Master's Degree Thesis

Master's Degree

in COMMUNICATIONS AND COMPUTER NETWORKS ENGINEERING (INGEGNERIA TELEMATICA E DELLE COMUNICAZIONI)

The Evolution of the Network Architecture from Hardware Defined Network to Software Defined Network and Network Function Virtualization

Politecnico di Torino

Politecnico di Torino

Advisor:
Prof. Roberto Garello

Candidate:
Abdelrhman Mohamed Wael Ahmed

Mostafa Elmofty

Academic Year

2021-2022

Abstract:

In this document there is a representation of the evolution of the traditional hardware defined network to a software-defined network. Moreover, the representation of the building points to build SDN-POP (Software-Defined-Network Point-of-Presence) and SDWAN architecture, and how Orange uses both technologies to serve the customers beside another technology which is Network Function Virtualization (NFV). Another representation was made for SIP protocol which will lead to the understanding of the high-level architecture of the voice Networks architecture of OBS.

Acknowledgments:

I would like to thank my thesis advisor Professor Roberto Garello for his support, advice and being available whenever I had any queries. Moreover, he gave me the chance to have this internship thesis which added a lot to my career.

I would like to thank Orange OBS for having me as a trainee in their group and special thanks for all voice team who they supported me a lot, I would like to thank all my teammates in the office and even the teammates I worked with through Microsoft team.

I would like to thank all my family members and friends who they supported me, and they were the reason to be here by believing in me.

Table of Contents

Index of Figures

1 Introduction:

1.1 Overview:

As all the technology is migrating to a software base, the network architecture has the benefit to virtualize the network nodes and having complete virtual network architecture. With this solution telecommunication network companies can reduce the Capex (Capital expenditures) and Opex (Operational expenditures) for hardware maintenance as telecommunication companies spend a lot of money to purchase and maintain the hardware nodes as they are expensive. Moreover, this solution makes the upgrading (services and features) and troubleshooting easier and cheaper.

Another benefit is lowering the power consumption by instead running hundreds or thousands of devices now we are using fewer devices running multi-function. That will lead to less cooling required and better utilization of the resources. The data traffic increases so a decision should be taken to solve that issue.

1.2 Introduction to Orange:

Orange Business Service (OBS) is an international company that is a part of the French Orange group.

The Orange group supply services in twenty-six (26) countries in the B2C (Business to Consumer) market. Having two-hundred-fifty-nine Million customers (259M) moreover having one-hundred-forty-two thousand (142,000) employees worldwide. Orange is the 1st mobile network in France, 1st European operator for patent registration, and the 91st Global brand in 2021 (top 100 Brands). Orange network reliability as an operator coupled with Orange agility as an integrator of digital solutions.

Orange is the 1st for the quality of mobile network in France for the 11th consecutive year (Arcep). For the 4G Orange network, almost 99% of the population was covered in 8 European countries and 17 countries in the Middle-East and Africa, while for the 5G network Orange had launched successfully the 5G network in 5 European countries. For the service of Orange's business customers, Orange is the 1st for digital convergence in Europe, Orange invested 4.7 billion Euros in networks in 2020, and Orange has 450,000 Km of submarine cables (10 times around the world).

Orange Business Services (OBS) is a global digital services company operating in the B2B (business to business) market. OBS analyzes 15 billion data each day with FluxVision, solved 19,000 cyber-incidents in 2020, there are more than 18.8 million objects connected to the OBS network, and more than 70 cloud datacenters over the five continents.

OBS is building and operating complex infrastructures, which are the 1st voice-data network in the world, covering 220 countries and territories that are supervised 24/7, OBS deployed SD-WAN platforms in more than 60 international airports around the world, OBS network is connecting FTTO (Fiber to the Office) for 55,000 clients sites in France, OBS is the leader for the 21st consecutive year in the Gartner "magic" study Quadrant for Global Network Services, OBS has

60,000 Units of security equipment, more than 8,000 IT experts, and had invested in 2020 in the DH2 (Digital Health 2) fund to accelerate the development of e-health.

OBS has 28500 employees who are present in 65 countries having 1000 muti national clients and 3300 large national accounts globally. OBS teams deploy and supervise customers networks and digital solutions daily. OBS has 17 CyberSoc (Cyber Security Operational Center) around the world that bring together the best expertise in threat analysis, monitoring and responding to events. OBS has 24/7/365 Major service centers (MSCs) on all continents for 24/7 support.

1.3 Objective:

The Objective is to migrate from the legacy network to the next phase of logical network architecture by launching software-driven services, transforming the operating model of the function of devices then install them in software environment and using virtual machines.

2 State of Art:

2.1 Network Function Virtualization (NFV):

The technology of the virtual machine is having several operating systems running on the same hardware. VMs (Virtual Machines) can be installed on servers. The NFV (Network Function Virtualization) takes the benefits of that technology and moves it to the next logical step. The idea is to be looking to a network device such as a router or a switch as a box doing a network function which is redirecting and directing the data traffic based on the IP address for the router and the Mac address for the switch, but inside the router itself or switch there is a logical software or operating system running inside any network device to do that function. So, the idea of NFV is to take that logical function of the (Router, Switch, Load balancer, Firewall, etc.) and runs it in a virtualized environment VMs (Virtual machines). So NFV needs a hosting environment such as a data center to run these VMs.

2.2 Software-defined Network:

2.2.1 Open Stack:

OpenStack is a VIM (Virtual Infrastructure Manager) which is an Iaas solution (Infrastructure as a Service). It is a python base open source updated every six months. OpenStack is a set of software tools for building and managing cloud computing platforms for public and private clouds. It controls large pools of storage, networking resources, and network connectivity through a data center managed by an application (OpenStack API).

It allows users deeply the parameters such as CPU, RAM, storage, and networking. As shown in figure 1. As mentioned before OpenStack is a set of tools working together so the Openstack architecture is composed of a dashboard which is Horizon, a compute Service which is Nova, a tool for managing the networking, which is Neutron, a Block Storage which is Cinder, an identity service which is Keystone and orchestration engine which is Heat. As shown in figure 2.

There are several OpenStack storage components that must be there like the root disk which the VM needs its capacity to boot, another component which is the Ephermal storage which is a storage for the VM but it is eliminated once the VM is terminated, while the persistent storage never eliminated which means that even when the VM is terminated it stays on, and finally the block storage which is the capacity storage attached to the VM. The image it's a file that describes all the filesystems of the VM which can one of several formats (ISO, QCOW2, etc.). The image is stored and managed by the Glance.

The instance is a VM that runs on a physical server where several instances can be spawned from the same image. Each instance runs its own copy of the image to avoid impacting other instances. The instance needs to be defined by (CPUs, Ram, storage, etc to be created).

To create an Instance (VM) by a user that already exist and allowed to log in the dashboard (Horizon) a certain procedure should be done. First, a request is sent by the dashboard/CLI to Keystone to be authorized. Then the keystone sends a token back to the dashboard. The dashboard sends then the request to nova-API with the token received by keystone. The nova-API will authenticate the request by sending the token to the keystone and awaits validation from it. After nova-API has the validation from keystone nova-API will impact the nova database to create an initial virtual machine. Then nova-API sends the request to the Queue which will send it to the nova-schedular which will do its algorithm based on the information it gets from the nova database and finds the best compute node for the request and send it back to the Queue which will send to nova-compute. The nova-compute will request the image data from the glance-API which will authenticate from keystone and sends it back to nova-compute. Then nova-compute will send a request from the neutron-server to get the networking data which will get the authentication first from keystone. Then the nova-compute will request the capacity volume of the storage of the virtual machine by sending a request to cinder-API which will again authorize it from the keystone and sends it back to nova-compute. The nova-compute after getting all data needed, it will request the Hypervisor to create the VM (virtual machine) according to the information it had. As shown in figure 3.

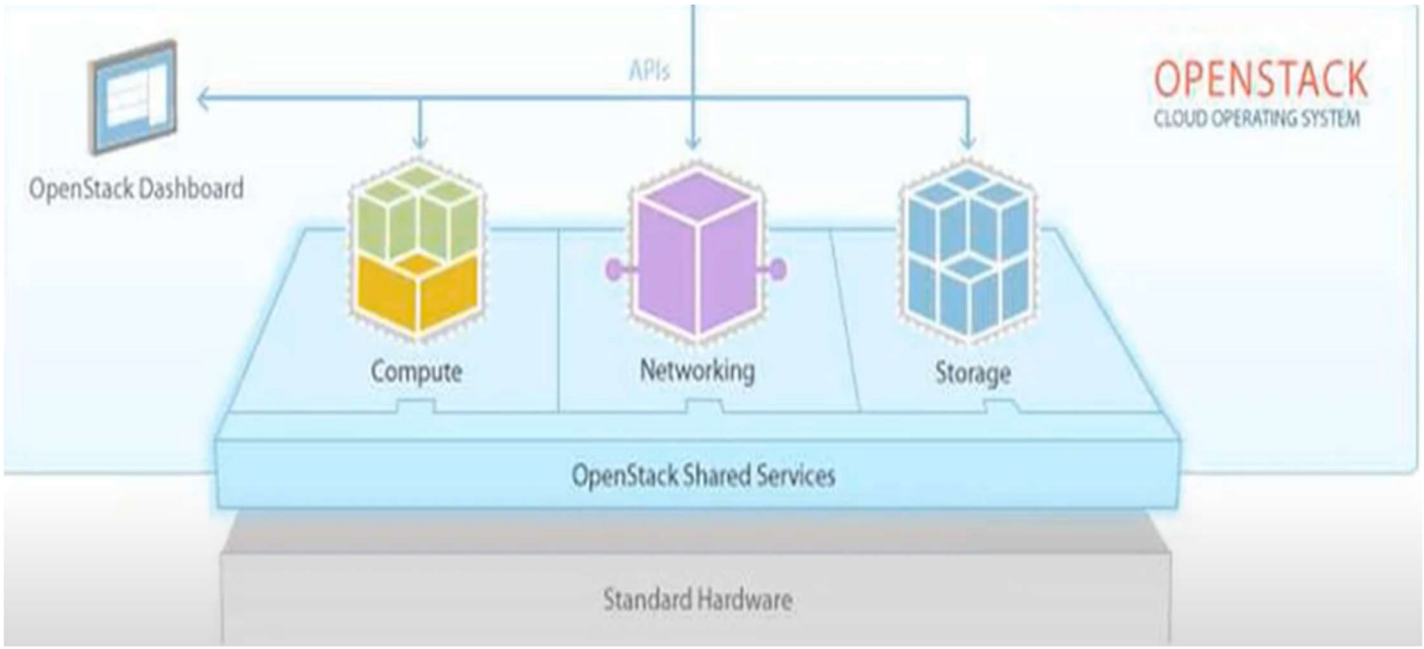

Figure 1 OpenStack

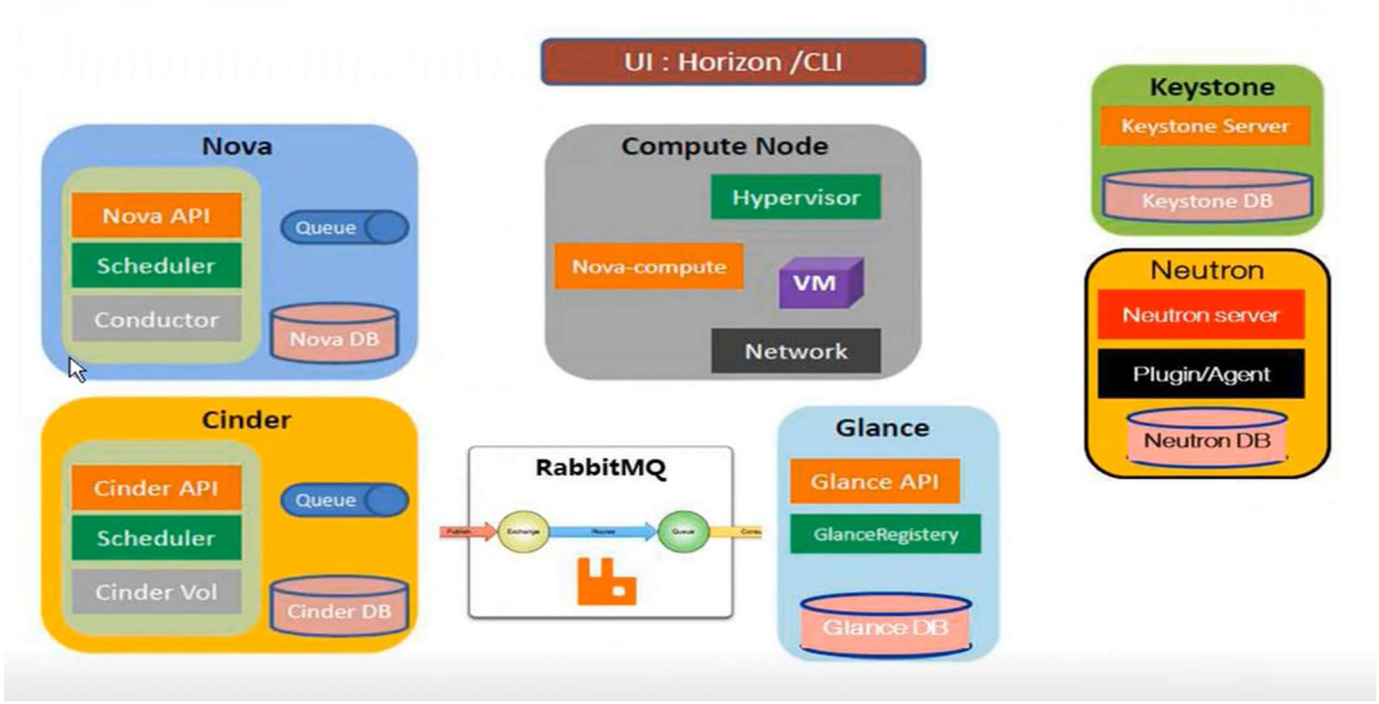

Figure 2 OpenStack compnents

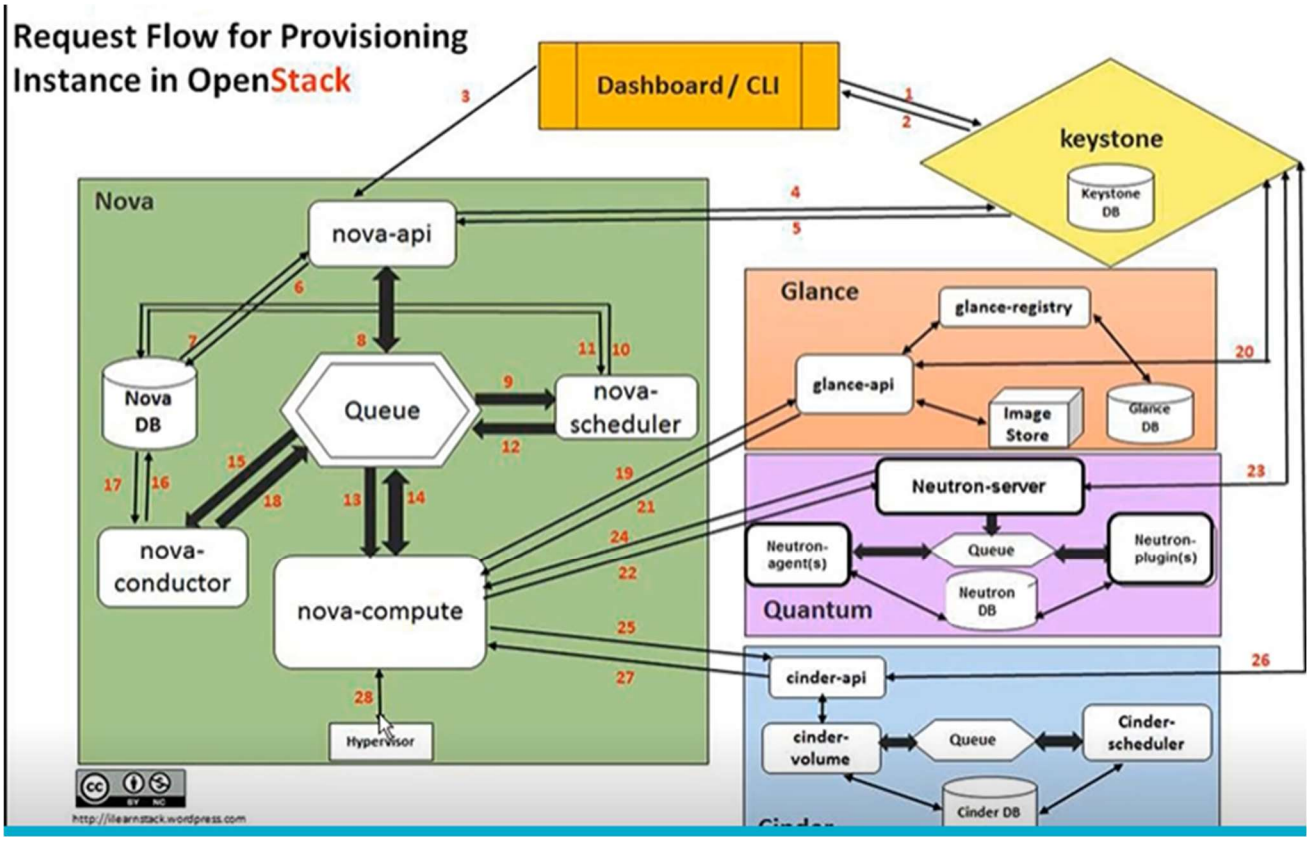

Figure 3Instructions to build a new OpenStack

2.2.2 SDN Controller:

The SDN Controller manages and controls VN (Virtual Networks) and NFV (Network Function Virtualization). It controls the routing between VNs and NFVs which runs on the VM and is attached to VN by using vRouters. An example of an SDN Controller is the Contrail that OBS uses. The Contrail has four main roles which are configuring nodes by hosting GUI (Graphical User Interface), controlling nodes by controlling the traffic between the SDN nodes more over it pushes the configuration towards the nodes, compute nodes which are the physical machine where the vRouters and VMs are running on, and the final is to analyses the traffic passes through the network elements. Contrail specifies to use of the BGP protocol for the traffic inside the pop and with external physical networks (SDN gateway) (MPLS/VPN) networks. Shown in figure 4.

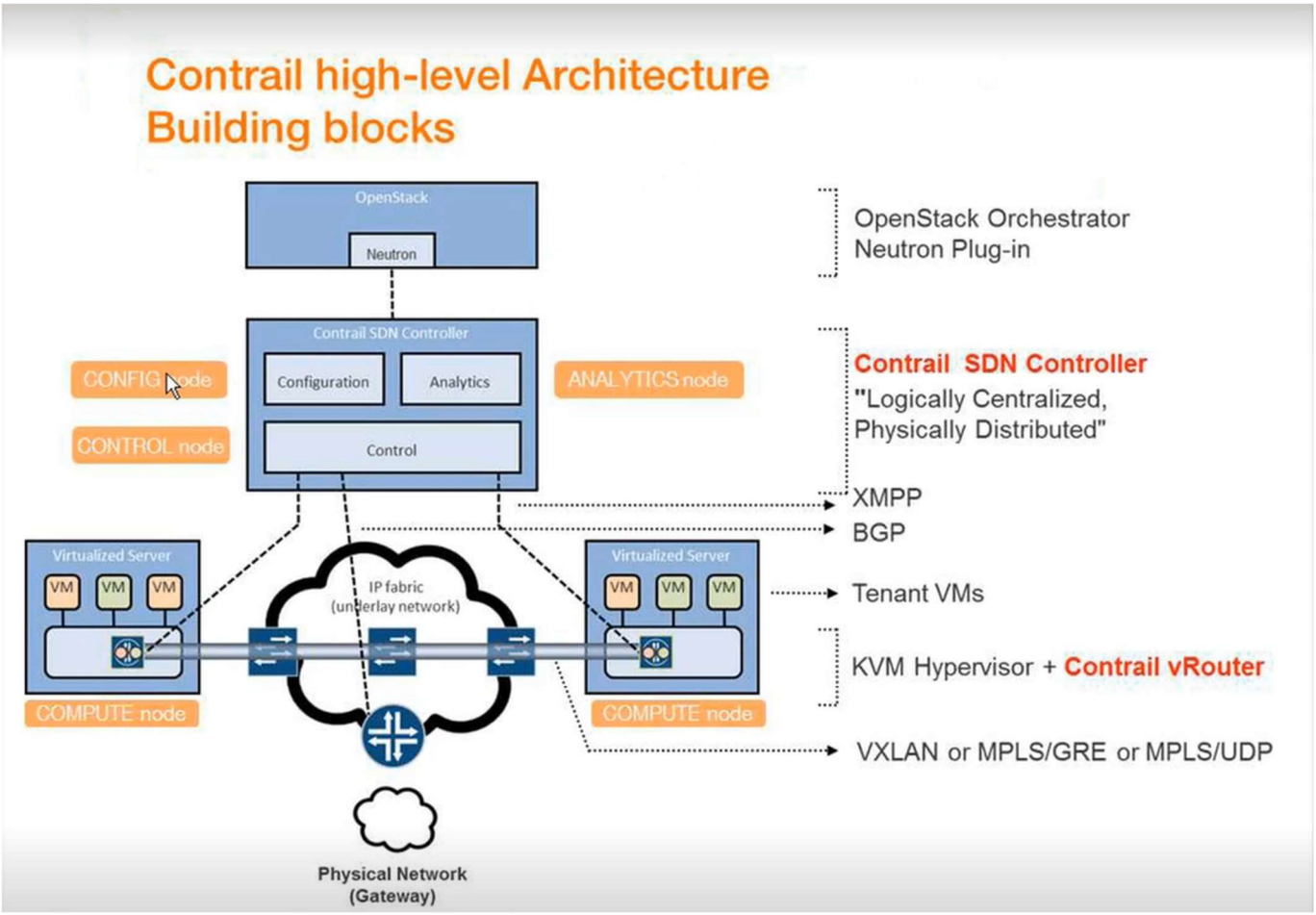

Figure 4 Contrail SDN controller

2.2.3 SDN POP Architecture:

SDN POP (Software Defined Network Point of Presence) Architecture is composed of two parts control zone and compute zone. The control zone is composed of several physical machines each running as a KVM (Kernal-Based Virtual machine).

KVM is an open-source technology that converts Linux into a hypervisor to be able to host virtual machines moreover it controls and switches traffic data between different VMS. The first KVM hosts the management virtual machine and acts as the director while the rest of the KVMS hosts four controlling VMS that controls the data traffic. The first VM is for the OSP controller which is part of OpenStack, the second is the contrail controller, the third is the contrail analytic engine and the final one is the contrail analytic database. The contrail controller, the contrail analytic, and the contrail analytic are part of Contrail Jupiter. The controlling KVMs work as redundant so if one of the KVMs went down the others can still do the controlling function (controlling traffic between different VMs). The KVMs are connected through a switch that is connected to a firewall which is connected to the compute zone.

The compute zone is composed of servers that host the virtual machines and again the first VM contains the management VM acting as the director. The rest servers of the compute zones have the compute servers that host the virtual machine built by the open stack. The switches that connect the Control zone and the Compute zone are connected to the SDN gateway to connect to outer VNs. The SDN POP architecture is shown in figure 5.

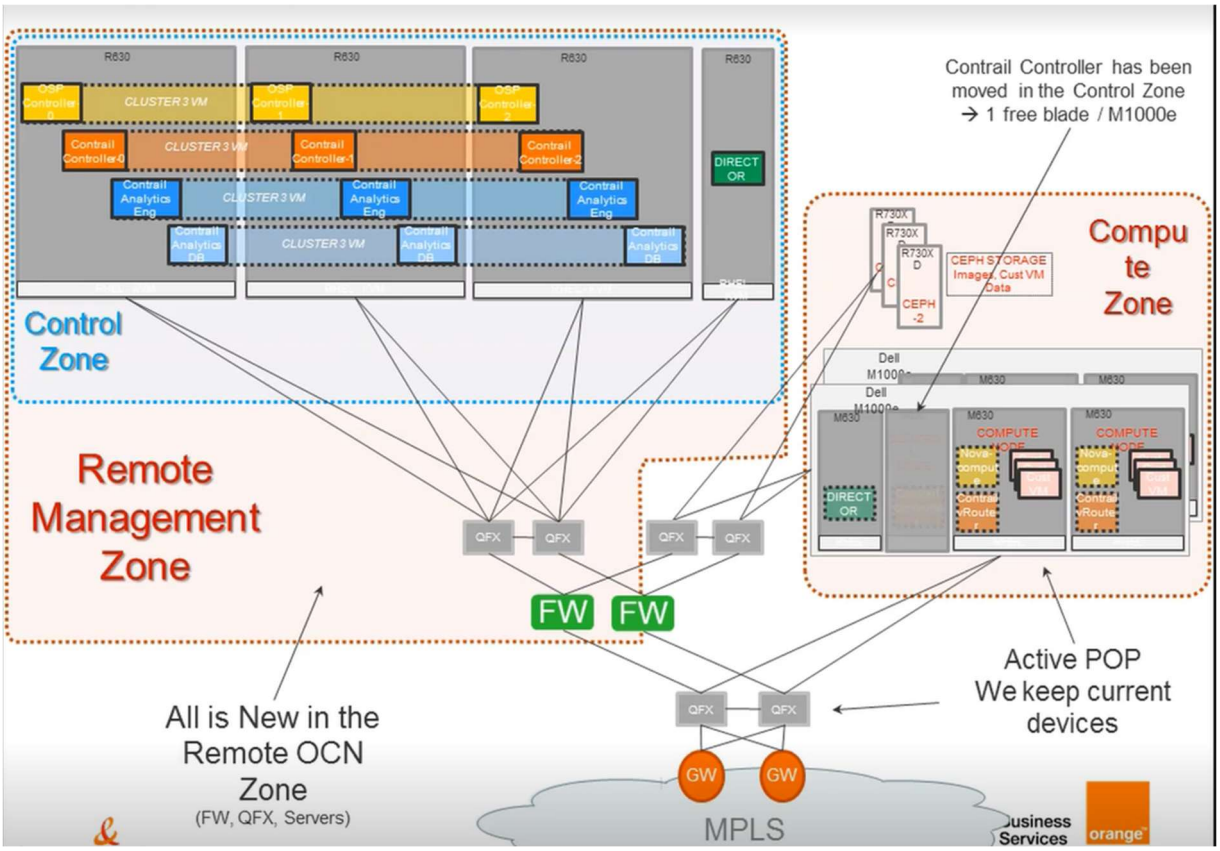

Figure 5 SDN POP

2.3 SDWAN:

2.3.1 Introduction to SDWAN:

To understand the idea of SDWAN, a quick review should be done on the traditional router and how it works. The traditional routers have three planes the management/policy plane, the control plane, and the data plane.

For example, OSPEF protocol and static route are reviewed for clarifying how the traditional routers work. The management plane is responsible for processing the configuration on the CLI or in the GUI and it sends it to the control plane also known as the decision plane.

When the control plane receives the routing protocol OSPEF that is on the control plane forms connections with neighbor routers and generates a neighbor table, then it receives the routing updates from its neighbors and forms a link state database table. On the link state database, the router performs its own OPSEF algorithm to calculate the best path toward the destination. The best path is placed on the IP routing table.

The static routes which are configured by the user on the management plane are installed directly onto the IP routing table. Once the IP routing table is ready it is shared with the data plane also known as the forwarding plane. The data plane adds the information of the physical interfaces of the next hope given by the control plane and creates a new table with that information called the forwarding table. Whenever a packet arrives at the router, the router determines the destination address from the header of the packet then processing is done by the forwarding table and the packet is sent to the next hop.

For the traditional network architecture, this local configuration is done on each router of the network configuring the same protocol moreover the same vendor, the same operating system, and the same applications needed to be used for each router. This processing and the network architecture are shown in the figures 6 and 7.

So, the processing in the traditional routers is done from the management plane to the control plane and then the data plane (from top to bottom). While in a switch the processing is done from the data plane to the control plane as a switch has only two planes the data plane which is the hardware of the physical ethernet port. So, whenever a device is connected to the ethernet the data plane and given to the control plane (the software of the switch) which performs a table with the ethernet port number and its corresponding mac address of the device which is connected to that ethernet port.

The basic idea of the SDWAN is to separate the control and management plane from the data plane and replace all the routers with switches that only know the physical interferences and

share it with the logically centralized control plane which is connected to all the switches in the network shown in the figure 8.

Although the switches are not smart as a router (because of the proccing in the router) but the switches are faster and cheaper than the routers. These switches will form the data plane. The connectivity between the control plane and the data plane will be known as the Application Programming Interface (API). By this, all the network operating systems will be removed, and applications will be lost as they don't have a run environment. So as a solution all the applications will be converted to control programs and will be moved to the control plane which will be kept in a virtual environment and stored in the cloud (control plane and management plane will be virtual functions connected to all the switches in the network) the basic architecture of the SDWAN architecture shown in the figure 9.

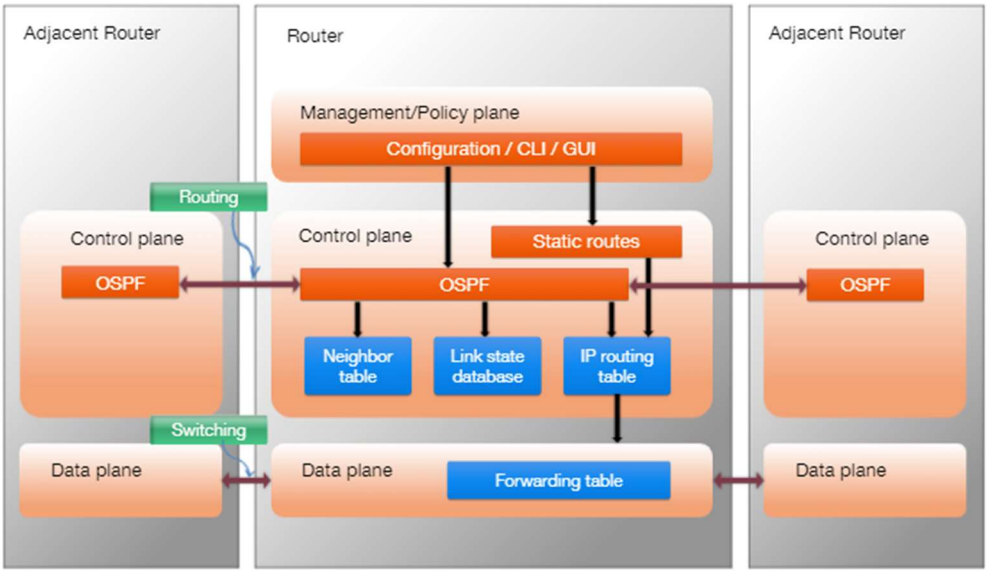

Figure 6 Tradditional Router

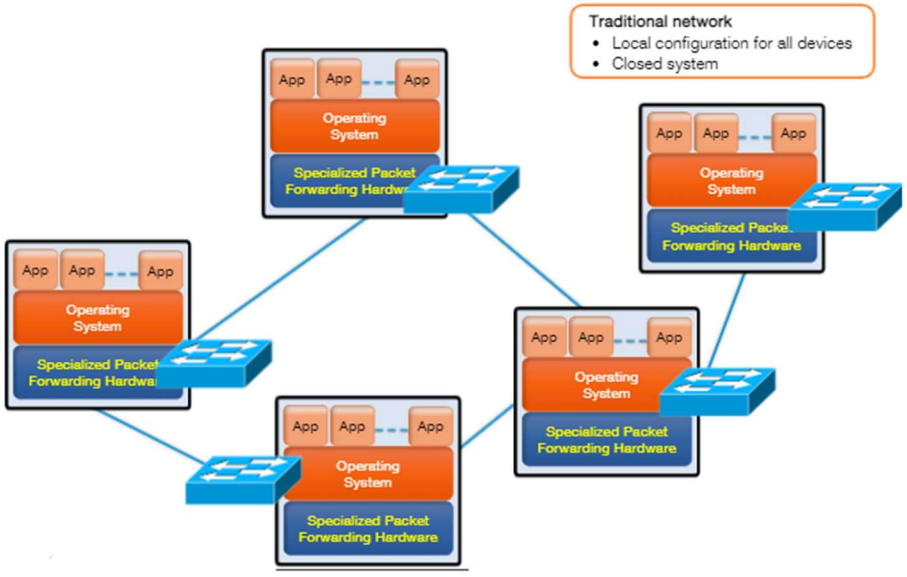

Figure 7 Traditional Network

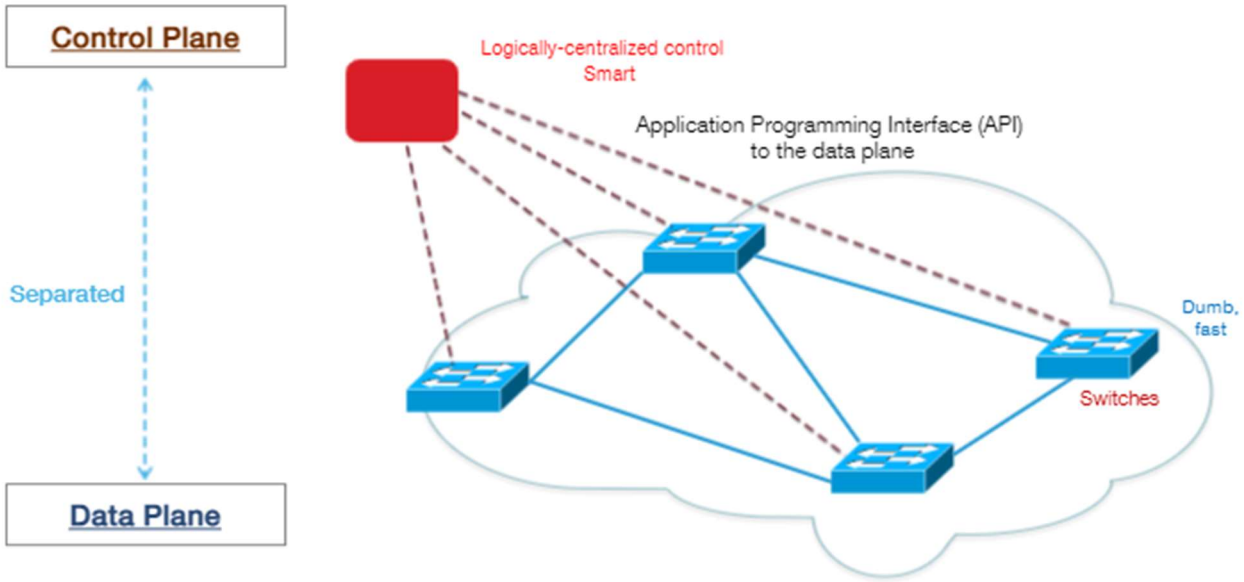

Figure 8 Basic concet of SDN

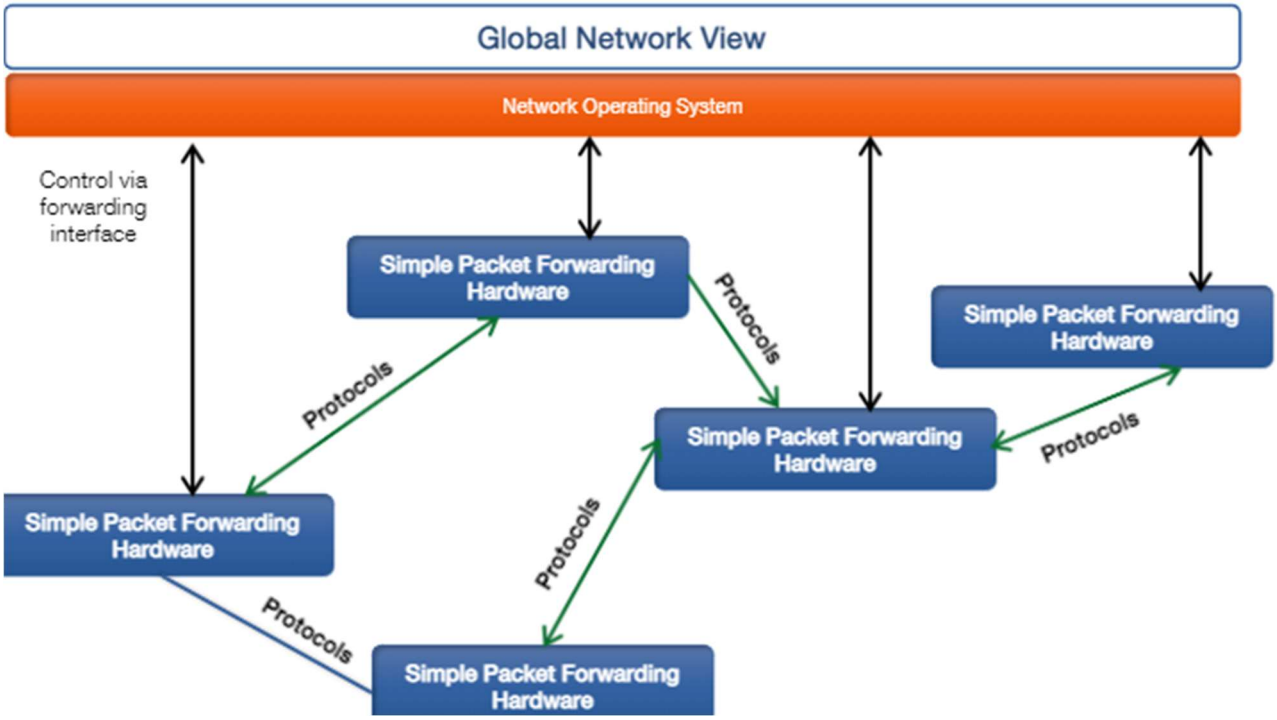

Figure 9 SDN

2.3.2 SDWAN Architecture and functions:

The SDWAN architecture is composed of three layers the management plane which configures the metrics of all the network and observes if a device is out of service or not, and the control plane which controls the traffic flow based on the metric provided by the management plane and the data plane which sends the data traffic between the nodes based on the information provided the control plane shown in figure 10.

There are many vendors that provide the SDWAN solution having the same three-layer model here the Cisco model Viptela model is represented. The first layer which the data plane which contains the vEdge routers, the vEdge router is the WAN edge router of a site (campus, data center or a cloud or etc..), where it can be a physical hardware device, or virtual software The vEdge acts as a traditional router as it can run traditional routing protocols such as (BGB, OSPF, etc..) for local networks and also it runs SDWAN protocol which is a highly secure protocol (OMP) to connect with the control plane. It also supports the zero-touch deployment.

The connectivity is independent of the transport of the data using (the internet, MPLS, and 4G/LTE) the Viptela rides on top of the under-relay network. The second layer which is the control plane contains two main functions of the network which are the vSmart controllers and the vBond. The vSmart controllers are the centralized brain of the SDWAN solution as it controls the data traffic throughout the overlay network. It runs as a virtual machine on a network server or as containers in a virtual container host. It also implements the control plane policies, such as the service chaining and multi-hop. Moreover, it controls the Bidirectional Forwarding Detection (BFD) or forward detection between vEdges and orchestrates secure data plane connectivity between the vEdges.

The control plane in Viptela contains another main function which is the vBond which orchestrates the connectivity, and it is the first point of authentication. It requires public IP Address. All the components in the network should have the information of the IP address of the vBond or the DNS information. It authorizes all control connections (the white-list model). It distributes the list of the vSmarts and the vManage controllers to all the vEdges. It helps in load balancing of vSmart controllers.

The third layer is the management plane which contains the vManage and the vAnalytic. The vManage is the network management system (NMS). The vManage monitors if any of the devices are down and assists in troubleshooting issues by collecting information and alerts. The vManage is the location to build the configuration templates for vEdges and overlay traffic engineering policies. On the management plane as mentioned there is another main function which is the vAnalytic which provides in-depth visibility of different applications. Moreover, provides metrics for different services and entire infrastructure. The Viptela network architecture is shown in the figures 10 and 11.

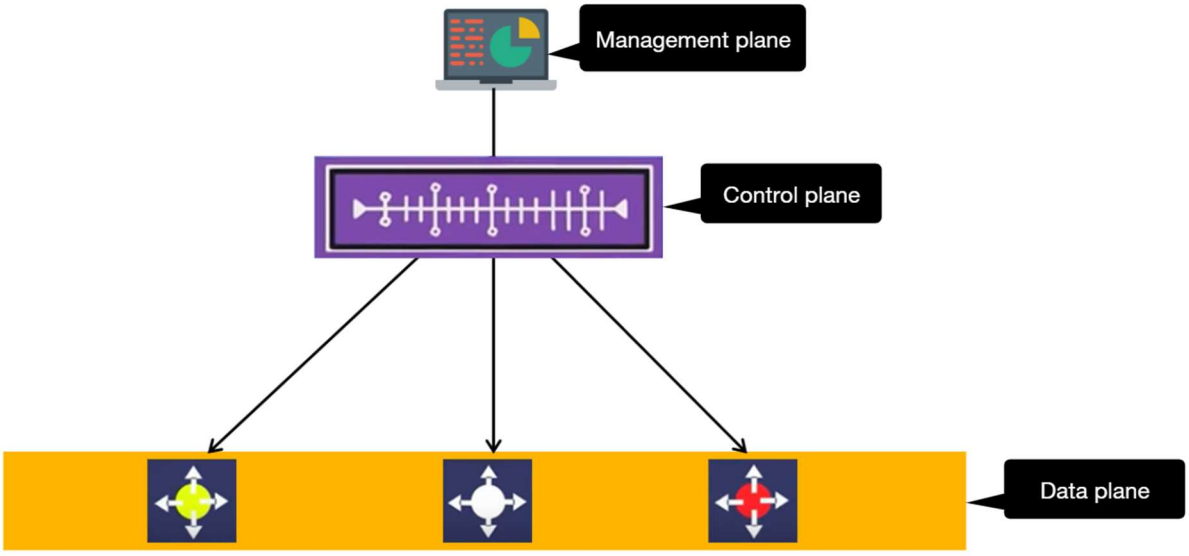

Figure 10 SDWAN

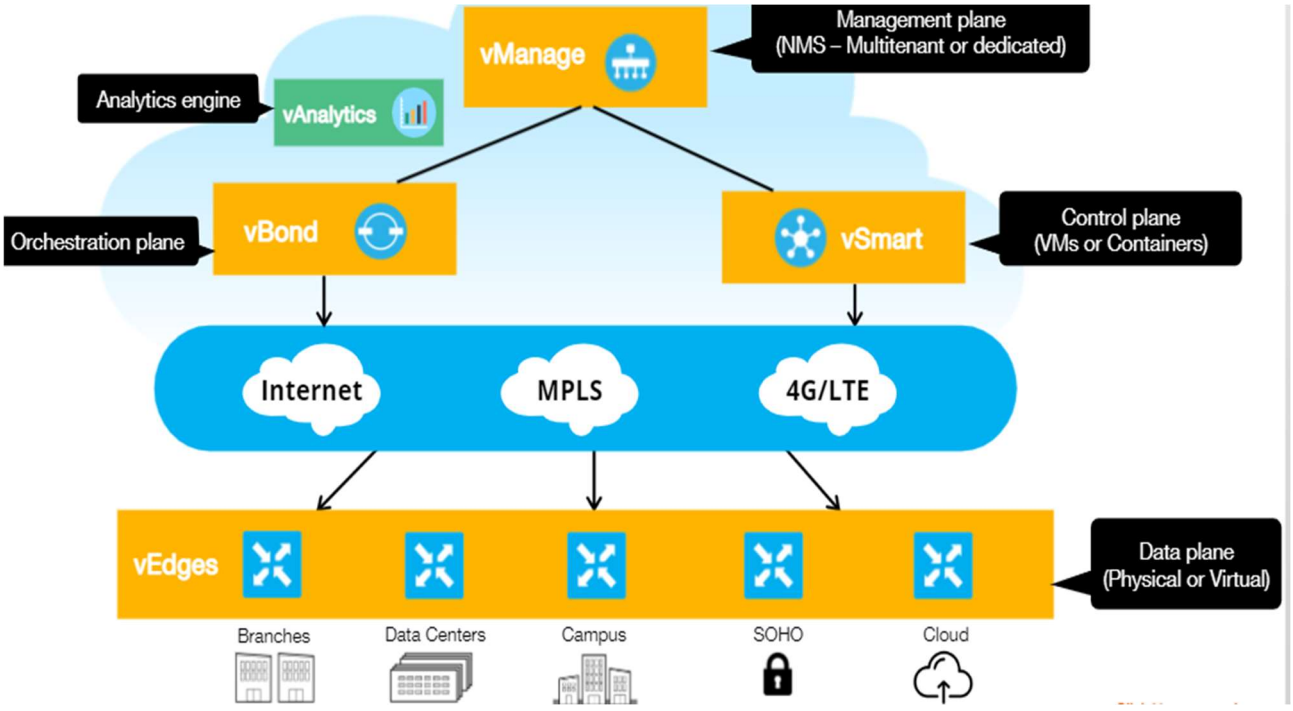

Figure 11 Viptela model

2.3.3 SDWAN connectivity:

The SDWAN connectivity is highly secured, where a set of authentications should be done on the controlling elements (vSmart Controller, vManage, and vBond Orchestrator). First, the controlling elements generate two keys a private key and a public key. The privet key is kept inside the control element while the public is shared to a server called Symantec. Symantec server is a server from the Viptela model which signs the certification through Root CA and then pushes it back to the controller. Now the controller element has a root CA trust chain for Avent Root CA, shown in figure 12.

After the certification is done through all the controller elements, the controller elements share their certificates with the other two controllers and verify their certificates. The vBond validates the vSmart certificate and the vManage certificate serial numbers through an authorized list available then the vSmart and the vManage validate the vBond certificate and organization name against the pre-configuration it has. If the validation is Two-way SSL authentication (Secure Sockets Layer) then a permanent DTLS/TLS connection (Datagram Transport Layer/The Transport Layer Security) is formed between the vSmart, vBond, and the vManage. If the validation between nodes is One-way SSL authentication, then a temporary DTLS/TLS connection will be formed between the controlling elements shown in figure 13.

When a new vEdge enters the network, it first has a certificate from the Symantec server after that it has a session connection with vBond by having its IP address in the pre-configuration. Then it has an authentication from vBond through the whitelist (The whitelist is a list done by network administrators on the vBond inserting the serial number of the vEdges that will join the network corresponding by a unique ID number given by network administrator so when a new vEdge is connected to network vBond checks its serial number if it is in the whitelist, then it verifies it). vBond also capable to authenticate the AVNET of the vEdge. Once the verification and the certification are done the vBond shares the IP addresses of the vSmart and the vManage shown in figure 14. Then two permanent DTLS7TLS tunnel is formed between vEdge with vSmart and vManage while the connection between vBond and vEdge breaks down as the function of the vBond is done and the connection is not needed anymore shown in figure 15.

vEdges are connected to vSmart and vManage using OMP (Overlay Management Protocol) which is an SDWAN protocol that runs by default on all SDWAN nodes which through the control plane provides the forwarding table, routing policy, and the management to the vEdges. The vEdges are connected to each other through IPsec tunnels which have segments over VPN therefore the routing is segmented and the connection between vEdges is highly secured shown in figure 16.

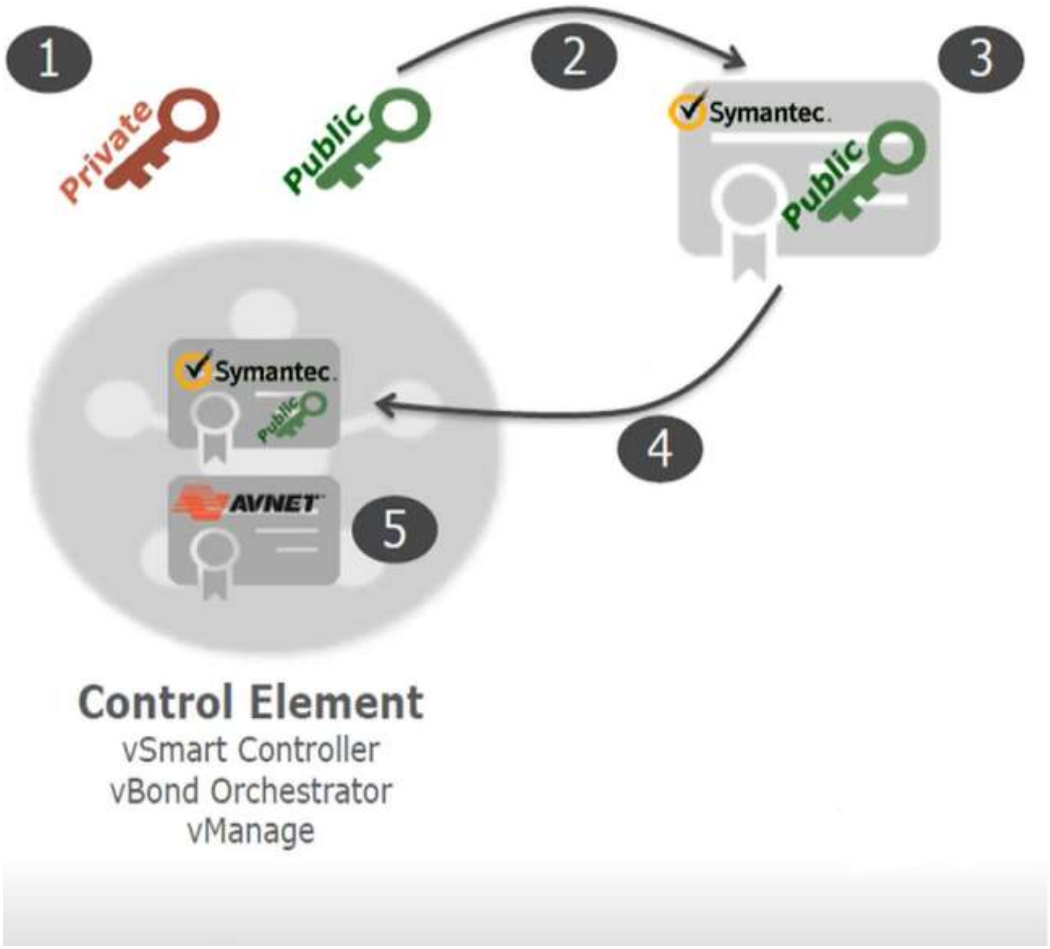

Figure 12 Viptela authentications

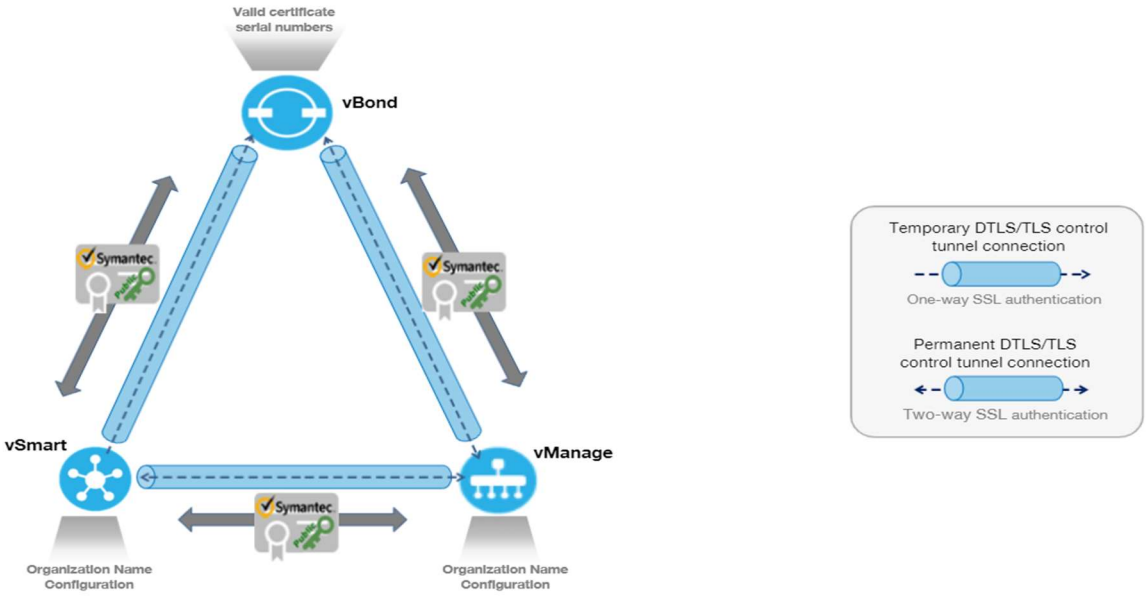

Figure 13 Viptela validation

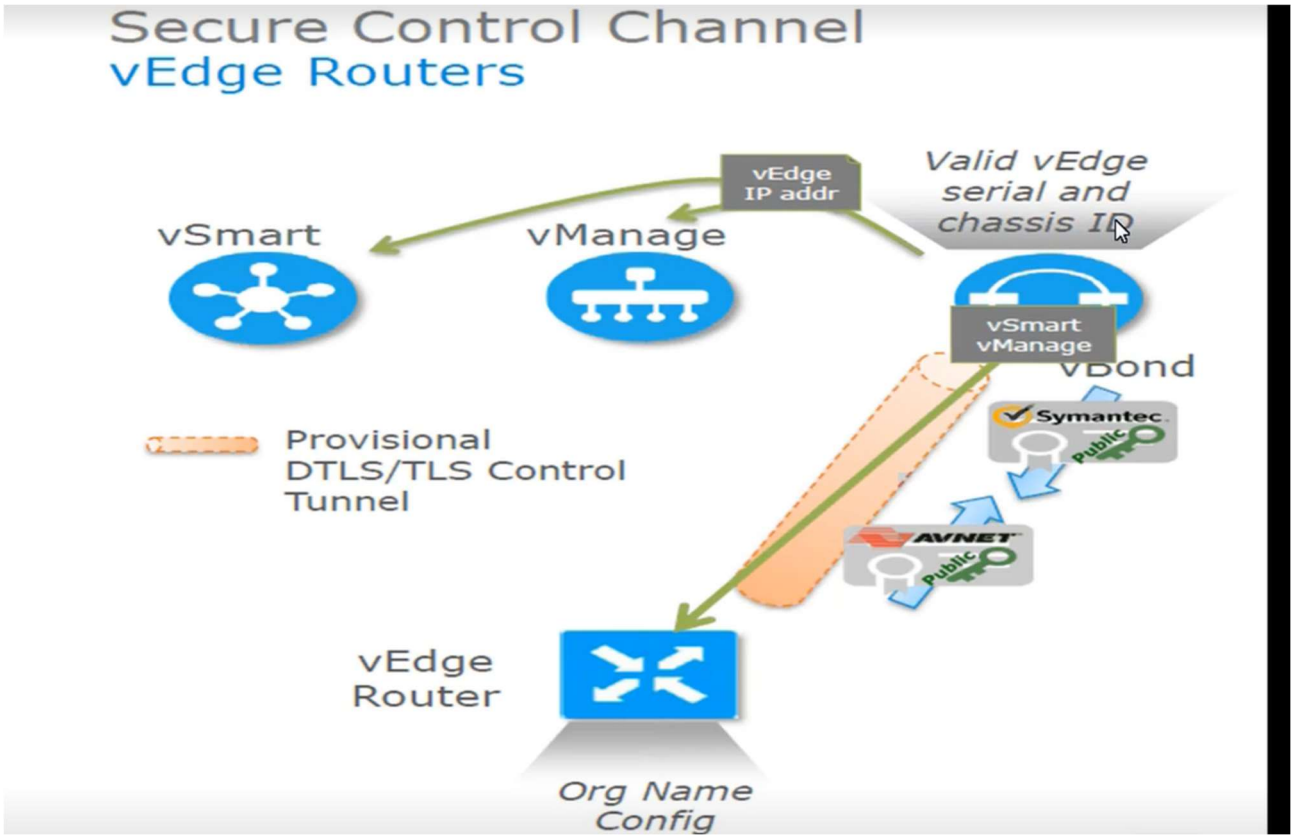

Figure 14 Vedges authentications

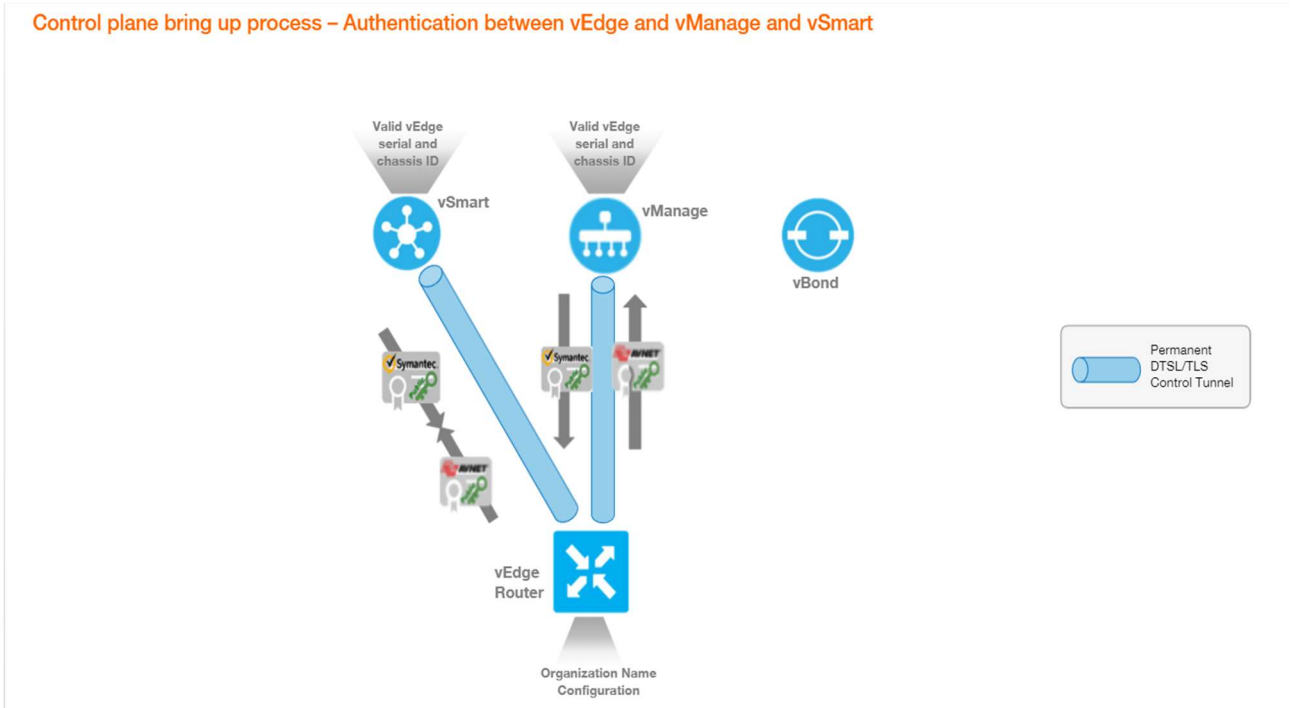

Figure 15 Conectivity between control plane and data plane

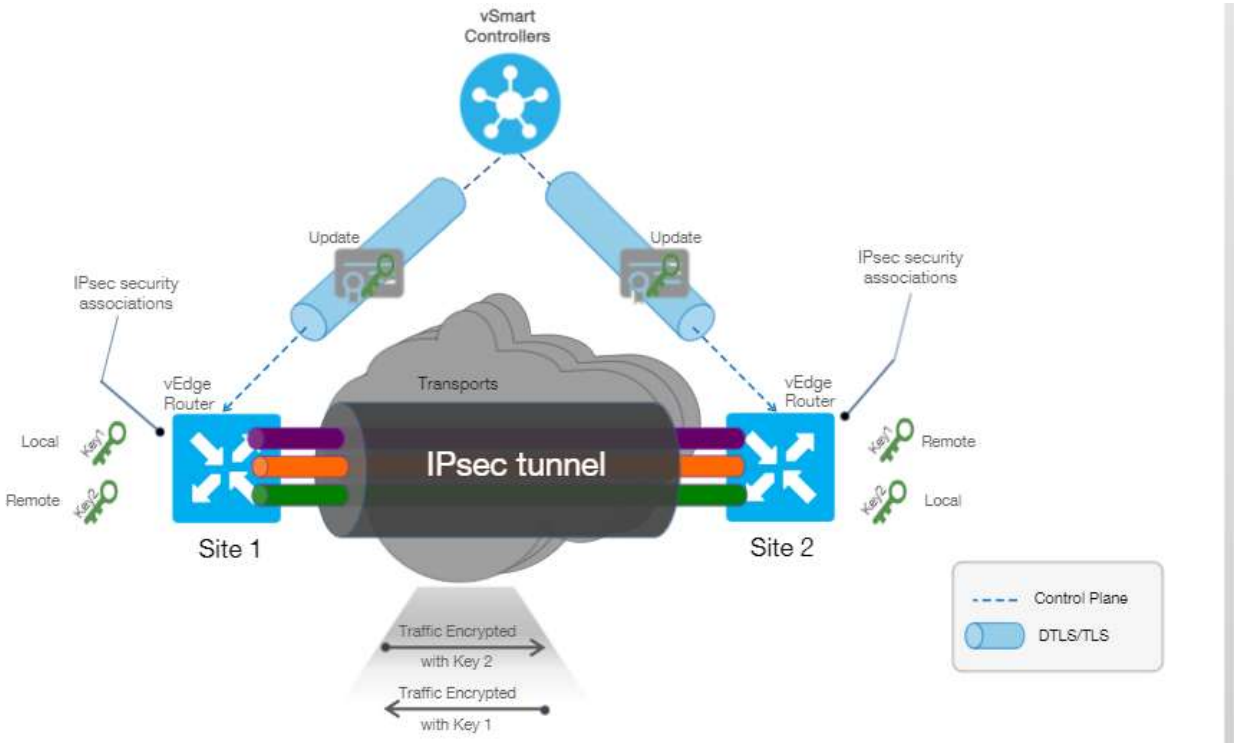

Figure 16 SDWAN Viptela connectivity

2.3.4 SDWAN applied by Orange OBS:

Orange is a service provider as known that provides cloud services and network services for Orange customers. Customers of Orange are connected to the Orange network either through Orange private Network IGN (IP Global Network) which is a VPN MPLS network that uses the BGB protocol, or they are connected to Orange through the internet using the OMP protocol.

The same customer may have sites that are connected to IGN and other sites connected to the internet. Orange had an infrastructure zone hosting SD-WAN Control Plane Elements (EMS) (vSmart, vAnalitic, vBond, and vManage) which connected over a cloud called OCN. The OCN is surrounded by several firewalls providing extra security. The vSmart and the vManage are connected to vEdges that are connected to the internet and use the SD-WAN OMP protocol.

For customers who use the SDN services but some of their sites are connected to the IGN they can still be connected to the vEdges using SDN through Orange SDN POP. Orange Built an SDN POP which hosts a SDN Gate Way which is connected to the OCN. The SDN POP introduces some delay as it connects different sites that uses different protocols (BGB and OMP) as it converts between the two protocols. Orange SDN pop connected to OCN shown in figure 17. Orange architecture is shown in figure 18.

Z

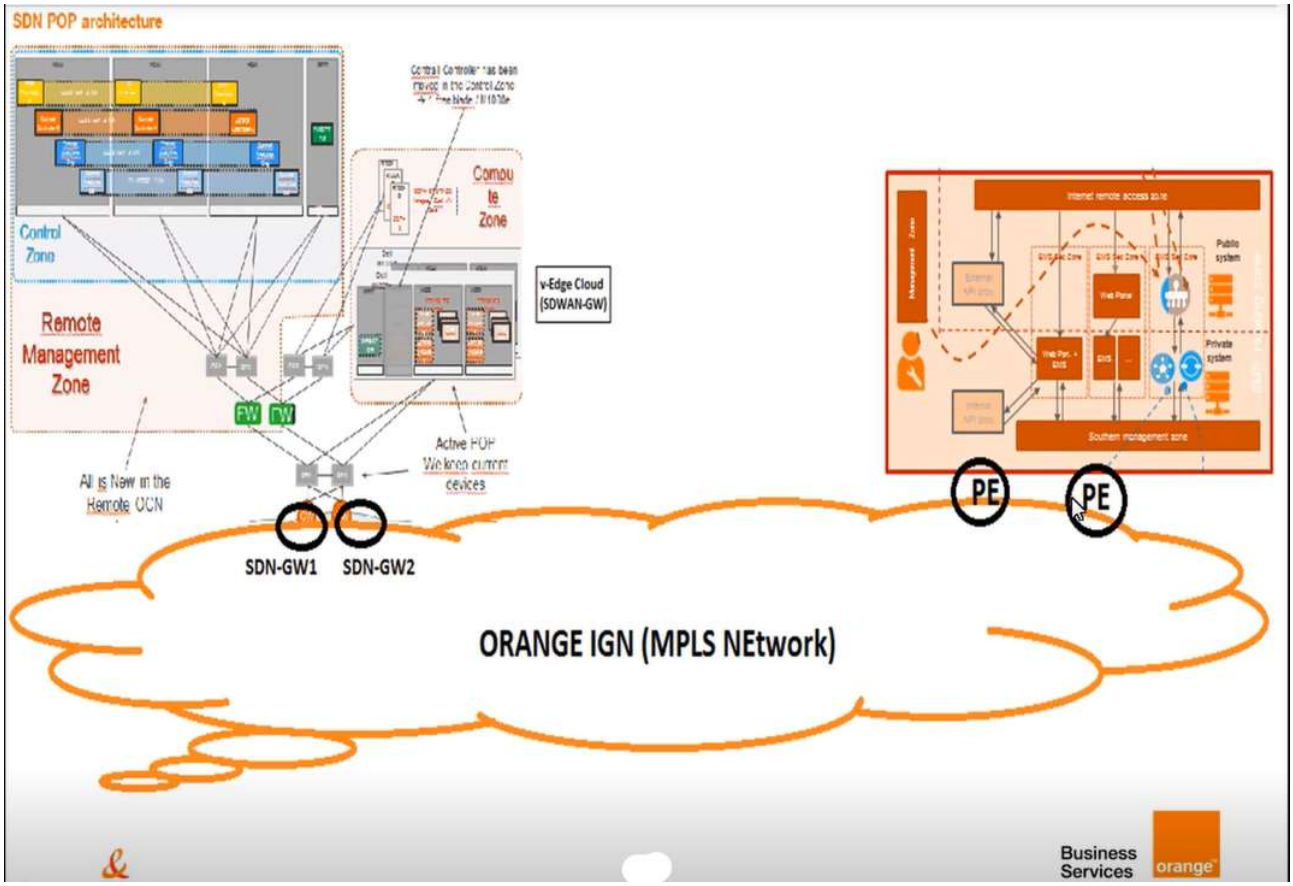

Figure 17 OBS using SDN POP and SDWAN

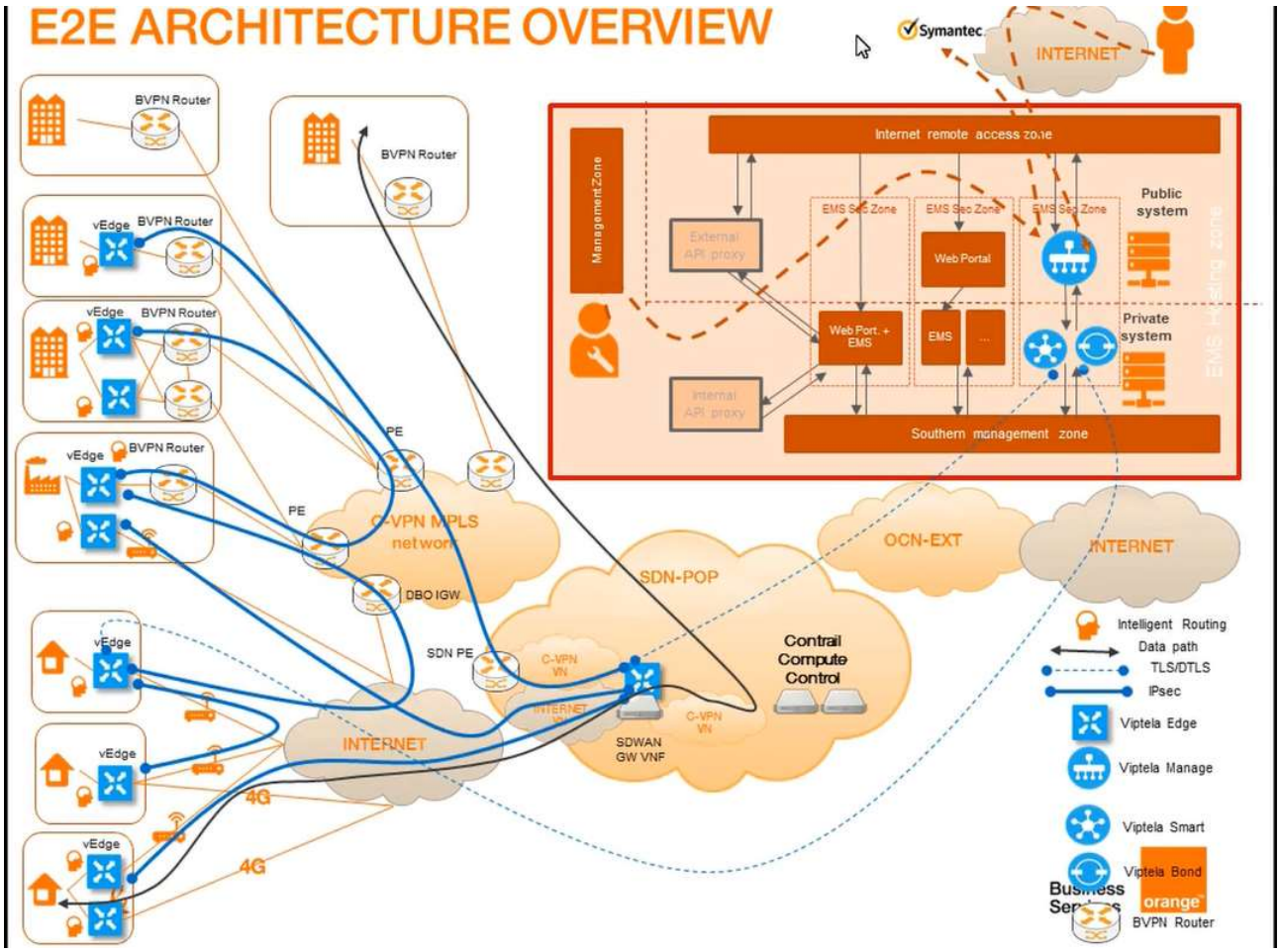

Figure 18 OBS IGN Architecture

3 SIP (Session Initiation Protocol):

3.1 What is SIP:

Session Initiation Protocol is a protocol that is used for voice calls over IP (VoIP). The SIP packet structure is the same as the IP (Internet Protocol) protocol, instead of depending on the multiplexing and demultiplexing physical techniques such as (TDM, FDM, OFDM, and CDM) it depends on packet switching (IP Packet) using IP addresses.

3.2 SIP Call Flow and SIP Functions:

A SIP user can have a SIP call by using the IP address of the destination user then the call is forwarded to the destination through routing protocols the same way as IP. When the other user accepts the call both users can exchange media. But what if the user doesn't have the destination IP address, the call can still go on through several SIP functions.

The first SIP function is the Registration services which function is to register each user who logs in to the network by creating a table with each address of record (email@orange.com) corresponding with the IP address in the SIP Registry. So, when the user calls another user using the address of record the call is forwarded to another function called the Location service which function to access the SIP Registry to get the destination IP address and forward the call to the destination, and when the destination accepts the IP addresses are shared to the two users and next SIP call the location service is not needed. The Location Service, the Registration Service, and the SIP Registry are installed on a server called Proxy.

All features of a call center such as (call forward to, conference call, redirect, etc.) are installed in a feature server so that any feature can be updated easily by replacing its server with the new updated server, moreover, adding a new feature can be added easily by adding a new server and configuring the routing rules. A SIP user can call another user from another domain (another private network) by using DNS the same as IP, but each private network uses a certain device on its edge layer called SBC (Session Border Controller) which protects its network.

The SBC does not only control the IP packets it is also able to modify the IP packet by saving the source IP address (internal IP address) and replacing it with an external IP address to protect network devices from malicious users and making it non-traceable when the SBC receives the response with the IP address that the SBC added it convert it back to the original IP address so it can be mapped in the network. SBC can detect attacks like denial of service and drop those packets.

The SBC is not a router it doesn't work on level 3 (routing layer in the OSI model) it works on the application level. A SIP user can still communicate with non-SIP users of other technologies such as (traditional landline telephones on the PSTN and telecommunication mobile phones) by using a signaling gateway and media gateway. The signaling gateway is a signaling protocol translator which converts the SIP protocol to any other protocol (depending on the other side) and vice versa. While the media gateway transcodes media from one form to the other, which leads to that media is compatible with the other protocol that the signaling gateway had translated.

3.3 Call setup:

To set up a SIP call, the SIP protocol uses the same mythology of the three-way handshake in TCP but instead seven specific packets (messages) should be exchanged between the two users. The caller sends an invite packet to the other user then he receives packets called 100 Trying these packets corresponds to the signaling through the network nodes searching for the destination, once the destination was found the caller receives another set of packets called 180 Ringing corresponds that it is ringing on the destination side (receiver) once the receiver accepts the call the caller receives a packet called 200 OK (to INVITE) then the caller sends an acknowledgment packet (ACK). After this stage, both users can exchange media then when they finish the call the user who ends the call sends a packet called BYE and receives another packet called 200 OK (to BYE) shown in Figure 19.

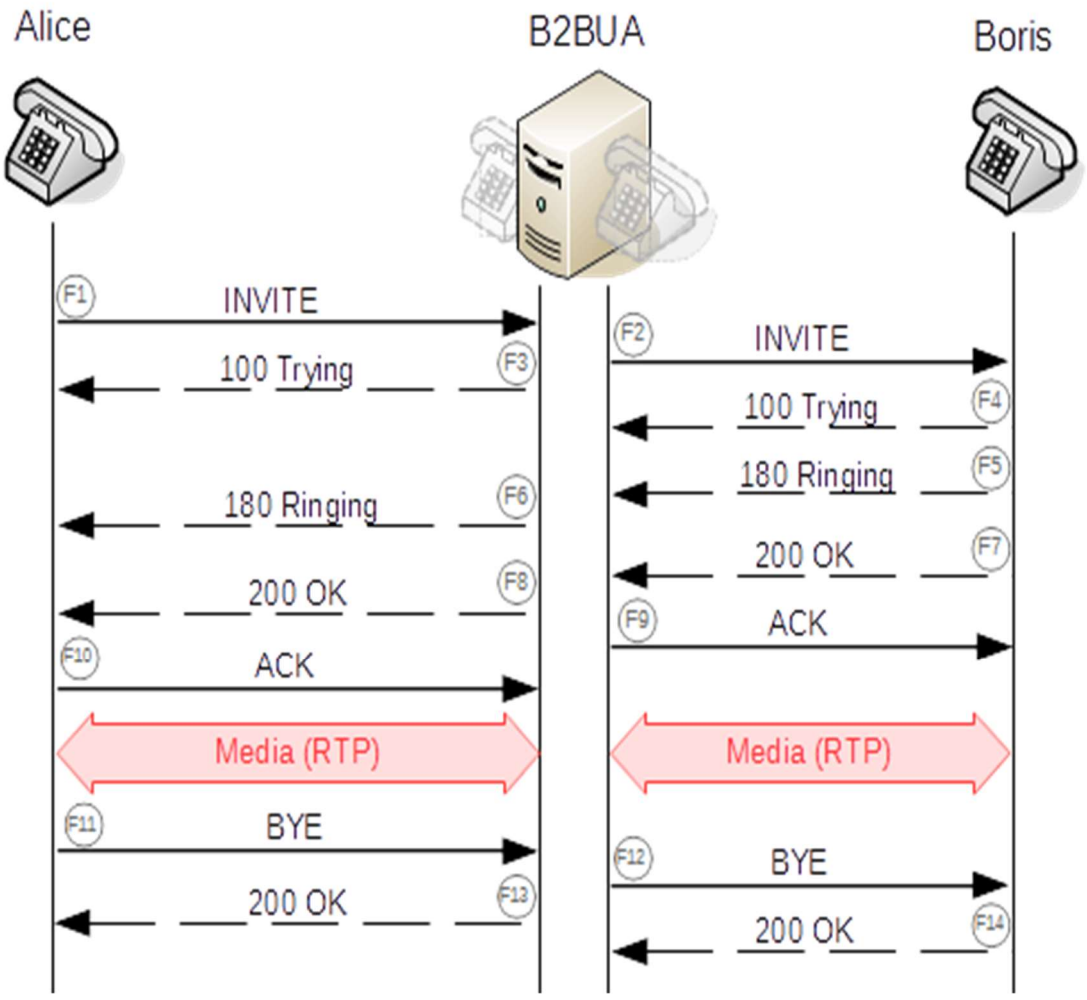

Figure 19 SIP packets

4 Current OBS Network Architecture:

4.1 Network functions and core connection:

OBS has its worldwide IP network called IGN which is the backbone of the voice network. OBS uses both IP protocol and SIP protocol for its IP network and voice network. Above all OBS networks, OBS uses an application server (AS) that runs all the applications that serve the networks, and it is the brain of OBS. One of the main applications running on the AS is Hookah which controls all the Incoming and Outgoing traffic. OBS uses an edge router connecting OBS to each carrier and customer called PE (Provider Edge Routing) All OBS voice networks are shown in Figures 22 and 23.

4.1.1 legacy network (NEO):

OBS had an old network called NEO (Next gEneration vOice) for voice traffic which almost migrated this network is used to connect carriers that use both SIP and TDM and customers that use TDM. NEO used RMG (remote media gateway) on the access layer that collects data from customers and carries that using TDM and converts TDM to IP packet and vice versa. While for the SIP carriers NEO used an SBC on the access layer. In the core layer, NEO uses OPM (Optical Peripheral Module) which is a TDM switch connected to RMG and VTCH (Virtual Terminal Call Handler) which handles the routing of the call connected to the SBC, and its function is to route the traffic to its correct path. OPM and VTCH are then connected to the AS. NEO architecture shown in figure 20

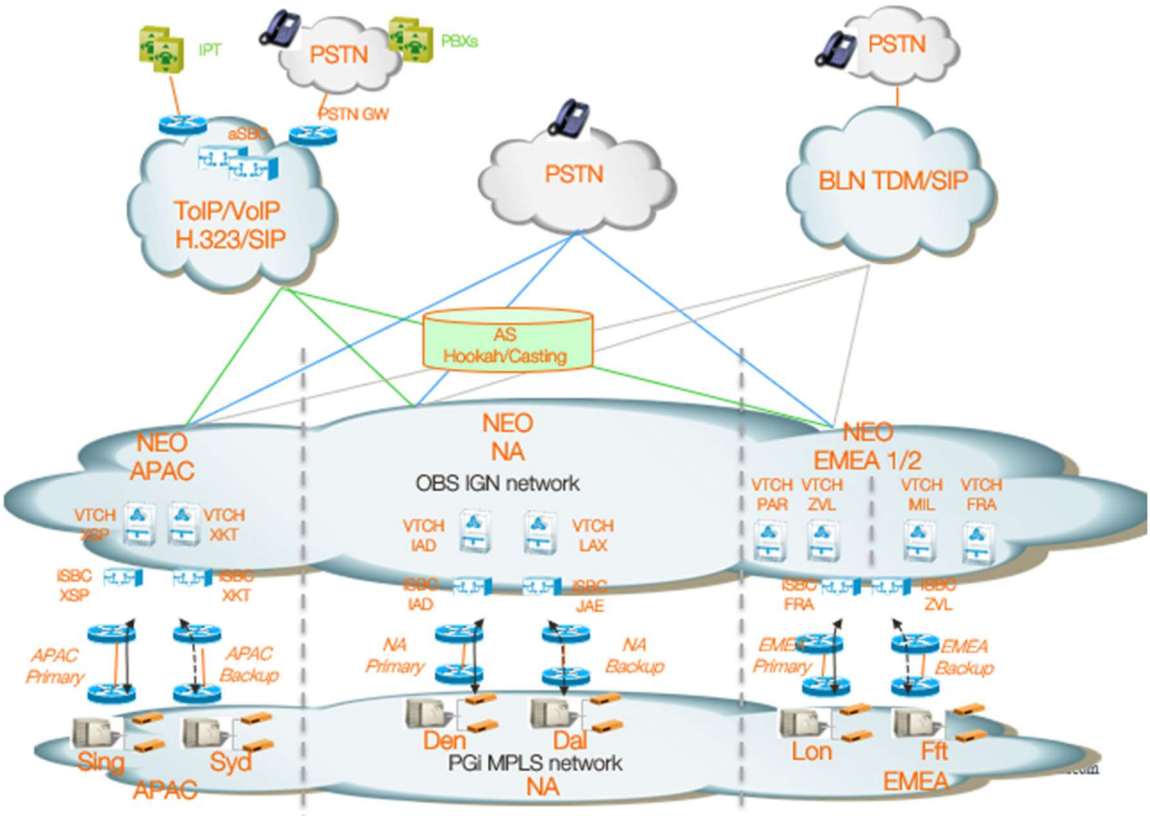

Figure 20 NEO

4.1.2 The new network (NBI):

NEO network is almost migrated to a new network called NBI (New Border Infrastructure) which only connected to carriers that use SIP on the access layer NBI uses SBC and in the core layer NBI uses PSX (Polices Server Exchange) which function is having all policy rules, routing logic and policy server, PSX acts as a SIP PROXI and providing configurations of the other network (SIP Trunking) on the SBC, and it is hosted on the IGN network. The NBI architecture shown in figure 21.

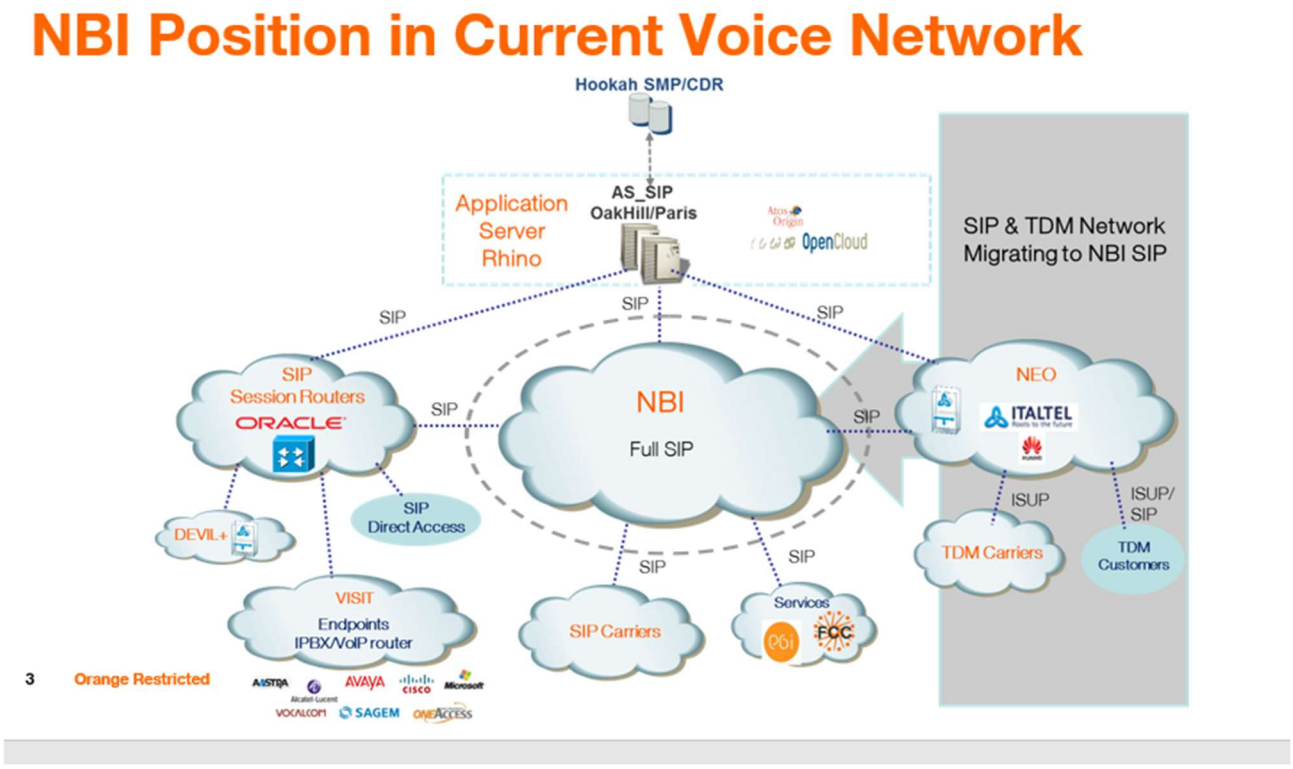

Figure 21 NBI

4.1.3 SIP Trunking:

SIP Trunking is an independent network that is connected to the customer providing the extra security of the data for OBS customers. SIP Trunking uses SBC in the access layer which performs security by hiding the topology and access and control while the core layer uses SR (Session Router) for the call routing and distribution, The SR manages the dynamic and real-time routing for each session for multiple sources and destinations within a highly distributed architecture. The SR routes control for SIP-based voice, video, instant messaging, and multimedia, which increase OBS efficiency services for customers more over the SR provides extra security features for the customers.

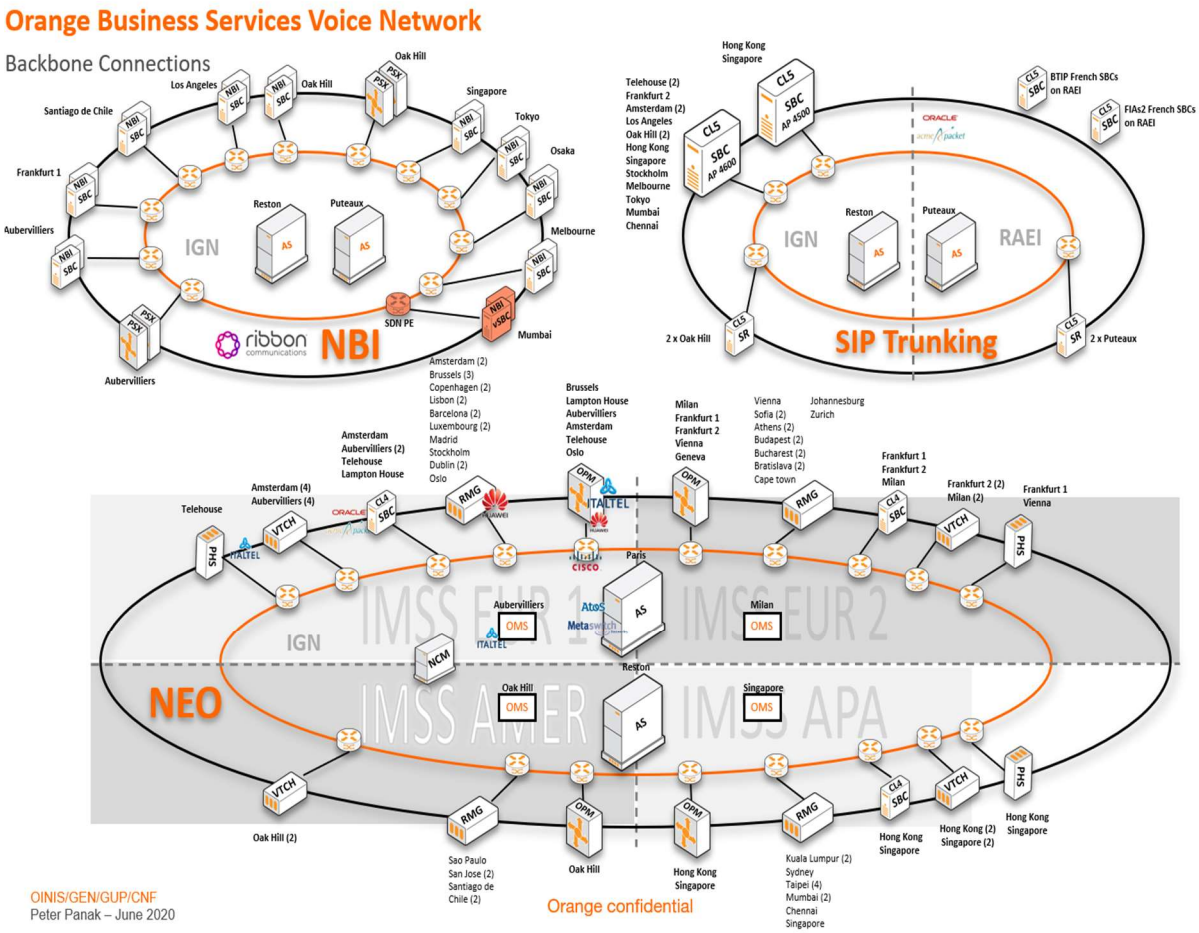

Figure 22 OBS Voice Networks

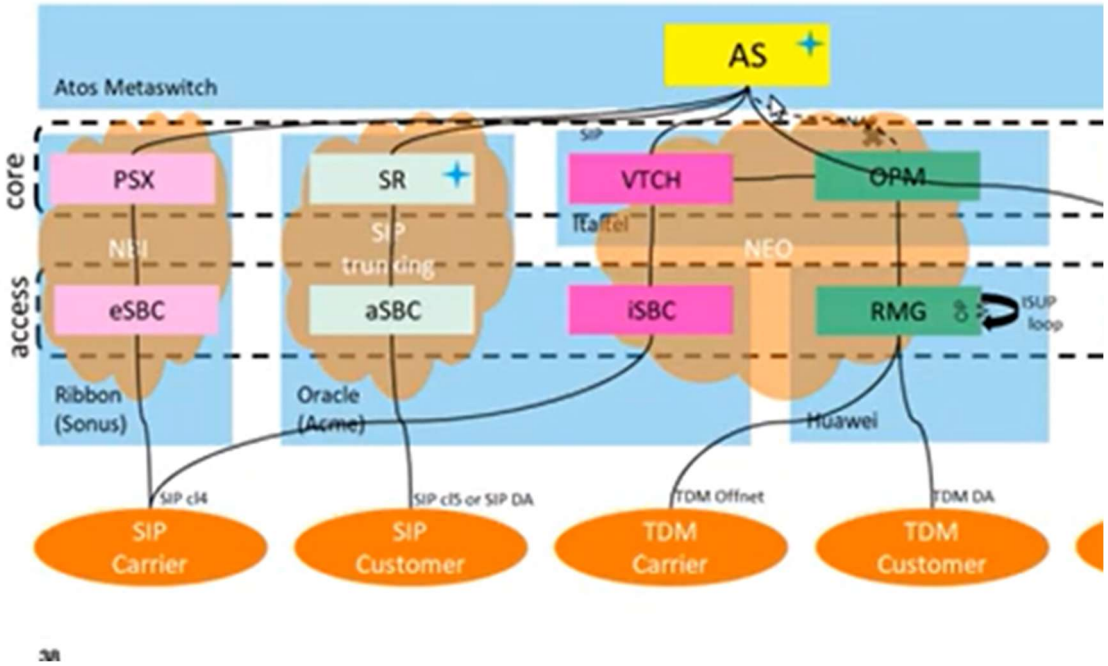

Figure 23 OBS Networks theory

4.2 Other networks connectivity:

4.2.1 Carrier connection:

OBS is connected to at least one carrier in each country where OBS provides its services in. For some countries, OBS is connected to the main carrier of the country. The carrier collects the data for OBS. This data is for voice services and internet services (IP services). Since we are interested in voice services the main concept is that the carrier assigns some numbers to OBS, when the carrier receives a call with a number that is assigned to OBS the call is forwarded to the OBS network (NBI).

OBS is connected to carries that use only SIP protocol so either the carrier converts data from TDM to SIP or for some countries, OBS is connected to an intermediate carrier that its job is to convert the data from TDM to SIP for carriers that use only TDM or any other protocol, then forward it to OBS. OBS is connected to the carrier as it is shown in Figure 24. Where two main PE are connected to the carrier with a mesh topology using a load balanced scenario. These two PEs are connected to our backbone network through the two SBCs in the access layer which controls the traffic and forwards it to its right path.

The PEs acts as a backup for each other. The traffic that passes through the link between the PE and the carrier is monitored by OBS offices so that it shouldn't exceed 50% of the capacity of the link. As if one SBC or PE went down for any technical issue, OBS doesn't have any loss in the traffic as if the data exceeded 50% and the connection was lost for any reason some of the data will be lost. As all the traffic would go through the other link so the capacity won't maintain all the traffic shown in Figure 25. By this, the data is collected to OBS providing services for the customer reviewed in the next section.

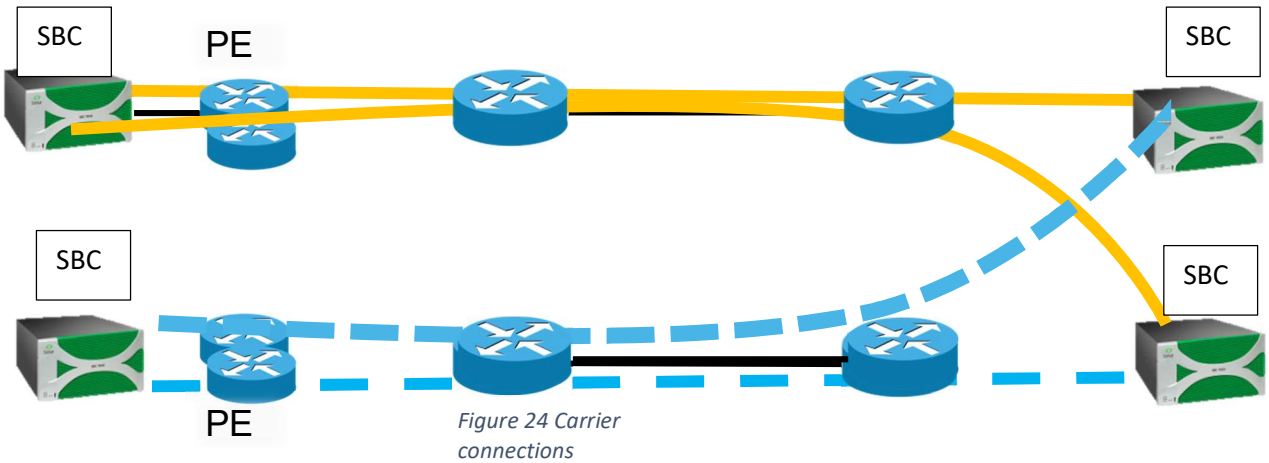

Figure 24 Carrier connections

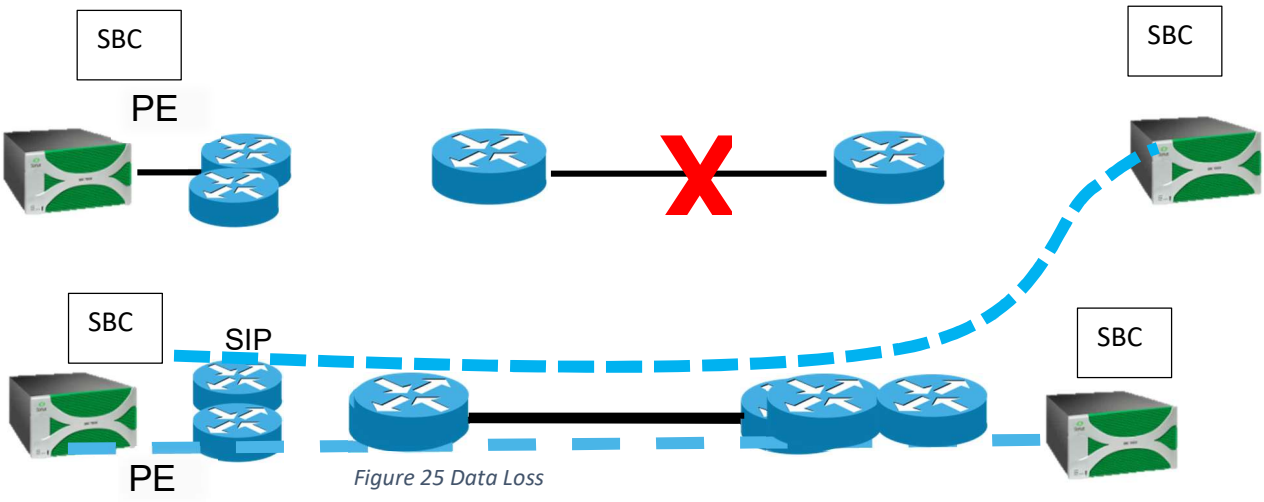

Figure 25 Data Loss

4..2.2 Customer Connection and call Flow:

After OBS collects all the incoming calls from the users through the carrier OBS adds routing features to the call and forwards the call to OBS's customer shown in figure 26. There are three main methods of services OBS is connected to the customer.

The first one which is the business call to a customer is directly connected to OBS network SIP Trunking. So when the signaling of the call is received by the SBC of the SIP Trunking network the SBC forward the signaling to the SR and the SR forward to signaling to the AS to know the location of the destination the AS locates the correct location of the PSX and the send back the SR and the SR forward the signaling to the correct PSX which was located by the AS then the PSX locates the correct SBC by knowing the carrier destination and forward signaling to SBC of the NBI which will forward it to the user through the carrier once the user accepts the call a channel is opened between the customer and the SBC of the SIP Trunking, also between the two SBCs and between the user and the SBC of the NBI network. This method doesn't change whether the customer is connected through a leased landline or a 4G network as shown in figures 27 and 28.

The second method is when the customer is connected through another party (another carrier) so the call flow will be within the NBI network only. When the SBC of the NBI network receives a signaling call the SBC forward the signaling to the PSX and the PSX forward the signaling to the AS to locate the destination since the customer is connected to another carrier so the call will be forwarded through the NBI network so the signaling is sent back to the PSX locating the correct SBC and the PSX forward the signaling to the correct SBC which will forward the call to the carrier and the carrier to the customer shown in figure 30.

Another service is called bridge by using the previous two methods OBS collects several signaling through SIP trunking network and NBI and the AS locates a bridge to host the call and all the signaling is forwarded to tat bridge and open a bridge for a conference call for several users and customers either they are connected to another carrier (NBI Network) or they are connected to OBS directly (SIP Trunking Network) shown in the figure 31

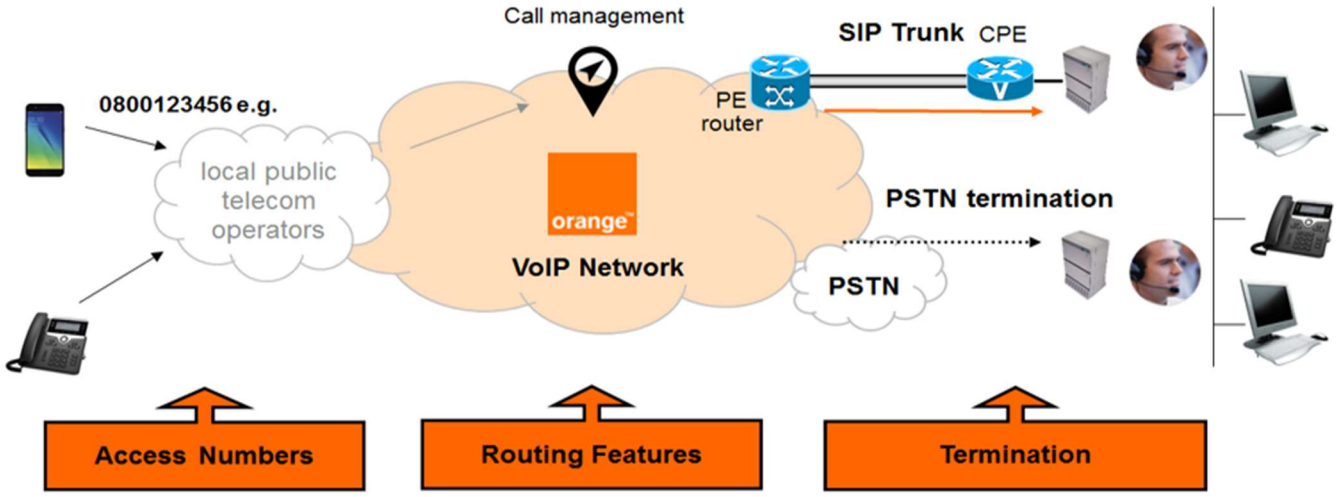

Figure 26 Data collected and delivered by OBS

Fig 26

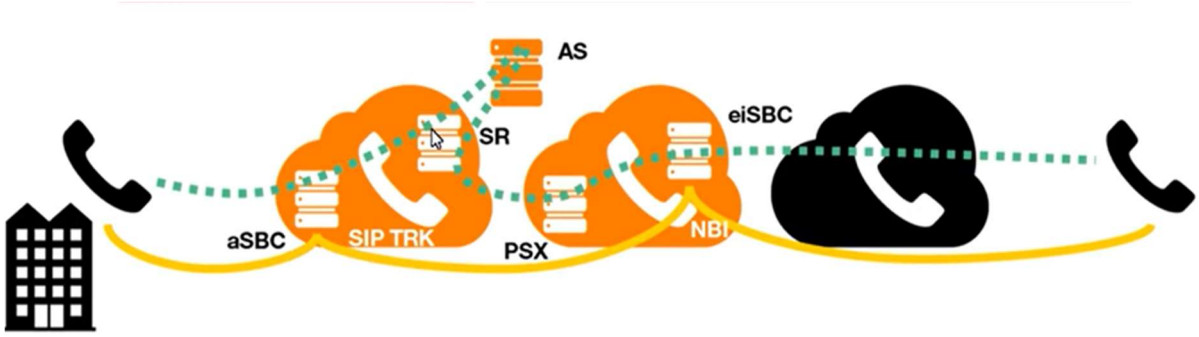

Figure 27 Call flow for a Carrier connected to OBS (SIP Trunking)

Figure 28Call flow for a Carrier connected to OBS (SIP Trunking) using a mobile

Fig 28

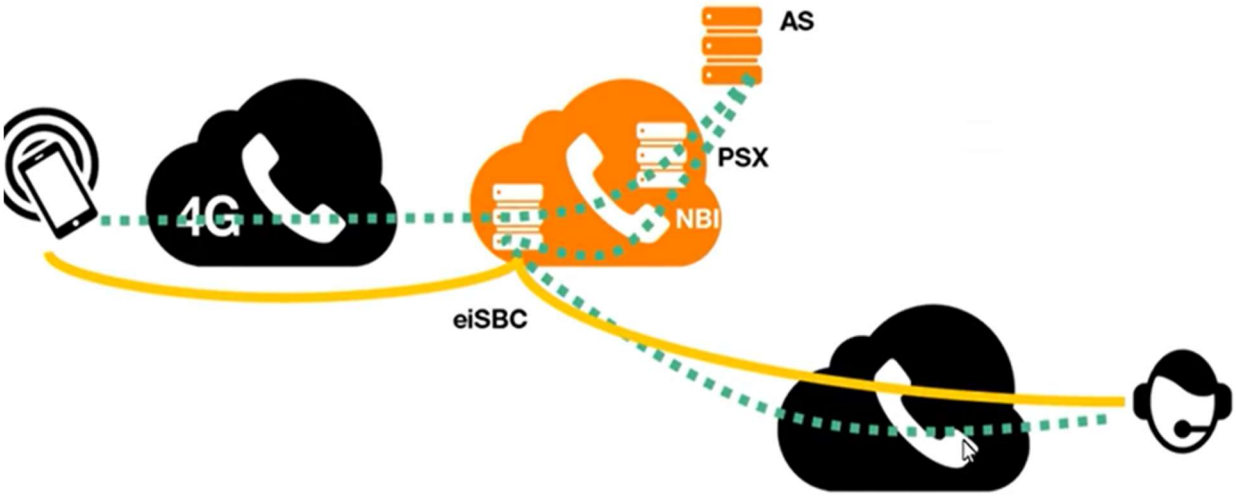

Figure 29 Customer connected to customer

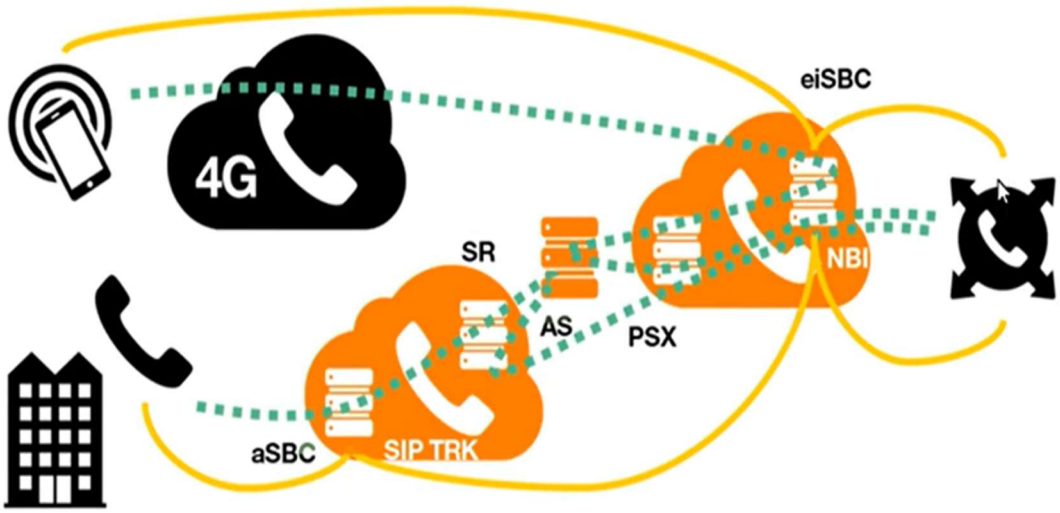

Figure 30 Confrence call

5 Conclusion:

In conclusion Network Architecture needs to move to the next logical phase of evolution where network nodes need to use both SDN and NFV technologies in order to reduce as much it can be the physical nodes and increase the virtual nodes as much as it can be with benefit with that the Capex is reduced, the network is more flexible, easier to manage, easier to configure, easier to troubleshoot, and having the benefit of life cycle management where for any update for the network features or solving a previous debug that can be installed easily on the new nodes by updating the new version on the central points that will automatically will be installed to all nodes.

Moreover, this migration will lead to zero-touch deployment which is that network administrators just configure the metrics on the management plane and a full network will be configured automatically having all the policies, authentications, and the connectivity between the nodes without any human interface. As benefit for that telecommunications companies can serve their customers with installing the parameters needed by the customer and a full automatic network will be generated.

6 References:

Orange learning hub

Different Orange Networks Architectures

Red Hat

CISCO SDWAN model Viptela

SIP sense