Here is a written network design plan that meets the user requirements mentioned above for Alliance Health's head office in Colombo and the new branch in Matara:

1. Network Topology:

The proposed network topology for the head office and branch is a combination of a star and a hub-and-spoke topology. The star topology is used in the head office where each department is connected to a central switch which acts as the hub. The hub-and-spoke topology is used to connect the branch office to the head office where the head office acts as the hub and the branch office acts as a spoke. In this topology, the head office is the central point of control for the entire network, with all communication between the two locations passing through it. This allows for easy management and monitoring of the network, as well as efficient use of network resources.

Each department in both locations is assigned a unique subnet to ensure separation and security. This means that devices in one department cannot communicate with devices in another department unless explicitly permitted by network policies. By implementing this level of separation and security, the network is better protected against potential security threats. Overall, this topology and subnetting scheme allows for efficient communication and management of the network, while also providing a high level of security and separation between departments.

1. Determine the IP addressing scheme and subnetting:

Based on the requirements, all departments must be separated with unique subnets, and the necessary IP address classes and ranges. Since the number of users in each department is relatively small, we can use a Class C network with a subnet mask of 255.255.255.0. Here's a suggested IP addressing scheme for the network:

* Head Office (Colombo):
* Sales & Marketing Department: 192.168.1.0/24
* Reception Area: 192.168.2.0/24
* Administration Department: 192.168.3.0/24
* HR Department: 192.168.4.0/24
* Accounting & Finance Department: 192.168.5.0/24
* Audit Department: 192.168.6.0/24
* Business Development Department: 192.168.7.0/24
* IT Department: 192.168.8.0/24
* Server Room: 10.254.9.0/24
* Video conferencing room 10.254.10.0/24
* Branch (Matara):
* Reception Area: 192.168.11.0/24
* Administration Department: 192.168.12.0/24
* HR Department: 192.168.13.0/24
* Accounting & Finance Department: 192.168.14.0/24
* IT Department: 192.168.15.0/24

1. Determine the VLANs:

Since each department must be separated with unique subnets, we can use VLANs to logically separate the network traffic. Here's a suggested VLAN scheme for the network:

* Head Office (Colombo):
* Sales & Marketing Department: VLAN 10
* Reception Area: VLAN 20
* Administration Department: VLAN 30
* HR Department: VLAN 40
* Accounting & Finance Department: VLAN 50
* Audit Department: VLAN 60
* Business Development Department: VLAN 70
* IT Department: VLAN 80
* Server Room: VLAN 90
* Video conferencing room VLAN 100

|  |  |  |
| --- | --- | --- |
| Department | Ip address range | VLAN |
| Sales & Marketing Department (192.168.1.0/24) | 192.168.1.1 - 192.168.1.10 | VLAN 10 |
| Reception Area (192.168.2.0/24) | 192.168.2.1 - 192.168.2.5 | VLAN 20 |
| Administration Department (192.168.3.0/24) | 192.168.3.1 - 192.168.3.30 | VLAN 30 |
| HR Department (192.168.4.0/24) | 192.168.4.1 - 192.168.4.20 | VLAN 40 |
| Accounting & Finance Department (192.168.5.0/24) | 192.168.5.1 - 192.168.5.15 | VLAN 50 |
| Audit Department (192.168.6.0/24) | 192.168.6.1 - 192.168.6.5 | VLAN 60 |
| Business Development Department (192.168.7.0/24) | 192.168.7.1 - 192.168.7.5 | VLAN 70 |
| IT Department (192.168.8.0/24) | 192.168.8.1 - 192.168.8.60 | VLAN 80 |
| Server Room (10.254.9.0/24) | VLAN 90 | |
| Video conferencing room (10.254.10.0/24) | VLAN 100 | |

* Branch (Matara):
* Reception Area: VLAN 110
* Administration Department: VLAN 120
* HR Department: VLAN 130
* Accounting & Finance Department: VLAN 140
* IT Department: VLAN 150

|  |  |  |
| --- | --- | --- |
| Department | Ip address range | VLAN |
| Reception Area (192.168.11.0/24) | 192.168.11.1 – 192.168.11.5 | VLAN 110 |
| Administration Department (192.168.12.0/24) | 192.168.12.1 – 192.168.12.10 | VLAN 120 |
| HR Department (192.168.13.0/24) | 192.168.13.1 – 192.168.13.7 | VLAN 130 |
| Accounting & Finance Department (192.168.14.0/24) | 192.168.14.1 – 192.168.14.8 | VLAN 140 |
| IT Department (192.168.15.0/24) | 192.168.15.1 – 192.168.15.50 | VLAN 150 |

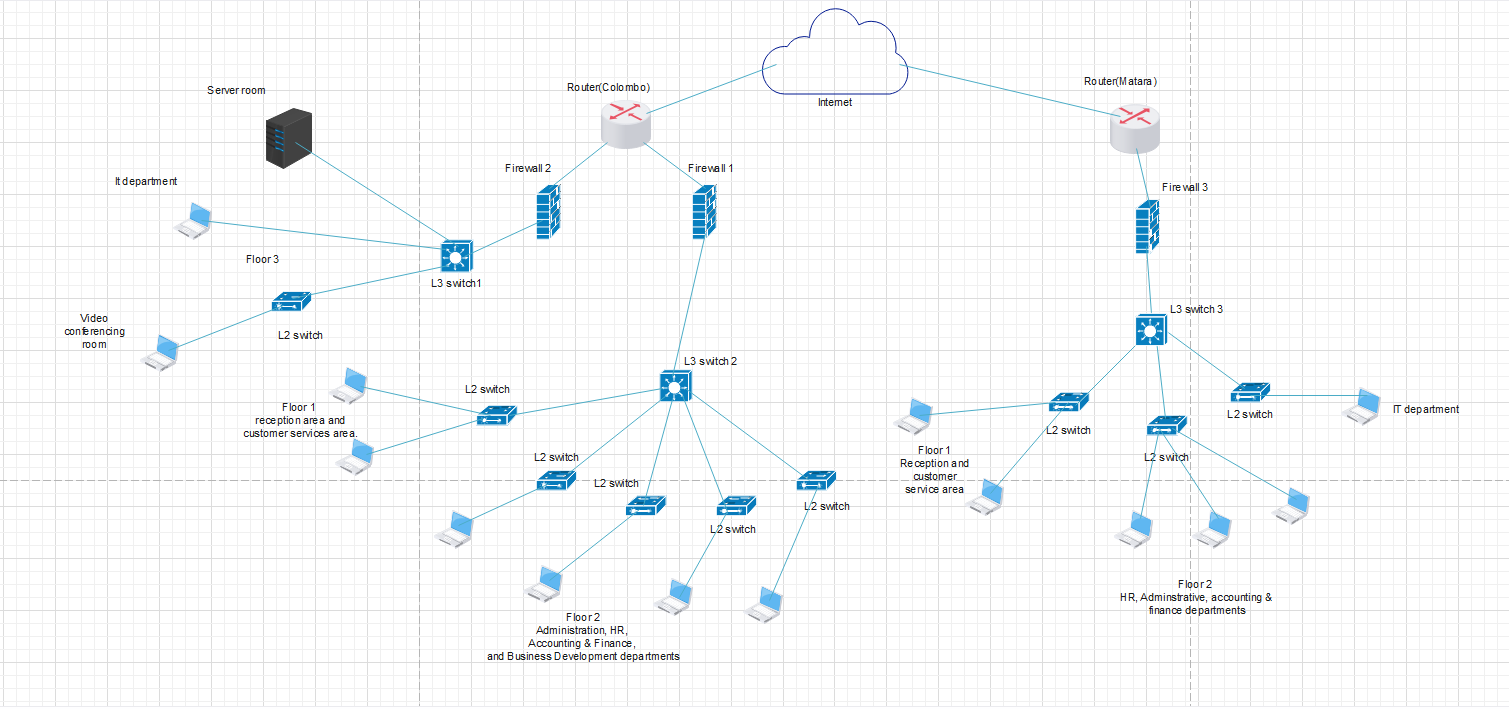
1. Determine the network components:

To implement the network design, we will need the following network components:

* Switches: We will need at least one Layer 3 switch at each location to support the VLANs and routing between them. For example, we could use a Cisco Catalyst 3850 switch at the head office and a Cisco Catalyst 2960 switch at the branch.
* Router: We will need a router to provide internet connectivity and to route traffic between the head office and the branch. For example, we could use a Cisco ISR 4000 series router.
* Access Points: We will need wireless access points to provide Wi-Fi connectivity in the conferencing room at the head office, the customer services area at each branch, and the sales & marketing department at the head office. For example, we could use Cisco Aironet 2800 series access points.
* Firewall: We will need a firewall to provide security for the network and to control access to resources. For example, we could use a Cisco ASA 5500 series

1. Network Security:

To ensure network security, the following measures will be implemented:

* Access Control: Access control lists (ACLs) will be configured on routers and switches to control access to sensitive network resources.
* Firewall: A Cisco Adaptive Security Appliance (ASA) will be installed at the head office to protect the network from external threats.
* VLANs: Each department will be assigned a unique VLAN to ensure separation and security.
* Password Policy: Strong password policies will be implemented to ensure that network resources are protected against unauthorized access.
* Encryption: Encryption will be used to protect sensitive data transmitted over the network
* Blueprint using EDrawMAX
* Implementing network design using GNS3

I have used GNS3 to implement the designed network. Here I have used two cisco routers for each branch like one for Colombo and one for Matara. And I have used FortiGate 7.45 as the firewall for the network and I have used two firewalls for Colombo branch and another one for Matara branch.

Based on the proposed network design for the Colombo branch, we would need a total of 6 layer 2 switches and 2 layer 3 switches.

On floor 1, we would need 1 layer 2 switch to connect the reception area and the customer services area.

On floor 2, we would need 4 layer 2 switches for the Administration, HR, Accounting & Finance, and Business Development departments. We would also need 1 layer 3 switch to provide inter-VLAN routing between these departments.

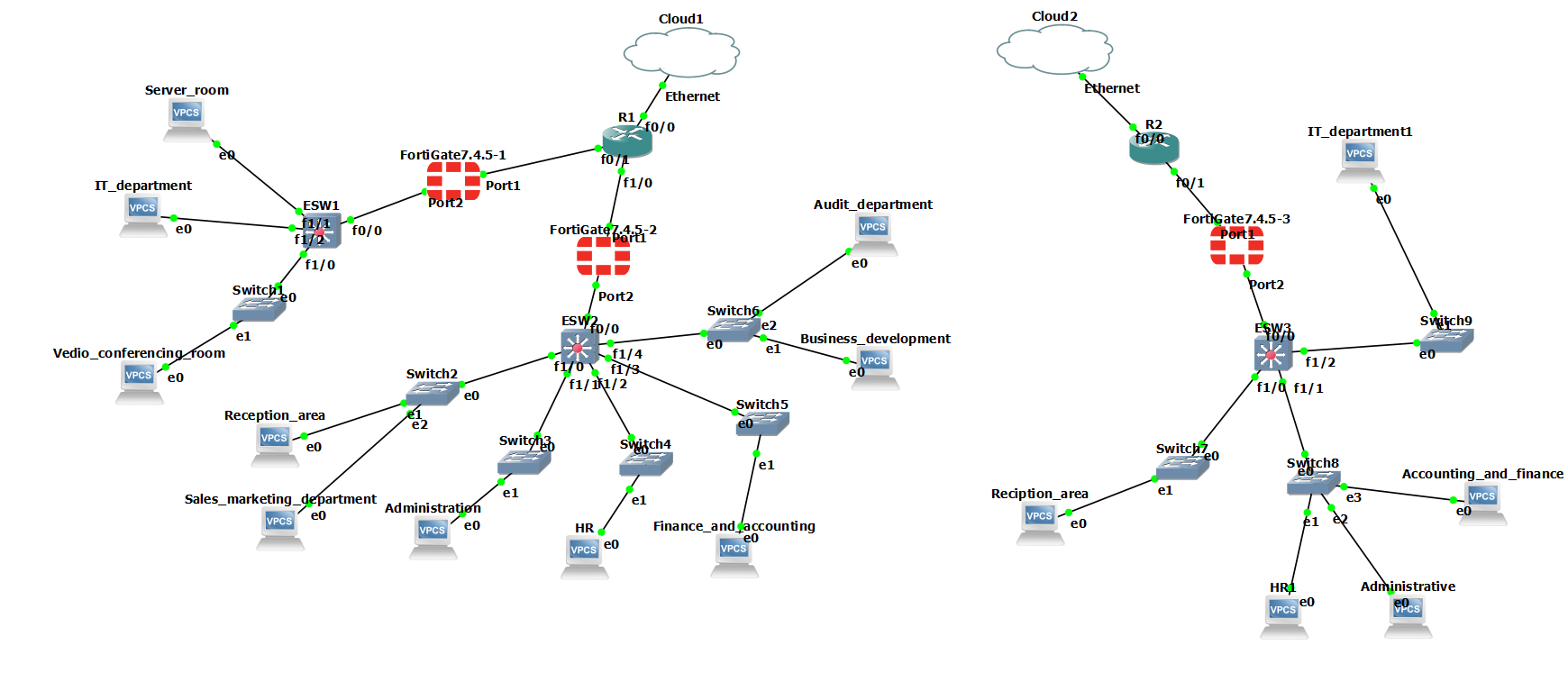
On floor 3, we would need 1 layer 2 switch for the video conferencing room and 1 layer 3 switch to provide connectivity to the IT department and server room.

Overall, the layer 2 switches would be used for connecting end devices, such as computers and printers, to the network within each department, while the layer 3 switches would be used for routing traffic between different VLANs and providing connectivity to other network devices, such as routers and firewalls.

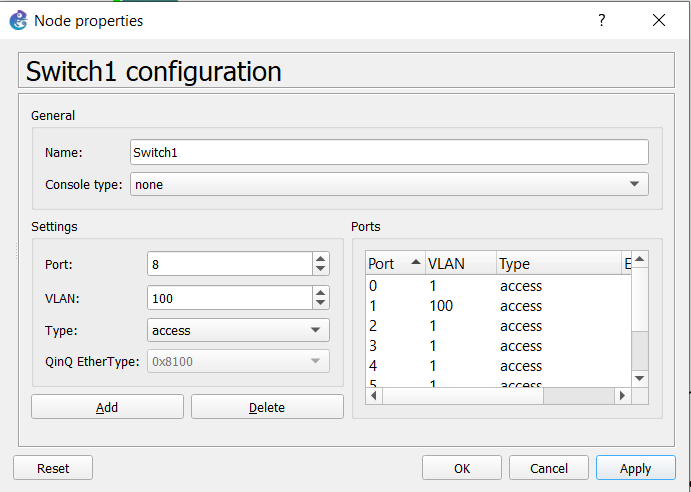
Consider about Matara branch I have used one layer 3 switch and three layer 2 switches. For floor one I have used one layer 2 switch and it will connect the reception area and customer service area within different VLANs. Same as for the administrative, HR and accounting and finance department I have used one layer 2 switch. Because of the higher population in the IT department, I have used one layer 2 switch for it.

Here are some assumptions which I have done when I design the network:

* The VLAN and IP subnetting scheme assumes that each department will have less than 254 devices connected to the network.
* The server room will be using static IP addresses.
* The number of wireless access points required will depend on the coverage area and density of devices.
* The bandwidth requirements and traffic patterns of the network have not been specified. The proposed network design assumes a typical office network with moderate traffic.



* Colombo branch
* Configuring switches and pcs on floor 3.



Text

Description automatically generated

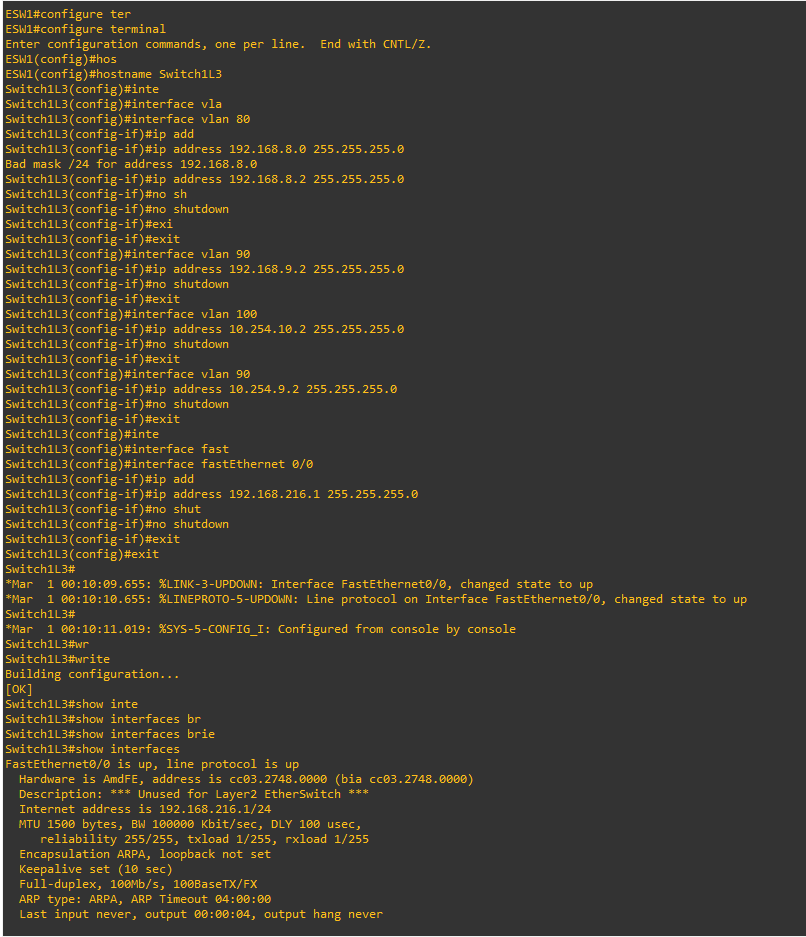
Text

Description automatically generated

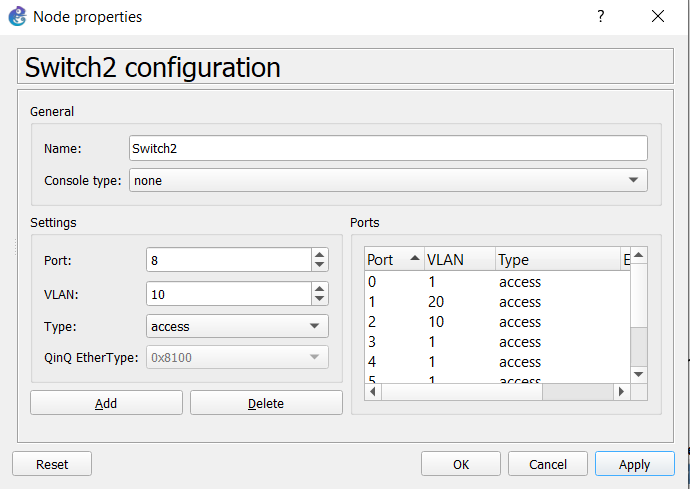
Text

Description automatically generated

* + - Configuring the layer 3 switch with VLANs.



* Configuring switches and pcs in floor 1.



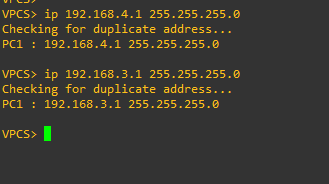
Text

Description automatically generated

Text

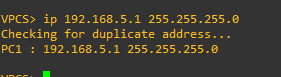
Description automatically generated

* + Configuring switches and pcs in floor 2.



Text

Description automatically generated



Text

Description automatically generated

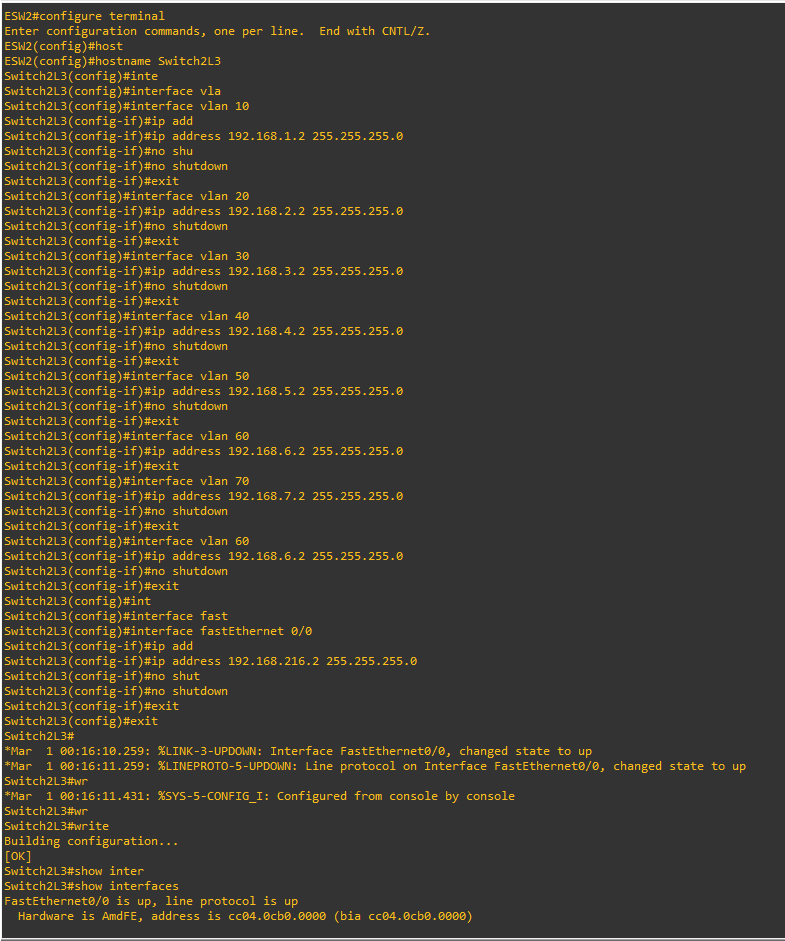
Text

Description automatically generated

Graphical user interface

Description automatically generated

* Configuring the second layer three switch in the colombo branch.



* Configuring devices in Matara branch.

Text

Description automatically generated

Text

Description automatically generated

Text

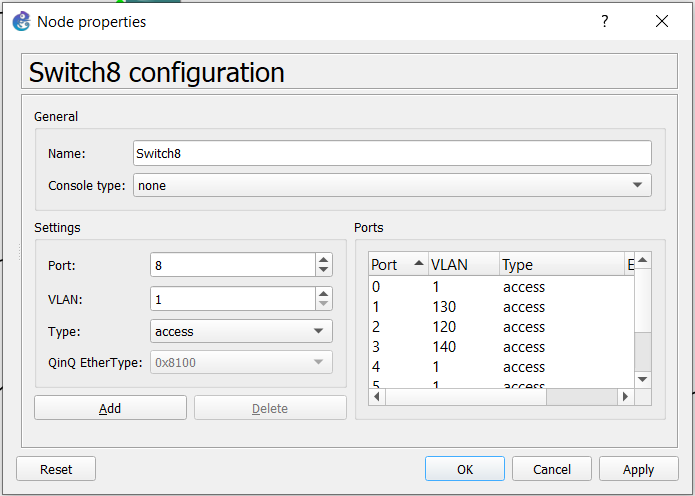
Description automatically generated

Text

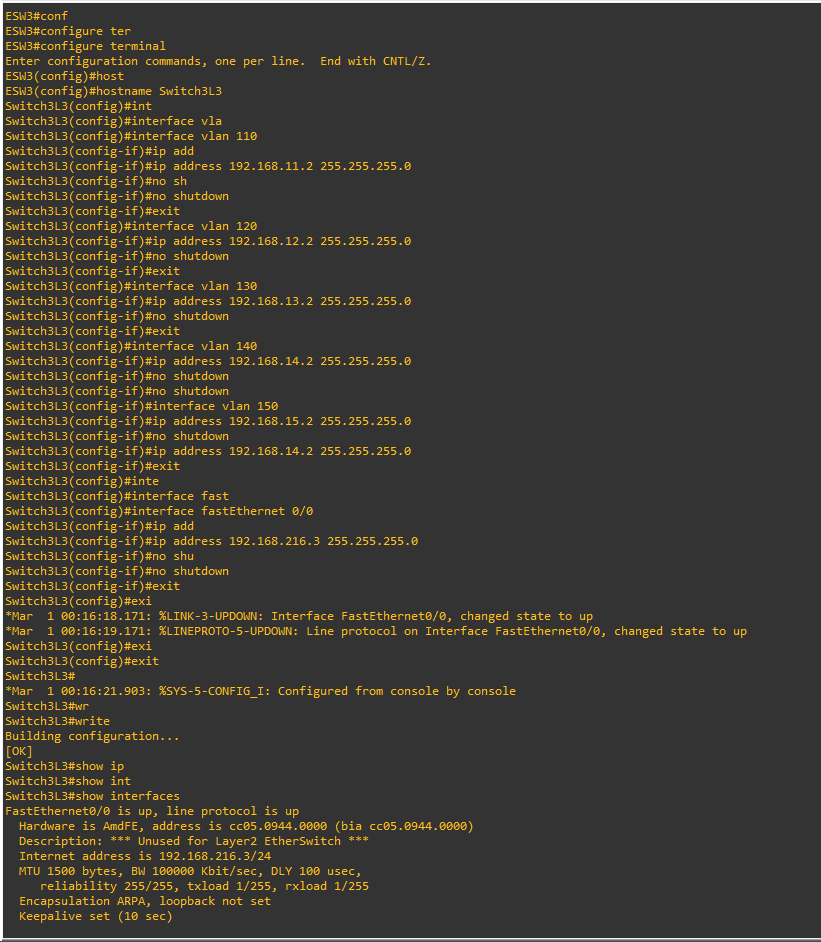
Description automatically generated

Text

Description automatically generated



* Configuring layer three switch on the matara branch.



* Configuring router 1 in colombo branch

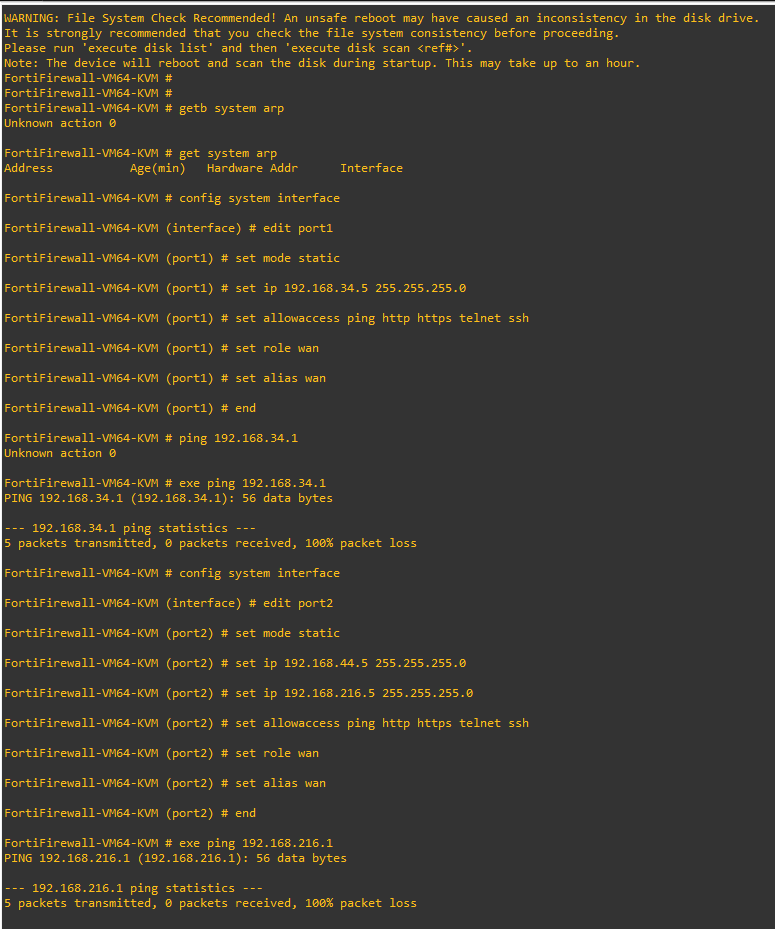


* Configuring router2 in matara branch

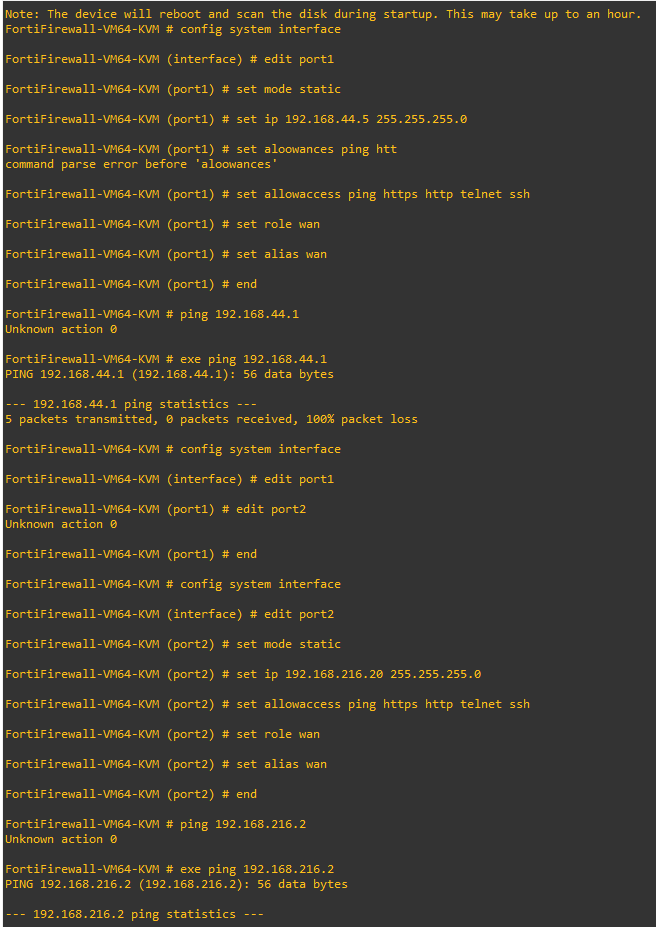
Text

Description automatically generated

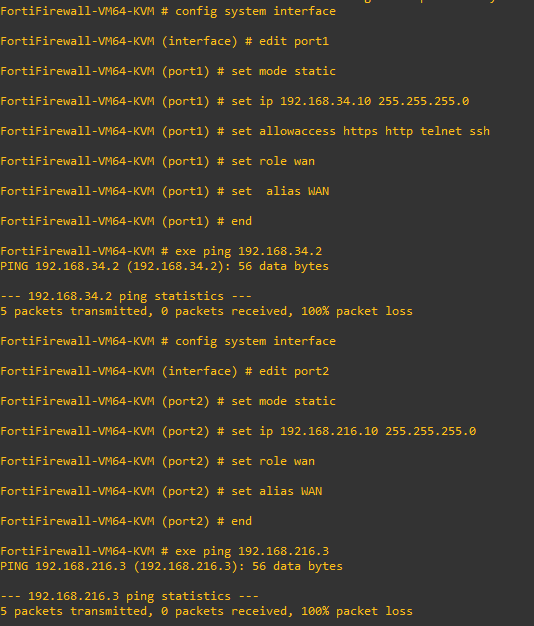
* Configuring firewall in floor 3 in colombo branch.



* Configuring firewall in floor 2 and 1 in colombo branch.



* Configuring the firewall in matara branch.



* Parameters of the virtual network

Graphical user interface, text, application

Description automatically generated

* Maintaining schedule:

The maintenance schedule for the proposed network design should include the following tasks:

* Regular backups: Regular backups of all configurations and device settings should be performed to ensure that in case of a hardware failure or unexpected changes, the network can be easily restored to its previous state. It is recommended to perform daily or weekly backups and store them in an offsite location.
* Security assessments: Regular security assessments should be conducted to identify potential vulnerabilities and threats to the network. This can be done by performing periodic penetration testing, vulnerability scanning, and risk assessments. Any identified issues should be promptly addressed to ensure the security of the network.
* Network monitoring: Regular monitoring of network performance should be performed to identify bottlenecks and areas for optimization. This can be done using network monitoring tools that can detect performance issues such as latency, packet loss, and bandwidth utilization. Monitoring should be done on a continuous basis to identify and address issues as they arise.
* Software updates and security patches: Software updates and security patches should be implemented in a timely manner to ensure the latest protections against security threats. This includes operating system updates, firmware updates, and application updates. These updates should be tested in a non-production environment before being applied to the live network.
* Testing and verification: Regular testing and verification of network infrastructure and services should be performed to ensure that they are operating correctly and meeting user requirements. This includes testing of all network components such as switches, routers, firewalls, and servers, as well as testing of network services such as email, file sharing, and web browsing.
* Maintenance windows: Maintenance windows should be scheduled in advance to minimize disruption to users. Maintenance windows should be planned for times when network usage is low, such as evenings or weekends. Notification should be provided to users in advance of any scheduled maintenance to minimize the impact on their work.
* Testing for the system.

Here is some testing which I have done for the system.

* Ping Test:

From a computer in the Sales and Marketing Department, ping the gateway IP address of their subnet.

From a computer in the Administration Department, ping the gateway IP address of their subnet.

From a computer in the IT Department, ping the gateway IP address of their subnet.

From the Server Room, ping the gateway IP address of the server subnet.

Expected Results:

All pings should be successful.

* Extended Ping Test:

From a computer in the Sales and Marketing Department, ping the IP address of a computer in the Administration Department.

From a computer in the Administration Department, ping the IP address of a computer in the Sales and Marketing Department.

From a computer in the IT Department, ping the IP address of a computer in the Administration Department.

From a computer in the Administration Department, ping the IP address of a computer in the IT Department.

From the Server Room, ping the IP address of a computer in each department subnet.

Expected Results:

All pings should be successful.

* Trace Route Test:

From a computer in the Sales and Marketing Department, trace route to the IP address of a computer in the Administration Department.

From a computer in the Administration Department, trace route to the IP address of a computer in the Sales and Marketing Department.

From a computer in IT Department, trace route to the IP address of a computer in Administration Department.

From a computer in the Administration Department, trace route to the IP address of a computer in the IT Department.

From the Server Room, trace route to the IP address of a computer in each department subnet.

Expected Results:

The trace route should show the path taken by the packets from the source computer to the destination computer.

* Telnet Test:

From a computer in the Sales and Marketing Department, telnet to the IP address of a computer in the Administration Department.

From a computer in the Administration Department, telnet to the IP address of a computer in Sales and Marketing Department.

From a computer in the IT Department, telnet to the IP address of a computer in Administration Department.

From a computer in the Administration Department, telnet to the IP address of a computer in IT Department.

Expected Results:

Telnet should establish a connection with the destination computer.

* SSH Test:

From a computer in the IT Department, SSH, to the IP address of a computer in Administration Department.

From a computer in Administration Department, SSH to the IP address of a computer in IT Department.

Expected Results:

SSH should establish a secure connection with the destination computer.

According to the system there are some enhancements which can be implemented on the system.

* Redundancy: Implementing redundancy in critical network components such as routers and switches can help ensure uninterrupted network availability in case of hardware failure.
* Network Monitoring: Implementing a network monitoring solution can help detect and troubleshoot network issues more efficiently, as well as provide valuable insights into network performance and utilization.
* Network Security: Enhancing network security measures, such as implementing firewalls, intrusion detection systems, and regular security audits, can help protect the network against potential cyber threats and attacks.