec
  3 172.16.3.1 30 msec 31 msec 30 msec
  4 172.16.3.2 30 msec *  27 msec
EPC#
```

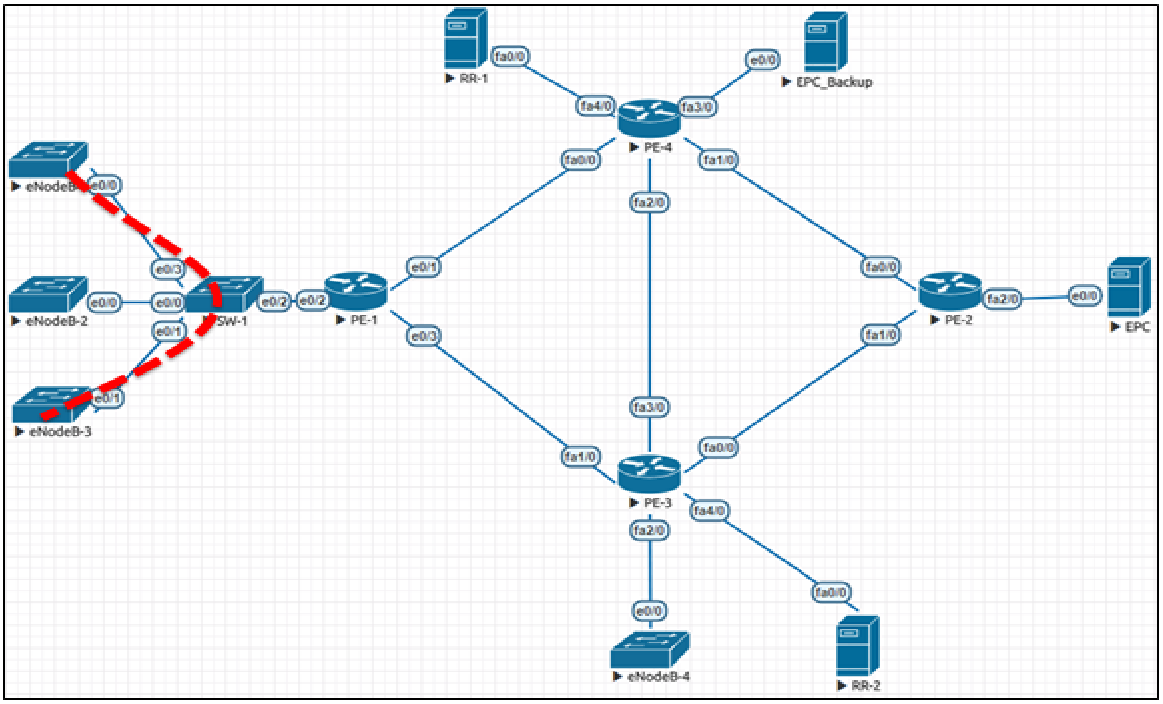
eNodeB-1 to eNodeB-4 and vice-versa (X2 interface communication without going via EPC):




```
eNodeB-1#ping 172.16.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 22/28/31 ms
eNodeB-1#traceroute 172.16.2.2
Type escape sequence to abort.
Tracing the route to 172.16.2.2
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.3.1 0 msec 0 msec 1 msec
  2 192.168.1.2 [MPLS: Labels 401/308 Exp 0] 25 msec 30 msec 30 msec
  3 172.16.2.1 40 msec 30 msec 31 msec
  4 172.16.2.2 40 msec *  42 msec
eNodeB-1#
```

```
eNodeB-4#ping 172.16.3.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.3.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/39/41 ms
eNodeB-4#
eNodeB-4#traceroute 172.16.3.2
Type escape sequence to abort.
Tracing the route to 172.16.3.2
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.2.1 4 msec 10 msec 10 msec
  2 192.168.1.10 [MPLS: Labels 402/110 Exp 0] 30 msec 30 msec 31 msec
  3 172.16.3.1 30 msec 30 msec 30 msec
  4 172.16.3.2 38 msec *  22 msec
eNodeB-4#
```

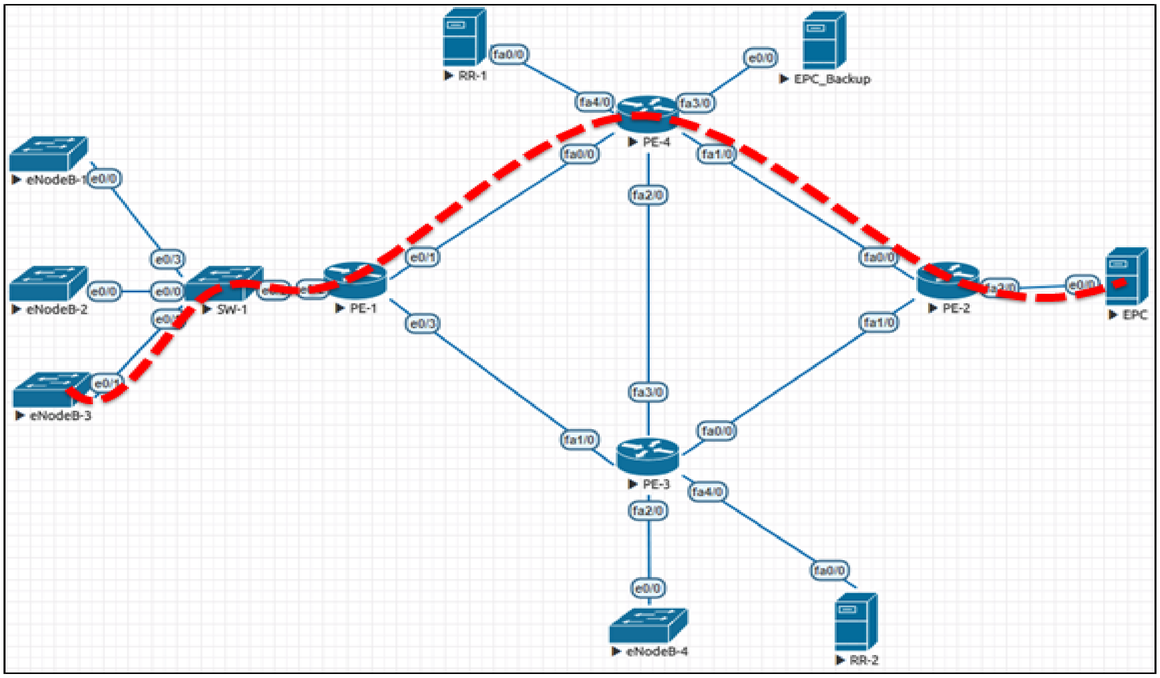
eNodeB-1 to eNodeB-3 and vice-versa (X2 interface communication without going via EPC):




```
eNodeB-1#ping 172.16.3.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.3.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
eNodeB-1#traceroute 172.16.3.4
Type escape sequence to abort.
Tracing the route to 172.16.3.4
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.3.4 1 msec *  0 msec
eNodeB-1#
```

```
eNodeB-3#ping 172.16.3.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.3.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/4/5 ms
eNodeB-3#
eNodeB-3#trac
eNodeB-3#traceroute 172.16.3.2
Type escape sequence to abort.
Tracing the route to 172.16.3.2
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.3.2 5 msec *  1 msec
eNodeB-3#
```

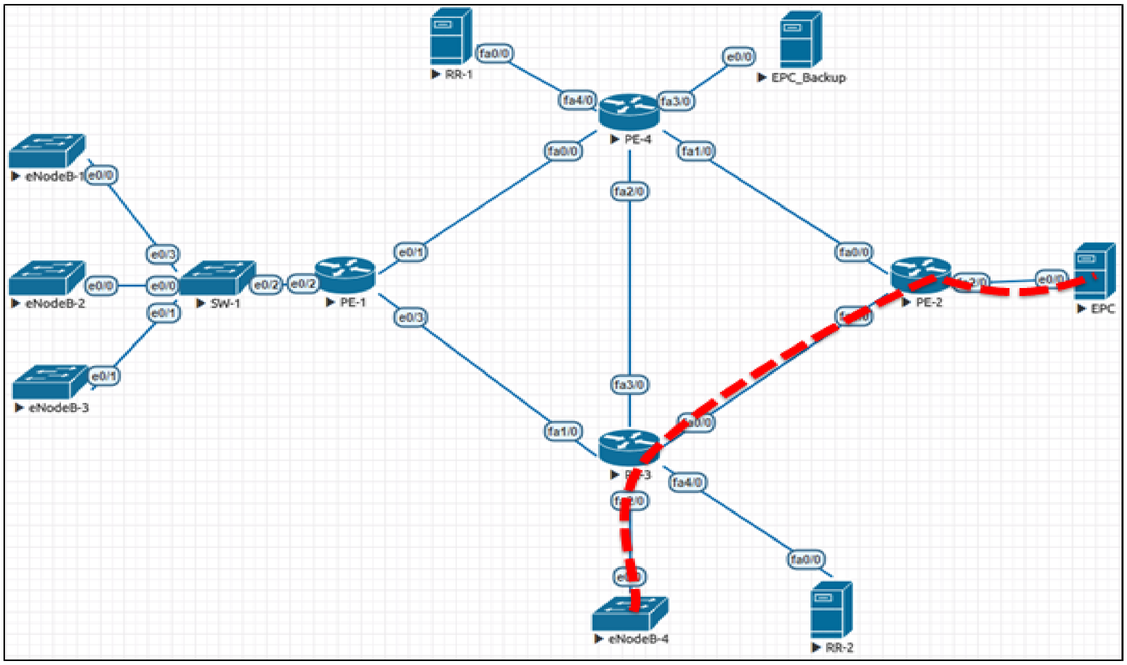
eNodeB-3 to EPC and vice-versa:




```
eNodeB-3#ping 172.16.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 22/28/31 ms
eNodeB-3#
eNodeB-3#traceroute 172.16.1.2
Type escape sequence to abort.
Tracing the route to 172.16.1.2
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.3.1 1 msec 1 msec 0 msec
  2 192.168.1.2 [MPLS: Labels 407/210 Exp 0] 16 msec 20 msec 20 msec
  3 172.16.1.1 20 msec 21 msec 20 msec
  4 172.16.1.2 30 msec *  26 msec
eNodeB-3#
```

```
EPC#ping 172.16.3.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.3.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 22/28/31 ms
EPC#
EPC#traceroute 172.16.3.4
Type escape sequence to abort.
Tracing the route to 172.16.3.4
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.1.1 8 msec 10 msec 10 msec
  2 192.168.1.17 [MPLS: Labels 402/110 Exp 0] 30 msec 31 msec 30 msec
  3 172.16.3.1 30 msec 30 msec 31 msec
  4 172.16.3.4 30 msec *  25 msec
EPC#
```

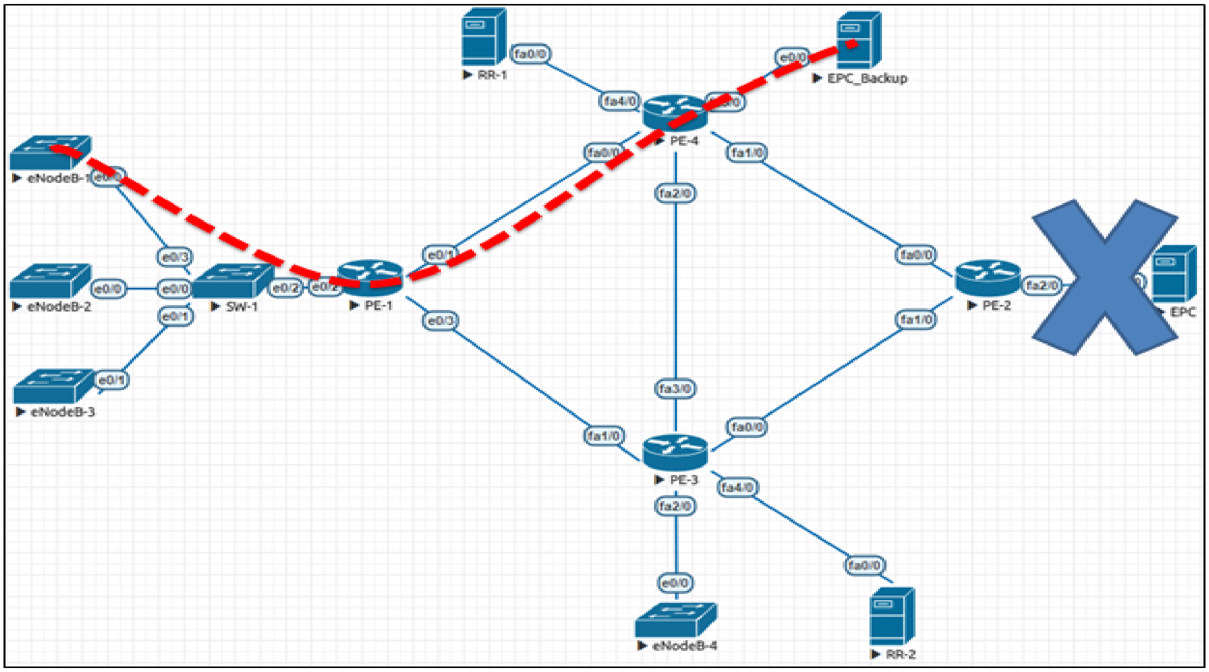
eNodeB-4 to EPC and vice-versa:




```
eNodeB-4#ping 172.16.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 21/28/31 ms
eNodeB-4#
eNodeB-4#traceroute 172.16.1.2
Type escape sequence to abort.
Tracing the route to 172.16.1.2
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.2.1 3 msec 10 msec 10 msec
  2 172.16.1.1 20 msec 20 msec 21 msec
  3 172.16.1.2 31 msec *  26 msec
eNodeB-4#
```

```
EPC#ping 172.16.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 22/28/31 ms
EPC#
EPC#traceroute 172.16.2.2
Type escape sequence to abort.
Tracing the route to 172.16.2.2
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.1.1 6 msec 10 msec 10 msec
  2 172.16.2.1 20 msec 20 msec 20 msec
  3 172.16.2.2 31 msec *  27 msec
EPC#
```

(EPC Failure Mode) eNodeB-1 to EPC_Backup and vice-versa:

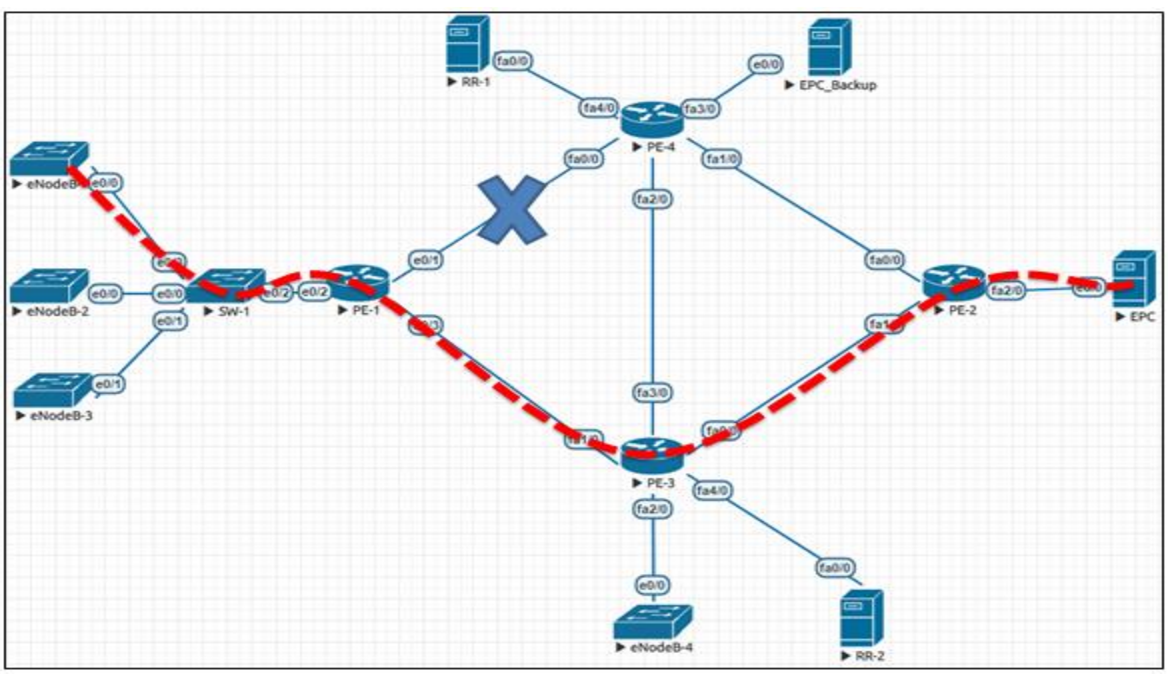



```
eNodeB-1#ping 172.16.1.2 re
eNodeB-1#ping 172.16.1.2 repeat 10000000
Type escape sequence to abort.
Sending 10000000, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.
Success rate is 99 percent (1014/1016), round-trip min/avg/max = 12/23/50 ms
eNodeB-1#
```

```
eNodeB-1#ping 172.16.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 19/19/20 ms
eNodeB-1#traceroute 172.16.1.2
Type escape sequence to abort.
Tracing the route to 172.16.1.2
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.3.1 1 msec 0 msec 2 msec
  2 172.16.1.1 15 msec 10 msec 10 msec
  3 172.16.1.2 20 msec *  17 msec
eNodeB-1#
```

```
EPC_Backup#ping 172.16.3.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.3.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 14/19/21 ms
EPC_Backup#
EPC_Backup#tra
EPC_Backup#traceroute 172.16.3.2
Type escape sequence to abort.
Tracing the route to 172.16.3.2
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.1.1 8 msec 10 msec 10 msec
  2 172.16.3.1 20 msec 20 msec 20 msec
  3 172.16.3.2 20 msec *  15 msec
EPC_Backup#
```

(Link {between PE-1 and PE-4} Failure Mode) eNodeB-1 to EPC and vice-versa:



```
eNodeB-1#ping 172.16.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 30/34/40 ms
eNodeB-1#
eNodeB-1#traceroute 172.16.1.2
Type escape sequence to abort.
Tracing the route to 172.16.1.2
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.3.1 1 msec 0 msec 1 msec
  2 192.168.1.6 [MPLS: Labels 305/211 Exp 0] 20 msec 20 msec 20 msec
  3 172.16.1.1 30 msec 20 msec 20 msec
  4 172.16.1.2 31 msec *  32 msec
eNodeB-1#
```

```
EPC#ping 172.16.3.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.3.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 27/29/31 ms
EPC#
EPC#traceroute 172.16.3.2
Type escape sequence to abort.
Tracing the route to 172.16.3.2
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.1.1 4 msec 10 msec 10 msec
  2 192.168.1.13 [MPLS: Labels 301/110 Exp 0] 40 msec 31 msec 30 msec
  3 172.16.3.1 30 msec 30 msec 31 msec
  4 172.16.3.2 30 msec *  24 msec
EPC#
```

12.0 Private LTE

This term refers to having wireless networks within an enterprise, business, service or production facilities. This technology allows any private organization to deploy, maintain and benefit from LTE radio technology and architecture. Private LTE is a method of having a high-performance wireless network within an organization floor without the need of having any licensed operator or their services. Here, a private LTE network is local, and all its equipment's are managed by the local enterprise/business.

Currently and even more in the future of the industrial environments, a greater extent of tasks are being automated. Facilities such as a production plant, manufacturing plant, airports, etc. are leaning towards using more and more 'smart' technologies and equipment. With more devices communicating to the local network, private LTE is the 'go-to' technology because of benefits such as locally controlled, improved productivity, control, visibility, optimized and readily deployment options. From security cameras, sensors, facility employees, robots to whatever 'smart' device it may be; everything can now be connected to a single local network where the LTE technology has the high capacity to serve with great reliability, lower latency, seamless mobility, better coverage and higher security.

Since private LTE is on a local basis and will only be used to cover an area owned or used by the business entity solely for the purpose of business and functionality needs, it can use both shared licensed or unlicensed spectrum. This network is similar to LTE mobile technology but in a much smaller scale but provides a solution that is much needed now and in the future. The following diagram is an example of how Private LTE architecture looks like:-

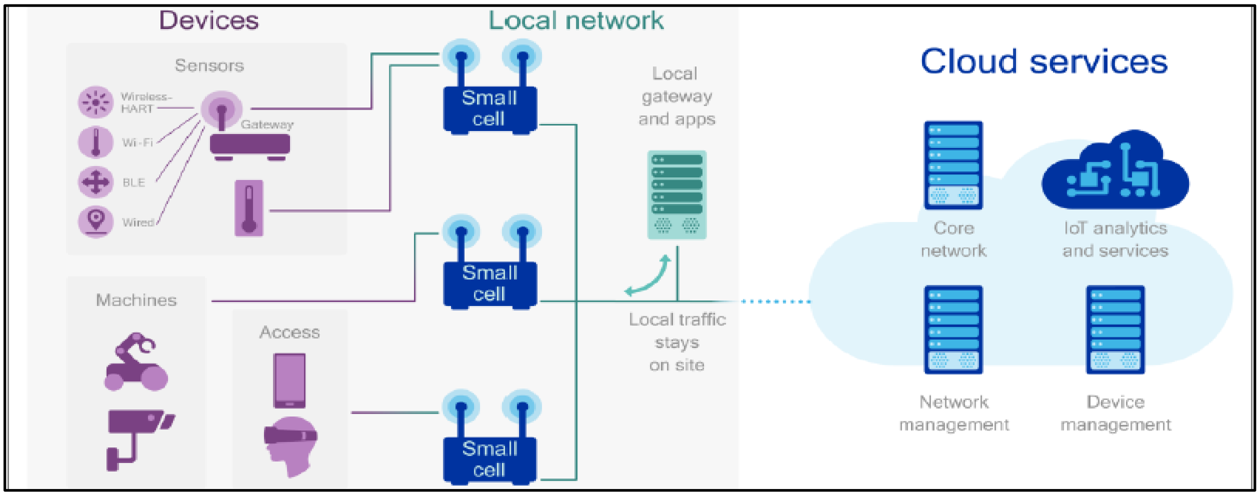


Figure 50: Local-Area Private LTE network architecture [31]

In Private LTE, where the wireless network is within a certain range/area/premises often may or may not have communications to other sites and/or offices. Though this network can be completely independent with local servers, database, etc.; it is possible that these equipment may be located offsite. Also, often when having multiple sites, each running their own private networks for operations, might need to communicate with each other. In such circumstances, where sites/organizations need to communicate via metro area networks provided by Foreign Service providers, Ethernet Private Line is a very viable and optimized solution. As discusses in Section 8 and 8.1, EPL will provide a point-to-point EVC between dedicated UNI's. This network service provides a higher degree of transparency, secure, high BW, low cost, low frame delay, variation and loss ratio. For sites using Private LTE, EPL will allow the customers to bypass the public internet, transmit traffic over a private connection with very high degree of SLA and QoS. In an example, the following customer sites are running Private LTE networks and are linked with EPL service over the MEN:

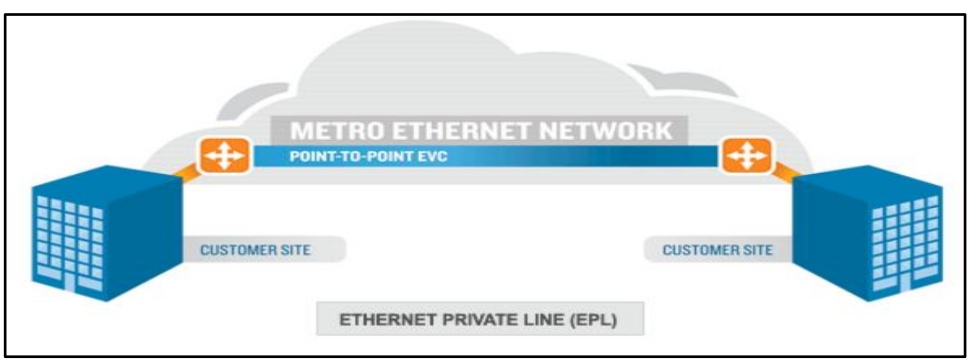


Figure 51: EPL supporting Private LTE sites [32]

13.0 Reference:

[1] Tuomas Taipale, '*Feasibility of wireless mesh for LTE-Advanced small cell access backhaul*,'M.S. thesis, Alto University, 2012.

[2] Fujitsu, *Understanding Mobile Wireless Backhaul*. [online]. Available: http://www.fujitsu.com/downloads/TEL/fnc/whitepapers/Fujitsu_Wireless_Backhaul.pdf

[3] E. Metsälä and J. Salmelin, *Mobile backhaul*, 1st ed. Chichester, West Sussex: John Wiley & Sons, Inc., 2012.

[4]A. Prakash, A. Prakash and V. profile, "UMTS Network Architecture", *Wcdmaforbeginners.blogspot.ca*, 2017. [Online]. Available: http://wcdmaforbeginners.blogspot.ca/2013/01/umts-network-architecture.html. [Accessed: 05- Jun- 2017]..

[5]"LTE E-UTRAN", *LongTermEvolution*, 2017. [Online]. Available: https://ltemobilezone.wordpress.com/2012/03/26/lte-e-utran/. [Accessed: 05- Jun- 2017]..

[6]"4G Impacts to Mobile Backhaul", 2009. [Online]. Available: http://www.fujitsu.com/downloads/TEL/fnc/whitepapers/4Gimpacts.pdf. [Accessed: 05- Jun- 2017].

[7] [2]"Carrier Ethernet Services | CE-Services", *Mef.net*, 2017. [Online]. Available: https://www.mef.net/carrier-ethernet/carrier-ethernet-services. [Accessed: 05- Jun- 2017].

[8] *200 Gb/s and 400 Gb/s Ethernet Task Force*, IEEE Standard P802.3bs, 2016

[9] "The 2015 Ethernet Roadmap | Ethernet Alliance", *Ethernetalliance.org*, 2017. [Online]. Available: http://www.ethernetalliance.org/the-2015-ethernet-roadmap-2/. [Accessed: 05- Jun- 2017]..

[10] "All you need to know on CE 2.0 E-Access - Telco Systems Blog", *Telco Systems Blog*, 2013. [Online]. Available: http://www.telco.com/blog/mef-ethernet-access-e-access-service-type/. [Accessed: 05- Jun- 2017].

[11] *Ethernet Access Services Definition*, MEF 33, 2012

[12] S. Sesia, I. Toufik and M. Baker, *LTE - the UMTS long term evolution*, 1st ed. Chichester: Wiley, 2011.

[13] *CE 2.0 Ethernet Access Service*, MEF Informational and Technical Paper, 2013

[14] "*White Papers - Maximizing LTE Benefits Using Carrier Ethernet Backhaul - Ciena*", *Ciena.com*, 2017. [Online]. Available: http://www.ciena.com/insights/white-papers/LTE-Benefits-Using-Carrier-Ethernet_prx.html. [Accessed: 05- Jun- 2017].

[15] "*LTE Transport Solution Workshop*", Huawei Technologies Co. Ltd., 2010

[16] "*Open Shortest Path First*", D-Link, Available: http://www.myshared.ru/slide/923175/. [Accessed: 05- Jun- 2017].

[17] [1]"External v.s. Internal BGP". [Online]. Available: http://merlot.usc.edu/cs551-m05/lectures/tentative/07a_ibgp.pdf. [Accessed: 05- Jun- 2017].

[18] Juniper Networks, "Mobile Backhaul Reference Architecture", 2011.

[19] "Synchronization in packet-based mobile backhaul networks | Ethernet Academy Articles | Papers", *Ethernetacademy.net*, 2009. [Online]. Available: http://www.ethernetacademy.net/Ethernet-Academy-Articles/synchronization-in-packet-networks. [Accessed: 05- Jun- 2017].

[20] "Synchronization in packet-based mobile backhaul networks | Ethernet Academy Articles | Papers", *Ethernetacademy.net*, 2009. [Online]. Available: http://www.ethernetacademy.net/Ethernet-Academy-Articles/synchronization-in-packet-networks. [Accessed: 05- Jun- 2017].

[21] "A Concise Guide to Mobile Backhaul Synchronization", VeEx Inc., 2012.

[22] "Configuration Guide - MPLS - Huawei", *Support.huawei.com*, 2014. [Online]. Available: http://support.huawei.com/enterprise/docinforeader.action?contentId=DOC1000019447&partNo=10072. [Accessed: 05- Jun- 2017].

[23] "Small Cell Backhaul Requirements", 2012. [Online]. Available: https://www.ngmn.org/uploads/media/NGMN_Whitepaper_Small_Cell_Backhaul_Requirements.pdf. [Accessed: 05- Jun- 2017].

[24] "Roadmaps for independent fixed and mobile network evolution", 2013. [Online]. Available: http://www.ict-combo.eu/data/uploads/pdf-combo/combo_d2.2_wp2_13sept2013_tid_v1.0.pdf. [Accessed: 05- Jun- 2017].

[25] "Backhauling X2", *Cambridge Broadband Networks Limited* [Online]. Available: http://cbnl.com/sites/all/files/userfiles/files/Backhauling-X2_0.pdf. [Accessed: 05- Aug 2017]

[26] "LTE X2 Handover Messaging", *EventHelix.com Inc,* 2013 [Online]. Available: http://www.eventhelix.com/lte/handover/LTE-X2-Handover-Messaging.pdf [Accessed: 07- Aug 2017]

[27] "Using Carrier Ethernet to Backhaul LTE", *Infonetics Research, Inc.* [Online] Available: http://www.infonetics.com/whitepapers/2011-infonetics-research-whitepaper-using-carrier-ethernet-to-backhaul-lte.pdf [Accessed 12- Aug 2017]

[28] "LTE Topology with X2", *Ceragon* [Online] Available: http://blog.ceragon.com/blog/blogs/backhaulforum/lte-topology-x2/ [Accessed 15- Aug 2017]

[29] "New FTTH-based Technologies and Applications and Technologies", *Fiber to the Home Council Europe –A White paper by the Deployment & Operations Committee* . [30] "Solutions: G.Fast", *Nokia* [Online] Available: https://networks.nokia.com/solutions/g.fast [Accessed: 15- Aug 2017][31] "Private LTE Networks", *Qualcomm* [Online]. Available: https://www.qualcomm.com/documents/read-white-paper-heavy-reading [Accessed 19- Aug 2017]

[32] "Ethernet Services", *Integra Telecom* [Online] Available: http://www.getintegra.com/services/Ethernet_Services.php [Accessed 20- Aug 2017]

[33] "Case Study IP RAN and Mobile Backhaul QOS part 2", [Online] Available: http://what-when-how.com/qos-enabled-networks/case-study-ip-ran-and-mobile-backhaul-qos-part-2/ [Accessed 20- Aug 2017]

14.0 Appendixes-A

eNodeB-1	eNodeB-2
version 15.1 service timestamps debug datetime msec service timestamps log datetime msec no service password-encryption service compress-config ! hostname eNodeB-1 ! boot-start-marker boot-end-marker ! ! no aaa new-model clock timezone EET 2 0 ! ip cef ! no ip domain-lookup no ipv6 cef ipv6 multicast rpf use-bgp spanning-tree mode pvst spanning-tree extend system-id ! vlan internal allocation policy ascending ! interface Ethernet0/0 description eNodeB-1_to_SW-1 no shutdown switchport trunk encapsulation dot1q switchport trunk allowed vlan 10 switchport mode trunk duplex auto ! interface Ethernet0/1 no shutdown shutdown duplex auto ! interface Ethernet0/2 no shutdown shutdown duplex auto	version 15.1 service timestamps debug datetime msec service timestamps log datetime msec no service password-encryption service compress-config ! hostname eNodeB-2 ! boot-start-marker boot-end-marker ! ! no aaa new-model clock timezone EET 2 0 ! ip cef ! no ip domain-lookup no ipv6 cef ipv6 multicast rpf use-bgp spanning-tree mode pvst spanning-tree extend system-id ! vlan internal allocation policy ascending ! interface Ethernet0/0 description eNodeB-2_to_SW-1 no shutdown switchport trunk encapsulation dot1q switchport trunk allowed vlan 10 switchport mode trunk duplex auto ! interface Ethernet0/1 no shutdown shutdown duplex auto ! interface Ethernet0/2 no shutdown shutdown duplex auto

! interface Ethernet0/3 no shutdown shutdown duplex auto ! interface Vlan10 no shutdown ip address 172.16.3.2 255.255.255.0 ! no ip http server ip route 0.0.0.0 0.0.0.0 172.16.3.1 ! control-plane ! line con 0 exec-timeout 0 0 logging synchronous line aux 0 line vty 0 4 exec-timeout 0 0 logging synchronous login transport input none ! End	! interface Ethernet0/3 no shutdown shutdown duplex auto ! interface Vlan10 no shutdown ip address 172.16.3.3 255.255.255.0 ! no ip http server ip route 0.0.0.0 0.0.0.0 172.16.3.1 ! control-plane ! line con 0 exec-timeout 0 0 logging synchronous line aux 0 line vty 0 4 exec-timeout 0 0 logging synchronous login transport input none ! end
eNodeB-3 version 15.1 service timestamps debug datetime msec service timestamps log datetime msec no service password-encryption service compress-config ! hostname eNodeB-2 ! boot-start-marker boot-end-marker ! no aaa new-model clock timezone EET 2 0 ! ip cef !	eNodeB-4 version 15.1 service timestamps debug datetime msec service timestamps log datetime msec no service password-encryption service compress-config ! hostname eNodeB-4 ! boot-start-marker boot-end-marker ! no aaa new-model clock timezone EET 2 0 ! ip cef !

```
!
no ip domain-lookup
no ipv6 cef
ipv6 multicast rpf use-bgp
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface Ethernet0/0
 description eNodeB-2_to_SW-1
 no shutdown
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10
 switchport mode trunk
 duplex auto
!
interface Ethernet0/1
 no shutdown
 shutdown
 duplex auto
!
interface Ethernet0/2
 no shutdown
 shutdown
 duplex auto
!
interface Ethernet0/3
 no shutdown
 shutdown
 duplex auto
!
interface Vlan10
 no shutdown
 ip address 172.16.3.3 255.255.255.0
!
no ip http server
ip route 0.0.0.0 0.0.0.0 172.16.3.1
!
control-plane
!
line con 0
 exec-timeout 0 0
 logging synchronous
line aux 0
line vty 0 4
 exec-timeout 0 0
 logging synchronous
```

```
!
no ip domain-lookup
no ipv6 cef
ipv6 multicast rpf use-bgp
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface Ethernet0/0
 description eNodeB-4_to_PE-3
 no shutdown
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10
 switchport mode trunk
 duplex auto
!
interface Ethernet0/1
 no shutdown
 shutdown
 duplex auto
!
interface Ethernet0/2
 no shutdown
 shutdown
 duplex auto
!
interface Ethernet0/3
 no shutdown
 shutdown
 duplex auto
!
interface Vlan10
 no shutdown
 ip address 172.16.2.2 255.255.255.0
!
no ip http server
ip route 0.0.0.0 0.0.0.0 172.16.2.1
!
control-plane
!
line con 0
 exec-timeout 0 0
 logging synchronous
line aux 0
line vty 0 4
 exec-timeout 0 0
 logging synchronous
```

login transport input none ! end	login transport input none ! end
EPC version 15.1 service timestamps debug datetime msec service timestamps log datetime msec no service password-encryption service compress-config ! hostname EPC ! boot-start-marker boot-end-marker ! no aaa new-model clock timezone EET 2 0 ! ip cef ! no ip domain-lookup no ipv6 cef ipv6 multicast rpf use-bgp spanning-tree mode pvst spanning-tree extend system-id ! vlan internal allocation policy ascending ! interface Ethernet0/0 description EPC_to_PE-2 no shutdown switchport trunk encapsulation dot1q switchport trunk allowed vlan 10 switchport mode trunk duplex auto ! interface Ethernet0/1 no shutdown shutdown duplex auto ! interface Ethernet0/2	EPC_Backup version 15.1 service timestamps debug datetime msec service timestamps log datetime msec no service password-encryption service compress-config ! hostname EPC_Backup ! boot-start-marker boot-end-marker ! no aaa new-model clock timezone EET 2 0 ! ip cef ! no ip domain-lookup no ipv6 cef ipv6 multicast rpf use-bgp spanning-tree mode pvst spanning-tree extend system-id ! vlan internal allocation policy ascending ! interface Ethernet0/0 description EPC_Backup_to_PE-4 no shutdown switchport trunk encapsulation dot1q switchport trunk allowed vlan 10 switchport mode trunk duplex auto ! interface Ethernet0/1 no shutdown duplex auto ! interface Ethernet0/2 no shutdown

no shutdown shutdown duplex auto ! interface Ethernet0/3 no shutdown shutdown duplex auto ! interface Vlan10 no shutdown ip address 172.16.1.2 255.255.255.0 ! no ip http server ip route 0.0.0.0 0.0.0.0 172.16.1.1 ! control-plane ! line con 0 exec-timeout 0 0 logging synchronous line aux 0 line vty 0 4 exec-timeout 0 0 logging synchronous login transport input none ! end	duplex auto ! interface Ethernet0/3 no shutdown duplex auto ! interface Vlan10 no shutdown ip address 172.16.1.2 255.255.255.0 ! no ip http server ip route 0.0.0.0 0.0.0.0 172.16.1.1 ! control-plane ! line con 0 exec-timeout 0 0 logging synchronous line aux 0 line vty 0 4 exec-timeout 0 0 logging synchronous login ! end
PE-1 version 15.1 service timestamps debug datetime msec service timestamps log datetime msec no service password-encryption service compress-config ! hostname PE-1 ! boot-start-marker boot-end-marker ! logging buffered 44444444 ! username cisco privilege 15 password 0 cisco	PE-2 version 15.2 service timestamps debug datetime msec service timestamps log datetime msec ! hostname PE-2 ! boot-start-marker boot-end-marker ! no aaa new-model ! ip vrf EPC rd 10:10 route-target export 10:10

```
no aaa new-model
clock timezone EET 2 0
!
ip vrf eNodeB-1-3
 rd 10:10
 route-target export 10:10
 route-target import 10:10
!
ip cef
!
no ip domain-lookup
no ipv6 cef
ipv6 multicast rpf use-bgp
mpls label range 100 199
mpls label protocol ldp
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface Loopback0
 no shutdown
 ip address 192.168.255.1 255.255.255.255
 ip ospf network point-to-point
!
interface Ethernet0/0
 description PE-1_to_SW-1
 no shutdown
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10
 switchport mode trunk
 duplex auto
!
interface Ethernet0/1
 description PE-1_to_PE-4
 no shutdown
 no switchport
 bandwidth 100000
 ip address 192.168.1.1 255.255.255.252
 ip ospf network point-to-point
 mpls label protocol ldp
 mpls ip
 bfd interval 100 min_rx 50 multiplier 3
!
interface Ethernet0/2
 no shutdown
 no switchport
 no ip address
```

```
 route-target import 10:10
!
no ip domain lookup
ip cef
no ipv6 cef
!
mpls label range 200 299
mpls label protocol ldp
multilink bundle-name authenticated
!
interface Loopback0
 ip address 192.168.255.2 255.255.255.255
 ip ospf network point-to-point
!
interface FastEthernet0/0
 description PE-2_to_PE-4
 ip address 192.168.1.18 255.255.255.252
 ip ospf network point-to-point
 duplex full
 mpls ip
 mpls label protocol ldp
!
interface FastEthernet1/0
 description PE-2_to_PE-3
 ip address 192.168.1.14 255.255.255.252
 ip ospf network point-to-point
 duplex full
 mpls ip
 mpls label protocol ldp
!
interface FastEthernet2/0
 no ip address
 duplex full
!
interface FastEthernet2/0.10
 description PE-2_to_EPC
 encapsulation dot1Q 10
 ip vrf forwarding EPC
 ip address 172.16.1.1 255.255.255.0
!
interface FastEthernet3/0
 no ip address
 shutdown
 duplex full
!
interface FastEthernet4/0
 no ip address
 shutdown
```

```
!
interface Ethernet0/2.10
 description PE-1_to_SW-1
 no shutdown
 encapsulation dot1Q 10
 ip vrf forwarding eNodeB-1-3
 ip address 172.16.3.1 255.255.255.0
!
interface Ethernet0/3
 description PE-1_to_PE-3
 no shutdown
 no switchport
 ip address 192.168.1.5 255.255.255.252
 ip ospf network point-to-point
 mpls label protocol ldp
 mpls ip
bfd interval 100 min_rx 50 multiplier 3
!
router ospf 1
 router-id 192.168.255.1
 passive-interface Loopback0
 network 192.168.1.1 0.0.0.0 area 0
 network 192.168.1.5 0.0.0.0 area 0
 network 192.168.255.1 0.0.0.0 area 0
 bfd all-interfaces
!
router bgp 65000
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 192.168.255.11 remote-as 65000
 neighbor 192.168.255.11 update-source
Loopback0
 neighbor 192.168.255.22 remote-as 65000
 neighbor 192.168.255.22 update-source
Loopback0
 !
 address-family ipv4
 exit-address-family
 !
 address-family vpnv4
  neighbor 192.168.255.11 activate
  neighbor 192.168.255.11 send-community
extended
  neighbor 192.168.255.22 activate
  neighbor 192.168.255.22 send-community
extended
 exit-address-family
 !
```

```
 duplex full
!
router ospf 1
 router-id 192.168.255.2
 passive-interface Loopback0
 network 192.168.255.2 0.0.0.0 area 0
 network 192.168.1.14 0.0.0.0 area 0
 network 192.168.1.18 0.0.0.0 area 0
!
router bgp 65000
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 192.168.255.11 remote-as 65000
 neighbor 192.168.255.11 update-source
Loopback0
 neighbor 192.168.255.22 remote-as 65000
 neighbor 192.168.255.22 update-source
Loopback0
 !
 address-family ipv4
 exit-address-family
 !
 address-family vpnv4
  neighbor 192.168.255.11 activate
  neighbor 192.168.255.11 send-community
extended
  neighbor 192.168.255.22 activate
  neighbor 192.168.255.22 send-community
extended
 exit-address-family
 !
 address-family ipv4 vrf EPC
  redistribute connected
 exit-address-family
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
mpls ldp router-id Loopback0
!
!
control-plane
!
!
```

address-family ipv4 vrf eNodeB-1-3 redistribute connected exit-address-family ! no ip http server ! mpls ldp router-id Loopback0 ! control-plane ! line con 0 exec-timeout 0 0 logging synchronous line aux 0 line vty 0 4 exec-timeout 0 0 logging synchronous login local ! end	line con 0 exec-timeout 0 0 logging synchronous stopbits 1 line aux 0 stopbits 1 line vty 0 4 exec-timeout 0 0 logging synchronous login ! ! end
PE-3 version 15.2 service timestamps debug datetime msec service timestamps log datetime msec ! hostname PE-3 ! boot-start-marker boot-end-marker ! no aaa new-model ! ip vrf eNodeB-4 rd 10:10 route-target export 10:10 route-target import 10:10 ! no ip domain lookup ip cef no ipv6 cef ! mpls label range 300 399 mpls label protocol ldp multilink bundle-name authenticated	PE-4 version 15.2 service timestamps debug datetime msec service timestamps log datetime msec ! hostname PE-4 ! boot-start-marker boot-end-marker ! no aaa new-model ! ip vrf EPC-Backup rd 10:10 route-target export 10:10 route-target import 10:10 ! no ip domain lookup ip cef no ipv6 cef ! mpls label range 400 499 mpls label protocol ldp multilink bundle-name authenticated

```
!
interface Loopback0
 ip address 192.168.255.3 255.255.255.255
 ip ospf network point-to-point
!
interface FastEthernet0/0
 description PE-3_to_PE-2
 ip address 192.168.1.13 255.255.255.252
 ip ospf network point-to-point
 duplex full
 mpls ip
 mpls label protocol ldp
!
interface FastEthernet1/0
 description PE-3_to_PE-1
 bandwidth 10000
 ip address 192.168.1.6 255.255.255.252
 ip ospf network point-to-point
 duplex full
 mpls ip
 mpls label protocol ldp
!
interface FastEthernet2/0
 no ip address
 duplex full
!
interface FastEthernet2/0.10
 description PE-3_to_eNodeB-4
 encapsulation dot1Q 10
 ip vrf forwarding eNodeB-4
 ip address 172.16.2.1 255.255.255.0
!
interface FastEthernet3/0
 description PE-3_to_PE-4
 ip address 192.168.1.9 255.255.255.252
 ip ospf network point-to-point
 duplex full
 mpls ip
 mpls label protocol ldp
!
interface FastEthernet4/0
 description PE-3_to_RR-2
 ip address 192.168.1.25 255.255.255.252
 ip ospf network point-to-point
 duplex full
!
router ospf 1
 router-id 192.168.255.3
```

```
!
interface Loopback0
 ip address 192.168.255.4 255.255.255.255
 ip ospf network point-to-point
!
interface FastEthernet0/0
 description PE-4_to_PE-1
 ip address 192.168.1.2 255.255.255.252
 ip ospf network point-to-point
 duplex full
 mpls ip
 mpls label protocol ldp
!
interface FastEthernet1/0
 description PE-4_to_PE-2
 ip address 192.168.1.17 255.255.255.252
 ip ospf network point-to-point
 duplex full
 mpls ip
 mpls label protocol ldp
!
interface FastEthernet2/0
 description PE-4_to_PE-3
 ip address 192.168.1.10 255.255.255.252
 ip ospf network point-to-point
 duplex full
 mpls ip
 mpls label protocol ldp
!
interface FastEthernet3/0
 no ip address
 duplex full
!
interface FastEthernet3/0.10
 description PE-4_to_EPC_Backup
 encapsulation dot1Q 10
 ip vrf forwarding EPC-Backup
 ip address 172.16.1.1 255.255.255.0
!
interface FastEthernet4/0
 description PE-4_to_RR-1
 ip address 192.168.1.21 255.255.255.252
 ip ospf network point-to-point
 duplex full
!
router ospf 1
 router-id  192.168.255.4
 network 192.168.255.4 0.0.0.0 area 0
```

network 192.168.255.3 0.0.0.0 area 0 network 192.168.1.0 0.0.0.255 area 0 ! router bgp 65000 bgp log-neighbor-changes no bgp default ipv4-unicast neighbor 192.168.255.11 remote-as 65000 neighbor 192.168.255.11 update-source Loopback0 neighbor 192.168.255.22 remote-as 65000 neighbor 192.168.255.22 update-source Loopback0 ! address-family ipv4 exit-address-family ! address-family vpnv4 neighbor 192.168.255.11 activate neighbor 192.168.255.11 send-community extended neighbor 192.168.255.22 activate neighbor 192.168.255.22 send-community extended exit-address-family ! address-family ipv4 vrf eNodeB-4 redistribute connected exit-address-family ! ip forward-protocol nd ! no ip http server no ip http secure-server ! mpls ldp router-id Loopback0 ! control-plane ! line con 0 exec-timeout 0 0 logging synchronous stopbits 1 line aux 0 stopbits 1 line vty 0 4 exec-timeout 0 0 logging synchronous login	network 192.168.1.0 0.0.0.255 area 0 ! router bgp 65000 bgp log-neighbor-changes no bgp default ipv4-unicast neighbor 192.168.255.11 remote-as 65000 neighbor 192.168.255.11 update-source Loopback0 neighbor 192.168.255.22 remote-as 65000 neighbor 192.168.255.22 update-source Loopback0 ! address-family ipv4 exit-address-family ! address-family vpnv4 neighbor 192.168.255.11 activate neighbor 192.168.255.11 send-community extended neighbor 192.168.255.22 activate neighbor 192.168.255.22 send-community extended exit-address-family ! address-family ipv4 vrf EPC-Backup redistribute connected metric 100000 exit-address-family ! ip forward-protocol nd ! no ip http server no ip http secure-server ! mpls ldp router-id Loopback0 ! control-plane ! line con 0 exec-timeout 0 0 logging synchronous stopbits 1 line aux 0 stopbits 1 line vty 0 4 exec-timeout 0 0 logging synchronous login !

! end	! end
RR-1 version 15.2 service timestamps debug datetime msec service timestamps log datetime msec ! hostname RR-1 ! boot-start-marker boot-end-marker ! no aaa new-model ! no ip domain lookup ip cef no ipv6 cef ! multilink bundle-name authenticated ! interface Loopback0 ip address 192.168.255.11 255.255.255.255 ip ospf network point-to-point ! interface FastEthernet0/0 description RR-1_to_PE-4 ip address 192.168.1.22 255.255.255.252 ip ospf network point-to-point duplex full ! interface FastEthernet1/0 no ip address shutdown duplex full ! interface FastEthernet2/0 no ip address shutdown duplex full ! router ospf 1 router-id 192.168.255.11 passive-interface Loopback0 network 0.0.0.0 255.255.255.255 area 0	RR-2 version 15.2 service timestamps debug datetime msec service timestamps log datetime msec ! hostname RR-2 ! boot-start-marker boot-end-marker ! no aaa new-model ! no ip domain lookup ip cef no ipv6 cef ! multilink bundle-name authenticated ! interface Loopback0 ip address 192.168.255.22 255.255.255.255 ip ospf network point-to-point ! interface FastEthernet0/0 description RR-2_to_PE-3 ip address 192.168.1.26 255.255.255.252 ip ospf network point-to-point duplex full ! interface FastEthernet1/0 no ip address shutdown duplex full ! interface FastEthernet2/0 no ip address shutdown duplex full ! router ospf 1 router-id 192.168.255.22 passive-interface Loopback0 network 0.0.0.0 255.255.255.255 area 0

```
!
router bgp 65000
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor IBGP peer-group
 neighbor IBGP remote-as 65000
 neighbor IBGP update-source Loopback0
 neighbor 192.168.255.1 peer-group IBGP
 neighbor 192.168.255.2 peer-group IBGP
 neighbor 192.168.255.3 peer-group IBGP
 neighbor 192.168.255.4 peer-group IBGP
 !
 address-family ipv4
 exit-address-family
 !
 address-family vpnv4
  neighbor IBGP send-community extended
  neighbor IBGP route-reflector-client
  neighbor 192.168.255.1 activate
  neighbor 192.168.255.2 activate
  neighbor 192.168.255.3 activate
  neighbor 192.168.255.4 activate
 exit-address-family
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
line con 0
 exec-timeout 0 0
 logging synchronous
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
!
end
```

```
!
router bgp 65000
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor IBGP peer-group
 neighbor IBGP remote-as 65000
 neighbor IBGP update-source Loopback0
 neighbor 192.168.255.1 peer-group IBGP
 neighbor 192.168.255.2 peer-group IBGP
 neighbor 192.168.255.3 peer-group IBGP
 neighbor 192.168.255.4 peer-group IBGP
 !
 address-family ipv4
 exit-address-family
 !
 address-family vpnv4
  neighbor IBGP send-community extended
  neighbor IBGP route-reflector-client
  neighbor 192.168.255.1 activate
  neighbor 192.168.255.2 activate
  neighbor 192.168.255.3 activate
  neighbor 192.168.255.4 activate
 exit-address-family
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
line con 0
 exec-timeout 0 0
 logging synchronous
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
!
end
```