5G IP-Core Network Planning and Optimization

Submitted in partial fulfillment of the requirements for the part of

SYSC5407- Planning and Design of Computer Networks

By

SAJIB KUMARKURI, ADITI BHARDWAJ, MOHAMAD AZZAM

24 March, 2020

Table of Contents

I. INTRODUCTION 3

II. BACKGROUND 4

III. NETWORK REQUIREMENT 6

IV. SOLUTION DESCRIPTION 9

V. NETWORK DESIGN 11

VI. RESULTS 17

VII. CONCLUSION 18

REFERENCES 18

I. INTRODUCTION

In our current era of 5G technology, High-speed communication requirements pose various hurdles on the existing network infrastructure when it comes to technology and business models. With this in mind, the demand from diverse applications must be met by the next-generation mobile network. The International Telecommunication Union (ITU) has classified 5G mobile network services into three classes: *Enhanced Mobile Broadband (eMBB), Ultra-reliable and Low-latency Communications (uRLLC), and Massive Machine Type Communications (mMTC)* [1].

- The goal of *eMBB* is, to satisfy the demand for an increasingly digital lifestyle, and prioritize applications that require high bandwidth, as the likes of high definition (HD) videos, virtual reality (VR), and augmented reality (AR).
- When it comes to *uRLLC*, the goal is to satisfy the anticipated demand from the digital industry and concentrate on latency-sensitive services, like assisted & automated driving and remote management.
- Lastly, *mMTC* objectives are to satisfy the demands for an advanced developed digital society and prioritize applications that comprise high connection density requirements, e.g. smart city and smart agriculture.

It is also important to note that the growth of the service scope for mobile networks improves the telecom network ecosystem. This is achieved by the contribution of several traditional industries, such as automotive, healthcare, energy, and municipal systems.

All in all, 5G is the start of the elevation of digitalization from personal entertainment to society's interconnection. Digitalization creates incredible opportunities for the mobile communication industry but introduces strict challenges towards mobile communication technologies [2].

To accommodate the 5G era, four new features will be to our IP networks i.e. new architecture, new interfaces, new protocols, and new O&M.

- **New interfaces**: The traditional/outdated networking interfaces are GE, 10GE, and 100GE. With the continual development of chip technology (optical-electrical (PAM4) technology), we can reduce the cost per bit by more than 30% thereby, further lowering operator network construction costs. With PAM4 technology maturing, the traditional networking interfaces (50GE, 200GE, and 400GE) have been defined by the IEEE as new standards for the next generation of Ethernet network interfaces.
- **New architecture**: With the continual development of chip technology, single-chip SOC has a capacity of 1.2 Tbit/s, allowing us to simplify the network layer. Meanwhile, the evolution of 5G and telecommunication cloud services are demanding higher network bandwidth and latency. Service operators are universally optimistic about simplifying the network layer, integrating the node functions, and implementing comprehensive service-independent bearer capabilities.

  In backbone networks, P+PE and MDS (multi-domain system) capabilities utilize integrated backbone solutions. FBB/MBB/private line networks are integrated through

physical devices, whereas still enabling logical partition management, significantly reducing IP backbone network construction expenses. As per the telecom cloud solutions, a cloud network architecture with discrete forwarding and control planes based on actual requirements, which resolves the three challenges: low resource utilization, complex management and maintenance, and slow service provisioning.

- **New O&M**: Telecom cloud and segment routing allowed some network roles to be centralized at the control layer and automated network configuration to be applied through an open and programmable centralized control plane. Meanwhile, the use of big data and AI has optimized network intelligence [3].
- **New protocols**: In order to meet service requirements and address network challenges, the 5G era will explicitly introduce a host of transport-related access network technologies and protocols. Out of the very network technologies and protocols, the following three are the most significant:
    - International Telecommunication Union's (ITU) Optical Transport Network (OTN);
    - The Institute of Electrical and Electronics Engineers' (IEEE) Time-Sensitive Networking;
    - The Internet Engineering Task Force's (IETF) segment routing standard, Source Packet Routing in Networking (SPRING).

Additionally, five other technologies/standards are 10 Gbit/s microwaves, the CPRI Consorti- um's eCPRI, Optical Internetworking Forum's (OIF) Flex Ethernet (FlexE), IEEE's 25 Gbit/s Ethernet and ITU-T's NGON2 [4].

In our project, we have focused on IP Network for 5G and provided a simulated solution based on Huawei Versatile Routing Platform Software. We proposed a hierarchical architecture H-VPN solution for a 5G network consisting of an access layer, an aggregation layer, and a core layer. In section 2 background or motivation is described, in section 3 network requirement and network topology is presented. Furthermore, solution description, network design and results of the simulation are discussed and show in following section 4, 5 and 6 simultaneously.

II. BACKGROUND

A backbone network is part of the computer network that interconnects various pieces of the network providing a path for information exchange between different LANs or subnetworks. The backbone provides services such as conventional Internet services, mobile, VoIP, video, VIP, and data center (DC) interconnection services. The backbone network runs MPLS VPNs to isolate services from one another and provides service quality based on service types. The growth of service traffic introduces challenges to the backbone network. These challenges involve network traffic monitoring, network traffic load balancing, and network bandwidth usage.

MPLS TE uses the TE technique to plan service paths. In addition to improving bandwidth usage efficiency, MPLS TE needs to survive on existing networks. The proliferation of services

has posed increasing demands for network resources (for example, bandwidth) and amplified network complexity and scale. The following challenges confront MPLS TE technology.

- Complex tunnel path planning: Although the traditional planning that establishes MPLS TE tunnels over explicit paths effectively uses bandwidth resources, manfully planning is sophisticated within a complex large network topology.
- Low bandwidth usage: Although MPLS TE can use the shortest path first (SPF) or Constrained Shortest Path First (CSPF) to automatically calculate paths, network use efficiency cannot be maximized because of drawbacks of the shortest path and CSPF distributed algorithm.
- Complex network O&M: Network O&M personnel cannot monitor the actual network traffic status or detect link congestion and must manually adjust paths to tackle link congestion.

To solve the problems faced we proposed the MPLS network optimization solution for the 5G network. We deployed the MPLS network optimization solution for IP Domain on the basis of the traditional MPLS network. The system consists of the traffic analysis, traffic optimization, and control system simulated based on a planning system to implement functions. Although there are controller systems, configuration management systems, network management, network maintenance, and traffic optimization management which are out of scope for the simulation project. We have separated our project in several segments as per Fig. 1 and developed our implementation solution based on that.

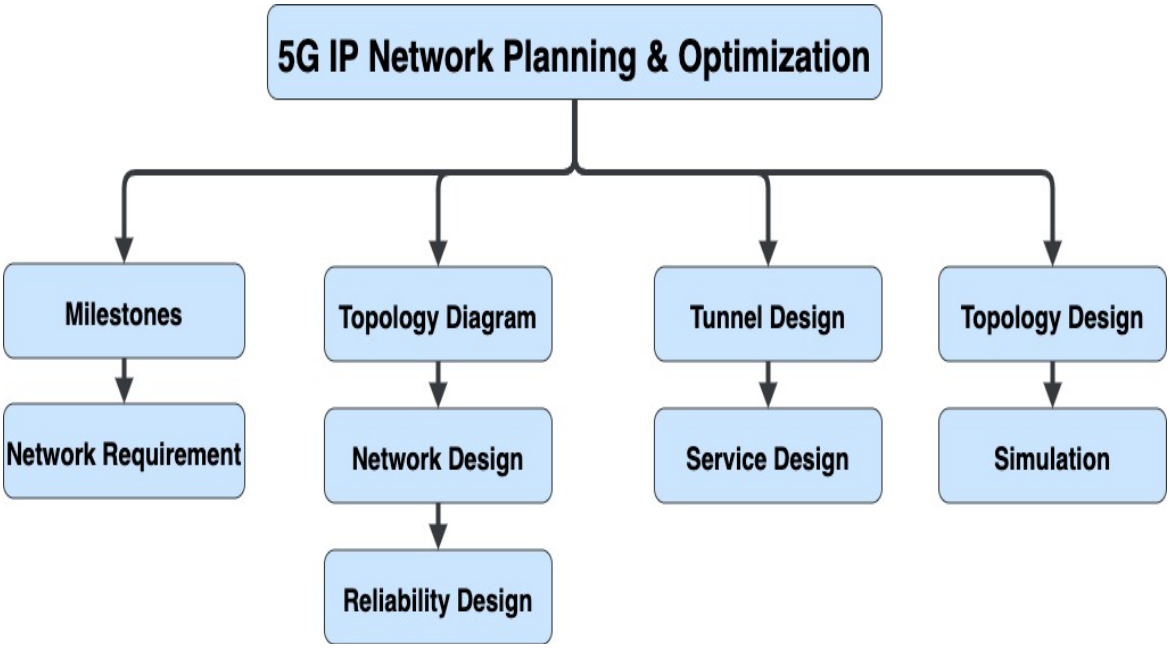

Fig. 1: Flow Diagram of 5G IP Network Planning and Optimization

III. NETWORK REQUIREMENT

Operating System	Windows 10
Simulator	Huawei Versatile Routing Platform Software VRP (R) software, Version 5.110 (eNSP V100R001C00)
Network Device	Routers-AR1220-S
Protocol	IS-IS, BGP, MPLS
Core Nodes (Dummy)	5G OTN, g-NodeB, IoT Gateway, Billing Server, 5G-RNC, Cloud Server

Table 1: Network Requirement for The Project Simulation

3.1 Network Topology:

A network based on the topology in Fig. 2 is created and NE names, device IP addresses, service interfaces, and user interfaces are configured.

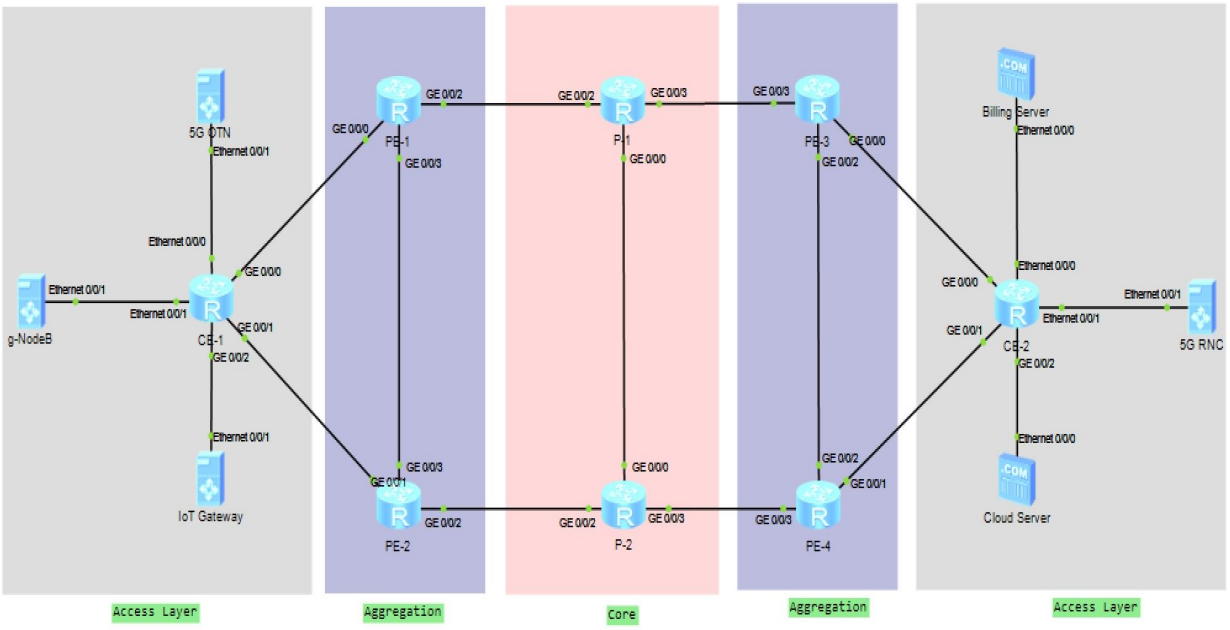

Fig. 2: Topology Diagram

The network has three layers in it, namely, the access layer, aggregation layer, and the core layer. The access layer is the level where host computers are connected to the network. The Aggregation layer connects the core layer and the access layer. The core network provides high-speed, highly redundant forwarding services to move packets between distribution-layer devices in different regions of the network. The network presented involves eight routers. And three stations, gNodeB, 5G OTN, and the IoT gateway. gNodeB, also known as gNB is a 5G term for network equipment that transmits and receives wireless communications between UE and a mobile

network). 5G-OTN, also known as an optical transport network, was designed to provide support for optical networking. The BGP/MPLS IP VPN model consists of the following parts: Customer Edge (CE) is an edge device on the customer network, which has one or more interfaces directly connected to the service provider network. Provider Edge (PE) is an edge device on the provider network, which is directly connected to the CE. In the MPLS network, PEs perform all the VPN related processing. The provider (P) is a backbone device on the provider network, which is not directly connected to the CE. Ps only need to possess basic MPLS forwarding capabilities and do not need to maintain information about VPNs.

3.2 Interface Data Plan:

NE Role	Local Interface	IP Address Interface	Description
CE-1	Loopback0	192.168.1.7/32	
	GigabitEthernet0/0/0	192.168.17.2/30	To_PE1
	GigabitEthernet0/0/1	192.168.27.2/30	To_PE2
PE-1	Loopback0	192.168.1.1/32	
	GigabitEthernet0/0/0	192.168.17.1/30	To_CE1
	GigabitEthernet0/0/2	192.168.13.1/30	To_PE2
	GigabitEthernet0/0/3	192.168.12.1/30	To_P1
PE-2	Loopback0	192.168.1.2/32	
	GigabitEthernet0/0/0	192.168.27.1/30	To_CE1
	GigabitEthernet0/0/2	192.168.12.2/30	To_PE1
	GigabitEthernet0/0/3	192.168.24.1/30	To_P2
P-1	Loopback0	192.168.1.3/32	
	GigabitEthernet0/0/0	192.168.34.1/30	To_P2
	GigabitEthernet0/0/2	192.168.13.2/30	To_PE1

	GigabitEthernet0/0/3	192.168.35.1/30	To_PE3
P-2	Loopback0	192.168.1.4/32	
	GigabitEthernet0/0/0	192.168.34.2/30	To_P1
	GigabitEthernet0/0/2	192.168.24.2/30	To_PE2
	GigabitEthernet0/0/3	192.168.46.1/30	To_PE4
PE-3	Loopback0	192.168.1.5/32	
	GigabitEthernet0/0/0	192.168.58.1/30	To_CE2
	GigabitEthernet0/0/2	192.168.56.1/30	To_PE4
	GigabitEthernet0/0/3	192.168.35.2/30	To_P1
PE-4	Loopback0	192.168.1.6/32	
	GigabitEthernet0/0/1	192.168.68.1/30	To_ CE2
	GigabitEthernet0/0/2	192.168.56.2/30	To_PE3
	GigabitEthernet0/0/3	192.168.46.2/30	To_P2
CE-2	Loopback0	192.168.1.8/32	
	GigabitEthernet0/0/0	192.168.58.2/30	To_PE3
	GigabitEthernet0/0/1	192.168.68.2/30	To_PE4

3.3 Product Details:

Network Layer	Role	Function	Product Model
	5G OTN	OTN fronthaul solution provided 4 x 25G eCPRI transmission, reaching a	-

Core Nodes (Source)		single-node bandwidth of 100 Gbps. 5G OTN fronthaul solution fully meet the requirements for a 5G fronthaul application	
	g-NodeB	g-NodeB is a 3GPP 5G Next Generation base station which supports the 5G New Radio. It adopts a uniform modular design (BBUs and RF modules) to provide various product forms	-
	IoT Gateway (EDGE/FOG)	IoT gateway is a bridge between IoT devices and cloud that enables remote control of the devices and machines. It will communicate with cloud through 5G backbone network	-
Core Nodes (Destination)	5G-RNC	Refers to a key node on a 5G network. Manages mobility, processes calls, manages links, and switches users on the access network	-
	Cloud Platform	Cloud platforms analyze data collected from IoT EDGE/FOG gateway to provide the ability to manage devices. Example: AWS, IBM Watson Platform, Microsoft Azure	-
Access Network	Cell Site Gateway (CSG)	Receives and processes various service signals from base stations and forwards them to devices at the aggregation layer	AR122-S
Aggregation network	Aggregation Site Gateway (ASG)	Aggregates service signals from CSGs and forwards them to RSG through P/RR	AR122-S
	Radio Service Gateway (RSG)	Connects to core controllers such as 5G-RNC, Cloud Server, Billing Server	AR122-S

IV. SOLUTION DESCRIPTION

Multiple solutions are available for deploying H-VPN solutions. Fig. 3 shows available solutions and for our project we have deployed an RR-Client solution for the proposed 5G network.

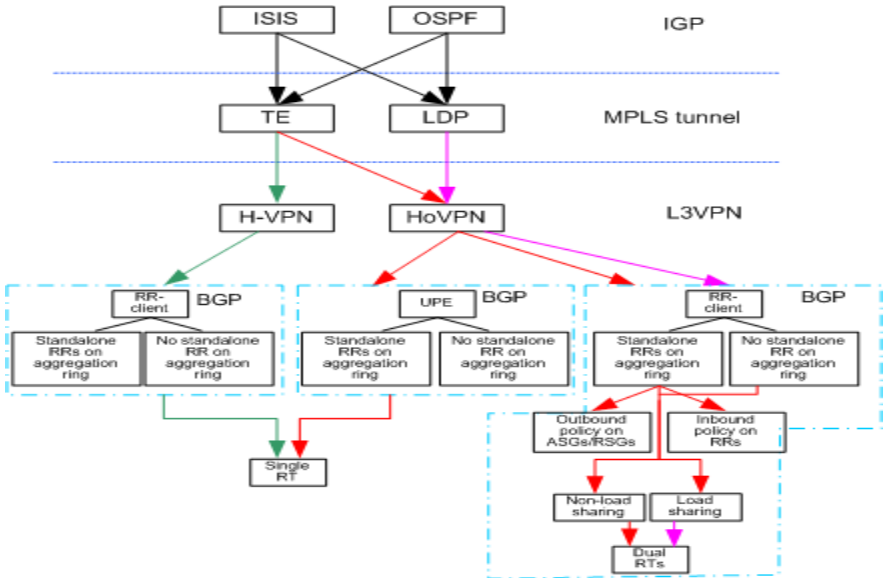

Fig. 3: Available solutions and deployment sequence [5]

4.1 Solution Deployment:

Technology	MPLS TE Bearer Mode
IGP	• IGP is deployed to isolate routes on the access ring from those on the aggregation ring • Bidirectional forwarding detection (BFD) for IGP needs to be enabled network-wide. • Transmission of TE information does not need to be enabled.
MPLS	• MPLS TE needs to be deployed • MPLS RSVP-TE needs to be enabled • BFD for RSVP-TE needs to be enabled. • MPLS TE tunnels need to be deployed and loose explicit paths need to be planned • BFD for TE needs to be configured for all tunnels on the access ring and aggregation ring. • BFD for LSP needs to be configured for all primary tunnels on the access ring and aggregation ring.
Ethernet Service Deployment	• MPLS TE tunnels are used to carry services • When MPLS TE tunnels carry Ethernet services, the H-VPN solutions can be deployed for E2E services • When MPLS TE tunnels carry Ethernet services, the BGP will deployed as RR

V. NETWORK DESIGN

Proposed hierarchical architecture H-VPN solution for 5G network consists of an access layer, an aggregation layer, and a core layer. A BGP/MPLS IP-VPN network in a hierarchical structure assists with this conversion process. The H-VPN solution distributes the functions of one PE to multiple PEs. These PEs play different roles and form a hierarchical architecture. H-VPN networking provides the following benefits:

- Flexible expandability
- Reduced interface resource requirements
- Simple configuration

The BGP/MPLS IP VPN model consists of the following parts:

- A Customer Edge (CE) is an edge device on the customer network, which has one or more interfaces directly connected to the service provider network.
- A Provider Edge (PE) is an edge device on the provider network, which is directly connected to the CE. In the MPLS network, PEs perform all the VPN-related processing for the entire network.
- A Provider (P) is a backbone device on the provider network, which is not directly connected to the CE. Ps only need to possess basic MPLS forwarding capabilities and do not need to maintain information about VPNs.

5.1 IGP Deployment Solution:

IS-IS is used inside an AS as IGP protocol, IS-IS is a link-state protocol which uses SPF algorithm to calculate routes. IS-IS has been called the de facto standard for large service provider network backbones. IS-IS is easier to extend than OSPF and more secure than OSPF protocol. ISIS is more scalable, has less overhead and also supports IPv4 and IPv6 in a single instance. Computation for large areas is much less CPU and memory intensive.

- An interface is added to a related IS-IS process according to the area to which the interface link belongs
- The PE loopback interface whose IP address is used as the LSR ID is added to an aggregation IGP process
- Configure IS-IS processes for aggregation ring and access rings to isolate their routes
- Set the cost to control route selection and deploy BFD for IGP to speed up service switching when faults occur

IS-IS Parameters:

Parameters	Value	Remarks

isis	area: 100	Enables IS-IS processes
network-entity	CE-1: 10.0000.0092.0168.1007.00 CE-2: 10.0000.0092.0168.1008.00 PE-1: 10.0000.0092.0168.1001.00 PE-2: 10.0000.0092.0168.1002.00 PE-3: 10.0000.0092.0168.1005.00 PE-4: 10.0000.0092.0168.1006.00 P-1: 10.0000.0092.0168.1003.00 P-2: 10.0000.0092.0168.1004.00	Set a Network Entity Title: ● The area ID is designed based on customer requirements. ● The system ID must be unique on the entire network ● Obtain the system ID using the IP address of the loopback0 interface
is-level	Level-2	Configures the level of the router
cost-style	Wide	Receives or advertises routes whose cost type is wide
bfd all-interfaces enable	-	Enables BFD for IS-IS.

5.2 MPLS / H-VPN Tunnels Solution:

Multiprotocol Label Switching (MPLS) is a routing technique that directs data optimization based on the existing MPLS network. MPLS avoids complex lookups in a routing table and speeding traffic flows using labels. Adjusts traffic optimization on the backbone network and improves network bandwidth utilization. We used MPLS TE tunnels, including Resource Reservation Protocol-TE (RSVP-TE) and Hot-Standby policy. MPLS TE tunnels have the following advantages:

- Tunnel establishment can be controlled, and is not based on FECs
- Bandwidth can be flexibly controlled through automatic bandwidth adjustment and optimization
- The security is high. Authentication can be performed based on peers or interfaces
- RSVP-TE provides various protection switching modes and supports tunnel protection groups. TE hot-standby is recommended

MPLS Parameters:

Parameters	Value	Remarks
mpls lsr-id	IP address of loopback0 interface on LSR	Other MPLS configuration commands are available only after the LSR ID is configured
mpls te	-	Enables the MPLS-TE function.
mpls rsvp-te	-	Enables the MPLS RSVP-TE function
mpls rsvp-te hello	-	Enables the RSVP-TE Hello mechanism globally
mpls te cspf	-	Enables the MPLS TE CSPF algorithm
mpls rsvp-te srefresh	-	Enables the RSVP summary refresh (Srefresh) feature
mpls rsvp-te bfd all interfaces	enable	Enables BFD for MPLS RSVP-TE
mpls rsvp-te bfd all interfaces min-tx-interval XXX min-rx-interval XXX	100	Sets the BFD interval to 100ms

MPLS TE tunnel parameters:

Parameters	Value	Remarks
interface Tunnel	Tunnel number: 0/0/XY XY: device numbers of source and destination nodes	Creates a tunnel interface
ip address unnumbered	interface LoopBack0	Configures the tunnel to use the IP address of the loopback0 interface
tunnel-protocol	mpls te	Sets the tunnel mode to CRLSP

destination	IP address of the loopback0 interface on the remote device	Specifies the IP address of the destination node
mpls te tunnel-id	Tunnel ID format: XY XY: device numbers of the source and destination nodes	Sets a tunnel ID
mpls te backup	hot-standby wtr 60	Sets the WTR time for the tunnel in hot-standby mode
mpls te reoptimization	frequency 3600	Sets the re-optimization interval. The default value 3600s is recommended

MPLS TE Tunnel Parameters:

Parameters	Value	Remarks
interface Tunnel	Tunnel number: 0/0/XY device numbers of the source and destination nodes	Creates a tunnel interface
ip address unnumbered	interface LoopBack0	Configures the tunnel to use the IP address of the loopback0 interface
tunnel-protocol	mpls te	Sets tunnel mode to CR-LSP
mpls te tunnel-id	Tunnel ID format: XY device numbers of the source and destination nodes	Sets a tunnel ID
mpls te backup	hot-standby wtr 60	Sets the WTR time for the tunnel in hot-standby mode
mpls te reoptimization	frequency 3600	Sets the re-optimization interval. The default value 3600s is recommended

5.3 BGP Deployment Solution:

Border Gateway Protocol (BGP) is a dynamic routing protocol used between autonomous systems (AS). Extension for BGP-4 (MP-BGP) is used to support multiple types of network layer protocols such as VPNv4 addresses. To improve reliability, it is recommended that two BGP connections be deployed in the same area to provide redundancy protection. We used I-BGP connections in the network to forward 5G data-traffic for network optimization solutions. BGP is deployed for setting up the BGP routing table so that services are forwarded along the planned paths.

The following shows the guidelines for deploying a hierarchical L3VPN (standalone RRs are deployed):

- The PEs are configured as inline RRs, with CEs being clients of the inline RRs. In addition, PEs are clients of standalone RRs on the aggregation side.
- In the upstream direction, CEs advertise specific routes to PEs. PEs forward the specific routes to RRs, with the next hop being changed to loopback0 address of the related destination PE. RRs reflect the specific routes to PEs.
- In the downstream direction, PEs advertise specific routes to RRs, and RRs reflect the specific routes to destination PEs. Destination PEs forward the specific routes to CEs, with the next hop being changed to the loopback0 address of the related PE.
- When routes are advertised between PEs and CEs and between source PEs and destination PEs, the value of local-preference in the routes is modified to determine the master/slave of PEs.

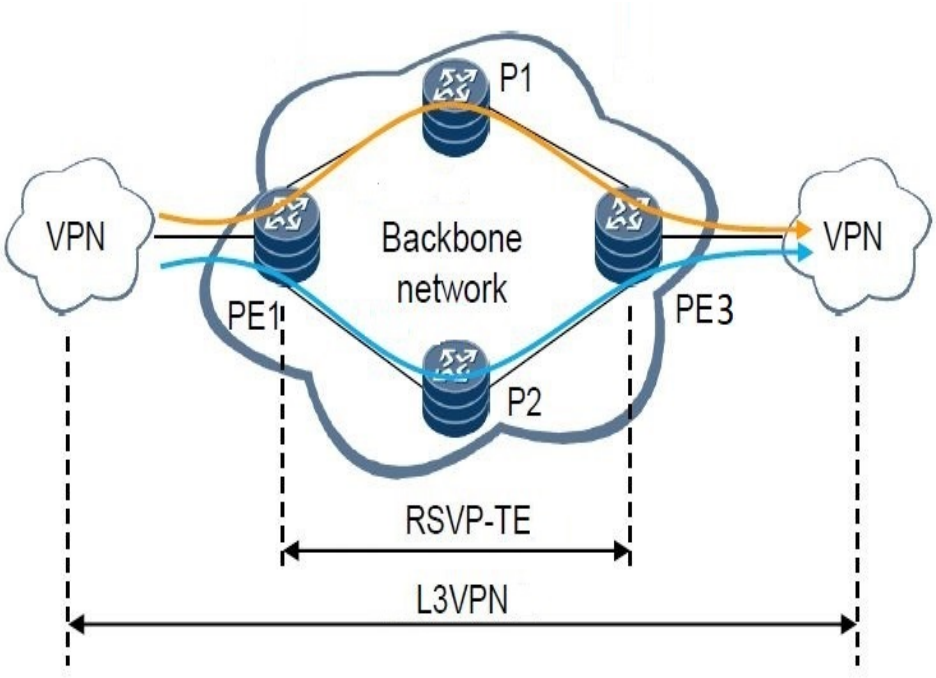

Fig. 4: E2E VPN Primary/Secondary Path

BGP Parameters:

Parameters	Value	Remarks
bgp xx	BGP autonomous system number	Creates a BGP AS (Example: bgp 100)
router-id	interface LoopBack0	Configures the router-id to use the IP address of the loopback0 interface
peers	Peer LoopBack0 address	Sets peer IP, AS number and connected interface
mpls te tunnel-id	Tunnel ID format: XY device numbers of the source and destination nodes	Sets a tunnel ID
ipv4-family unicast	unicast address in case of IPv4 peer	Undo synchronization
ipv4-family vpnv4	VPNv4 address family	Peer enable, reflect-client, advertise-community

MPLS VPN Parameters:

Parameters	Value	Remarks
VPN instance name	5G-Network-Slicing	-
RD value	5000:1	Advised to set the RD values to the same for CEs and PEs
RT value	CE: Export RT 5000:1, Import RT 5000:1 PE: Export RT 5000:1, Import RT 5000:1	The RT parameter settings for all CEs must be the same
Distributing Label Mode	apply-label per-instance	Allocate private network route labels based on the one label-to-one VPN instance rule
Binding Tunnel-Policy	5G-Network-Slicing	-

VI. RESULTS

In this section, we have presented related results which includes IS-IS peering, BGP peering, MPLS TE tunnel information and VPN instance routing details. We have run ping test of 1000 packets with 50 milliseconds and tested the optimization solution from CE-1 to CE-2 and found 99% accuracy on tunnel path shifting.

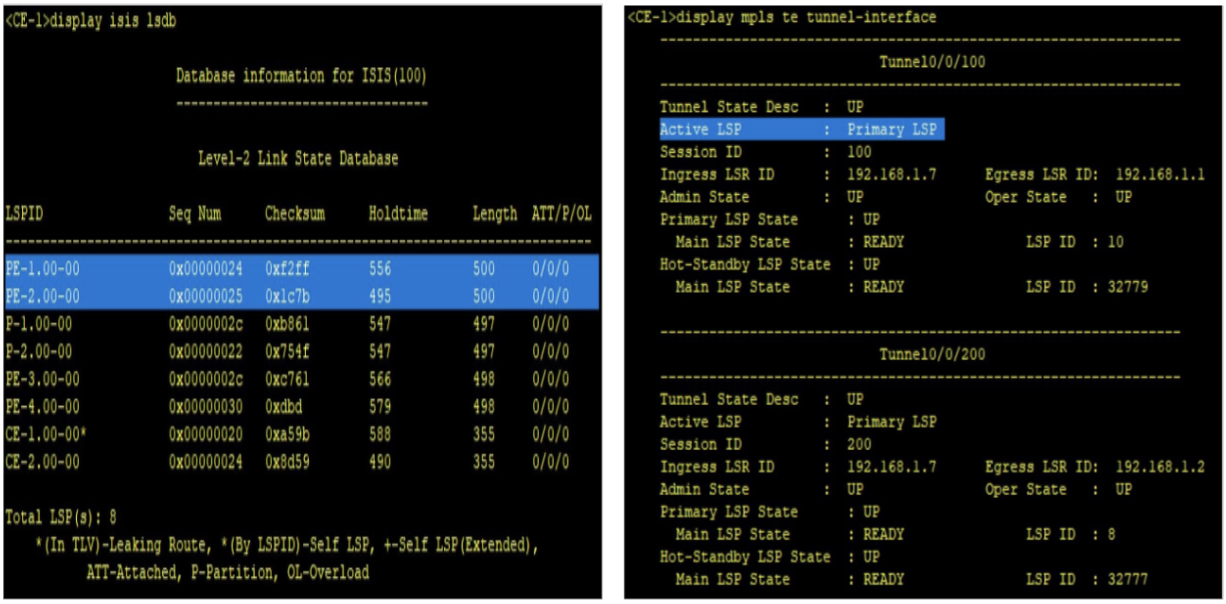

Fig. 5 (a): IS-IS Peer and MPLS TE Tunnel on CE-1 towards PEs

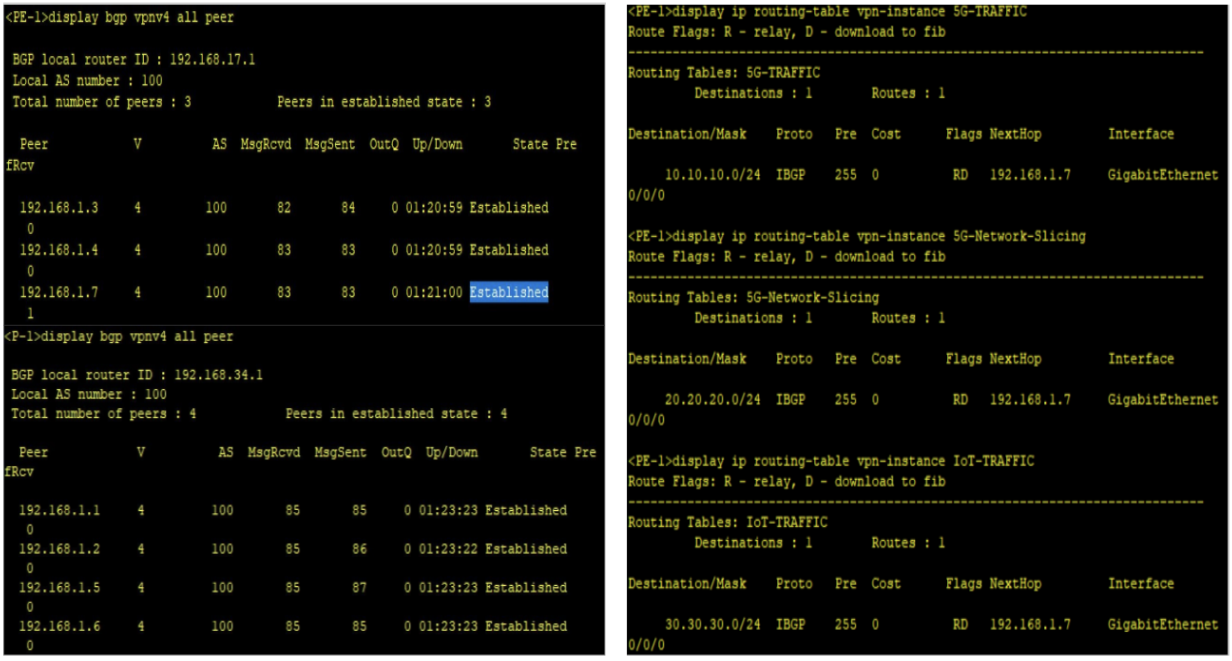

Fig. 5 (b): BGP Peer and VPN instance routing table on PE-1

VII. CONCLUSION

As per R15 release of 3GPP standard [6], commercial use of 5G is generating pace and the focus is now based on transport network to provide technical solution for eMBB, URLLC etc. For IP domain to support 4G service automation and 5G services consequently segment routing and E2E VPN service (such as H-VPN) provision will take place. For our project simulation, we have developed the solution for E2E VPN solution. Segment routing is out of scope due to limitation of simulation program. Network simulation software are not capable enough to handle segment routing yet and our future work will focus on segment routing. Meanwhile, our proposed method is capable of partitioning the physical network into slices based on service intents and can isolate service traffic on the 5G network while also ensuring service latency and security.

REFERENCES

[1] System architecture milestone of 5G Phase 1, https://www.3gpp.org/news-events/1930-sys_architecture

[2] https://www.huawei.com/minisite/hwmbbf16/insights/5G-Nework-Architecture-Whitepaper-en.pdf

[3] https://www.huawei.com/en/about-huawei/publications/communicate/87/building-comprehensive-ip-network-for-the-5g-and-cloud-era

[4] https://carrier.huawei.com/~/media/CNBG/Downloads/Technical%20Topics/Fixed%20Network/HR-Huawei-5G-Transport-WP.pdf

[5] https://support.huawei.com/carrier/docview?path=PBI1-7275726/PBI1-7301428/PBI1-7318422/PBI1-21115496&nid=SE0000736423

[6] https://www.3gpp.org/release-15