20 FEB, 2022

ADVANCE NETWORKING

ENTERPRISE NETWORK DESIGN

SUBMITTED TO

MANOJ TAMANG

SUBMITTED BY

MILAN DANGOL
190213

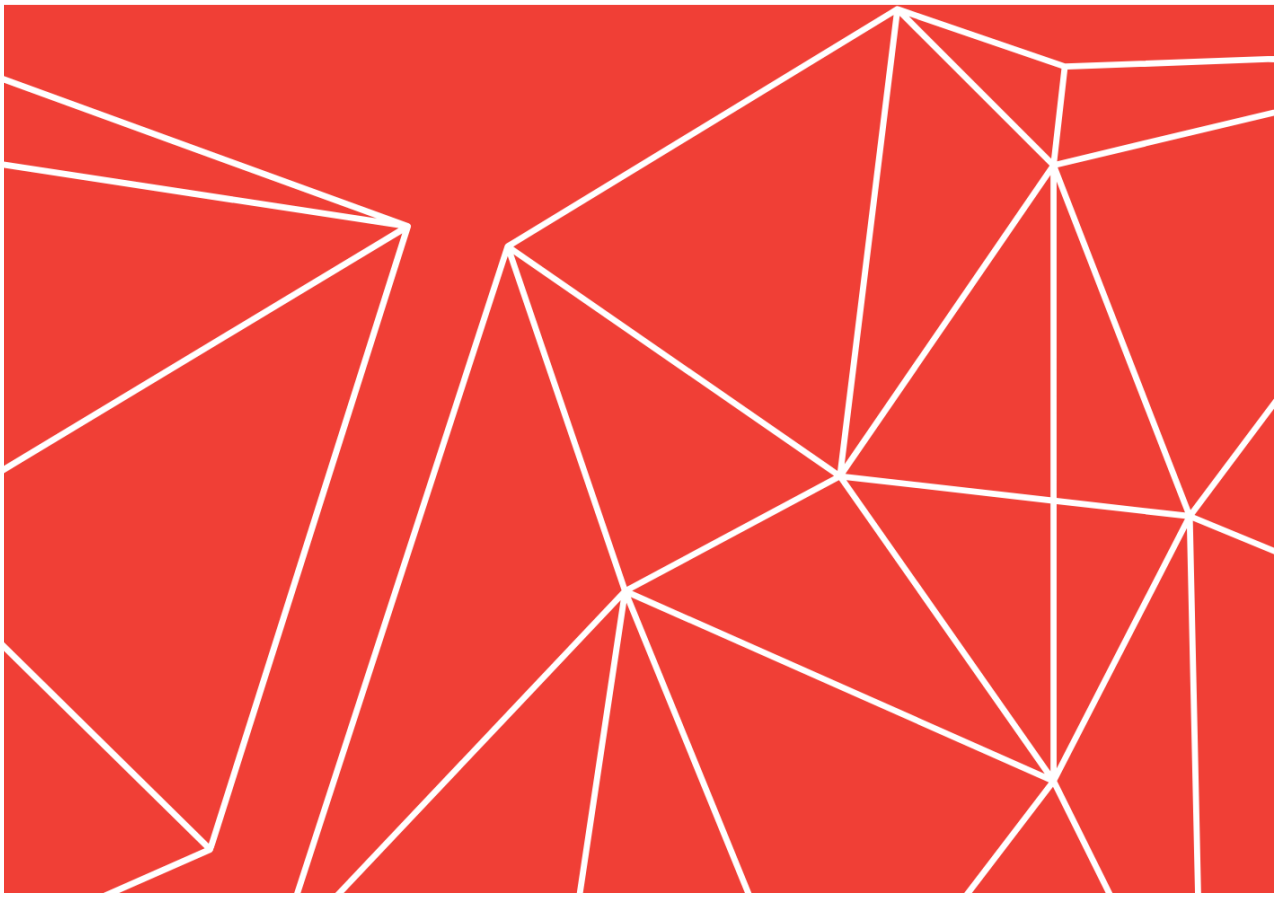


TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

INTRODUCTION

This report depicts the network architecture of "Network Hats Pvt. Ltd." This style is comprised of three layers: core, distribution, and access. The physical and logical layouts are created in Visio and Cisco Packet Tracer, respectively. VLAN allocation, IP addressing, routing protocol, GRE tunneling, and remote access VPN are all operational. Public and private IP addresses are connected using NAT.

NETWORK DESIGN SCENARIO

Assuming that the company consists of 5 stories building with different requirements.

1. The IT floor, which will have 20 computers and wireless internet access, will be on the top floor.
2. HR will be on the third floor, and management will be responsible for providing a wired connection to 20 and 50 PCs for each department, as well as wireless access.
3. A server room, firewall, DMZ, and core routers and switches will all be located on the second floor.
4. The first floor will be dedicated to marketing, with a wired and wireless connection required for 80 PCs.
5. The sales and helpdesk areas on the ground floor will require a cable connection to 50 and 30 PCs, respectively, as well as a wireless connection.

PHYSICAL LAYOUT OF THE COMPANY

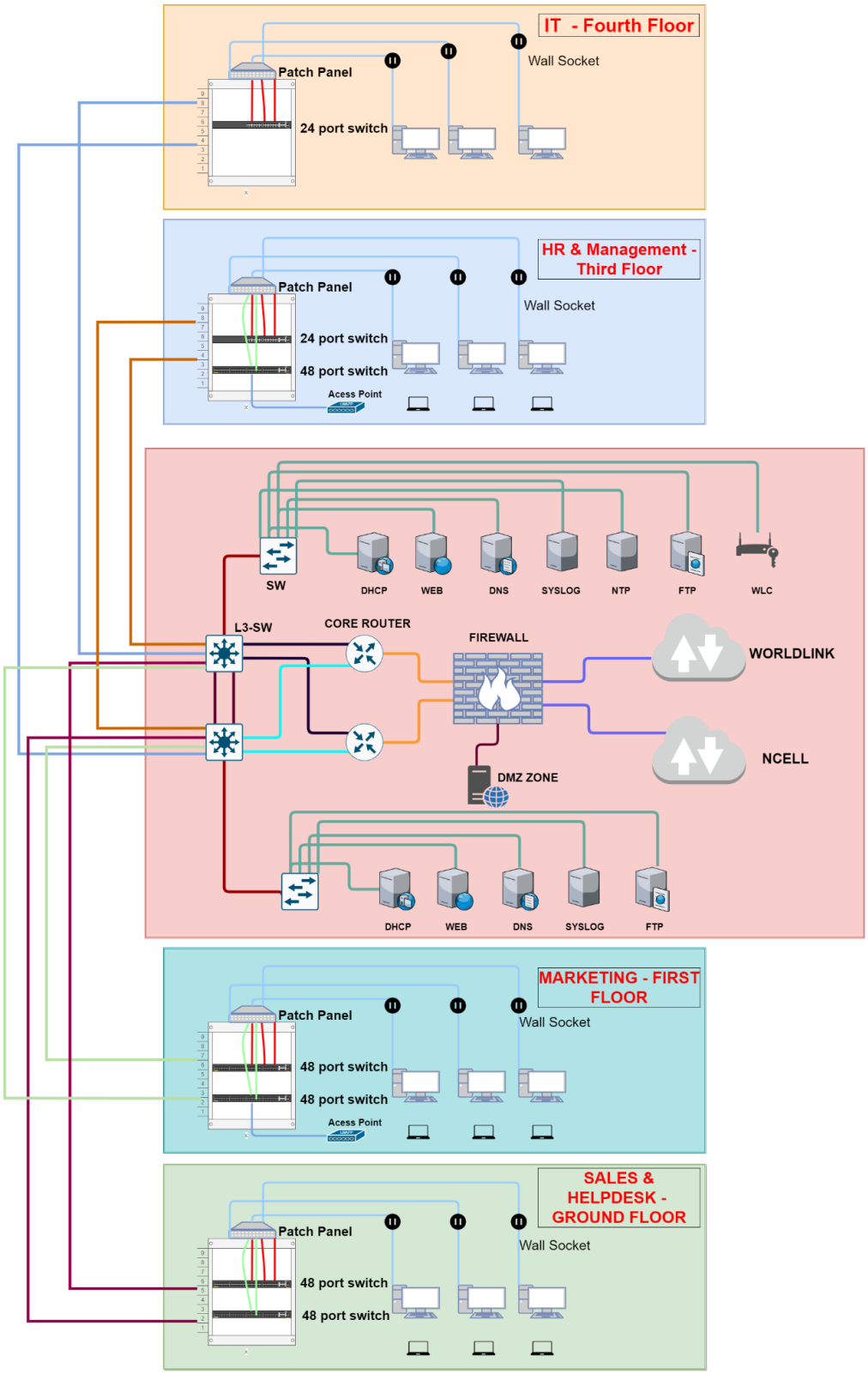


Figure 1 Floor Planning

BRANCH, VPN AND THE COMPANY ASSUMPTIONS LAYOUT

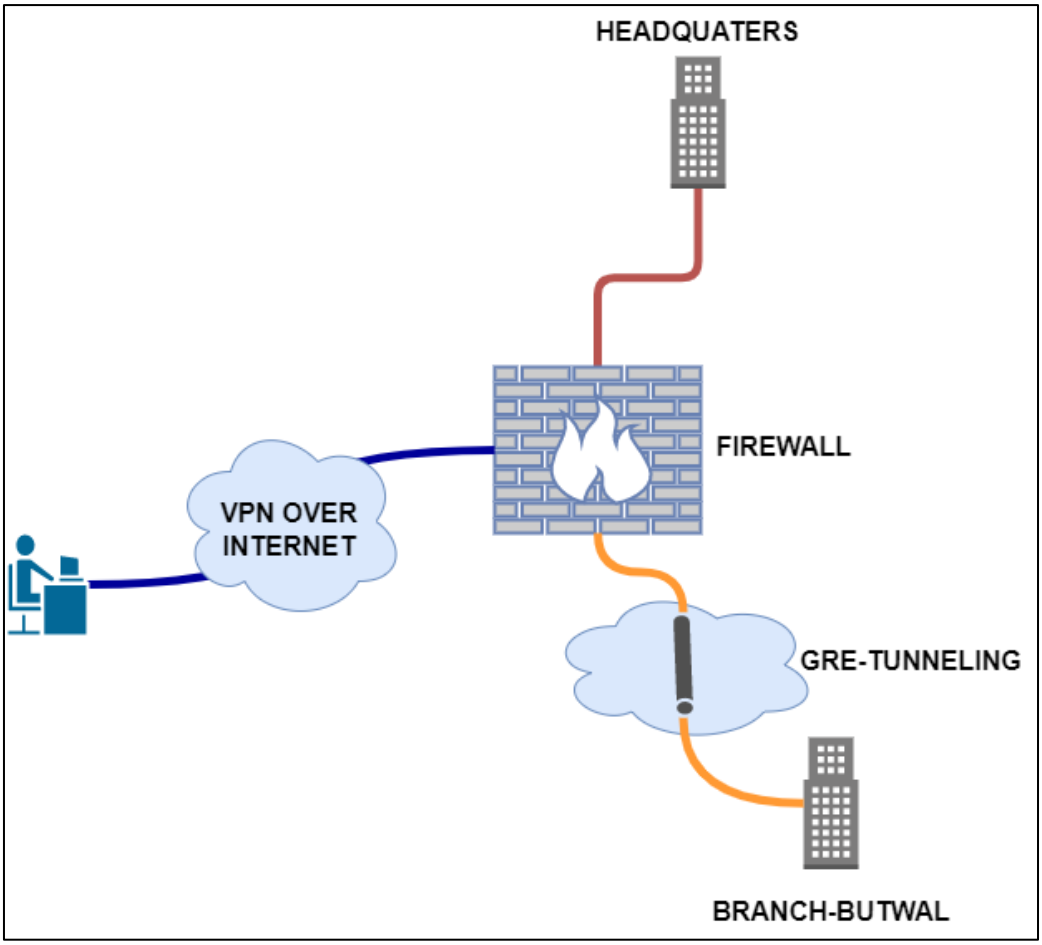
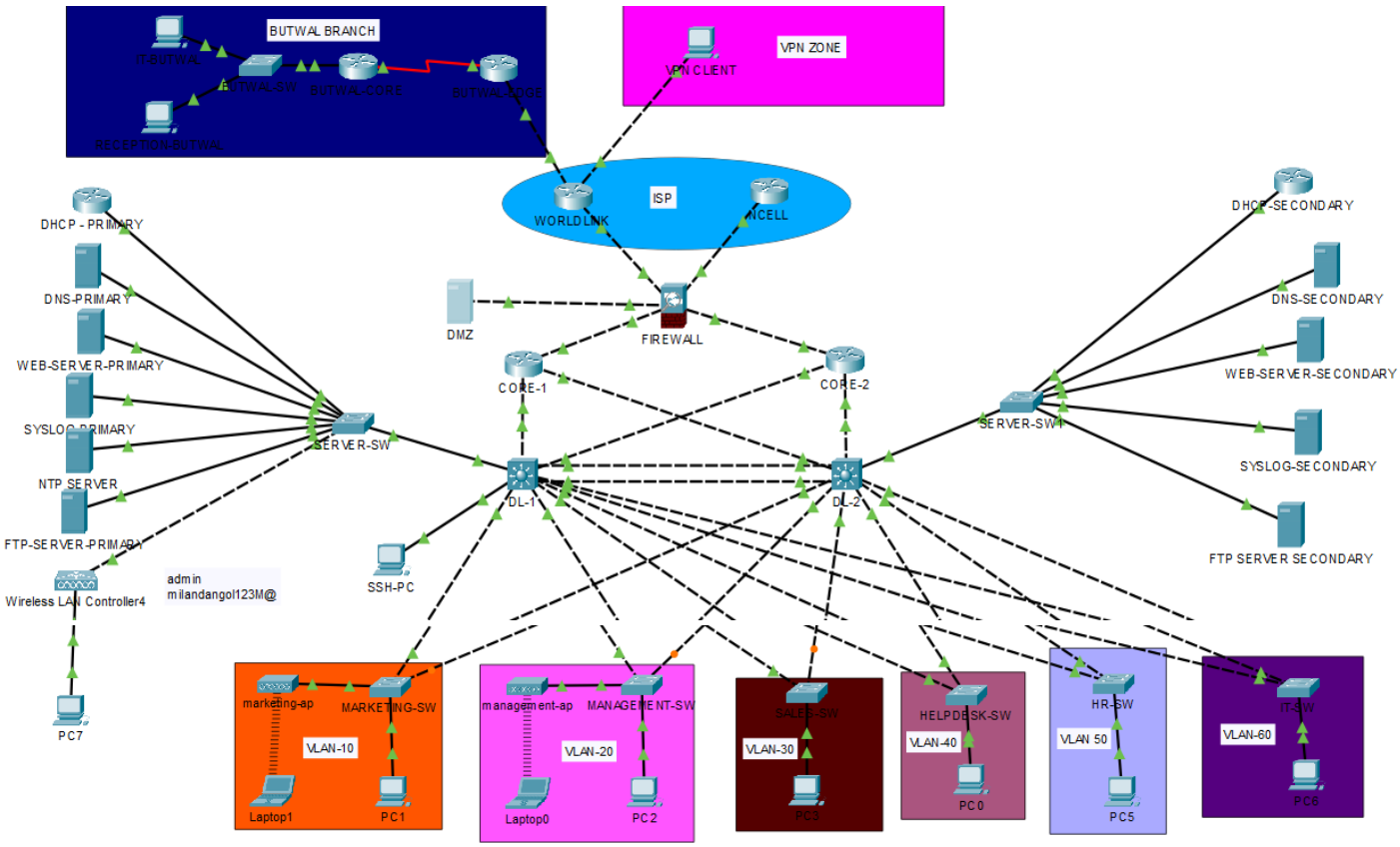


Figure 2 Branch and VPN company assumptions

Assumptions made on the connection between the branch, remote worker, and main site.

- ➔ The branch office is located in a remote location from the main office. As a result, the cost of connecting the main site and the branch site through leased line is higher. As a result, GRE tunneling is carried out across the internet to address this issue.
- ➔ As of 2022, People are still doing work from home. Taking that into consideration, **VPN** over the internet using **IPsec** remote access is also implemented.

➔ Since the branch office is situated far, The maintenance for core routers and switches of the branch is done via **SSH** connection.



LOGICAL LAYOUT OF THE COMPANY

Configurations considerations of the network architecture

Standardized cabling is a highly successful network architectural concept. Subsystems are specified components that make up a structured wire. The subsystems have included an user input facility where the whole the ISP network connects with employees' devices, equipment rooms with various devices for this and other network components that serve employees within the building, strong backbone cables linking different floors to high relative cables, and horizontal cables connecting components on the same floor.

The horizontal cabling in this network architecture consists of 100Mb/s Ethernet cables (Twisted Pair – CAT6) that indeed directly connect the wall sockets (terminating point of wired workstations) with the patch screen's back pane.

The telecommunication enclosure subsystem in this network architecture consists of switch chassis and patch panels. Using a patch panel in this network has a number of advantages, which are listed below:

- Identification
- Minor network cabling enhancements have no effect on switch chassis switches.

A key component of this subsystem is the switch chassis. Because around 20 wired end-user connections are required on the top level, switch (one 24 port switch) were employed in this design (IT). The primary advantages are as follows:

- Network maintenance
- Scalability
- Redundancy

On the third level, two switches (one 48 and one 24 port) are setup as stackable in the switch chassis, two switches (two 48 port switches) are installed on the first floor, and two switches (48 port) are configured on the ground floor.

This network architecture also includes **backbone cabling**. With backbone cabling, fiber optic cabling connects the rear glass of the switch chassis with the core switch on the second level. Two backbone links connect the two core switches on each floor (core switch 1 and core switch 2). In the case of a failure, two backbone links are used as backup connections.

On the second floor, the server hub will indeed be. It has two core switches, two core routers, a firewall, a server room, and a demilitarized zone (DMZ) where web servers are hosted for both internal and external access. The usage of two core switches ensures reliability and eliminates the possibility of single points of failure (SPOF). Both of these core switches have distinct fiber optic terminations. EtherChannel is used to connect these fundamental switches (port link aggregation technology). The core router handles traffic both within and outside the building. Redundancy is ensured and SPOF is eliminated by using two core routers. Separate high-speed cables were used

to connect two core routers to two core switches. The webserver is hosted in a DMZ because it is intended to be utilized by both insiders and outsiders. As a result, if an intruder tries to attack the web server, the accompanying network disturbance will be limited. The DMZ web server is directly connected to the firewall via a high-speed connection. Traffic intended for the internal network is processed through a firewall. The access control list on the firewall is configured to achieve this (ACL). On the inside, the firewall connects to core routers and the site server, while on the outside, it connects to the Internet.

The **server room** includes a **DNS server**, **DHCP server, FTP server, SYSLOG server, NTP server, Webserver**(private users only)**,** and **WLC controller**. Since redundancy and load balancing is the main goal of this network design, therefore there are **two** servers each except the WLC controller and NTP server. Since there is a total number of 6 VLANs for end-users, to achieve load balancing. VLAN 10,20, and 30 each have one primary server group, whereas VLAN 40,50, and 60 each have two. If one of the primary server groups experiences problems, HSRP will assist in routing traffic to the secondary server group. All servers in the server room are assigned static private IP addresses, while the site server in the DMZ is assigned a static public IP address. The primary server is connected to a primary server switch via 100Mbps cables, and the switch is connected to core switch 1 via 1Gps speed cables on its own. Similarly, the secondary server is connected to a secondary server switch via 100Mbps cables, and the switch is connected to core switch 2 via 1Gps speed cables on its own.

Configurations considerations between the firewall and the Internet Service Provider (ISP).

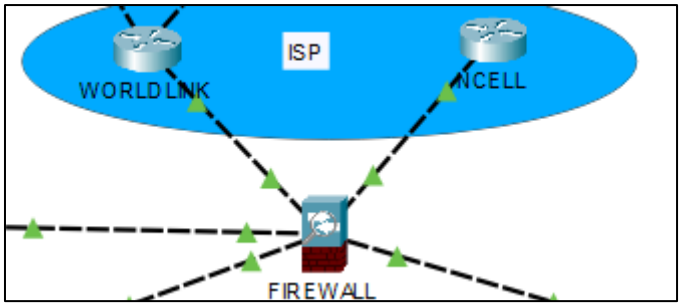


Figure 3 Configuration between Firewall and ISP

```
interface Ethernet1/1
 ip address 102.50.50.2 255.255.255.252
 ip nat outside
 duplex auto
 speed auto
!
interface Ethernet1/2
 ip address 103.45.45.5 255.255.255.252
 ip helper-address 10.10.10.2
 ip helper-address 10.10.10.6
 duplex auto
 speed auto
```

Figure 5 interface IP

```
ip local pool VPNCLIENT 172.31.0.1 172.31.0.254
ip nat inside source list 100 interface Ethernet1/0 overload
ip nat inside source list 101 interface Ethernet1/1 overload
ip classless
ip route 0.0.0.0 0.0.0.0 103.45.45.1 10
ip route 0.0.0.0 0.0.0.0 102.50.50.1 20
ip route 103.45.45.8 255.255.255.252 103.45.45.1
!
```

Figure 4 NAT and Default route

```
access-list 55 permit host 90.90.90.2
access-list 100 permit ip 192.168.0.0 0.0.0.255 any
access-list 100 permit ip 172.16.0.0 0.0.0.127 any
access-list 100 permit ip 172.16.0.128 0.0.0.63 any
access-list 100 permit ip 172.16.0.192 0.0.0.63 any
access-list 100 permit ip 172.16.1.0 0.0.0.31 any
access-list 100 permit ip 172.16.1.32 0.0.0.31 any
access-list 100 permit ip 172.16.1.64 0.0.0.31 any
access-list 101 permit ip 192.168.0.0 0.0.0.255 any
access-list 101 permit ip 172.16.0.0 0.0.0.127 any
access-list 101 permit ip 172.16.0.128 0.0.0.63 any
access-list 101 permit ip 172.16.0.192 0.0.0.63 any
access-list 101 permit ip 172.16.1.0 0.0.0.31 any
access-list 101 permit ip 172.16.1.32 0.0.0.31 any
access-list 101 permit ip 172.16.1.64 0.0.0.31 any
```

Figure 6 ACL list

- In this network design, two ISP (WorldLink, Ncell) are taken as enterprise customers. Both core routers are connected from the firewall and then connected to ISPs. **Default route was done in the firewall to form a link between both the ISPs.**
- For this network design, WorldLink is considered as primary ISP whereas Ncell is considered as standby ISP, meaning all the endnotes are connected to the internet via WorldLink.If there is any kind of issue with the link of WorldLink traffic is shifted towards Ncell.
- **Access Control List (ACL)** is implemented in Firewall to prevent unauthorized devices to enter or exit the company network.
- All the end-users private IP addresses are **PATed** with a public IP address at the firewall.

Configurations considerations between the headquarter and the branch.

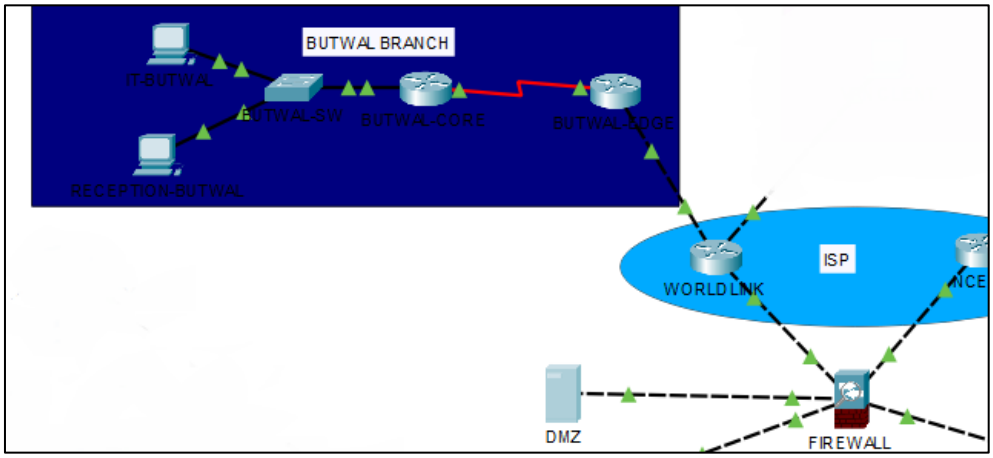


Figure 7 Configuration between Branch and headquarter.

```
interface Tunnel1
 ip address 192.168.13.2 255.255.255.252
 mtu 1476
 tunnel source Ethernet1/0
 tunnel destination 103.45.45.9
!
```

Figure 11 interface tunnel

```
router eigrp 10
 redistribute ospf 1 metric 1 1 255 255 1
 network 103.45.45.4 0.0.0.3
 network 192.168.13.0 0.0.0.3
```

Figure 10 EIGRP configuration

```
ip local pool VPNCLIENT 172.31.0.1 172.31.0.254
ip nat inside source list 100 interface Ethernet1/0 overload
ip nat inside source list 101 interface Ethernet1/1 overload
ip classless
ip route 0.0.0.0 0.0.0.0 103.45.45.1 10
ip route 0.0.0.0 0.0.0.0 102.50.50.1 20
ip route 103.45.45.8 255.255.255.252 103.45.45.1
```

Figure 9 static route to branch

```
line vty 0 4
 access-class 55 in
 transport input ssh
line vty 5 15
 access-class 55 in
 transport input ssh
!
!
!
```

Figure 8ssh

```
!
username admin secret 5 $1$mERr$vTbHul1N28cEp81kLqr0f/
!
!
license udi pid CISCO2811/K9 sn FTX10171720-
!
!
!
```

- The branch office is situated far from the main headquarters. As a result, **GRE tunnelling** is done through the internet.

- Worldlink has provided another public IP to the Butwal branch. With the help of that IP, a **static route** was done between headquarter firewall and Butwal's edge router, and a private IP was provided in the interface of the tunnel.
- The firewall acts as one end of the tunnel whereas Butwal's edge router acts as another end of the tunnel.
- **SSH configuration** has been done to both the core and edge routers of the branch for maintenance or to keep logs with **ACL**.
- To exchange routes, **EIGRP** was configured in the firewall and core router (branch)
- Since the firewall also has routes of the branch, **redistribution** was done.

Configurations considerations of the branch.

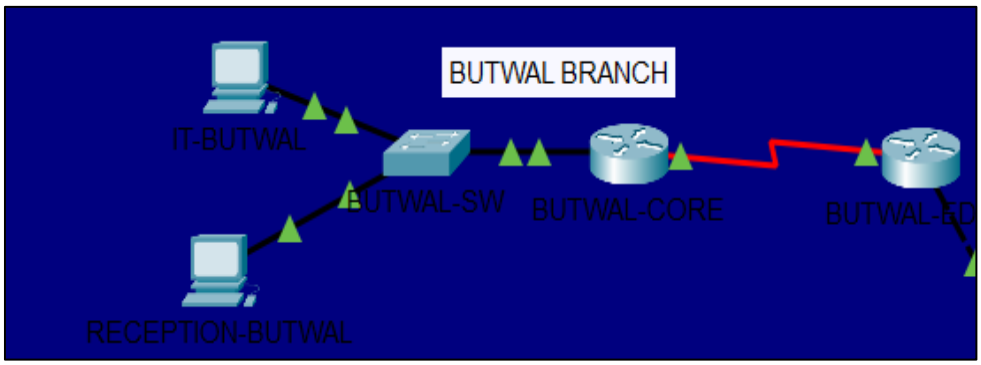


Figure 12 Branch Configuration

```
router eigrp 10
 redistribute ospf 10 metric 1 1 255 255 1
 network 192.168.13.0 0.0.0.3
 network 60.60.60.0 0.0.0.3
!
router ospf 10
 log-adjacency-changes
 redistribute eigrp 10 subnets
 network 60.60.60.0 0.0.0.3 area 0
!
router rip
!
ip nat inside source list NAT_ACL interface GigabitEthernet0 overload
ip nat inside source static tcp 192.168.3.2 8443 172.1.1.1 8443
ip classless
ip route 103.45.45.0 255.255.255.252 103.45.45.10
!
ip flow-export version 9
!
!
ip access-list standard NAT_ACL
 permit 192.168.0.0 0.0.255.255
access-list 55 permit host 90.90.90.2
```

Figure 13 OSPF, Static Route and ACL

```
interface Tunnel1
 ip address 192.168.13.1 255.255.255.252
 mtu 1476
 tunnel source GigabitEthernet0
 tunnel destination 103.45.45.2
!
!
interface Tunnel0
 no ip address
 mtu 1476
!
!
interface GigabitEthernet0
 ip address 103.45.45.9 255.255.255.252
 ip nat outside
 duplex auto
 speed auto
```

Figure 14 IP interface

```
line vty 0 4
 access-class 55 in
 login local
 transport input ssh
line vty 5 15
 access-class 55 in
 login local
 transport input ssh
```

Figure 15 SSH

```
ip dhcp excluded-address 80.80.80.1
ip dhcp excluded-address 80.80.90.1
!
ip dhcp pool IT-BUTWAL
 network 80.80.80.0 255.255.255.252
 default-router 80.80.80.1
 dns-server 10.10.10.10
ip dhcp pool RECPTION-BUTWAL
 network 80.80.90.0 255.255.255.252
 default-router 80.80.90.1
 dns-server 10.10.10.10
!
!
!
ip cef
no ipv6 cef
!
!
!
username admin secret 5 $1$mERr$nQOtpBRHIKYFaRhCuVumM1
```

Figure 16 DHCP POOL

```
interface FastEthernet0/1
 switchport access vlan 80
 switchport mode access
!
interface FastEthernet1/1
 switchport access vlan 90
```

Figure 17 IP Interface

- **OSPF** routing protocol is used between the core and edge routers with the **process id 10**.
- Since the edge router also has routes of headquarter, **redistribution** was done between the edge and core router of the branch.
- The core router acts as a **DHCP** server to two VLANs.

Configurations considerations of the Remote Access VPN.

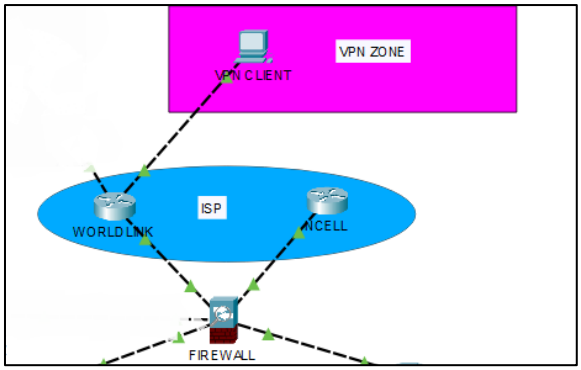


Figure 18 REMOTE ACCESS VPN

```
crypto isakmp policy 100
 encr aes 256
 authentication pre-share
 group 5
 lifetime 3600
!
!
!
crypto isakmp client configuration group vpngroup
 pool VPNCLIENT
!
crypto isakmp client configuration group GroupVPN
 key cisco
 pool VPNCLIENT
!
!
crypto ipsec transform-set SetVPN esp-aes esp-sha-hmac
!
crypto dynamic-map DynamicVPN 100
 set transform-set SetVPN
 reverse-route
!
crypto map StaticMap client authentication list UserVPN
crypto map StaticMap isakmp authorization list GroupVPN
crypto map StaticMap client configuration address respond
crypto map StaticMap 20 ipsec-isakmp dynamic DynamicVPN
!
```

Figure 19 IPsec config

```
ip local pool VPNCLIENT 172.31.0.1 172.31.0.254
ip nat inside source list 100 interface Ethernet1/0 overload
ip nat inside source list 101 interface Ethernet1/1 overload
ip classless
ip route 0.0.0.0 0.0.0.0 103.45.45.1 10
ip route 0.0.0.0 0.0.0.0 102.50.50.1 20
ip route 103.45.45.8 255.255.255.252 103.45.45.1
```

Figure 20 Pool for VPN CLIENT

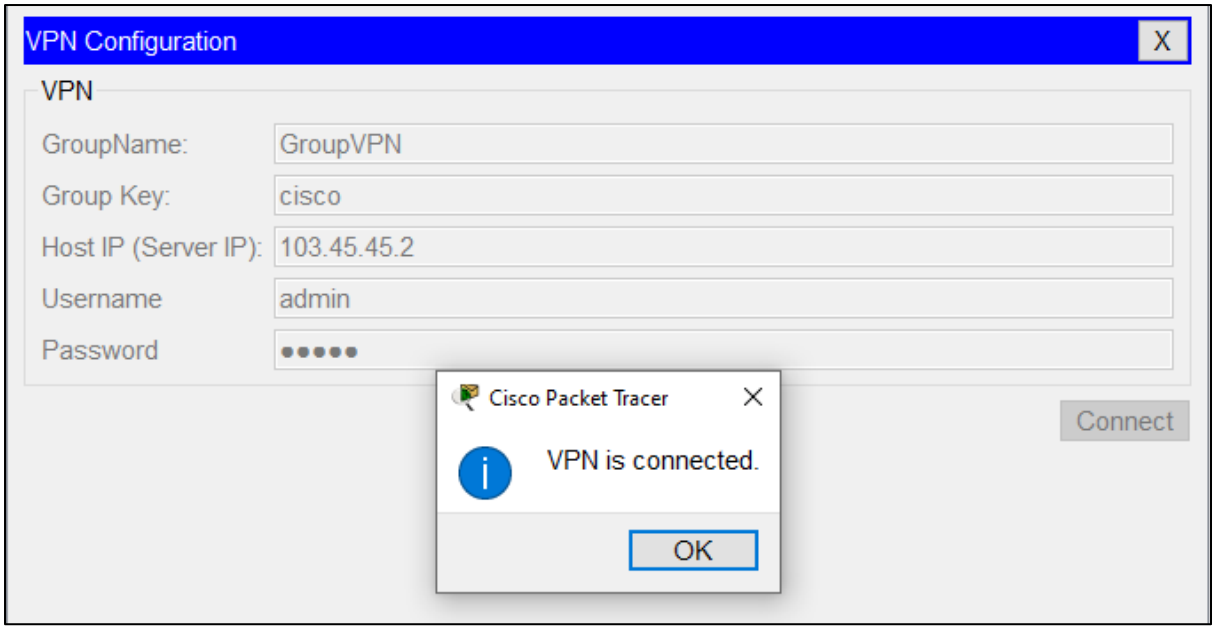


Figure 21 VPN verification

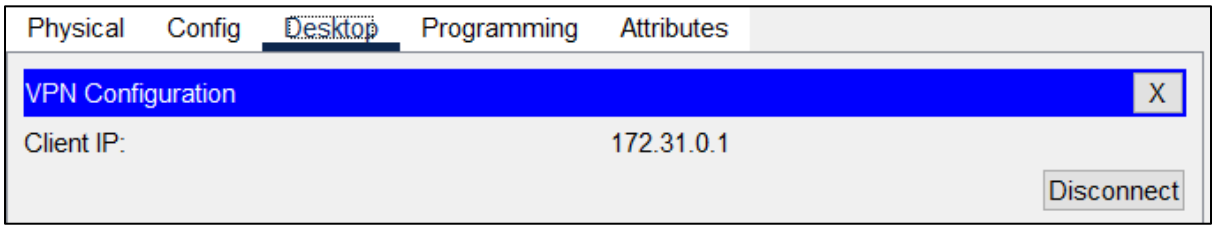


Figure 22 VPN IP verification

- Since Covid is still a thing, many people need to work from home. Between the main site and the home worker, a virtual private network is used for connectivity. The **IPsec VPN server** is hosted at the firewall.
- A **local pool** is created in the firewall that is later given to an employee who is connected via VPN.
- VPN server was created with an **IPsec tunnel(encrypted tube)** so that only **authorized** employees can access the internal network.

Configurations considerations between the firewall and core layers.

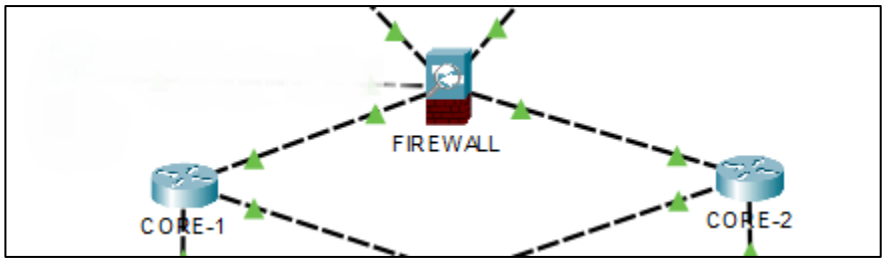


Figure 23 Configuration between firewall and core layers

```
interface FastEthernet0/0
 ip address 50.50.50.17 255.255.255.252
 ip nat inside
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 50.50.50.22 255.255.255.252
 ip nat inside
 duplex auto
 speed auto
```

```
interface GigabitEthernet6/0
 ip address 50.50.50.18 255.255.255.252
 duplex auto
 speed auto
!
```

Figure 24 IP Interface

```
router ospf 1
 log-adjacency-changes
 network 50.50.50.16 0.0.0.3 area 0
 network 50.50.50.20 0.0.0.3 area 0
 network 103.45.45.4 0.0.0.3 area 0
 default-information originate
!
```

Figure 25 OSPF

```
!
line vty 0 4
 access-class 55 in
 transport input ssh
line vty 5 15
 access-class 55 in
 transport input ssh
!
```

Figure 26 SSH

- OSPF routing protocol is done between the firewall and core layers with **process id 1 and area 0.**
- **SSH configuration** has been done to both the firewall and core layers, with **ACL**.
- Since the firewall also has routes of the branch with the help of **EIGRP**, **redistribution** was done between core layers.

Configurations considerations between the core layers and distribution layers.

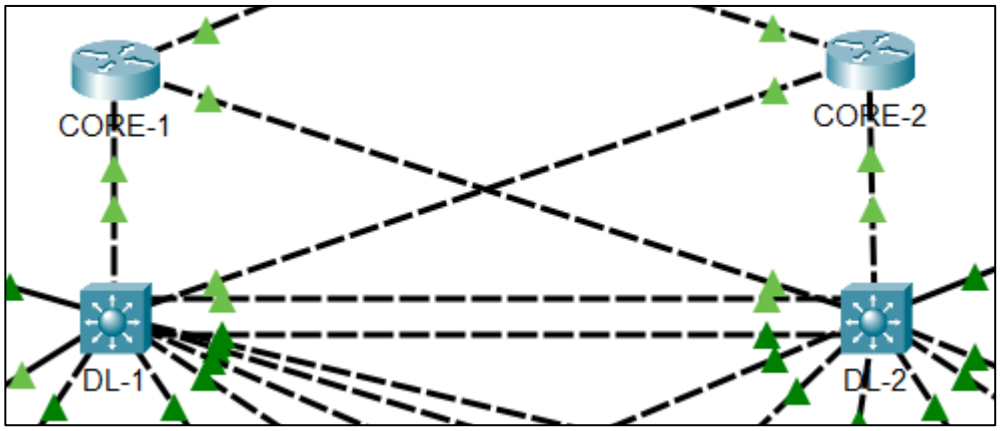


Figure 27 Configuration between core and distribution layers

```
interface FastEthernet0/0
 ip address 50.50.50.2 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet1/0
 ip address 50.50.50.9 255.255.255.252
 duplex auto
 speed auto
```

Figure 28 IP Interface

```
interface GigabitEthernet6/0
 ip address 50.50.50.18 255.255.255.252
 duplex auto
 speed auto
!
router ospf 1
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 network 50.50.50.0 0.0.0.3 area 0
 network 50.50.50.8 0.0.0.3 area 0
 network 50.50.50.16 0.0.0.3 area 0
```

Figure 29 OSPF

```
line vty 0 4
 access-class 55 in
 login local
 transport input ssh
line vty 5 15
 access-class 55 in
 login local
 transport input ssh
!
```

Figure 30 SSH

```
access-list 55 permit host 90.90.90.2
!
!
!
!
!
snmp-server community write RW
snmp-server community read RO
```

Figure 31 SNMP CONFIG

- **OSPF** routing protocol is done between the distribution and core layers with **pro**
- **SSH configuration** has been done to both the distribution and core layers, by implementing **ACL**.
- Since the distribution layer also has routes of the servers and VLANs, **redistribution** was done between the layers.
- Both the core routers are configured as **SNMP** servers**.**

Configurations considerations between distribution layers and access layers.

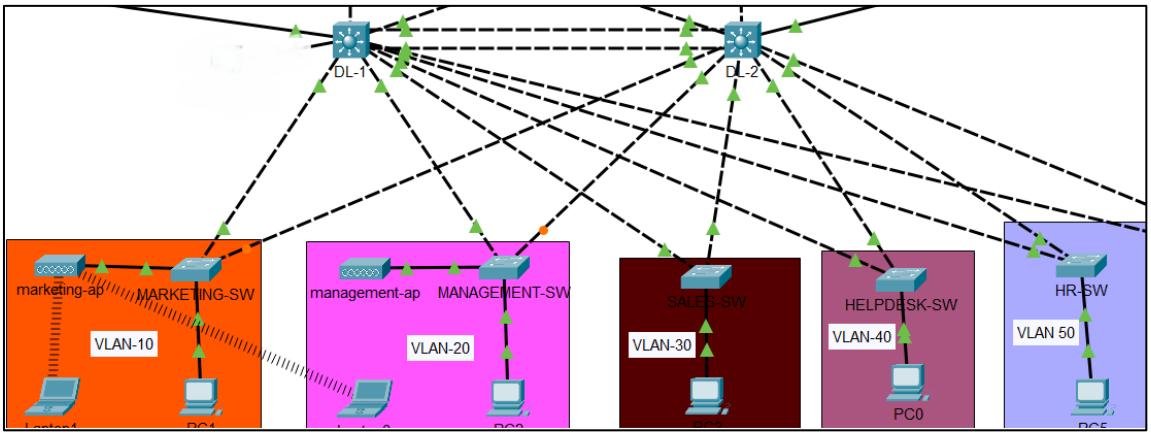


Figure 32 Config between distribution and access layer

```
10   marketing                      active
20   management                     active
30   sales                          active
40   helpdesk                       active
50   hr                             active
60   it                             active
100  DHCP-PRIMARY                   active
101  DHCP-SECONDARY                 active
110  DNS-PRIMARY                    active
111  DNS-SECONDARY                  active
120  WEB-SERVER-1                   active
121  WEB-SERVER-2                   active
130  SYSLOG-PRIMARY                 active
131  SYSLOG-SECONDARY               active
140  FTP-PRIMARY                    active
141  FTP-SECONDARY                  active
150  WLC-AP                         active
160  NTP-SERVER                     active
676  SW-MARKETING-MANAGEMENT        active
677  SW-MANAGEMENT-MANAGEMENT       active
678  SW-SALES-MANAGEMENT            active
679  SW-HELPDESK-MANAEGMENT         active
680  SW-HR-MANAGEMENT               active
681  SW-IT-MANAGEMENT               active
```

Figure 33 VLAN Configuration

```
ip dhcp snooping vlan 10,20,30,40,50,60
ip dhcp snooping
!
ip ssh version 2
ip domain-name networkhats.com
!
!
spanning-tree mode rapid-pvst
spanning-tree vlan 10,20,30 priority 24576
spanning-tree vlan 40,50,60 priority 28672
```

Figure 34 DHCP Snooping, RPVST+ AND SSH

```
interface FastEthernet0/6
 ip dhcp snooping trust
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 1 mode desirable
!
interface FastEthernet0/7
 ip dhcp snooping trust
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 1 mode desirable
```

Figure 35 IP Interface

```
interface Vlan10
 mac-address 0001.4209.1a01
 ip address 172.16.0.2 255.255.255.128
 ip helper-address 10.10.10.2
 ip helper-address 10.10.10.6
 standby 1 ip 172.16.0.1
 standby 1 priority 105
 standby 1 preempt
!
interface Vlan20
 mac-address 0001.4209.1a02
 ip address 172.16.0.130 255.255.255.192
 ip helper-address 10.10.10.2
 ip helper-address 10.10.10.6
 standby 1 ip 172.16.0.129
 standby 1 priority 105
 standby 1 preempt
!
interface Vlan30
 mac-address 0001.4209.1a03
 ip address 172.16.0.194 255.255.255.192
 ip helper-address 10.10.10.2
 ip helper-address 10.10.10.6
 standby 1 ip 172.16.0.193
 standby 1 priority 105
 standby 1 preempt
```

```
interface Vlan40
 mac-address 0001.4209.1a04
 ip address 172.16.1.2 255.255.255.224
 ip helper-address 10.10.10.6
 ip helper-address 10.10.10.2
 standby 1 ip 172.16.1.1
!
interface Vlan50
 mac-address 0001.4209.1a05
 ip address 172.16.1.34 255.255.255.224
 ip helper-address 10.10.10.6
 ip helper-address 10.10.10.2
 standby 1 ip 172.16.1.33
!
interface Vlan60
 mac-address 0001.4209.1a06
 ip address 172.16.1.66 255.255.255.224
 ip helper-address 10.10.10.6
 ip helper-address 10.10.10.2
 standby 1 ip 172.16.1.65
```

Figure 36 VLAN interface and HSRP Configuration

```
router eigrp 1
 redistribute ospf 1 metric 1 1 255 255 1
 network 10.10.10.0 0.0.0.3
 network 172.16.0.0 0.0.0.127
 network 172.16.0.128 0.0.0.63
 network 10.10.10.16 0.0.0.3
 network 192.168.0.0
 network 172.16.0.192 0.0.0.63
 network 172.16.1.0 0.0.0.31
 network 172.16.1.32 0.0.0.31
 network 172.16.1.64 0.0.0.31
 network 10.10.10.8 0.0.0.3
 network 10.10.10.20 0.0.0.3
 network 10.10.10.12 0.0.0.3
 network 90.90.90.0 0.0.0.3
 auto-summary
!
router ospf 1
 log-adjacency-changes
 redistribute eigrp 1 subnets
 auto-cost reference-bandwidth 1000
 network 50.50.50.0 0.0.0.3 area 0
 network 50.50.50.4 0.0.0.3 area 0
```

Figure 37 EIGRP AND OSPF

```
access-list 10 deny 172.16.0.0 0.0.0.127
access-list 10 permit any
access-list 55 deny any
access-list 55 permit host 90.90.90.2
!
!
!
!
!
snmp-server community read RO
snmp-server community write RW
!
logging 10.10.10.18
```

Figure 38 SNMP, SYSLOG AND ACL

```
!
line vty 0 4
 access-class 55 in
 login local
 transport input ssh
line vty 5 15
 access-class 55 in
 login local
 transport input ssh
!
!
!
ntp server 10.10.10.41
```

Figure 39 SSH AND NTP

```
VTP Version capable             : 1 to 2
VTP version running             : 1
VTP Domain Name                 : milan.com
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0007.EC24.9200
Configuration last modified by 0.0.0.0 at 2-16-22 00:13:48
Local updater ID is 172.16.0.2 on interface Vl10 (lowest numbered VLAN interface found)

Feature VLAN :
--------------
VTP Operating Mode              : Server
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 29
Configuration Revision            : 1213
MD5 digest                        : 0x82 0xA7 0x6A 0x50 0x60 0xEF 0x7B 0xE3
                                    0x85 0xAB 0x31 0xA5 0x6C 0xB6 0x8F 0x1E
```

Figure 40 VTP configuration

- The link between the layers is made **trunk**.
- In distribution, **L3 switches** are used. Two L3 switches are linked by **EtherChannel (**port link aggregation technology).
- Since the device are of CISCO, Port Aggregation Protocol (**PAgP**) is used.
- All the switches in distribution and access layers are in spanning tree protocol (**Rapid PVST+**).
- Both the L3 switches are in Hot Standby Router Protocol (**HSRP**).
- In order to achieve load-balancing between VLANs, The **Priority of VLANs** is given in L3 switches.
- **VLAN** for every department and servers are also configured.
- **Inter-VLAN routing** is done between the layers.
- VLAN Trunking Protocol (**VTP**) is done between the layers, Both L3 switches are configured as servers and all the switches in access layers are configured as Client.
- Both the L3 switches are configured as **SNMP** servers.
- **SSH configuration** has been done to both the layers, with **ACL**.
- Distribution layers are configured as **DHCP relay agents** to clients.
- **DHCP snooping** is configured in both layers.
- **EIGRP** routing protocol is used to share routes between the end-notes.
- Since the distribution layer also has routes of the core routers, **redistribution** was done between the layers.

Configurations considerations between distribution layer and server room.

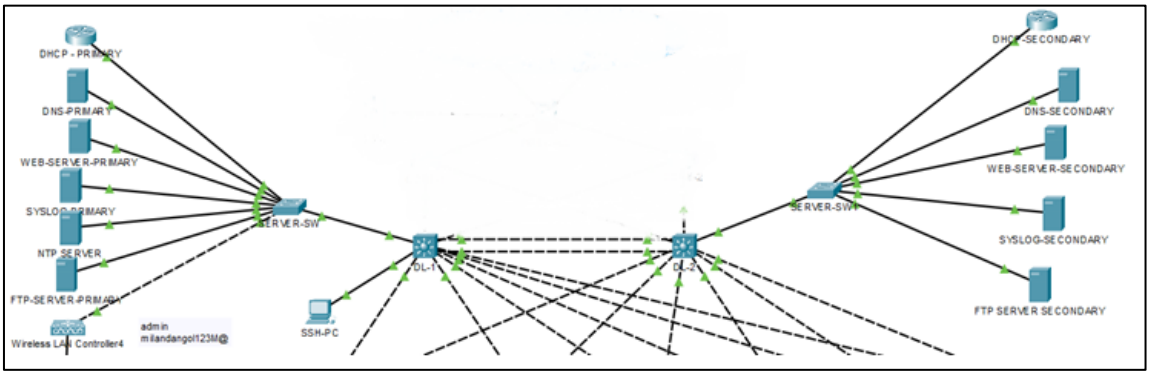


Figure 41 Configuration between distribution layer and server room

```
100  DHCP-PRIMARY                     active
101  DHCP-SECONDARY                   active
110  DNS-PRIMARY                      active
111  DNS-SECONDARY                    active
120  WEB-SERVER-1                     active
121  WEB-SERVER-2                     active
130  SYSLOG-PRIMARY                   active
131  SYSLOG-SECONDARY                 active
140  FTP-PRIMARY                      active
141  FTP-SECONDARY                    active
150  WLC-AP                           active
160  NTP-SERVER                       active
```

Figure 42 Vlan

```
interface Vlan100
 mac-address 0001.4209.1a07
 ip address 10.10.10.1 255.255.255.252
interface Vlan110
 mac-address 0001.4209.1a08
 ip address 10.10.10.9 255.255.255.252
interface Vlan120
 mac-address 0001.4209.1a09
 ip address 10.10.10.13 255.255.255.252
interface Vlan130
 mac-address 0001.4209.1a0a
 ip address 10.10.10.17 255.255.255.252
interface Vlan140
 mac-address 0001.4209.1a0b
 ip address 10.10.10.21 255.255.255.252
interface Vlan150
 mac-address 0001.4209.1a0c
 ip address 192.168.0.1 255.255.255.0
 ip helper-address 10.10.10.2
 ip access-group 10 in
 ip access-group 10 out
interface Vlan160
 mac-address 0001.4209.1a0d
 ip address 10.10.10.42 255.255.255.252
```

Figure 43 VLAN interface

```
ip dhcp relay information trust-all
!
!
ip dhcp excluded-address 172.16.0.1 172.16.0.3
ip dhcp excluded-address 172.16.0.129 172.16.0.131
ip dhcp excluded-address 172.16.0.193 172.16.0.195
ip dhcp excluded-address 172.16.1.1 172.16.1.3
ip dhcp excluded-address 172.16.1.33 172.16.1.35
ip dhcp excluded-address 172.16.1.65 172.16.1.67
ip dhcp excluded-address 192.168.0.1 192.168.0.100
ip dhcp excluded-address 103.45.45.5
```

Figure 44 DHCP EXCLUDE ADDRESS

```
ip dhcp pool marketing
 network 172.16.0.0 255.255.255.128
 default-router 172.16.0.1
 dns-server 10.10.10.10
ip dhcp pool management
 network 172.16.0.128 255.255.255.192
 default-router 172.16.0.129
 dns-server 10.10.10.10
ip dhcp pool sales
 network 172.16.0.192 255.255.255.192
 default-router 172.16.0.193
 dns-server 10.10.10.10
ip dhcp pool helpdesk
 network 172.16.1.0 255.255.255.224
 default-router 172.16.1.1
 dns-server 10.10.10.10
ip dhcp pool hr
 network 172.16.1.32 255.255.255.224
 default-router 172.16.1.33
 dns-server 10.10.10.10
ip dhcp pool it
 network 172.16.1.64 255.255.255.224
 default-router 172.16.1.65
 dns-server 10.10.10.10
ip dhcp pool WLC-AP
 network 192.168.0.0 255.255.255.0
 default-router 192.168.0.1
 dns-server 10.10.10.10
ip dhcp pool DMZ
 network 103.45.45.4 255.255.255.252
 default-router 103.45.45.5
```

Figure 45 DHCP POOL

```
dhcp-primary#show ip dhcp b
dhcp-primary#show ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
172.16.0.4       0001.C765.23A5           --                     Automatic
172.16.0.132     00E0.F934.32E7           --                     Automatic
172.16.0.196     0030.A3E0.2E84           --                     Automatic
172.16.1.4       00E0.F9BC.0C02           --                     Automatic
172.16.1.36      0040.0B53.1093           --                     Automatic
172.16.1.68      0002.16AA.2106           --                     Automatic
192.168.0.102    00D0.58E7.6201           --                     Automatic
192.168.0.101    00E0.F77A.6501           --                     Automatic
192.168.0.103    0010.1136.EAB3           --                     Automatic
192.168.0.104    0040.0BDA.85CD           --                     Automatic
103.45.45.6      0002.17A1.943D           --                     Automatic
```

Figure 46 DHCP Binding

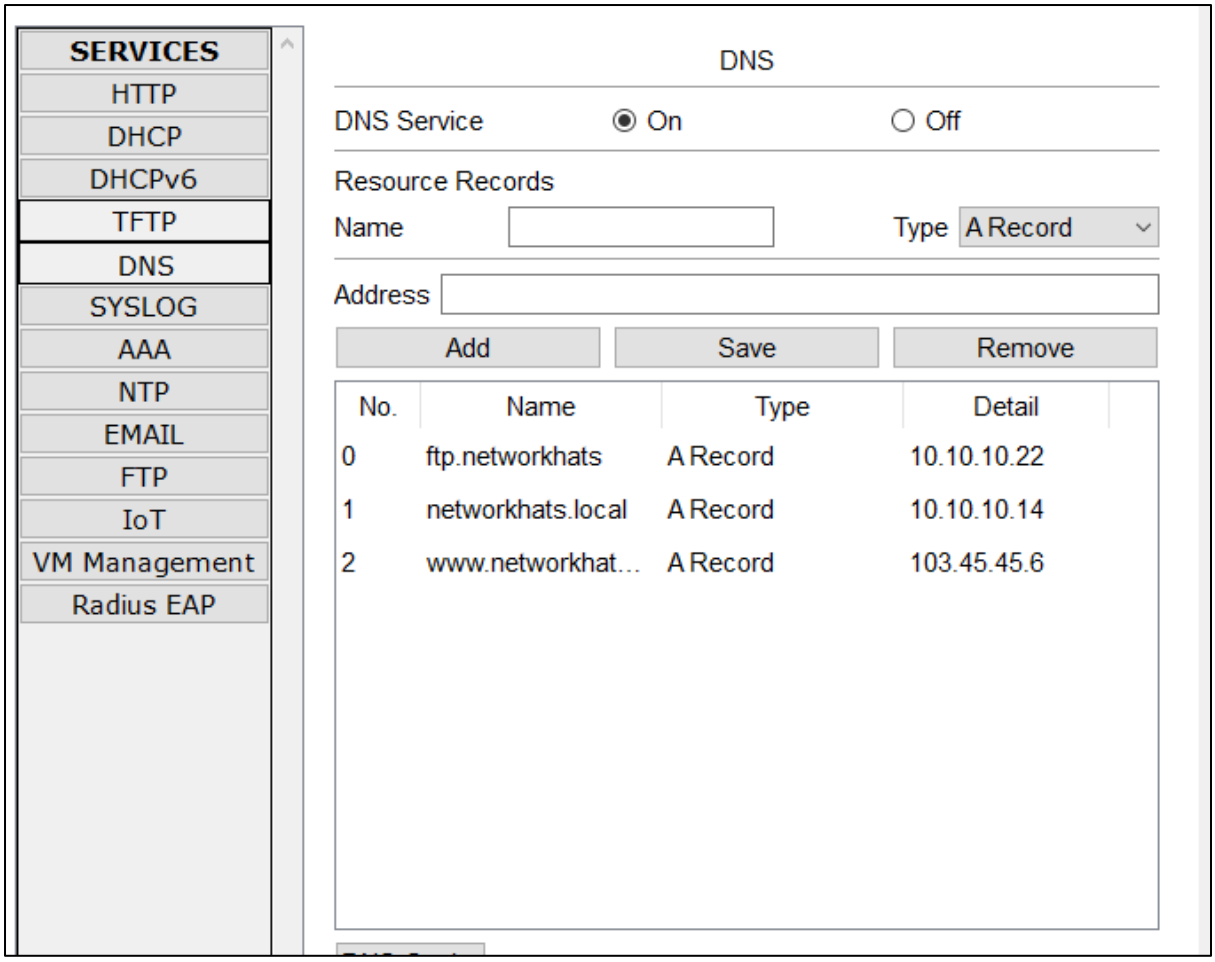


Figure 47 DNS Configuration

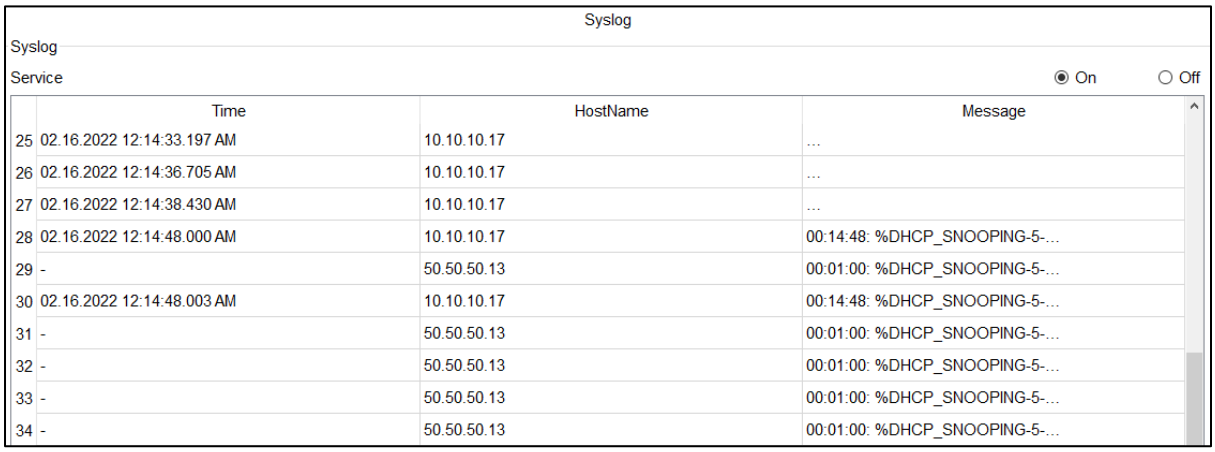


Figure 48 Syslog Configuration

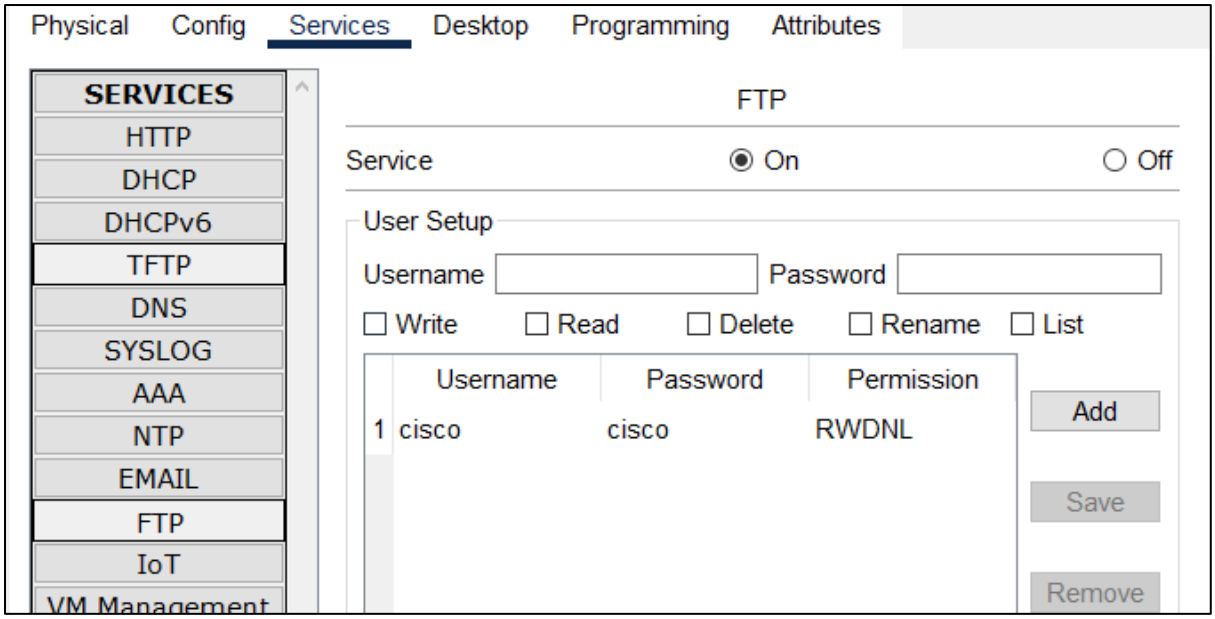


Figure 49 FTP Configuration

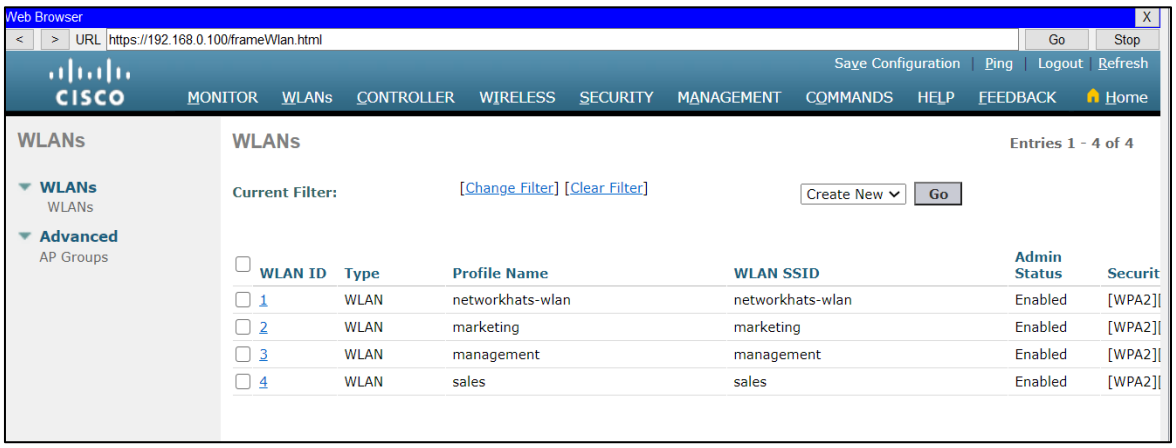


Figure 50 WLC configuration

- For each server, different **VLAN IDs** are given.
- Between DHCP servers and the distribution layer, the **EIGRP** routing protocol is used.
- FTP, WEB, SYS LOG, NTP, DNS, DHCP servers, and WLC controllers are configured.
- In the **WLC controller (WPA2-PSK (AES))**, the latest AES encryption method is configured.
- **DNS server** is used to give **hostnames** to FTP and WEB server.
- Redundancy and load-balancing are configured across the server room and distribution.

Configurations considerations between access layers and end nodes.

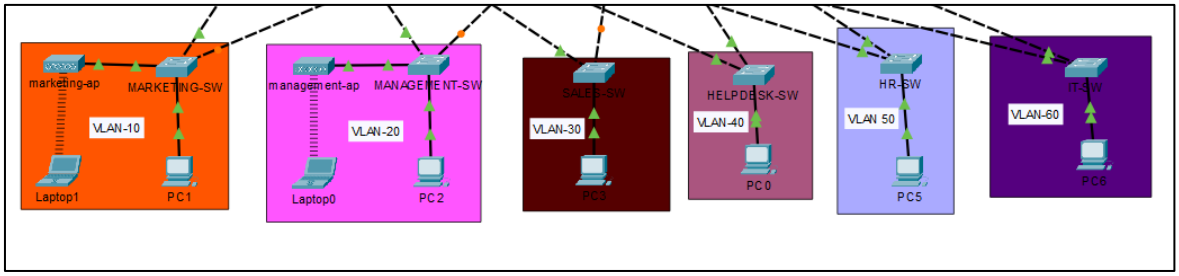


Figure 51 Configuration between access and end nodes

```
ip dhcp snooping vlan 10,150
ip dhcp snooping
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport trunk allowed vlan 10,150,676
 ip dhcp snooping trust
 switchport mode trunk
!
```

Figure 52 DHCP SNOOPING, RPVST

```
interface FastEthernet1/1
 switchport access vlan 10
 switchport mode access
 switchport port-security mac-address sticky
 switchport port-security violation protect
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet2/1
 switchport trunk allowed vlan 10,150,676
 ip dhcp snooping trust
 switchport mode trunk
!
interface FastEthernet3/1
 switchport access vlan 150
 switchport mode access
```

Figure 53 PORT SECURITY

```
676  SW-MARKETING-MANAGEMENT          active
677  SW-MANAGEMENT-MANAGEMENT         active
678  SW-SALES-MANAGEMENT              active
679  SW-HELPDESK-MANAEGMENT           active
680  SW-HR-MANAGEMENT                 active
681  SW-IT-MANAGEMENT                 active
```

Figure 54 MANAGEMENT VLAN

```
MARKETING-SW(config)#do show vtp sta
VTP Version                     : 1
Configuration Revision          : 1213
Maximum VLANs supported locally : 255
Number of existing VLANs        : 29
VTP Operating Mode              : Client
VTP Domain Name                 : milan.com
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x65 0xA3 0x16 0xE2 0x61
0x62 0x21 0x68
Configuration last modified by 0.0.0.0 at 3-1-93 00:00:00
```

Figure 55 VTP CONFIGURATION

- **Management IP** is given to all the switches in this layer to build an **SSH** connection.
- **Port-security** is given to all the access ports with **BPDU guard** enabled.
- Trunk ports are also configured as **Trusted DHCP snooping**.
- **VTP mode client** is configured across all the switches in this layer.
- Only allowed VLANs are given to the **access ports**.
- The **access points** are also configured in this layer.

CONFIGURATION OF FIREWALL

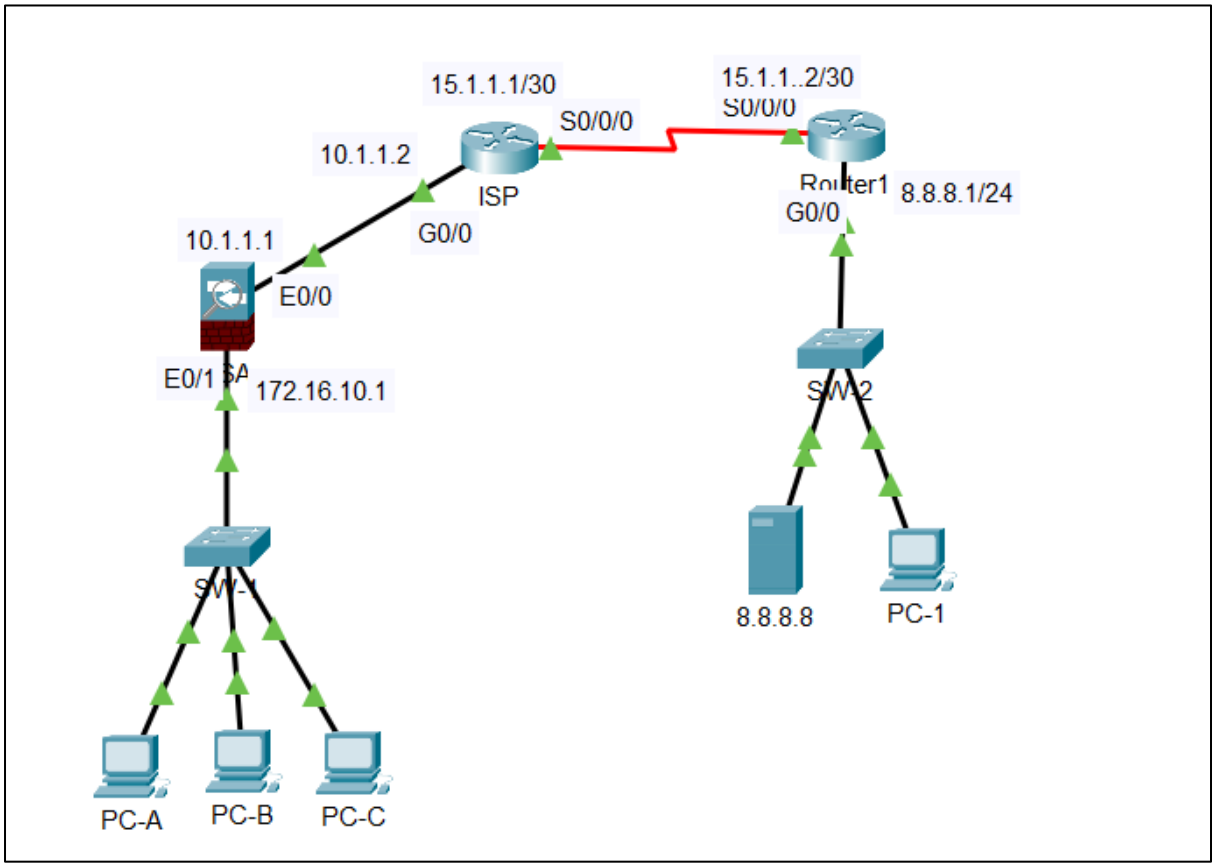


Figure 56 CONFIGURATION OF FIREWALL

```
interface Vlan1
 nameif inside
 security-level 100
 ip address 172.16.10.1 255.255.255.0
!
interface Vlan2
 nameif outside
 security-level 0
 ip address 10.1.1.1 255.255.255.0
!
object network INSIDE
 subnet 172.16.10.0 255.255.255.0
 nat (inside,outside) dynamic interface
!
route outside 0.0.0.0 0.0.0.0 10.1.1.2 1
!
access-list INTERNET extended permit tcp any any
access-list INTERNET extended permit icmp any any
!
!
access-group INTERNET in interface outside
access-group INTERNET out interface outside
```

Figure 57 IP interface, NAT and ACL

```
telnet timeout 5
ssh timeout 5
!
dhcpd auto_config outside
!
dhcpd address 172.16.10.5-172.16.10.10 inside
dhcpd enable inside
!
```

Figure 58 DHCP

```
interface GigabitEthernet0/0
 ip address 10.1.1.2 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 ip address 15.1.1.1 255.255.255.252
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 clock rate 2000000
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 log-adjacency-changes
 network 10.1.1.0 0.0.0.255 area 0
 network 15.1.1.0 0.0.0.3 area 0
```

Figure 59 OSPF

```
interface GigabitEthernet0/0
 ip address 8.8.8.1 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 ip address 15.1.1.2 255.255.255.252
!
interface Serial0/0/1
 no ip address
 clock rate 2000000
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 log-adjacency-changes
 network 8.8.8.0 0.0.0.255 area 0
 network 15.1.1.0 0.0.0.3 area 0
```

Figure 60 IP interface and OSPF

```
C:\>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:

Reply from 8.8.8.8: bytes=32 time<1ms TTL=252
Reply from 8.8.8.8: bytes=32 time=2ms TTL=252
Reply from 8.8.8.8: bytes=32 time<1ms TTL=252
Reply from 8.8.8.8: bytes=32 time=2ms TTL=252

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 1ms
```

Figure 61 VERIFICATION OF ISP

VERIFICATION FROM END NODES.

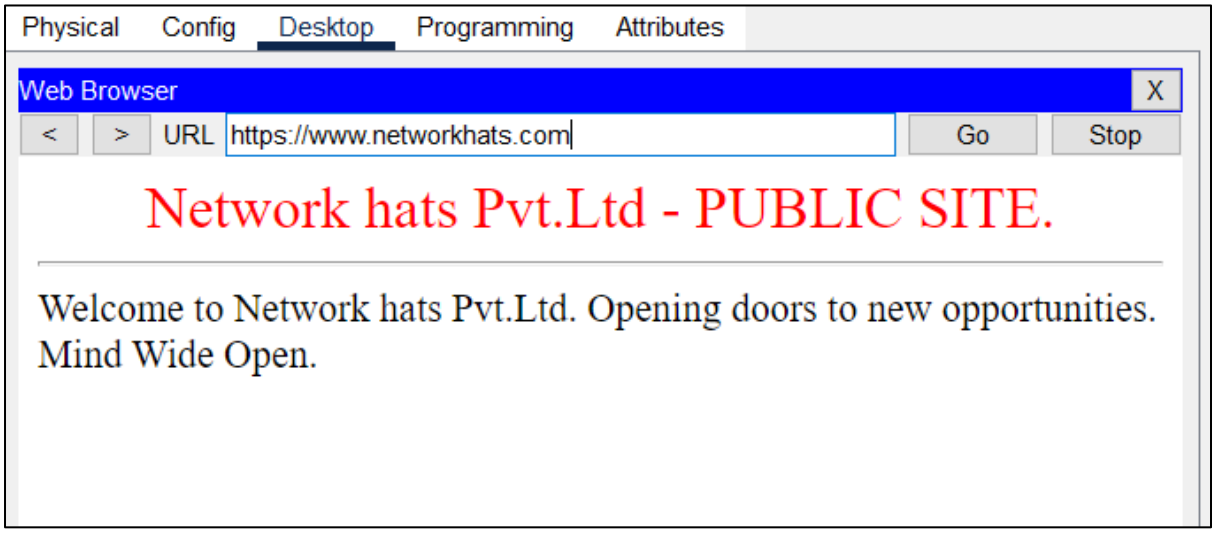


Figure 62 DMZ Verification

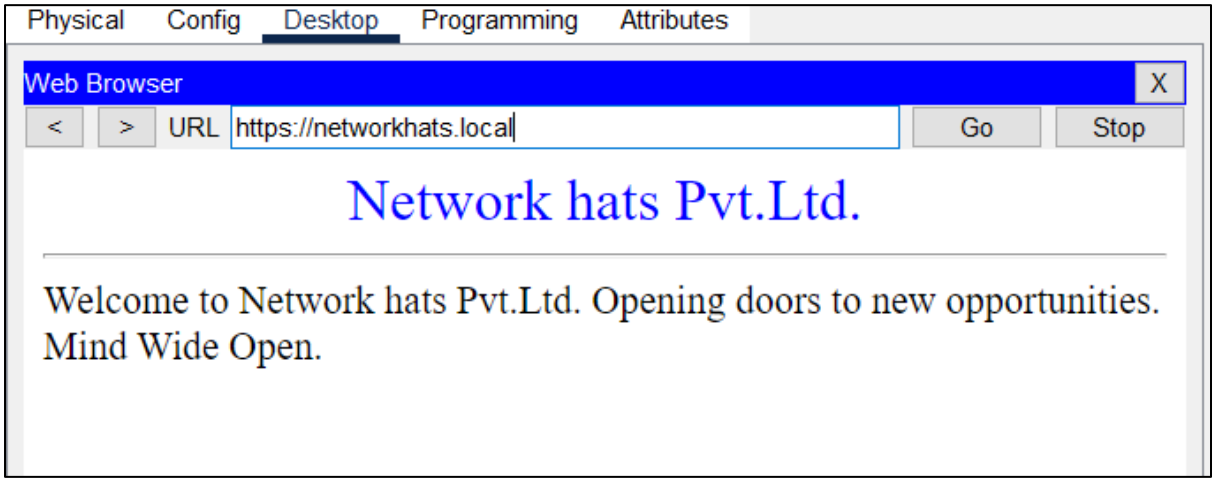


Figure 63 Webserver Verification

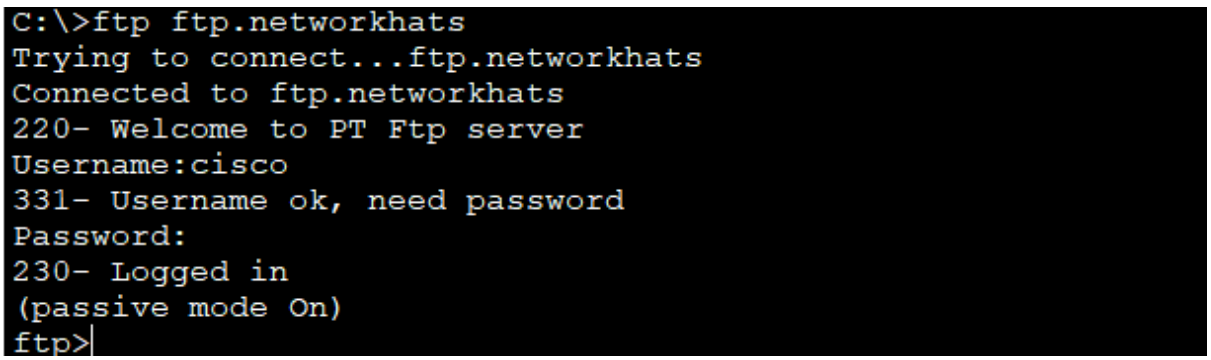


Figure 64 FTP configuration

```
C:\>ipconfig /renew

   IP Address.....................: 172.16.0.4
   Subnet Mask....................: 255.255.255.128
   Default Gateway................: 172.16.0.1
   DNS Server.....................: 10.10.10.10
```

Figure 65 DHCP Verification

```
C:\>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:

Reply from 8.8.8.8: bytes=32 time<1ms TTL=252
Reply from 8.8.8.8: bytes=32 time=2ms TTL=252
Reply from 8.8.8.8: bytes=32 time<1ms TTL=252
Reply from 8.8.8.8: bytes=32 time=2ms TTL=252

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 1ms
```

Figure 66 ISP verification from Departments

```
C:\>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:

Request timed out.
Reply from 8.8.8.8: bytes=32 time=7ms TTL=252
Reply from 8.8.8.8: bytes=32 time=8ms TTL=252
Reply from 8.8.8.8: bytes=32 time=8ms TTL=251

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 8ms, Average = 7ms
```

Figure 67 ISP Verification from wireless network

```
C:\>ssh -l admin 90.90.90.1

Password:



DL-1>en
Password:
DL-1#
```

Figure 68 SSH verification

Wireless Access Security

Creating a separate VLAN for wireless networking and using the WPA2-PSK (AES) protocol provide safe wireless connectivity for the office. For this wireless network, the WPA2-PSK (AES) protocol adds an extra layer of encryption and uses the latest AES encryption method. WPA2-PSK (AES) uses long passwords to secure data and offers a more secure network for home users. It aids in the centralization of wireless network management.

VLAN PLANNING

VLAN ID	VLAN NAME	VLAN DESCRIPTION
10	Marketing	This is used to group the 80 wired machines on the first floor.
20	Management	This is used to group the 50 wired machines on the third floor.
30	Sales	This is used to group the 50 wired machines on the ground floor.
40	Helpdesk	This is used to group the 30 wired machines on the ground floor
50	HR	This is used to group the 20 wired machines on third floor
60	IT	This is used to group the 20 wired machines on top floor

80	IT-BRANCH	This is used to group the IT department of butwal branch.
90	Reception-BRANCH	This is used to group the reception department of butwal branch.
100	DHCP-PRIMARY	This is used to connect the server and L3 switch in server room
101	DHCP-SECONDARY	This is used to connect the server and L3 switch in server room
110	DNS-PRIMARY	This is used to connect the server and L3 switch in server room
120	WEB-SERVER-1	This is used to connect the server and L3 switch in server room
130	SYSLOG-1	This is used to connect the server and L3 switch in server room
140	FTP-1	This is used to connect the server and L3 switch in server room
111	DNS-SECONDARY	This is used to connect the server and L3 switch in the server room

121	WEB-SERVER-2	This is used to connect the server and L3 switch in server room
131	SYSLOG-2	This is used to connect the server and L3 switch in server room
141	FTP-2	This is used to connect the server and L3 switch in server room
150	WLC	This is used to connect the server and L3 switch in server room
160	NTP-SERVER	This is used to connect the server and L3 switch in server room
676	SW-Marketing-Management	This is used to connect switch via SSH connection
677	SW-Management-Management	This is used to connect switch via SSH connection
678	SW-Sales-Management	This is used to connect switch via SSH connection
679	SW-Helpdesk-Management	This is used to connect switch via SSH connection

680	SW-HR-Management	This is used to connect switch via SSH connection
681	SW-IT-Management	This is used to connect switch via SSH connection

Table 1 VLAN PLANNING

IP ADDRESS PLANNING (Headquarter)

For this network design,

1. Private IP for departments - 172.16.0.0/23.
2. Private IP for server room - 10.10.10.0 /26.
3. Private IP between distribution - core layers - firewall - 50.50.50.0/27.
4. Private IP for WLC controller- 192.168.0.0/24
5. Private IP for SSH PC- 90.90.90./30
6. Public IP between ISPs- 103.45.45.0/30 (Worldlink) and 102.50.50.0/30 (Ncell)
7. Public IP between DMZ and Firewall - 103.45.45.4/30

Private IP for departments

VLAN Name	Hosts Size	Network	Mask	Subnet Mask	Virtual IP (HSRP)	Assignable Range
Marketing	80	172.16.0.0	/25	255.255.255.128	172.16.0.1	172.16.0.1 - 172.16.0.126
Management	50	172.16.0.128	/26	255.255.255.192	172.16.0.129	172.16.0.129 - 172.16.0.190

Sales	50	172.16.0.192	/26	255.255.255.192	172.16.0.193	172.16.0.193 - 172.16.0.254
Helpdesk	30	172.16.1.0	/27	255.255.255.224	172.16.1.1	172.16.1.1 - 172.16.1.30
HR	20	172.16.1.32	/27	255.255.255.224	172.16.1.33	172.16.1.33 - 172.16.1.62
IT	20	172.16.1.64	/27	255.255.255.224	172.16.1.65	172.16.1.65 - 172.16.1.94

Table 2 Private IP for departments

Private IP for Server Room

Subnet Name	Hosts Size	Network	Mask	Subnet Mask	Assignable Range
DHCP-PRIMARY	2	10.10.10.0	/30	255.255.255.252	10.10.10.1 - 10.10.10.2
DHCP-SECONDARY	2	10.10.10.4	/30	255.255.255.252	10.10.10.5 - 10.10.10.6
DNS-PRIMARY	2	10.10.10.8	/30	255.255.255.252	10.10.10.9 - 10.10.10.10

WEB-SERVER-1	2	10.10.10.12	/30	255.255.255.252	10.10.10.13 - 10.10.10.14
SYSLOG-1	2	10.10.10.16	/30	255.255.255.252	10.10.10.17 - 10.10.10.18
FTP-1	2	10.10.10.20	/30	255.255.255.252	10.10.10.21 - 10.10.10.22
DNS-SECONDARY	2	10.10.10.24	/30	255.255.255.252	10.10.10.25 - 10.10.10.26
WEB-SERVER-2	2	10.10.10.28	/30	255.255.255.252	10.10.10.29 - 10.10.10.30
SYSLOG-2	2	10.10.10.32	/30	255.255.255.252	10.10.10.33 - 10.10.10.34
FTP-2	2	10.10.10.36	/30	255.255.255.252	10.10.10.37 - 10.10.10.38

Table 3 Private IP for Server Room

Private IP for WLC Controller AND SSH PC

Subnet Name	Hosts Size	Network	Mask	Subnet Mask	Assignable Range
WLC	200	192.168.0.0	/24	255.255.255.0	192.168.0.1-0.255

SSH-PC	2	90.90.90.0	/30	255.255.255.252	90.90.90.1-90.2

Table 4 Private IP for WLC AND SSH PC

Private IP between distribution - core layers - firewall

1. Acronym for distribution layer switch 1 - DL1
2. Acronym for distribution layer switch 2 - DL2
3. Acronym for core layer router1 - CR1
4. Acronym for core layer router 1 - CR2

Name	Hosts Needed	Network	Mask	Subnet Mask	Usable Range
DL1-CR1	2	50.50.50.0	/30	255.255.255.252	50.50.50.1 - 50.50.50.2
DL1-CR2	2	50.50.50.4	/30	255.255.255.252	50.50.50.5 - 50.50.50.6
DL2-CR1	2	50.50.50.8	/30	255.255.255.252	50.50.50.9 - 50.50.50.10
DL2-CR2	2	50.50.50.12	/30	255.255.255.252	50.50.50.13 - 50.50.50.14
CR1-F	2	50.50.50.16	/30	255.255.255.252	50.50.50.17 - 50.50.50.18

CR2-F	2	50.50.50.20	/30	255.255.255.252	50.50.50.21 - 50.50.50.22

Table 5 Private IP between distribution - core layers - firewall

Public IP from ISPs

PUBLIC IP	NETWORK
FIREWALL-WORLDLINK	103.45.45.0/30
FIREWALL - NCELL	102.50.50.0/30
FIREWALL - DMZ	103.45.45.4/30

Table 6 Public IP from ISPs

IP ADDRESS PLANNING (Branch)

For this network design,

1. Private IP for IT-department - 80.80.80.0/30.
2. Private IP for Reception-department - 80.80.90.0/30.
3. Private IP between core layer - edge - 60.60.60.0/30.
4. Private IP for tunnelling - 192.168.13.0/30.
5. Public IP between ISP- 103.45.45.8/30 (Worldlink)

Private IP for IT and Reception-department.

Name	Hosts Needed	Network Address	Mask	Subnet Mask	Usable Range
IT-Branch	1	80.80.80.0	/30	255.255.255.252	80.80.80.1 - 80.80.80.2
Reception-Branch	1	80.80.90.0	/30	255.255.255.252	80.80.90.1 - 80.80.90.2

Table 7 Private IP for IT and Reception-department.

Private IP between the core layer and edge router and Tunnelling.

Name	Hosts Needed	Network Address	Mask	Subnet Mask	Usable Range
Core - Edge Router	2	60.60.60.0	/30	255.255.255.252	60.60.60.1 - 60.60.60.2
Tunnelling	2	192.168.13.0	/30	255.255.255.252	192.168.13.1 - 192.168.13.2

Table 8 Private IP between the core layer and edge router and Tunnelling.

Public IP between the ISP.

PUBLIC IP	NETWORK
Edge Router-WORLDLINK	103.45.45.8/30

Table 9 Public IP between the ISP.

IP ADDRESS PLANNING (VPN Users)

For this network design,

1. Private IP for IT-department - 172.31.0.0/24.

Name	Hosts Needed	Network Address	Slash	Mask	Usable Range
VPN Users	250	172.31.0.0	/24	255.255.255.0	172.31.0.1-172.31.0.254

Table 10 Public IP between the ISP.

Network protocols implemented in this design.

Routing

1. **OSPF**- For internal routing, the OSPF routing protocol is utilized as an interior gateway protocol. OSPF is a simple and open standard protocol that enables a network to scale effortlessly. OSPF provides stronger support for service providers and data centers because it is widely employed in traditional systems. It also facilitates the sharing of routing expertise.
2. **EIGRP**- The Enhanced Interior Gateway Routing Protocol (EIGRP) is a dynamic routing protocol that determines the best path for a packet to travel between two layer 3 devices. EIGRP uses protocol number 88 to operate on the network layer of the OSI model. It calculates the best path between two

EIGRP-enabled layers 3 devices using (EIGRP basics. 2018a)measurements (routers or switches). (Basics of EIGRP, 2018b)

3. **Static Route**- Static routing is a network routing strategy. Static routing is not a routing protocol; instead, it refers specifically to the manually configuration and better selection of a network path by the network administrator. So when network properties and also the immediate environment are believed to remain constant, this method is applied. (Techopedia,)
4. **Default route-** The default route takes effect when there are no other options for an IP destination address. The next-hop address of another routing device doing the same function is frequently included in the default route. The procedure is continued until the packet reaches its final destination.
5. **Inter VLAN routing** – Layer-3 switches are used to route traffic between different VLANs on the network. The traffic will be routed through the switch through the trunk link to the core routers. All VLAN networks are shown as directly linked routes in the routing table.

HSRP (Hot Standby Router Protocol)

In this network, HSRP is configured by combining the two layer-3 switches. As a result, the two layer-3 switches will function as one virtual router for internal hosts. One switch will be the active router for a set of Vlans IDs, while the other will be the active router for the remaining Vlans IDs, and the two switches will be standby routers for each other. The standby router takes over in the event that the current router fails. Because the new forwarding router utilizes the same MAC and IP addresses as the old router, the hosts can continue to talk without interruption even if one switch fails.

VLAN (Virtual Local Area Network)

There are 26 VLANs in this network. A wireless network has its own VLAN, with each floor having its own VLAN. This would prevent uncontrolled broadcast traffic from spreading to neighboring networks. VLAN adds another degree of network security and cost savings by logically dividing hosts connected to the same switch. A subnet is assigned to each VLAN.

Rapid PVST+

Each floor's switches are linked to the two core switches on the second floor through a redundant link. Two core routers and two core switches, as well as a server room switch and two core switches, now have redundant links. The purpose of having a backup connection is to ensure that even if one link fails, network components can still communicate with one another via the backup link. The network will become less crowded as a result of this. Adding a second link between network switches, on the other hand, increases the likelihood of a broadcast storm (loop). To prevent this, RPVST+ is effectively RSTP running in a single layer 2 domain per-VLAN. In a multi-VLAN network, VLAN tagging is used on ports to allow redundant links in one VLAN to be blocked while non-redundant lines in another VLAN can be used. (techhub.hpe.com,)

NAT (Network Address Translation)

A private IP address range for Classes is used within this network. The hosts, however, are unable to connect with this private IP address since private IP addresses are not routable on the Internet. As a result, NAT is an important part of this network architecture. The firewall maps one or two public IP addresses provided by the ISP to the private IP addresses used within the network using PAT (Port Address Translation). Using PAT, you can limit the number of public IP addresses that are used for translation.

IPSec VPN (VIRTUAL PRIVATE NETWORK)

Many people need to work from home because Covid is still active. A virtual private network is utilized for communication between the main site and the home worker. At the firewall, the VPN server is housed. IPsec VPN employs an encrypted tube for data transfer via the present Internet backbone. As a result, data transmission can be both dependable and cost-effective.

GRE Tunnelling (Generic Routing Encapsulation)

The branch office is located in a remote location from the main office. As a result, the cost of connecting the main site and the branch site through leased line is higher. As a result, GRE tunneling is carried out across the internet to address this issue. GRE is a technique for encapsulating data packets from one routing protocol inside packets from a different routing protocol. Encapsulating refers to the process of enclosing one data packet within another, much like putting a box inside another.

Port Security

With BPDU guard activated, all access ports receive port security. The MAC address of a frame is learned by the switch when it is routed through a switch port. Admin can limit the number of MAC addresses that can be taught to a port, specify static MAC addresses, and apply penalties on that port if it is used by an unauthorized user. To limit, switch off, or safeguard, the Admin can utilize port-security directives.

SNMP(Simple Network Management Protocol)

SNMP stands for Simple Network Management Protocol, and it is a networking protocol that is used to control and monitor network-connected devices in Internet Protocol networks. The SNMP protocol is built into a wide range of local devices, including routers, switches, servers, firewalls, and wireless access points. (*SNMP Ports & Protocol - What is it?* | *ThousandEyes.*)

Servers that are implemented in this design.

DNS (Domain Name System)

The DNS server, which is housed in the server room on the second floor, has been set up. Computers cannot decipher the domain name. IP addresses, which are numbers, must be converted. As a result, the DNS server records the domain name and IP address for each host. As a result, the complexity of the network and its management can be reduced.

DHCP (Dynamic Host Configuration Protocol)

The service is hosted by the DHCP node in the server room. For different VLANs, the DHCP server can create an IP address pool. As a result, the DHCP server dynamically distributes IP addresses to network hosts. The IP address pool can be cleaned up by removing the VLAN's static IP address. The main advantage of utilizing this protocol is that it offers hosts with consistent IP address setup and reduces network management. DHCP. In the access and distribution layers, DHCP Snooping is also set up. It's a layer 2 security measure built into a competent network switch's operating system that rejects DHCP traffic that's deemed unsuitable. DHCP Snooping identifies and prevents unauthorized (rogue) DHCP servers from supplying IP addresses to DHCP clients. The DHCP Snooping functionality is responsible for performing the following tasks:

FTP (File Transfer Protocol)

The main purpose of an FTP server is for users to be able to upload and download files. A computer having an FTP address dedicated to receiving FTP connections is known as an FTP server. FTP is a file transfer protocol that allows you to send and receive files over the internet between a server and a client (receiver). An FTP server is a computer that uses the FTP protocol to distribute files for download. (Claudio Buttice,)

SYSLOG

Syslog is a protocol for sending and receiving specialized notifications from various network devices. In the messages, you'll find timestamps, event messages, severity, host IP addresses, diagnostics, and other data. Level 0 is an emergency, level 5 is a warning, System Unstable is critical, and levels 6 and 7 are informational and debugging, respectively. (stackify, 2017)

NTP (Network Time Protocol)

The goal of NTP is to keep all participating computers within a few milliseconds of Coordinated Universal Time (UTC). It uses the intersection approach, a modified version of Marzullo's technique, to select accurate time servers, which is intended to mitigate the effects of changing network latency. NTP can retain time to tens of

milliseconds on the public Internet and to one millisecond in local area networks under ideal conditions. Asymmetric pathways and network congestion can both result in errors of 100 milliseconds or more. (*What is Network Time Protocol (NTP)? - Definition from WhatIs.com.*)

WEBSERVER

A web server stores and serves the content of the website. Depending on the client's preferences, images, phrases, application data, movies, and other forms may be used. The web browser asks data from the website when a user clicks on a certain link or chooses to download a document from the browser.(Ish Upadhya,)

WLC CONTROLLER

A wireless local area network (WLAN) is a network architecture that was created to meet the changing needs of networks. Wireless network access points allow wireless devices to connect to the network, and a WLAN controller is in charge of controlling them. (*What Is a WLAN Controller? (WLC).*)

Other Techniques used

1. **ACL (Access Control list)** – Data entering the internal network from the outside world is processed by the firewall using access control lists. This keeps attackers out of the network and keeps potentially dangerous traffic out.
2. **SSH (Secure Shell)** - All the routers and switches have been configured with ssh because it helps to secure remote access, easy to execute commands remotely, deliver security patches,

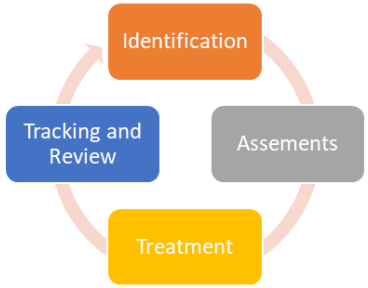
RISK MANAGEMENT

The process of identifying, assessing, and implementing activities that regulate how an organization tackles potential repercussions is known as risk management.

Objectives:

1. To recognize and manage potential dangers.
2. Risks should be prioritized based on their severity.
3. to comprehend, analyze, and communicate the risk

Figure 69 Risk Management



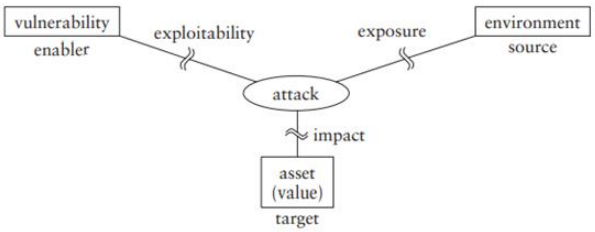


Figure 70 Risk Management

1. Risk identification

The key goal is to determine the origins of threats, triggers, effects, etc., of internal and external risks that impact the organization's protection before they cause harm to the organization.

2. Risk assessments

This technique analyzes the company's risks and determines their probability and impact. In order to assess risk's quantitative and qualitative significance, this is a continual iterative process that assigns risk priority and execution targets.

3. Risk treatment

If suitable controls are chosen and applied to mitigate the identified risk, it is the procedure. The risk treatment approach addresses and tackles the hazards in accordance with the severity degree. Risk assessments are used to make judgments at this point.

4. Risk tracking and review

The monitoring method ensures that the company's operations are under control, as well as that the protocol is understood and followed. The evaluation phase assesses the effectiveness of risk management strategies that have been put in place. (aspen,)

ETHICAL ISSUES

This network design has both Private and Public networks. So ethical issue for this network design is divided into 2 parts.

Ethical issues in a private network

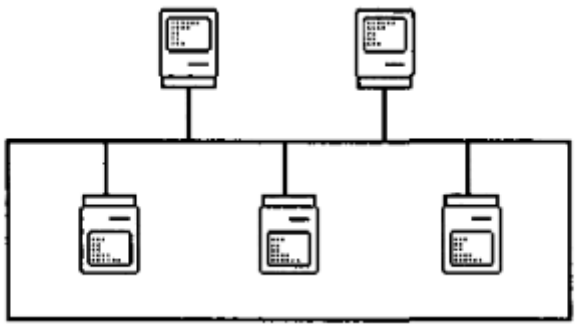


Figure 71 Ethical issues in a private network

It is important to remember that all computer networks must be administered or serviced to function properly. By definition, the person performing administrative functions must have total control over 'their' system. This means that an individual user is completely reliant on their administrator's ethical ideas. If one takes a casual approach to data examination, no file can be considered private, and no email can be considered secure. If an organization has not set clear rules and norms, there is nothing that can be done to prevent a network administrator from abusing their access other than an individual sense of responsibility. Individual users, who may be completely unconscious of any tampering with their data, are, of course, completely unaware of such exploitation. A firm may at times rely on unethical network system administration.

The ethical issues associated with network monitoring are obvious – users of closed network systems must be informed of any oversight of their activity. It is inadequate and unworkable to leave such matters unexplained in the belief that people would figure it out on their own. In these situations, management should communicate the company's expectations of employee behavior.

Ethical issues in a public network

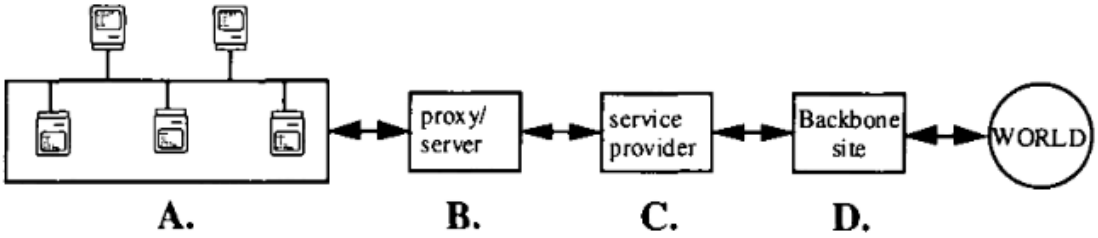


Figure 72 Ethical issues in a public network

We may encounter a circumstance in which a single corporate user wishes to visit a Worldwide Website in another nation, for example. The diagram above depicts the actions that must be taken; but, what does going through this chain of connections imply?

- To begin, the user has direct control over only the original computer. (In the case of a company computer network) All subsequent steps in the user's

connection to the Internet are, inevitably, dependent on others and, as a result, are typically controlled and influenced by variables outside of the user's control. Such control can and, in most cases, is invisible.

- Second, because access to the Internet entails access to and dissemination of information and data, it is critical to understand that specific access may be limited or regulated.
- Third, the technological constraints of a networked system might limit access. For example, there is a direct link between a network's traffic volume and its functional efficiency. Because of the enormous increase in Internet traffic, many users are experiencing issues with speed and access. Despite increased network bandwidth, such issues will only increase. The needs of a high number of new Internet users are increased by technological advancements, such as the bandwidth requirements of full-motion Internet video. Individual users will unavoidably be affected by routing algorithms and hardware options made to mitigate these issues. (Langford, 1997)

LEGAL ISSUES

The Information Commissioner's Office (ICO) is the UK's GDPR supervisory authority, in charge of promoting and enforcing the Act, as well as offering information and assistance to organizations and people. (ncsc.gov.uk,)

When an organization is found in violation of such regulation (for example, failing to properly safeguard customer data against a breach or failing to notify their supervisory authority within 48 hours), it could face fines of up to 20 million euros or 4% of annual turnover, whichever is higher. Because the stakes are so high, companies must ensure that their activities across the board – including network security – are compliant with the rule.

Where GDPR intersects with network security

Three of the GDPR articles are directly connected to network security:

- Article 32 requires data controllers and processors to use adequate technological and organizational measures to guarantee an acceptable degree of security for the level of risk.

- Article 35 compels enterprises to perform risk assessments for data security (DPIA)
- Article 83 requires data controllers and processors to assess the risks inherent in data processing and then take risk mitigation measures (Jeffrey Starr, 2018)

MINIMIZATION OF THE RISK OF INTRUSION

A network intrusion is defined as any illegal activity on a digital network. In most cases, network invasions result in the theft of valuable network resources, and they almost invariably compromise network and/or data security. To minimise this danger, the measures mentioned below are carried out.

1. Identification and Authentication

   The procedure of assuring a user's identity in the system is known as identification. The term "authentication" refers to the process of determining whether or not a claim is true.

   - The user must offer something that they already possess (e.g.: token)
   - The user must submit information that only they have access to (e.g.: password)
   - The user must supply information about himself or herself (e.g.: biometric)

2. Access Control

   It contributes to the security, integrity, and availability of information.

   - User Identity
   - Role membership
   - Group membership

3. Intrusion Detection

   The procedure for tracking occurrences in a computer or network and analyzing intrusion indications that have been detected as illegal actions.

   - Users who have been granted access to the network are attempting to obtain further rights that they are not currently granted.
   - Users that allow their privileges to be abused are unauthorized users.
   - Attackers who use the internet to get access to systems

4. Firewall

   It regulates the flow of network traffic between networks or between hosts. A firewall's function is to:

   - Because it is the single location where communications travel through, it serves as a defensive shield.
   - It prevents traffic by restricting ports and restricts access to only particular IP addresses or domain names.
   - Four mechanisms to restrict traffic is
     - Packet filter, Circuit-level Gateway, Proxy server, Application gateway.
   - Malicious code is defended using stringent protocols and numerous layers of security.
   - As it attempts to spread, this malware can be blocked by hardware security and access control software.

5. Vulnerability Scanners

   Software that looks for flaws in computers and networks.

   - It's utilized to figure out where the system's flaws are.
   - It includes a vulnerability database that is used to detect and prevent security breaches.

PROTECTION OF ORGANIZATION AND CUSTOMER'S DATA

With data breaches on the rise and their impact expected to wreak havoc on businesses for years to come, cyber thieves are becoming more sophisticated in their approach to stealing their targets' systems.

Companies should prioritize consumer data protection more than ever before now that data protection legislation such as GDPR is in full force.

1. Implementing spam, malware, and potentially dangerous file types filtering on endpoints, networks, and email.

2. Employees should be taught to be wary of emails, especially those with attachments, and to notify IT if they get any odd emails or attachment behavior.
3. Check that your operating system and apps are up to date with the latest security patches by utilizing a patch assessment tool. The majority of exploit kits succeed due to flaws in software for which a fix is already available but hasn't been deployed.
4. To detect and prevent exploit kits from infiltrating your machines, install endpoint security software and/or a secure online gateway.
5. Crooks are interested in your back-end databases, PoS network, and testing network, not just one user's password and personal information. Consider partitioning your networks using next-generation firewalls that perceive your internal departments as potentially hostile to one another, rather than having one massive "inside" fenced off from the much larger "outside."
6. Implement a device management plan to detect and regulate the use of removable storage devices; this will not only keep bad content out, but it will also keep personally identifiable information (PII) and intellectual property (IP) out.
7. Implement complete disk protection before exchanging sensitive data housed on servers or removable media with business partners.
8. Use application control to keep an eye on and ban extraneous software that isn't adding any value to the system.
9. Create a data security policy that teaches employees how to protect personal information.
10. When migrating to the cloud, data should be encrypted – both in the cloud and when being transmitted. (Ben Rossi, 2019)

REFERENCES

aspen.*RISK MANAEGMENT.* https://aspen.eccouncil.org/

Ben Rossi. (2019, -12-03T11:15:19+00:00). 10 ways businesses can protect customer data. https://www.information-age.com/10-ways-businesses-can-protect-customer-data-123459341/

Claudio Buttice.*What is an FTP Server? - Definition from Techopedia.* Techopedia.com. http://www.techopedia.com/definition/26108/ftp-server

EIGRP fundamentals. (2018a, -04-19T00:38:09+00:00). https://www.geeksforgeeks.org/eigrp-fundamentals/

EIGRP fundamentals. (2018b, -04-19T00:38:09+00:00). https://www.geeksforgeeks.org/eigrp-fundamentals/

Ish Upadhya. (). What is a Web Server? An Overview. https://www.jigsawacademy.com/blogs/cyber-security/what-is-a-web-server/

Jeffrey Starr. (2018). *Aligning Network Security with GDPR.* algosec. https://www.algosec.com/blog/aligning-network-security-with-gdpr/

Langford, D. (1997). Ethical Issues in Network System Design. *Australasian Journal of Information Systems, 4*(2)10.3127/ajis.v4i2.367

ncsc.gov.uk.General Data Protection Regulation (GDPR). https://www.ncsc.gov.uk/information/GDPR

SNMP Ports & Protocol - What is it? | *ThousandEyes.* https://www.thousandeyes.com/learning/techtorials/snmp-simple-network-management-protocol

stackify. (2017). *Syslog Tutorial: How It Works, Examples, Best Practices, and More.* Stackify. https://stackify.com/syslog-101/

techhub.hpe.com.*About RPVST+.* techhub.hpe.com. https://techhub.hpe.com/eginfolib/networking/docs/switches/YA-YB/15-18/5998-8157_yayb_2530_atmg/content/ch06s11.html#:~:text=Basically%2C%20RPVST%2B%20is%20RSTP%20operating,redundant%20use%20by%20another%20VLAN.

Techopedia.*What is Static Routing? - Definition from Techopedia.* Techopedia.com. http://www.techopedia.com/definition/26161/static-routing

What Is a WLAN Controller? (WLC). Cisco. https://www.cisco.com/c/en/us/products/wireless/wireless-lan-controller/what-is-wlan-controller.html

What is Network Time Protocol (NTP)? - Definition from WhatIs.com. SearchNetworking. https://www.techtarget.com/searchnetworking/definition/Network-Time-Protocol