**NETWORKING PROJECT 5: SECURE HEALTH CARE NETWORK**

**Project Statement**

A close-up of a document

Description automatically generated

A close-up of a document

Description automatically generated

A close up of a document

Description automatically generated

A close-up of a document

Description automatically generated

A white text with black text

Description automatically generated

**Network Hardware**

According to the problem statement, the company is spread over 3 floors (35, 36 & 37) with each floor containing the following departments

|  |  |
| --- | --- |
| **Floors** | **Departments** |
| 35 | Pharmacy & medical lab, reception & guest area |
| 36 | Doctors & Consultancy, Procurement, HR &Finance |
| 37 | Internal Auditors & Corporate Functions, IT |

We have like around 6 departments in general which is a combination or 2 or more departments. We will need 6 access layer switches

DMZ contains the servers and storage devices

We will need a PC to manage wireless LAN device

Required Hardware and basic network topology

A diagram of a network

Description automatically generated

* In each departmental switch the ports 21 to 24 have been designated for wireless access points and ports 3 to 20 have been designated for LAN users.
* To Implement an ether channel we interconnect the 2 distribution layer switches from port 21 to 24 on either side using copper straight through cables.

A diagram of a network

Description automatically generated

Fully connected network diagram

* To facilitate efficient VOIP services, a separate router will be added such that the p[primary router is concerned only about aggregating traffic to and from the firewall.

**Configuring Access layer Switches**

**Pharmacy and Medical Lab Switch**

* + En
  + Config t
  + Hostname PharmMed
  + Banner motd \*No Unauthorized Access\* [**banner message**]
  + Enable password cisco [**enables password**]
  + Line console 0
  + Password cisco
  + Login
  + Exit
  + No ip domain-lookup [**disables domain look up**]
  + Service password encryption [**encrypts all passwords**]
  + Ip domain-name project5.com
* Configure SSH
  + Username cisco password cisco
  + Crypto key generate rsa general-keys modulus 1024
  + Ip ssh version 2
  + Do wr

Repeat the same steps for the other department switches as well as the main router and the WAP switch .

**VLAN, STP Portfast and BPDUguard Configuration**

* Any port on the access layer switch that connects to the distribution layer switch should be turned to trunk.
  + Int range fa0/1-2
  + Switchport mode trunk
  + Exit
  + Do wr
* The other ports should be configured as access ports. Before switching to access mode we will create the vlans as mentioned in the problem statement.
  + Vlan 10
  + Name LAN
  + Do wr
  + Ex
  + Vlan 50
  + Name WLAN
  + Do wr
  + Ex
  + Vlan 99
  + Name VoIP
  + Do wr
  + Ex
* Now switch the interfaces from 3 to 20 to access mode and let them access both data [10] and voice vlans [99]
  + Int range fa0/3-20
  + Switchport mode access
  + Switchport access vlan 10
  + Switchport voice vlan 99
  + Ex
  + Do wr
* Now switch the interfaces from 21 to 24 to access mode and allow them to access the wireless vlan
  + Int range fa0/21-24
  + Switchport mode access
  + Switchport access vlan 50
  + Ex
  + Do wr
* Configuring BPDUguard and STP PortFast on the access ports. These protocols reduce the time interval between listening and learning states and allows a device to be connected to the network immediately. BPDUguard blocks the Bridge Protocol Data Units sent from unauthorized devices and will disable the port receiving the BPDU. This should only be used on ports that connect to the external network as it can disrupt internal communication.
  + Int range fa0/3-24
  + Spanning-tree portfast
  + Spanning-tree bpduguard enable
  + Ex
  + Do wr

A screenshot of a computer

Description automatically generated

* We can see that the portfast and bpduguard options have been enabled and the connection of new devices will be instantaneous.
* Repeat the same steps for all other department switches.

**Configure the Wireless Lan controller Switch**

* The port to which the WLC is connected should be in the same VLAN as the ports to which the WAP is connected in the department level (access layer) switches
* The ports connected to any router and the multilayer (distribution layer) switches should be trunk
* Any end device connected to the switch should be on vlan 10
  + En
  + Config t
  + Int range fa0/1-3
  + Switchport mode trunk
  + Ex
  + Do wr
  + Vlan 10
  + Name LAN
  + Do wr
  + Ex
  + Vlan 50
  + Name WLAN
  + Do wr
  + Ex
  + Vlan 99
  + Name VoIP
  + Do wr
  + Ex
  + Int range fa0/4-20
  + Switchport mode access
  + Switchport access vlan 10
  + Switchport voice vlan 99
  + Ex
  + Int range fa0/21-24 **🡪 Any device connected to these ports will be in VLAN 50**
  + Switchport mode access
  + Switchport access vlan 50
  + Ex
  + Do wr
  + Int range fa0/4-24
  + Spanning-tree portfast
  + Spanning-tree bpduguard enable
  + Ex
  + Do wr

**Configuring the Multilayer Switch**

* The ports connecting the multilayer switch and the access layer switches should be turned to trunk
  + Int range gig1/0/2-8
  + Switchport mode trunk
  + Ex
  + Do wr
* Create the 3 vlans on each multilayer switch
  + Vlan 10
  + Name LAN
  + Do wr
  + Ex
  + Vlan 50
  + Name WLAN
  + Do wr
  + Ex
  + Vlan 99
  + Name VoIP
  + Do wr
  + Ex
* Configuring **Ether Channel Protocol**. Ether channel is a Link Aggregation Control Protocol in which multiple physical ports are grouped into one logical link to provide high speed links and redundancy. A maximum of 8 links can be aggregated to form a single link.
  + Int range gig1/0/21-24
  + Channel-group 1 mode active
  + Ex
  + Int port-channel 1
  + Switchport mode trunk
  + Ex
  + Do wr

Repeat on the second multilayer switch

**Configuring IP Addressing**

* IP Addrerssing info required by the company is as follows:

A screenshot of a computer

Description automatically generated

* Setting the network between the routers and the multilayer switch
* Switch 1
  + En
  + Config t
  + Int gig1/0/1
  + No switchport 🡪 **Turns a switchport into layer 3 interface**
  + Ip address 10.30.10.5 255.255.255.252
  + No shut
  + Ex
  + Do wr
* Switch 2
  + En
  + Config t
  + Int gig1/0/1
  + No switchport 🡪 **Turns a switchport into layer 3 interface**
  + Ip address 10.30.10.9 255.255.255.252
  + No shut
  + Ex
  + Do wr
* Primary Router
  + En
  + Config t
  + Int range fa0/0-1
  + No shut
  + Ex
  + Int fa1/0
  + No shut
  + Ex
  + Do wr
  + Int fa0/0
  + Ip address 10.30.10.6 255.255.255.252
  + Ex
  + Do wr
  + Int fa0/1
  + Ip address 10.30.10.10 255.255.255.252
  + Ex
  + Do wr
  + Int fa1/0
* ISP Router
  + En
  + Config t
  + Int range gig0/0/0-2
  + No shut
  + Ex
  + Int gig0/0/0
  + Ip address 197.200.100.1 255.255.255.252
  + Ex
  + Do wr
  + Int gig0/0/1
  + Ip address 20.20.20.2 255.255.255.252
  + Ex
  + Do wr
* Cloud Router
  + En
  + Config t
  + Int range gig0/0/0-2
  + No shut
  + Ex
  + Int gig0/0/0
  + Ip address 20.20.20.1 255.255.255.252
  + Ex
  + Do wr
  + Int gig0/0/1
  + Ip address 30.0.0.1 255.0.0.0
  + Ex
  + Do wr
* Next step is to assign static IP Address to the Cloud servers and Virtual machines as well as the application, email and other servers in the DMZ. One server in the DMZ acts as the DNS server containing Active Directory and facilitates DHCP ip Addressing for all the devices in the network.

**Configuring HSRP Protocol and Inter-VLAN Routing**

* One way to achieve near-100 percent network uptime is to use HSRP, which provides network redundancy for IP networks, and ensures that user traffic immediately and transparently recovers from first hop failures in network edge devices or access circuits. When two or more routers share an IP address and a MAC (Layer 2) address, they can act as a single "virtual" router. The members of the virtual router group continually exchange status messages. This way, one router can assume the routing responsibility of another if one is out of commission for either planned or unplanned reasons. Hosts continue to forward IP packets to a consistent IP and MAC address, and the changeover of devices that do the routing is transparent.
* In this project the 2 distribution layer switches will function as simulated routers with 3 VLANs each having their own IP networks. The implementation of the HSRP protocol will generate a virtual router between the 2 switches to enable networking. We will configure HSRP along with the Inter-VLAN routing configuration
* For the L3 switch to forward the DHCP requests to the DHCP server located in the server farm an ip helper address should be specified.
* Active Router (L3 Switch 1)
  + En
  + Config t
  + Int vlan 10 🡪 **Switch Virtual Interface**
  + Ip address 192.168.0.2 255.255.240.0
  + Ip helper-address 10.20.10.2 **🡪 Address of the DHCP server in the DMZ**
  + Standby 10 priority 180 [here the group number is 10 and priority is the highest]
  + Standby 10 ip 192.168.0.1 **[IP address for the virtual router]**
  + Ex
  + Do wr
  + Int vlan 50 🡪 **Switch Virtual Interface**
  + Ip address 10.10.0.2 255.255.0.0
  + Ip helper-address 10.20.10.2 **🡪 Address of the DHCP server in the DMZ**
  + Standby 50 priority 180
  + Standby 50 ip 10.10.0.1 **[IP address for the virtual router]**
  + Ex
  + Do wr
* Standby Router (Switch 2)
  + int vlan 10 🡪 **Switch Virtual Interface**
  + ip address 192.168.0.2 255.255.240.0
  + ip helper-address 10.20.10.2 **🡪 Address of the DHCP server in the DMZ**
  + standby 10 priority 160
  + standby 10 ip 192.168.0.1 **[IP address for the virtual router]**
  + int vlan 50 🡪 **Switch Virtual Interface**
  + ip address 10.10.0.2 255.255.0.0
  + ip helper-address 10.20.10.2 **🡪 Address of the DHCP server in the DMZ**
  + standby 50 priority 160
  + standby 50 ip 10.10.0.1 **[IP address for the virtual router]**
  + ex
  + do wr

A screenshot of a computer

Description automatically generated

**HSRP configuration on L3Switch 1**

A screenshot of a computer program

Description automatically generated

**HSRP configuration on L3Switch 2**

* Settiing the preempt on the L3 switch (simulated router) with a higher priority value wil allow that switch to take control from the existing active switch and become the new active switch and forcing all traffic to go through it.
  + - * **Standby <vlan number/ group number> preempt**

**DHCP Configuration on the Server in the DMZ**

* Open the configuration menu
* Go to services tab
* Click on DHCP
* Set the starting IP and subnet mask and everything else to 0 and save
* The turn on the DHCP service and create IP Pools for LAN and WLAN
* The default gateway would be the ip address of the vlan in the virtual router

|  |  |
| --- | --- |
| Wireless Pool (Vlan 50) | 10.10.0.1 |
| LAN Pool (Vlan 10) | 192.168.0.1 |

* The DNS server would be the ip address of the server hosting the DHCP (10.20.10.2)
* Wireless pool provides ip address to the devices connecting through wifi provided by the WAP. The WAPs are controlled by the WLC. The ip address of the WLC should be specified while creating the ip pool

A screenshot of a computer

Description automatically generated

**DHCP Configuration on ESXI Server in DMZ**

**Configuring OSPF on the Firewall, Routers and Switches**

* Active Router
* Router ospf 25
* Router id 1.2.1.2
* network 10.30.10.4 255.255.255.252 area 0
* network 10.10.0.0 255.255.0.0 area 0
* network 192.168.0.0 255.255.240.0 area 0
* network 172.16.0.0 255.255.240.0 area 0
* ex
* do wr
* Standby Router
* router ospf 25
* router-id 1.3.1.3
* network 10.30.10.8 255.255.255.252 area 0
* network 10.10.0.0 255.255.0.0 area 0
* network 192.168.0.0 255.255.240.0 area 0
* network 172.16.0.0 255.255.240.0 area 0
* Primary WAN Router
* router ospf 25
* router-id 1.4.1.4
* network 10.30.10.0 255.255.255.252 area 0
* network 10.30.10.4 255.255.255.252 area 0
* network 10.30.10.8 255.255.255.252 area 0
* ex
* do wr
* ISP Router
* router ospf 25
* router-id 1.5.1.5
* network 197.200.100.0 255.255.255.252 area 0
* network 20.20.20.0 255.255.255.252 area 0
* ex
* do wr
* AWS Router
* router ospf 25
* router-id 2.1.2.1
* network 20.20.20.0 255.255.255.252 area 0
* network 30.0.0.0 255.0.0.0 area 0
* ex
* do wr

**Configuring the FireWall**

* Basic Settings
* en
* config t
* hostname Perimeter-Firewall
* Domain-name AVM.com
* Setting Security zones and Levels
* Int gig1/1
* No shut
* ip address 10.30.10.1 255.255.255.252
* nameif INSIDE [Name the interface connecting the internal network. Default security level of 0]
* security-level 100 [Security level of INSIDE changed to 100 {Fully Trusted}]
* ex
* int gig1/2
* no shut
* ip address 10.20.10.1 255.255.255.192
* nameif DMZ
* security-level 50
* ex
* int gig1/3
* no shut
* ip address 197.200.100.2 255.255.255.252
* nameif EXTERNAL
* security-level 0
* ex
* wr mem
* OSPF Configuration
* router ospf 25
* router-id 1.9.1.9
* network 10.30.10.0 255.255.255.252 area 0
* network 10.20.10.4 255.255.255.192 area 0
* network 197.200.100.0 255.255.255.252 area 0
* ex
* wr mem
* Static Routing
* route EXTERNAL 0.0.0.0 0.0.0.0 197.200.100.1 [rout traffic from any external ip address with any subnet mask to the ISP]
* Setting UP NAT
* Object network LAN-INTERNET
* Subnet 192.168.0.0 255.255.240.0
* Nat (INSIDE,EXTERNAL) dynamic interface
* Ex
* Wr mem
* Object network WLAN-INTERNET
* Subnet 10.10.0.0 255.255.0.0
* Nat (INSIDE,EXTERNAL) dynamic interface
* Ex
* Wr mem
* Object network VoIP-INTERNET
* Subnet 172.16.0.0 255.255.240.0
* Nat (INSIDE,EXTERNAL) dynamic interface
* Ex
* Wr mem
* Setting Up Firewall Policies (creating Access Control LIsts)
* Access-list INSIDE-DMZ extended permit icmp any any
* Access-list INSIDE-DMZ extended permit tcp any any eq 80 [web requests]
* Access-list INSIDE-DMZ extended permit udp any any eq 57 [DHCP]
* Access-list INSIDE-DMZ extended permit udp any any eq 58 [DHCP]
* Access-list INSIDE-DMZ extended permit tcp any any eq 53 [DNS]
* Access-list INSIDE-DMZ extended permit udp any any eq 53 [DNS]
* Access-group INSIDE-DMZ in interface DMZ

Once the ACL is up and running we can see that the devices have started to obtain IP addresses from the dhcp server

**Implementing Wireless LAN Controller**

* In order to control a WAP through a WLC the CAPWAP status on the WAP should be “connected”

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Click Next and then Apply.

Once the reset is done, go back to the browser and hit the IP of the WLC again. But this time with https

A screenshot of a computer

Description automatically generated

Click on login

A screenshot of a computer

Description automatically generated

We have created 4 wifi networks

A screenshot of a computer

Description automatically generated

|  |  |
| --- | --- |
| **SSID** | **PASSWORD** |
| Internal Network | Internal123! |
| Guest | Guest123 |
| Corporate | Corporate123 |
| External Audit | External123 |

\*\*\* Passwords to be changed after testing\*\*\*

The CapWAP status has changed to connected to 10.10.0.15 on all access pointsd and each access point is advertising the above 4 networks.

**Configuring VoIP**

* En
* Config t
* Int range fa0/0-1
* No shut
* Ex
* Do wr

Create a Sub interface for intervlan routing

* Int fa0/0.99
* Encapsulation dot1q 99
* Ip address 172.16.0.1 255.255.240.0
* Ex

Create DHCP Pool

* Service dhcp
* Ip dhcp pool VoIP
* Network 172.16.0.0 255.255.240.0
* default-router 172.16.0.1
* option 150 ip 172.16.0.1
* ex

Set up the Telephony service

* telephony-service
* max-ephones 20
* max-dn 20
* ip source-address 172.16.0.1 port 2000
* auto assign 1 to 20
* ex
* ephone-dn 1
* number 3001 -🡪>> goes up to 20

A screenshot of a computer

Description automatically generated

Finally we are able to ping the EC2 instance in the cloud from the internal PC0

A screenshot of a computer program

Description automatically generated