AL-Azhar university

Faculty of Engineering

Computer & systems Dep.

جامعة الأزهر

كلية الهندسة

قسم نظم وحاسبات

Full Emulation To Enterprise Network & Security Infrastructure

Supervised By:-

Dr / Mohamed Ashraf Madkor

Presented to:-

Prof.Dr : Ali El Semari

Team members:

Name	No.
Ahmed Adel Hussein	9
Abdallah Adel Abdallah	67
Abdallah Mohammed Ahmed	69
Mohammed Samy Hussein	97
Mohamed Farag Abd ElHalem	114

Table of content :-

Abstract

Our project main idea is to build a network infrastructure suitable to maintain traffic between departments on a different sites , how they connect together, and how clients can connect to this network and benefit from the enterprise services by optimizing the network to be in its full functionality, putting in mind security concerns using the most recent security policies using **Fortigate**(from **Fortinet**) Firewall ,and applying it using a simulation software and VMs to apply the Idea.

We will also include **Service provider** part to connect between the branches on different sites, we also included a **Data center** branch to maintain all the data for the branches since the flow on the data center will be heavy we maintained it to provide reliability and speed as well as the security needed to keep the data up and clean.

In order to make things clear we assumed that we have 2 branches of **CIB** bank one on **Cairo** and the other in **Alexandria** , and they wish to connect to each other , so we provided it with the right protocols and infrastructure needed to make that connection reliable throw the whole session.

Tools:

1. Eve (for simulating) 2. VMware workstation

1) EVE :

It’s a Emulated virtual environment platform for Network, Security & DevOps simulation uses web friendly GUI to maintain its components with the use of a VM interface to connect with the pc network and configure its settings .

Why we use EVE ?

Using the EVE (Emulated Virtual Environment) program for simulating network projects is preferred for several reasons, including:

1- Ease of use: EVE is characterized by an easy-to-use interface that enables users to set up and run simulations quickly and easily.

2- Flexibility: EVE allows users to configure network simulations in a way that suits their individual needs.

3- Efficiency: EVE is efficient and fast in running simulations, allowing users to perform tests and experiments effectively and accurately.

4- Community support: EVE enjoys significant support from the user community, providing beginners and advanced users with resources and assistance in solving problems and achieving their goals.

5- Compatibility: EVE is compatible with many different systems and programs, allowing users to benefit from it in multiple areas.

2) VMware workstation:-

VMware Workstation is a line of Desktop Hypervisor products which lets users run virtual machines, containers and Kubernetes clusters.

We use it because it provides us with the needed systems without the need of having it as a hardware , also it’s a safe place to test functionalities and vulnerabilities without damaging your own device or take more cost by bringing the real device.

Devices we will use:

1- Cisco Routers
2- Cisco Switches
3- Cisco servers (for data center)
4- TP cables (for internal network devices)
5- Fiber optic cables (Between branches and SP)
6- End devices (ie.pc’s)

1- Cisco Routers:-

The network router is quickly transforming from a device dedicated to connecting disparate networks to an integrated services device capable of multiple functions beyond routing. More Cisco customers are deploying integrated services routers - sophisticated network routers that deliver voice, video, data and Internet access, wireless, and other applications.

2- Switches

Cisco Network switches deliver performance and security. They are scalable and cost-efficient and meet the need for any size of business .

3- Servers:

Cisco Unified Computing System (UCS) is a **data center server** computer product line composed of server hardware, virtualization support, switching fabric, and management software, introduced in 2009 by Cisco Systems.

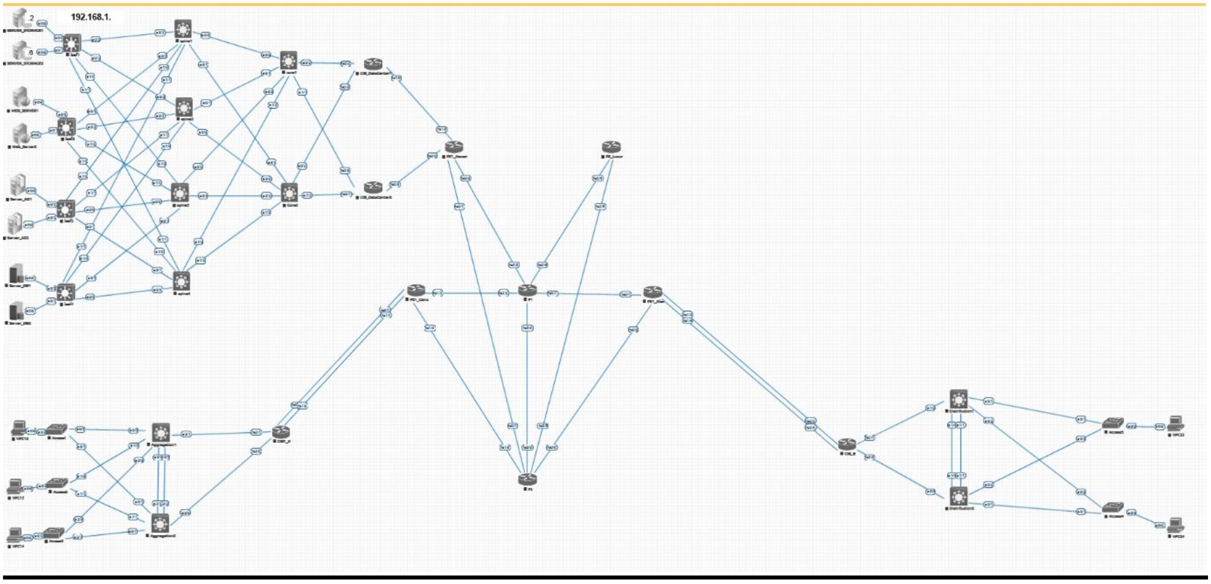
Simulation

We want to connect between :

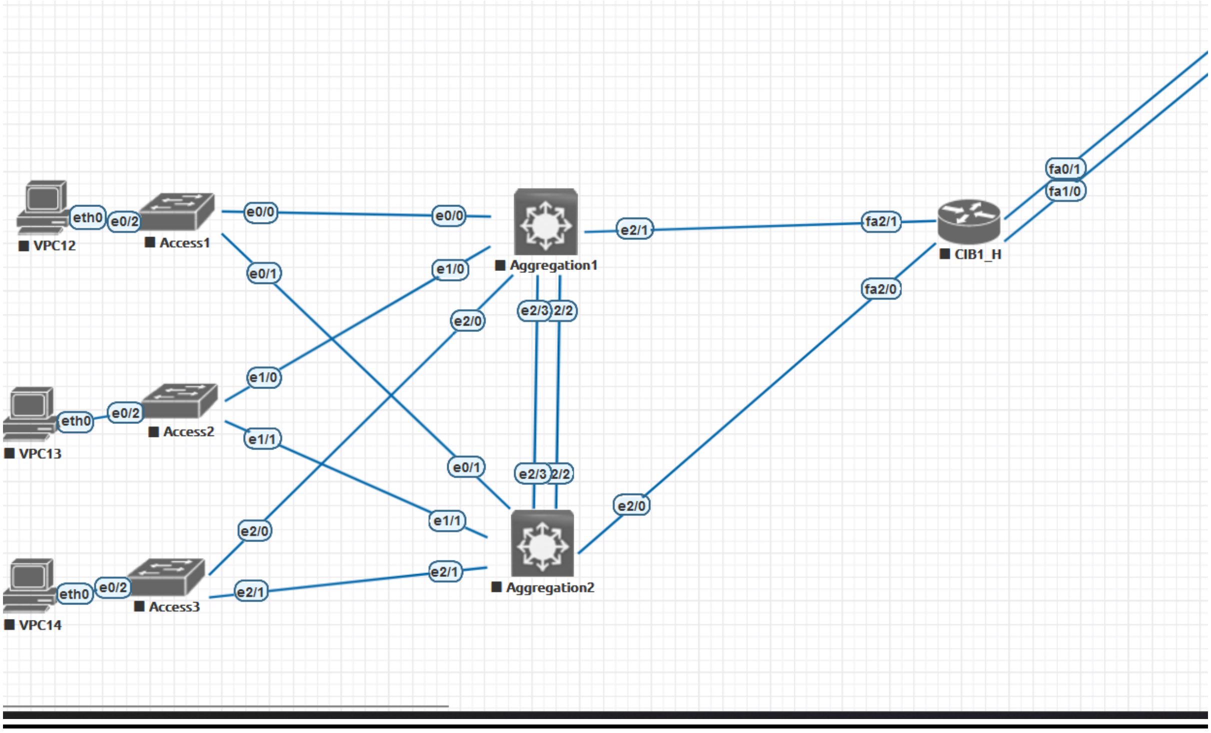
CIB HQ which contain about **Access**, **Aggregation** And CIB branch which contain about **Access**, **DHCP Server** with **Data Center.**

Also for security we enabled spanning tree port security

Initial Idea implementation :-



CIB Head quarter :



CIB Head quarter potocols:

(Access 1,2,3)

Protocols used :

1-Port security : the process of restricting access to a network by limiting which devices can connect to the network, and how they can connect. Only specific devices or MAC addresses can access it. It is a way of controlling which devices can access the network

1- MST

MST (Multiple Spanning Tree) is a Cisco protocol that allows for the creation of multiple spanning trees on a network. This allows for better load balancing and redundancy than the standard Spanning Tree Protocol. MST groups can be configured to map VLANs to specific instances of the spanning tree.

2- BPDUGuard enable

BPDUGuard is a network feature that prevents loops and potential network outages by disabling a port that receives a BPDU (Bridge

Protocol Data Unit) message. When enabled on a port, BPDUGuard immediately shuts down the port upon detecting a BPDU message, which typically indicates the presence of a bridge or switch on that port. This feature helps maintain network stability and prevents malicious attacks or misconfigurations that can disrupt network operations.

3- VTP

VTP (VLAN Trunking Protocol) is a Cisco proprietary protocol used to manage VLANs across a network. It allows switches to share VLAN information, reducing the need for manual configuration. A VTP domain is a group of switches that share the same VLAN configuration.

(Aggregation1,2)

Protocols used :

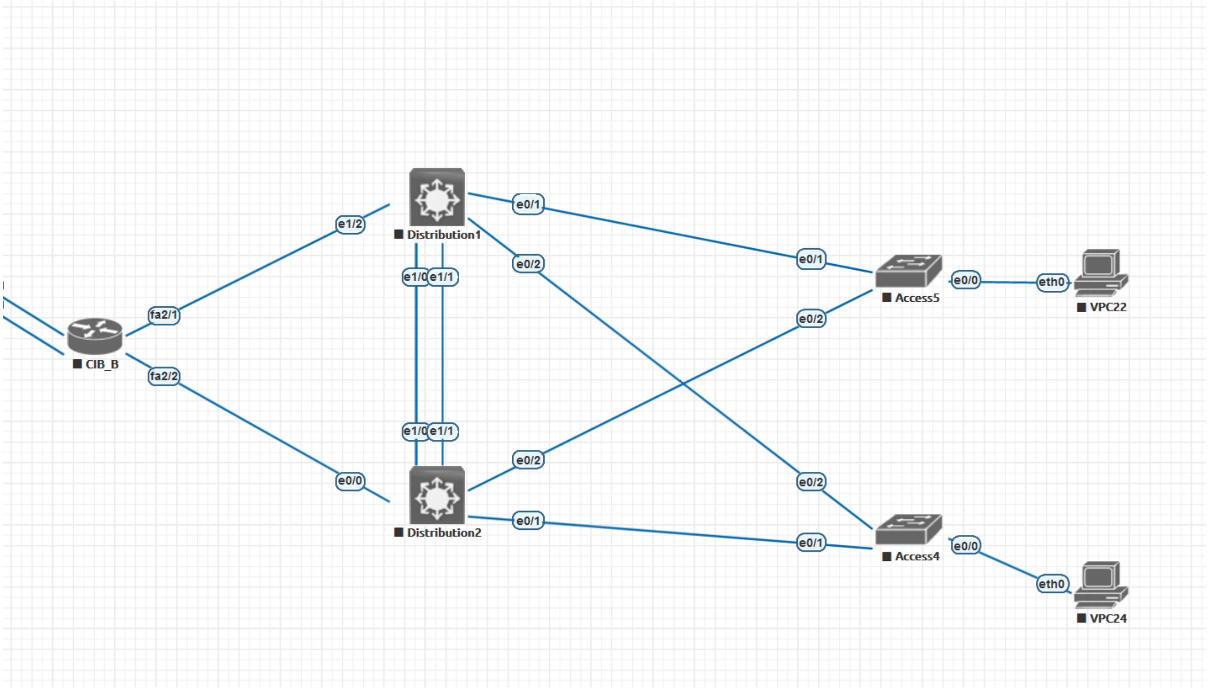
1- OSPF
OSPF (Open Shortest Path First) is a link-state routing protocol used in IP networks. It is designed to scale well for large networks and supports variable-length subnet masking. OSPF routers communicate with each other to build a topology map of the network, allowing for efficient routing decisions based on the shortest path to a destination.

2- HSRP
HSRP (Hot Standby Router Protocol) is a Cisco protocol used to provide redundancy for IP networks. It allows for two or more routers to share a virtual IP address and act as a single gateway for hosts on a network. HSRP routers communicate with each other to determine the active router and the standby routers.

3- MST

4- VTP

CIB branch:



(Distribution1 ,2)

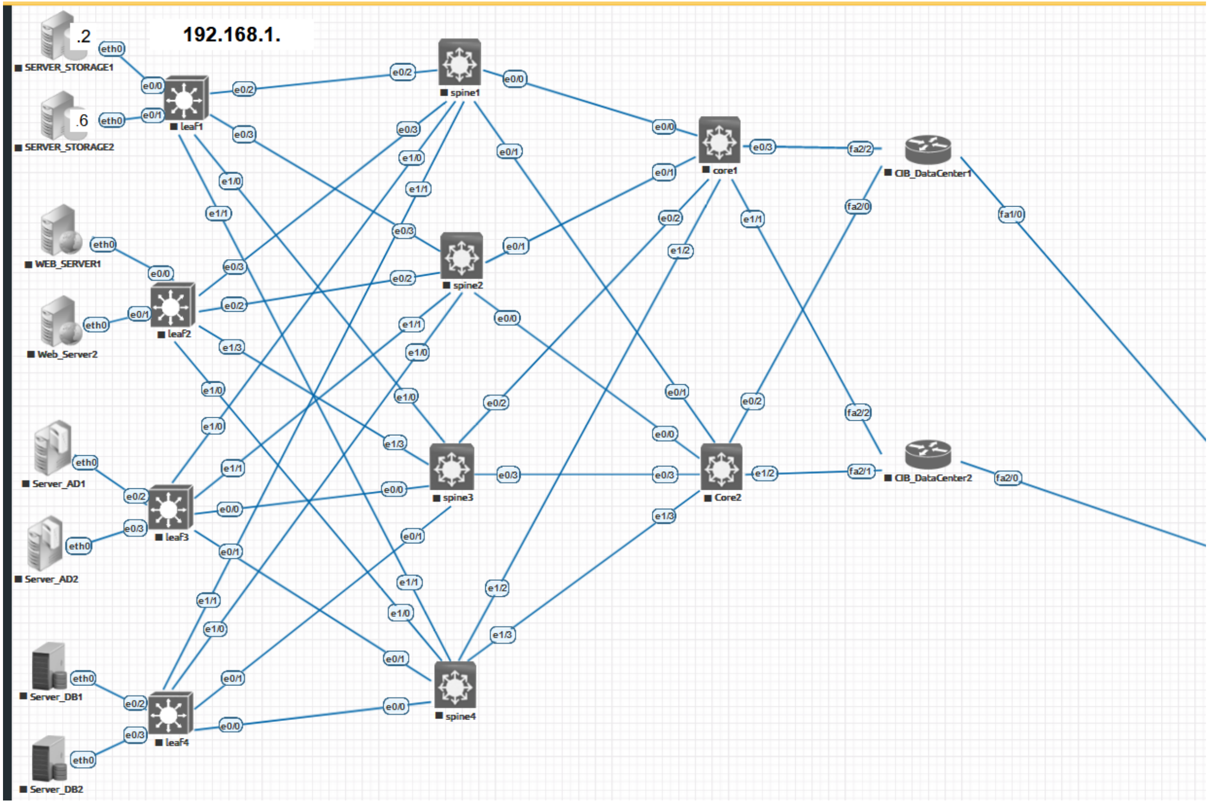
Protocols used :

1- rapid-pvst

   Rapid PVST+ (Per-VLAN Spanning Tree Plus) is a Cisco proprietary protocol that is an enhancement of the original Spanning Tree Protocol (STP). It provides rapid convergence times by using separate instances of STP for each VLAN, rather than a single instance for all VLANs. Rapid PVST+ includes features such as portfast, UplinkFast and BackboneFast to optimize the network topology and minimize downtime.

2- VTP
3- OSPF
4- HSRP

Data center:-



What is a Datacenter?

A data center is a facility that centralizes an organization’s IT operations and equipment for the purposes of storing, processing and disseminating data and applications. Because they house an organization's most critical and proprietary assets, data centers are vital to the continuity of daily operations. Consequently, security and reliability are among any organization’s top priorities.

In the past, data center infrastructures were highly controlled, physical environments, but the public cloud has since changed that model. Most modern infrastructures have evolved from on-premises physical servers to virtualized infrastructure that supports applications and workloads across multicloud environments. Application workloads are moving across multiple data centers and private, public and hybrid clouds.

The Role of the Datacentre:

Data centers are an integral part of the enterprise, designed to support business applications and provide services such as:

- Data storage, management, backup and recovery
- Productivity applications, such as email
- High-volume e-commerce transactions

Protocols used :

HTTPS: Is a secure version of the HTTP protocol that uses the SSL/TLS protocol for encryption and authentication. HTTPS is specified by RFC 2818 (May 2000) and uses port 443 by default instead of HTTP's port 80.

The HTTPS protocol makes it possible for website users to transmit sensitive data such as credit card numbers, banking information, and login credentials securely over the internet. For this reason, HTTPS is especially important for securing online activities such as shopping, banking, and remote work. However, HTTPS is quickly becoming the standard protocol for *all* websites, whether or not they exchange sensitive data with users.

Design: using spine-leaf

Why we use spine-leaf architecture?

A spin-2e-leaf architecture helps datacentre networks reduce network latency and hop count and improve network efficiency.

What is spine-leaf architecture?

Spine-leaf, or leaf-spine, is a two-layer network topology composed of spine and leaf switches. A spine-leaf architecture helps data center networks reduce network latency and hop count and improve network efficiency.

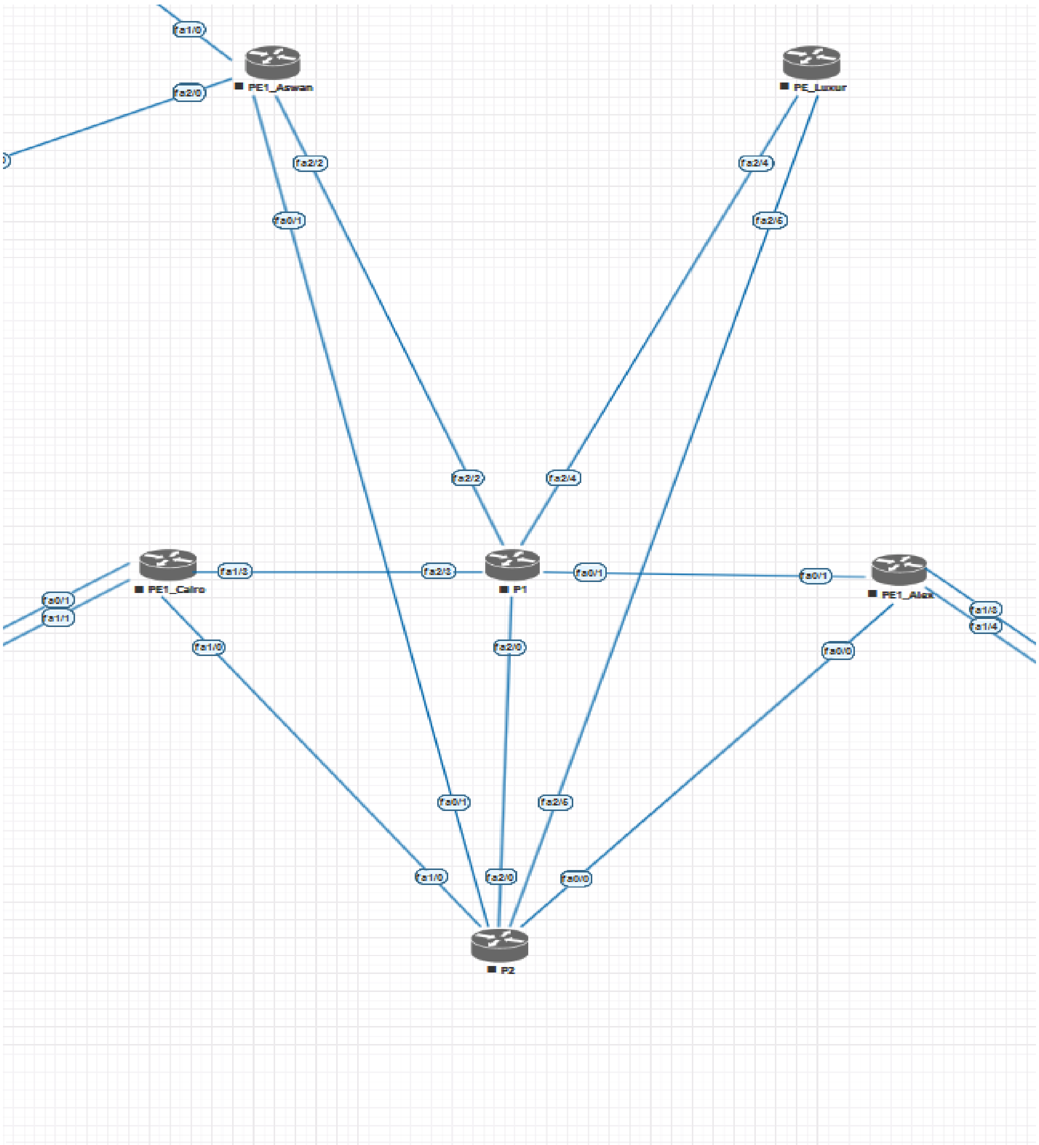
This two-layer full-mesh network topology was designed as an alternative to three-tier architectures and is suitable for modern data centers that experience more east-west network traffic than north-south or switch-to-switch traffic. East-west traffic flows transfer data packets from server to server within a data center. The two-tier topology is composed of the following:

Spine switches. Leaf switches connect to spine switches and mesh into the spine, forming the access layer that delivers network connection points for servers.

Leaf switches. Servers and storage connect to leaf switches and consist of access switches that aggregate traffic from servers. They connect directly to the spine.

<u>Service provider:</u>

The main Idea from designing service provider is to support many customers with an easy way and easy trouble shooting .



Protocols That Enable On This Branch:

1- MPLS
2- OSPF

(PE 1,2)

Protocols That Enable On This Branch:

1- BGP
2- OSPF

Some information about the protocols we used :-

(1) MPLS to provide the following:-

1- Assigns labels to each data packet, controlling the path the packet follows. MPLS greatly improves the speed of traffic, so users don't experience downtime when connected to the network.

2-Virtual routing and forwarding provides a path to configuring multiple routing instances on either a router or Layer 3 switch. The purpose is to keep customer traffic and routing separate but through the same hardware.

(2) BGP to provide the following:-

1- The PEs in the provider network using MPLS BGP use the Multiprotocol-Border Gateway Protocol (MP-BGP) to dynamically communicate with each other.

2- To carry MPLS labels between routers .

(3) OSPF as dynamic routing protocol:-

To exchange network between routers.

Implementation of some of the protocols we used

First (MPLS usage):-

In service provider network we use new address family**,**

it called (VPNv4)

VPNv4 consists of two addresses:-

1- Route distinguisher to differentiate customer networks (RD _ 96 bit).
2- Route target to vrfs (RT _ 64 bit).

Second (MP_BGP usage):-

1- In the design we used Route reflector routers (P1 and P2) to support redundancy, availability and reduce number of BGP sessions between routers .
2- MP_BGP carries RD and RT attributes .

Some commands for configuration:-

(Basic configuration to VRF) Cairo branch:-

```
ip vrf CIB
rd 1:1
route-target 1:1

int loo 0
ip add 50.50.50.50 255.255.255.255
ip ospf 1 area 0

int loo 1
ip vrf forwarding CIB
ip add 40.40.40.40 255.255.255.255

int f0/1
ip vrf forwarding CIB
ip add 2.0.0.2 255.255.255.252
no sh

int f1/1
no swit
ip vrf forwarding CIB
ip add 1.0.0.2 255.255.255.252
no sh
```

(Basic configuration to mp_bgp)

```
 router bgp 200
neighbor 100.100.100.100  remote-as 200
neighbor 100.100.100.100 update-source Loopback0
neighbor 200.200.200.200  remote-as 200
neighbor 200.200.200.200 update-source Loopback0

address-family vpnv4 unicast
neighbor 100.100.100.100 activate
neighbor 100.100.100.100 send-community extended
neighbor 200.200.200.200 activate
neighbor 200.200.200.200 send-community extended


address-family ipv4 vrf CIB
neighbor 10.10.10.10 remote-as 100
neighbor 10.10.10.10 activate
neighbor 10.10.10.10 update-source Loopback1
neighbor 10.10.10.10 ebgp-multihop
```

note:-

(the same configuration on Alex and Aswan with difference in IPS)

Upcoming Features

- **Adding Fortigate firewall for security concerns.**
- **Applying more level-2 security protocols.**
- **Implementing a basic enterprise polices to the end devices.**
- **Adding more code and configuration explanation.**
- **Adding DMVPN feature.**
- **Adding a Radius server .**