Networking & IT Infrastructure

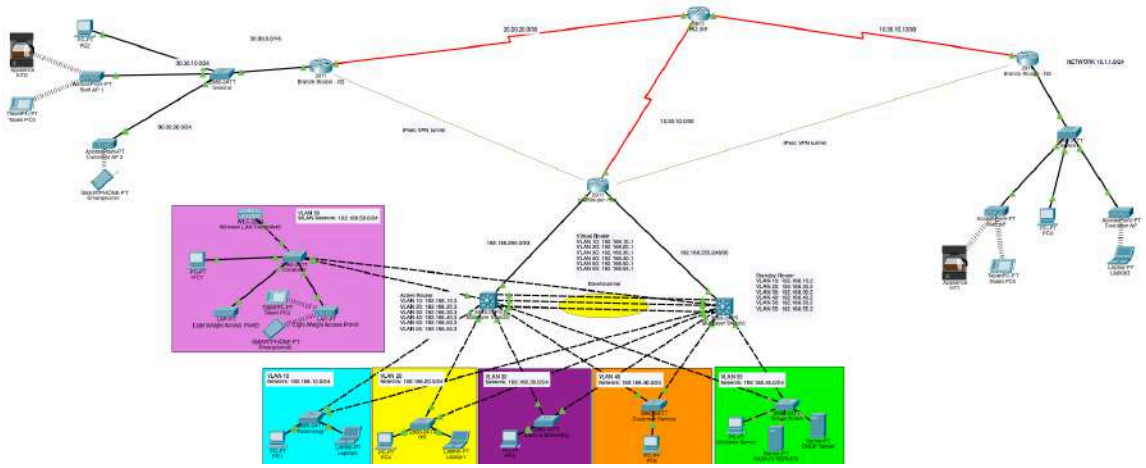
Overview

The network architecture adopts a best-in-class approach by implementing a 3-tier hierarchical design for the headquarters and a relatively simple design for the branches, widely acknowledged as an industrial best practice for creating reliable, scalable, and cost-effective networks (GeeksforGeeks, 2022). This design optimises network performance, facilitates seamless scalability to accommodate future growth, and ensures cost efficiency in network management and maintenance. The hierarchical structure provides a clear separation of functions, enhancing overall network reliability and robustness.

Distribution & Core Layer:

- The network infrastructure is designed with a robust and resilient architecture, featuring a single HQ-router complemented by two multilayer switches for efficient inter-VLAN routing and enhanced redundancy through HSRP configuration. An EtherChannel is implemented between the switches to optimise bandwidth and load balancing, significantly boosting overall network performance. The utilisation of subnets and VLANs in tandem forms a multilayer security approach, strategically addressing vulnerabilities in both Layers 2 and 3.
- To future-proof the network for business growth, subnet selection follows Cisco's addressing guide recommendations, employing VLSM while allowing space for growth /16 and /24 for the HQ and various departments, ensuring scalability. Layer 2 security is prioritised with measures like PortFast, BPDUguard, port security, and auto-trunking disabling to fortify against potential attacks.
- Routing is achieved through OSPF, chosen for its compatibility with heterogeneous networks, as opposed to EIGRP, which is limited to homogeneous networks. WLAN security is bolstered with RADIUS server authentication, providing users with unique username and password combinations for heightened access control. For secure site-to-site connections, IPSec VPNs are implemented.

Network Diagram & Specifications



Subnet Assignment

Location	VLAN	Subnet/Network	Department
Headquarters		192.168.0.0/16	
	10	192.168.10.0/24	Technology
	20	192.168.20.0/24	HR
	30	192.168.30.0/24	Sales & Marketing
	40	192.168.40.0/24	Customer Service
	50	192.168.50.0/24	WLAN
	55	192.168.55.0/24	Server
	99	192.168.99.0/24	Management
Branch 1		10.1.0.0/16	
	10	10.1.10.0/24	Staff
	20	10.1.20.0/24	Customers
Branch 2		30.30.0.0/16	
	10	30.30.10.0/24	Staff
	20	30.30.20.0/24	Customers

Table 2.1: Subnet address range.

MLS1-WAN	192.168.255.0/30
MLS2-WAN	192.168.255.248/30
HQ Router-ISP	10.30.10.0/30
ISP-BRANCH 1	20.20.20.0/30
ISP-BRANCH 2	10.30.10.12/30

Table 2.2: IP network addresses between the interfaces.

IP Addressing Scheme

The devices in the network are assigned the following IP Address range as defined in Table 2.3.

Device Type	Assignable IP Addresses
HQ	
Any wired device in Technology (VLAN 10)	192.168.10.4 to 192.168.10.243
Any wired device in HR (VLAN 20)	192.168.20.4 to 192.168.20.243
Any wired device in Sales(VLAN 30)	192.168.30.4 to 192.168.30.243
Any wired device in Customer Service (VLAN 40)	192.168.40.4 to 192.168.40.243
Any wirelessly connected device (VLAN 50)	192.168.50.4 to 192.168.50.243
Active Directory Windows Server (VLAN 55)	192.168.55.6
DHCP Server (VLAN 55)	192.168.55.4
RADIUS Server (VLAN 55)	192.168.55.5
JEWEL BRANCH	
Any wired or wireless device - Staff (VLAN 10)	10.1.10.2 to 10.1.10.254
Any wireless device - Customers (VLAN 20)	10.1.20.2 to 10.1.20.254
ORCHARD BRANCH	
Any wired or wireless device - Staff (VLAN 10)	30.30.10.2 to 30.30.10.254
Any wireless device - Customers (VLAN 20)	30.30.20.2 to 30.30.20.254

Table 2.3: Allotment of IPv4 addresses for different device types.

System Configurations

HQ - Switches & Routers

Basic Device Configuration (VLAN Creation for HQ switches).

Creating VLANs on switches

```
configure terminal
vlan 10
name Technology
exit
vlan 20
name HR
exit
vlan 30
name Sales
exit
vlan 40
name Cust
exit
vlan 50
name WLAN
exit
vlan 55
name Server
exit
vlan 99
name Management
exit

int range fa0/1-2
switchport mode trunk
exit

int range fa0/3-24
switchport mode access
switchport access vlan 10
exit
```

Figure 2.1: Sample configuration for VLAN creation and setting up trunk ports on HQ switches.

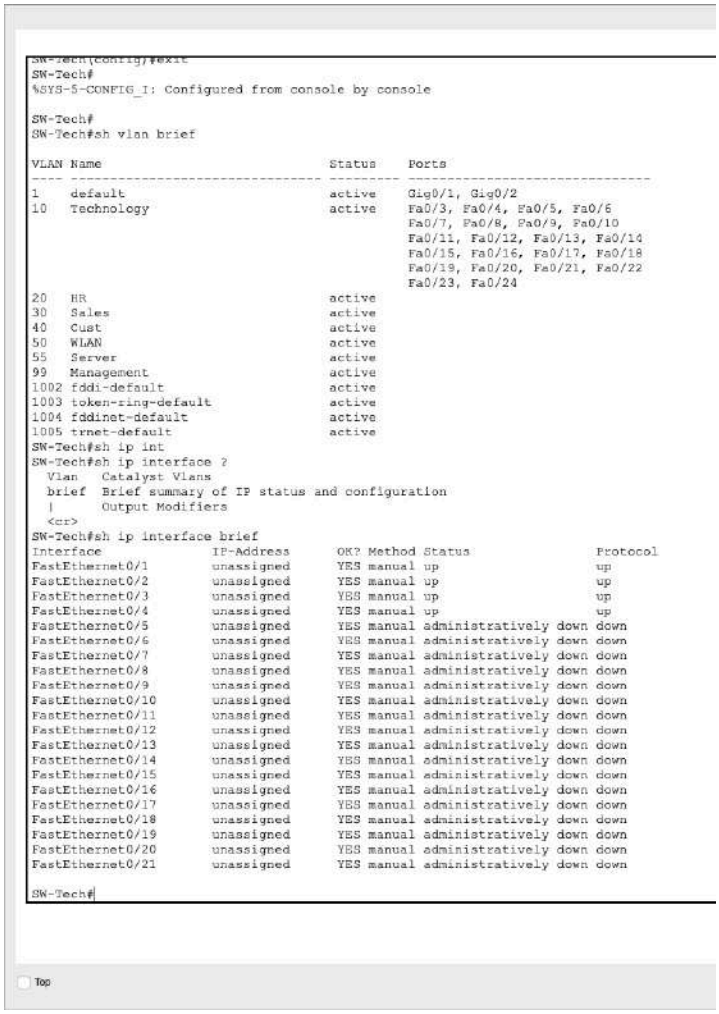


Figure 2.2: Verification of VLANs and port allocations and shutdown of unused ports for added security.

```
int vlan 55
ip add 192.168.55.2 255.255.255.0
no shut
standby 55 priority 90
standby 55 ip 192.168.55.1
exit


Config for OSPF
router ospf 25
router-id 1.3.1.3
network 192.168.255.248 0.0.0.3 area 0
network 192.168.10.0 0.0.0.255 area 0
network 192.168.20.0 0.0.0.255 area 0
network 192.168.30.0 0.0.0.255 area 0
network 192.168.40.0 0.0.0.255 area 0
network 192.168.50.0 0.0.0.255 area 0
network 192.168.55.0 0.0.0.255 area 0
```

Figure 2.3: Commands for configuration of MLSs of VLAN interfaces, HSRP & OSPF.

Similar commands execute the VLANs created on the MLSs to the switches i.e:
vlan 10
name Technology
Then, the VLAN interfaces are created, and an IP address is assigned. For HSRP, we put a priority number and then allocate a standby IP address of the virtual router. Following that, we can configure the OSPF routing protocol for the MLSs by advertising the adjacent networks.

```
MLS1-HQ#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Vl10        10   100   Active   local           192.168.10.2    192.168.10.1
Vl20        20   100   Active   local           192.168.20.2    192.168.20.1
Vl30        30   100   Active   local           192.168.30.2    192.168.30.1
Vl40        40   100   Active   local           192.168.40.2    192.168.40.1
Vl50        50   100   Active   local           192.168.50.2    192.168.50.1
Vl55        55   100   Active   local           192.168.55.2    192.168.55.1
MLS1-HQ#
```

```
MLS-HQ2#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Vl10        10   90    Standby  192.168.10.3    local           192.168.10.1
Vl20        20   90    Standby  192.168.20.3    local           192.168.20.1
Vl30        30   90    Standby  192.168.30.3    local           192.168.30.1
Vl40        40   90    Standby  192.168.40.3    local           192.168.40.1
Vl50        50   90    Standby  192.168.50.3    local           192.168.50.1
Vl55        55   90    Standby  192.168.55.3    local           192.168.55.1
MLS-HQ2#
```

Figure 2.4: MLS1 & MLS2 HSRP verification.

```
router ospf 25
 router-id 1.2.1.2
 log-adjacency-changes
 network 192.168.10.0 0.0.0.255 area 0
 network 192.168.20.0 0.0.0.255 area 0
 network 192.168.30.0 0.0.0.255 area 0
 network 192.168.40.0 0.0.0.255 area 0
 network 192.168.50.0 0.0.0.255 area 0
 network 192.168.55.0 0.0.0.255 area 0
 network 192.168.255.0 0.0.0.3 area 0
!
router rip
!
ip classless
!

MLS1-HQ#
```

```
router ospf 25
 router-id 1.3.1.3
 log-adjacency-changes
 network 10.30.10.8 0.0.0.3 area 0
 network 192.168.10.0 0.0.0.255 area 0
 network 192.168.20.0 0.0.0.255 area 0
 network 192.168.30.0 0.0.0.255 area 0
 network 192.168.40.0 0.0.0.255 area 0
 network 192.168.50.0 0.0.0.255 area 0
 network 192.168.55.0 0.0.0.255 area 0
 network 192.168.255.248 0.0.0.3 area 0
```

Figure 2.5: MLS1 & MLS2 ospf verification with 1.2.1.2 & 1.3.1.3 as their respective router-ids

EtherChannel Configuration & Verification

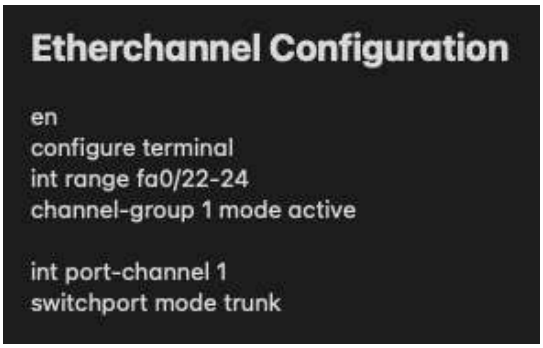
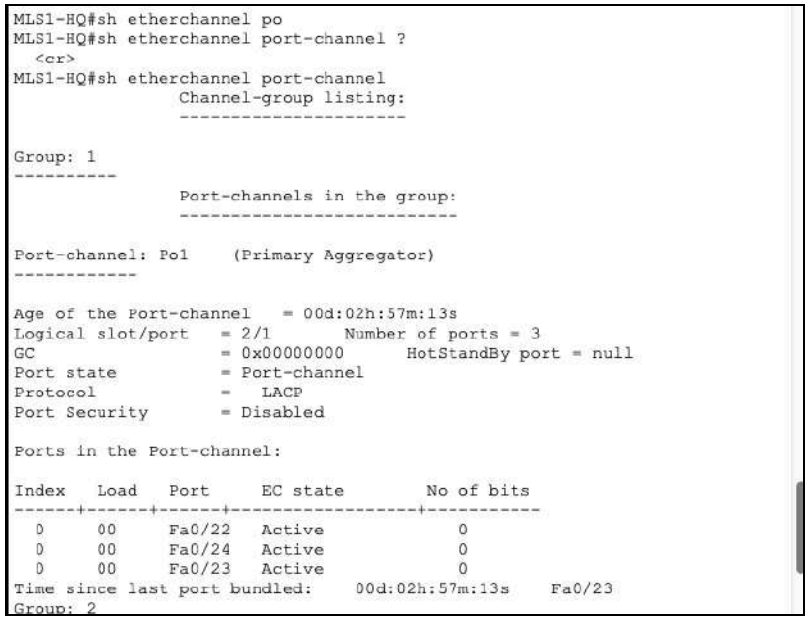


Figure 2.6: Etherchannel configuration between the multilayer switches.



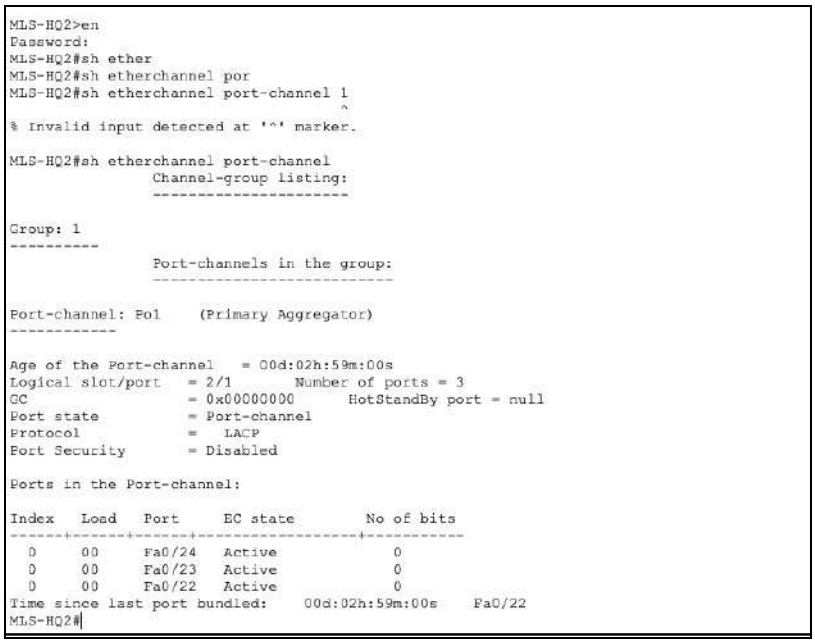


Figure 2.7: Verification of EtherChannel created between the two multilayer switches.

Router OSPF and NAT configuration

```
WAN#sh ip ospf
 Routing Process "ospf 25" with ID 1.4.1.4
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 It is an area border router
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 2. 2 normal 0 stub 0 nssa
 External flood list length 0
    Area BACKBONE(0)
        Number of interfaces in this area is 3
        Area has no authentication
        SPF algorithm executed 20 times
        Area ranges are
        Number of LSA 14. Checksum Sum 0x07782b
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
    Area 3
        Number of interfaces in this area is 0
        Area has no authentication
        SPF algorithm executed 3 times
        Area ranges are
        Number of LSA 15. Checksum Sum 0x06b0c4
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0

WAN#
WAN#
WAN#
WAN#sh ip ospf ne
WAN#sh ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
1.2.1.2           1   FULL/BDR        00:00:36    192.168.255.2   GigabitEthernet0/0
1.3.1.3           1   FULL/BDR        00:00:37    192.168.255.250 GigabitEthernet0/2
10.30.10.1        0   FULL/  -        00:00:33    10.30.10.1      Serial0/0/0
WAN#
```

Figure 2.8: HQ WAN router OSPF verification.

DHCP Pools & Verification

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
vlan20serverpool	192.168.20.1	0.0.0.0	192.168.20.4	255.255.255.0	240	0.0.0.0	0.0.0.0
vlan50serverpool	192.168.50.1	0.0.0.0	192.168.50.4	255.255.255.0	240	0.0.0.0	0.0.0.0
vlan40serverpool	192.168.40.1	0.0.0.0	192.168.40.4	255.255.255.0	240	0.0.0.0	0.0.0.0
vlan30serverpool	192.168.30.1	0.0.0.0	192.168.30.4	255.255.255.0	240	0.0.0.0	0.0.0.0
vlan10serverpool	192.168.10.1	0.0.0.0	192.168.10.4	255.255.255.0	240	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	192.168.55.0	255.255.255.0	512	0.0.0.0	0.0.0.0

Figure 2.9: DHCP pool of IP addresses for leasing for each subnet.

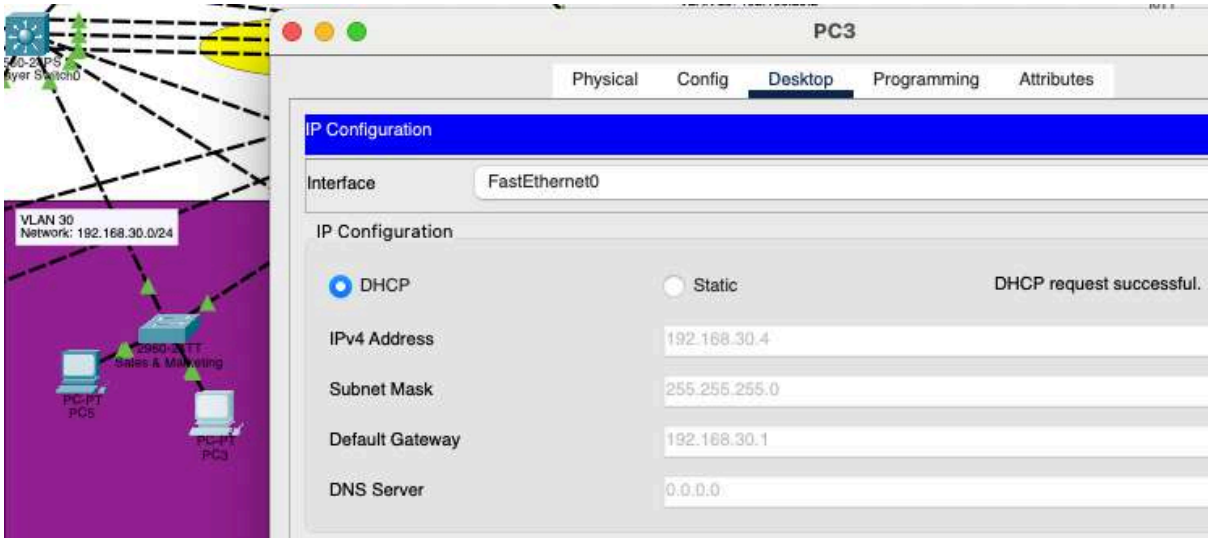
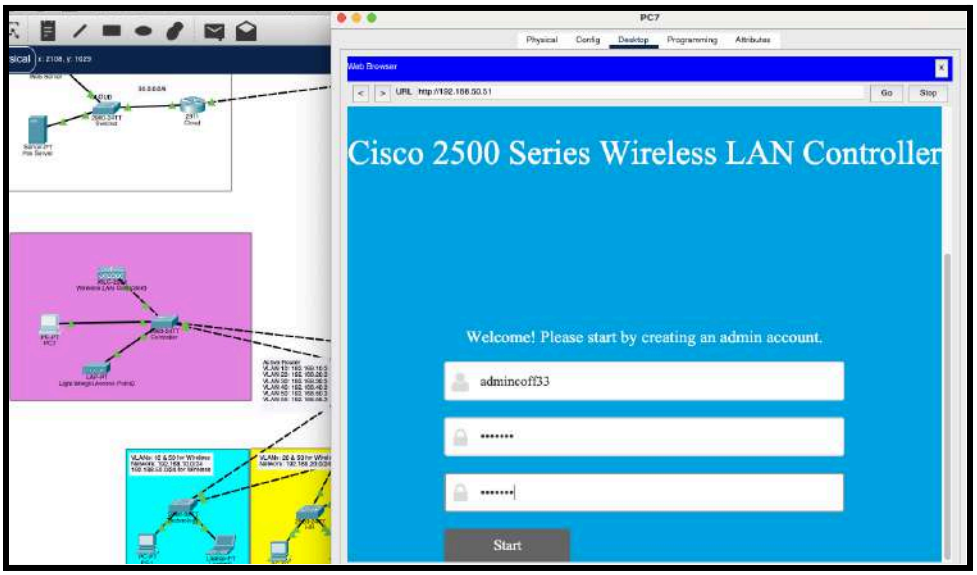
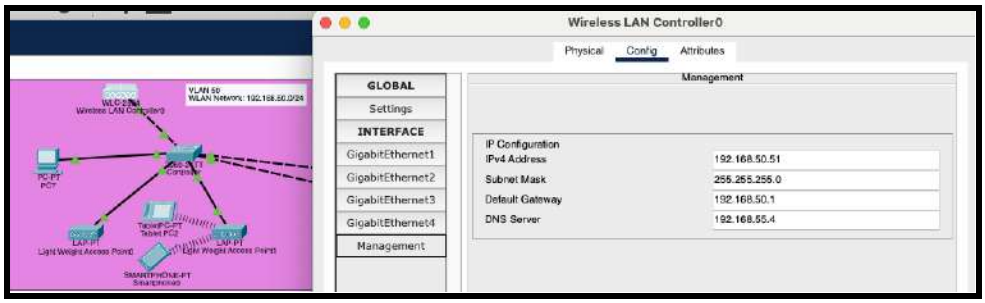


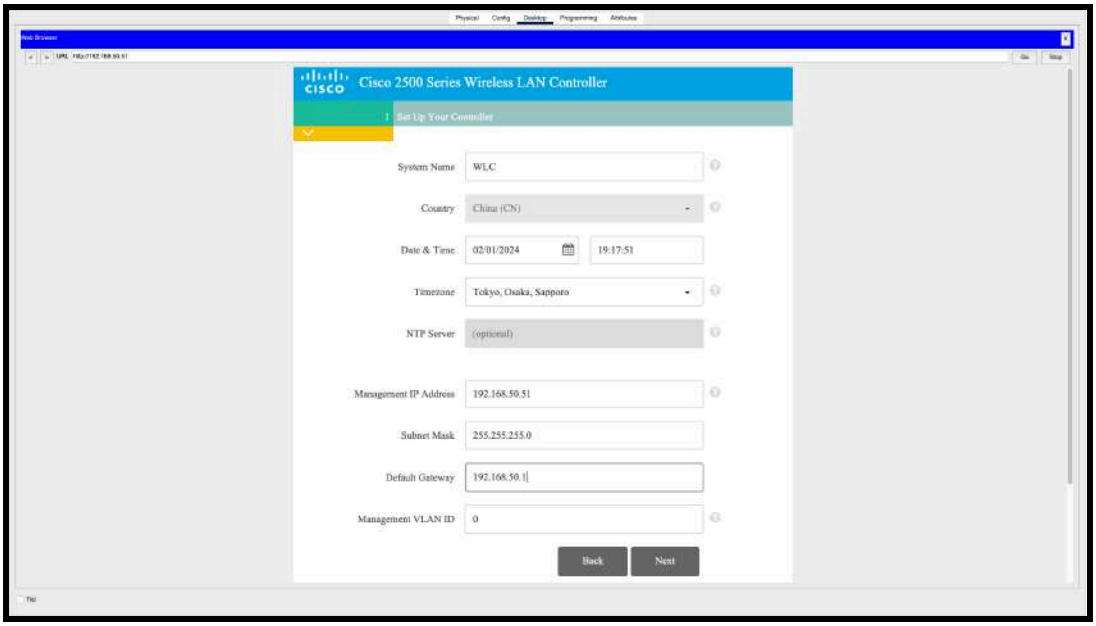
Figure 2.10: Verification and successful assignment of IP address by DHCP server.

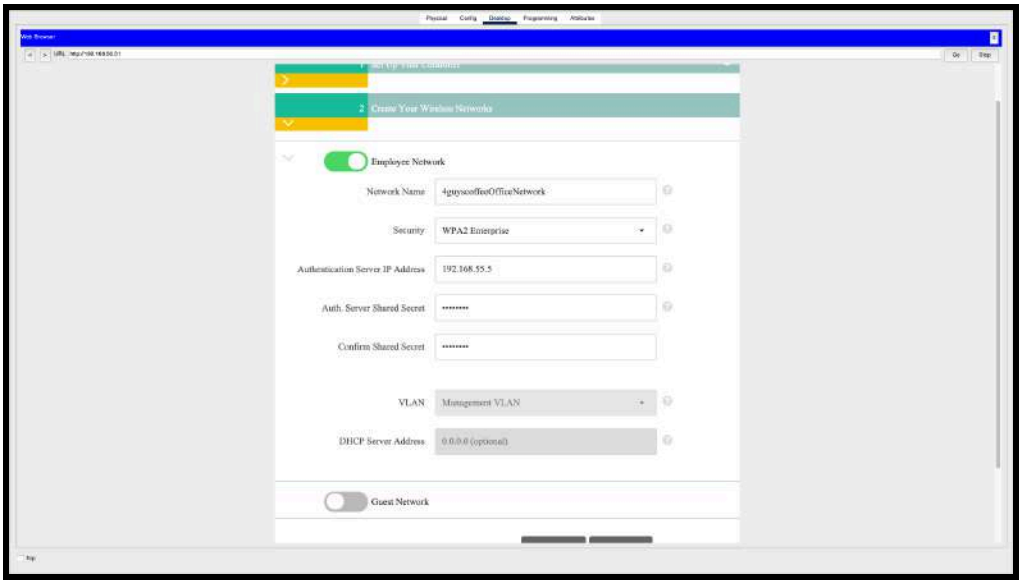
WLC Configuration & RADIUS Server Authentication

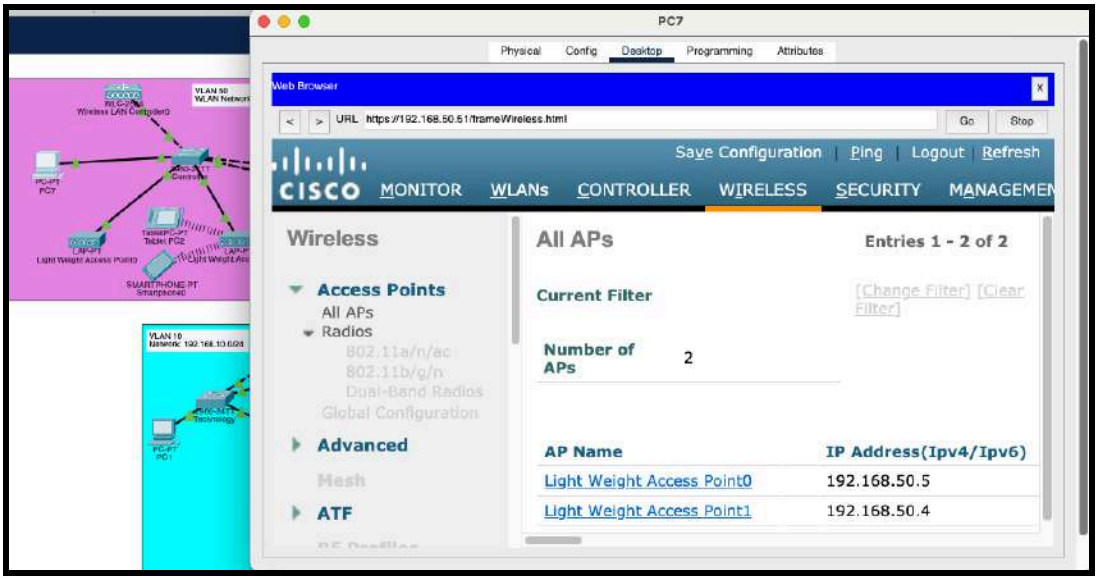
We have set up a WLC to manage our WLAN, which is also scalable, should additional networks be added. As seen from the screenshots below, there are two access points on the configuration web page and our leading network, 4guyscoffeeOfficeNetwork. WLCs provide an added layer of security to APs by providing authentication at a higher level, detecting rogue devices, and protecting the network behind a firewall. WLCs allow for centralised AP deployment. They simplify network maintenance operations. Also, we included a RADIUS server for authentication, requiring login credentials for staff users in the office HQ to access the wifi network instead of a wired connection.

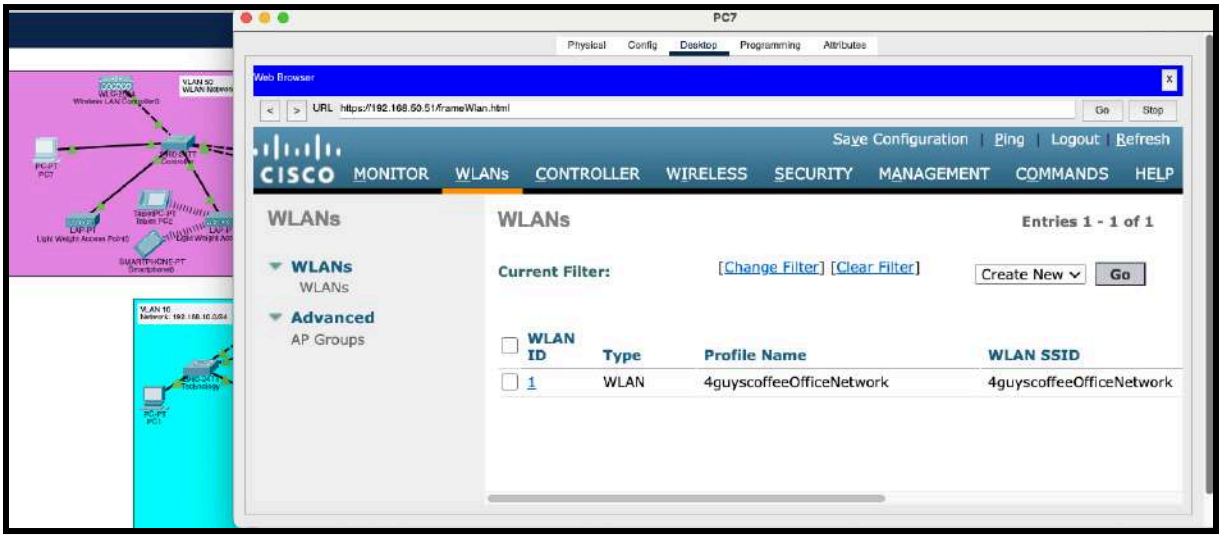



Wireless LAN Controller0
Physical
Config
Attributes
GLOBAL
Settings
INTERFACE
GigabitEthernet1
GigabitEthernet2
GigabitEthernet3
GigabitEthernet4
Management
Management
IP Configuration
IPv4 Address
192.168.50.51
Subnet Mask
255.255.255.0
Default Gateway
192.168.50.1
DNS Server
192.168.55.4


Cisco 2500 Series Wireless LAN Controller
Set Up Your Controller
System Name
WLC
Country
China (CN)
Date & Time
02/01/2024
19:17:51
Timezone
Tokyo, Osaka, Sapporo
NTP Server
(optional)
Management IP Address
192.168.50.51
Subnet Mask
255.255.255.0
Default Gateway
192.168.50.1
Management VLAN ID
0
Back
Next


2 Create Your Wireless Networks
Employee Network
Network Name
4guyscoffeeOfficeNetwork
Security
WPA2 Enterprise
Authentication Server IP Address
192.168.55.5
Auth. Server Shared Secret
Confirm Shared Secret
VLAN
Management VLAN
DHCP Server Address
0.0.0.0 (optional)
Guest Network


PC7
Physical
Config
Desktop
Programming
Attributes
Web Browser
URL https://192.168.50.51/frameWireless.html
Go
Stop
Save Configuration | Ping | Logout | Refresh
CISCO
MONITOR
WLANs
CONTROLLER
WIRELESS
SECURITY
MANAGEMEN
Wireless
Access Points
All APs
Radios
802.11a/n/ac
802.11b/g/n
Dual-Band Radios
Global Configuration
Advanced
Mesh
ATF
All APs
Entries 1 - 2 of 2
Current Filter
[Change Filter] [Clear Filter]
Number of APs
2
AP Name
IP Address(Ipv4/Ipv6)
Light Weight Access Point0
192.168.50.5
Light Weight Access Point1
192.168.50.4


PC7
Physical
Config
Desktop
Programming
Attributes
Web Browser
URL https://192.168.50.51/frameWlan.html
Go
Stop
Save Configuration | Ping | Logout | Refresh
CISCO
MONITOR
WLANs
CONTROLLER
WIRELESS
SECURITY
MANAGEMENT
COMMANDS
HELP
WLANs
WLANs
WLANs
Advanced
AP Groups
WLANs
Entries 1 - 1 of 1
Current Filter:
[Change Filter] [Clear Filter]
Create New
Go
WLAN ID
Type
Profile Name
WLAN SSID
1
WLAN
4guyscoffeeOfficeNetwork
4guyscoffeeOfficeNetwork

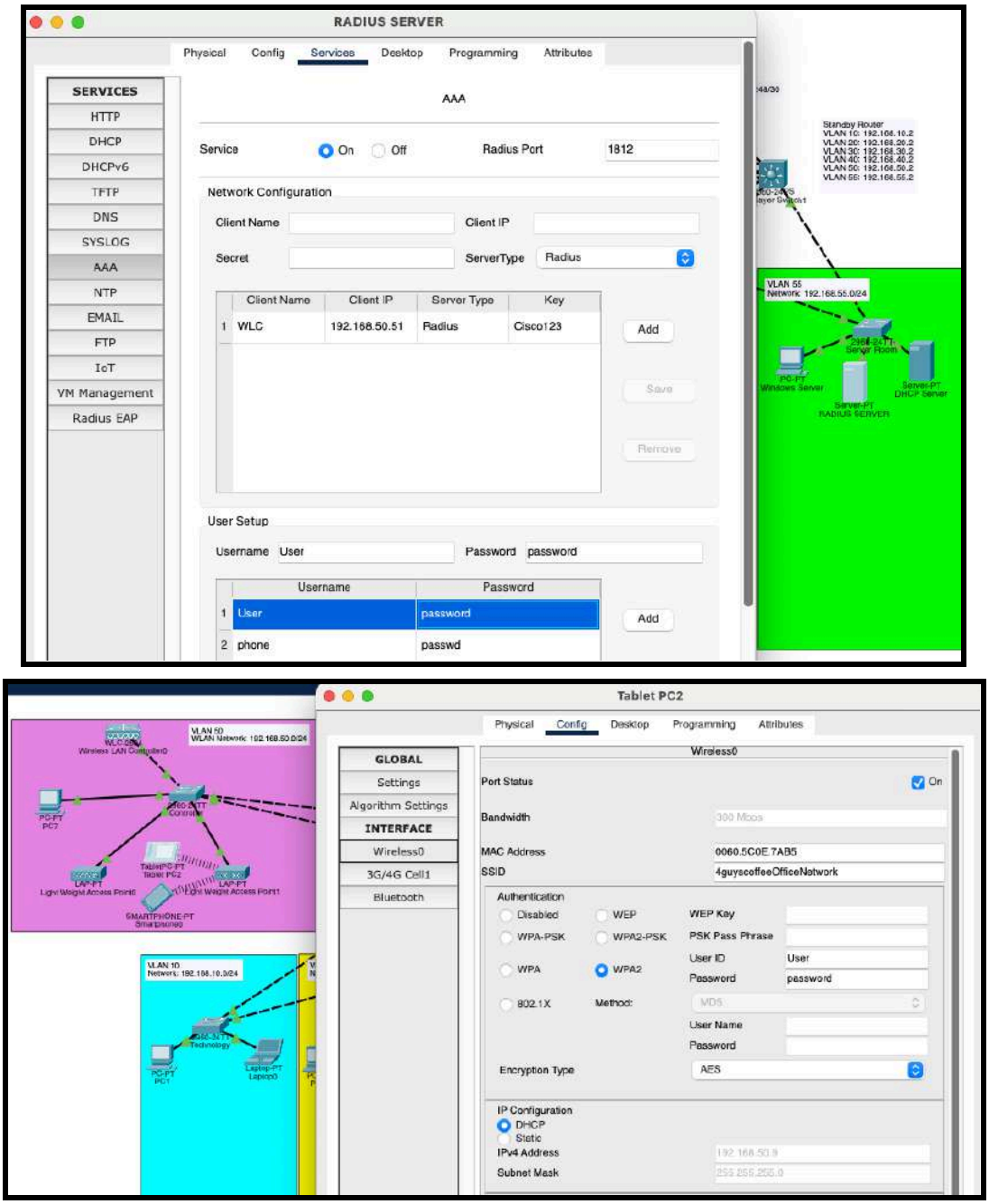


Figure 2.11-2.18: Series of screenshots for WLC and RADIUS server configuration.

Branch - Switches & Routers

Our cafe branches are dine-in cafes with wifi access for customers to use. We have set up the cafe with separate access points, different VLANs, and networks for multilayered security. We used a simple router-on-a-stick topology to facilitate inter-vlan connectivity as it is simple to set up and use SVIs. Both network topology and configurations of the branches are similar.

Switch VLANs

Table 4: VLAN table for the switches in each branch.

VLAN	Name
10	Staff
20	Customers

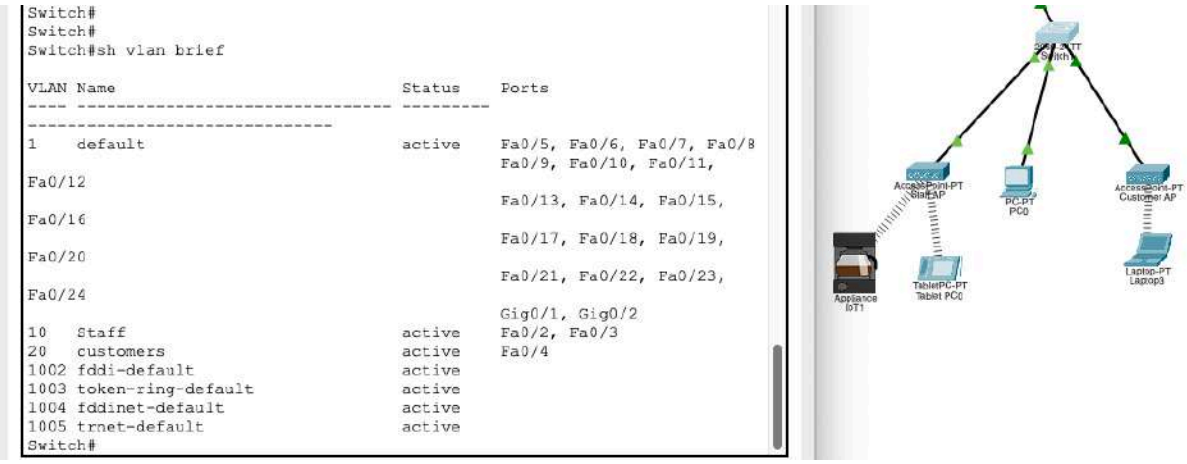


Figure 2.19: Verification of the VLANs on the switches in the branches.

Router

SVIs on Router for Inter-VLAN routing

Figure 2.20: Configuration commands for SVIs on Router.

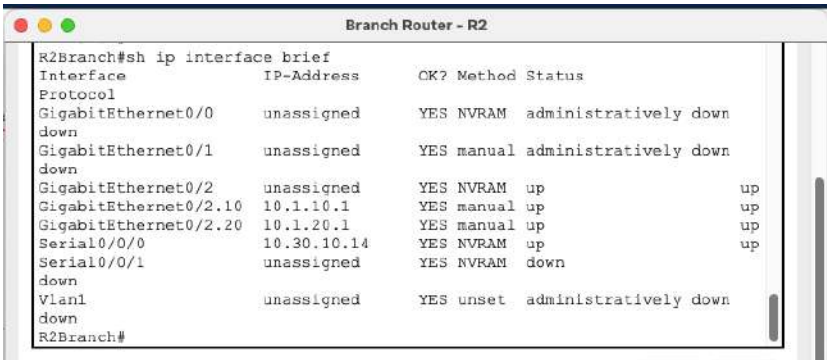


Figure 2.21: SVIs verification for branch router.

Router as DHCP

As it would be expensive to have a dedicated DHCP server for every branch, we have also configured the router branch to be a DHCP server.

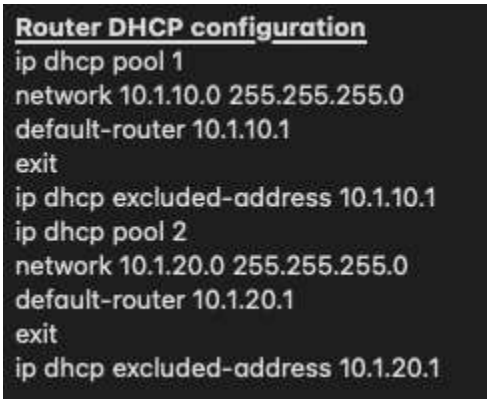


Figure 2.22: Configuring branch router as DHCP server.

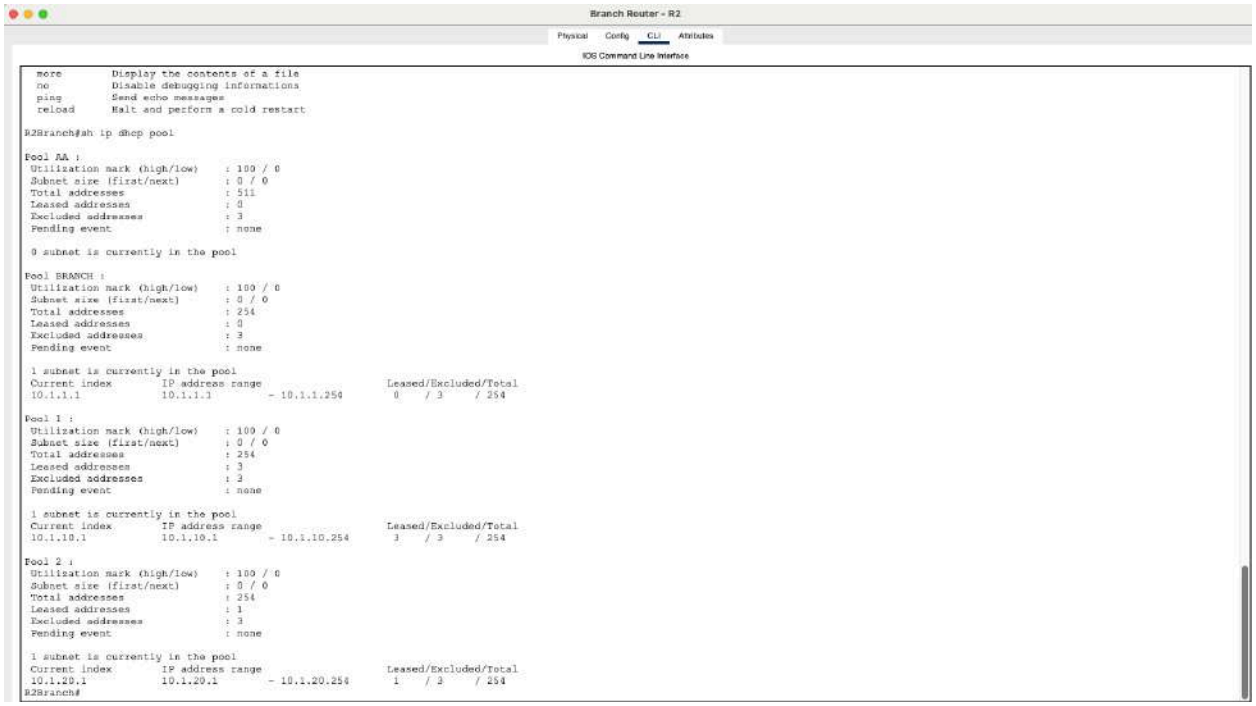


Figure 2.23: Router DHCP verification.

Router OSPF verification

```
R2Branch#sh ip ospf database
            OSPF Router with ID (10.30.10.12) (Process ID 25)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
10.30.10.12     10.30.10.12     382         0x8000000d 0x00bb7d 4
10.30.10.1      10.30.10.1      385         0x8000000f 0x006bcf 6
20.20.20.1      20.20.20.1      384         0x8000000d 0x00e5f7 4
1.4.1.4         1.4.1.4         353         0x80000010 0x00bb94 4
1.3.1.3         1.3.1.3         344         0x80000017 0x00560b 7
1.2.1.2         1.2.1.2         341         0x80000017 0x002031 7

                Net Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum
192.168.55.2    1.3.1.3         354         0x80000029 0x005229
192.168.255.1   1.4.1.4         353         0x80000011 0x00efd7
192.168.255.249 1.4.1.4         353         0x80000012 0x003e8d
192.168.50.2    1.3.1.3         349         0x8000002a 0x0087f7
192.168.20.2    1.3.1.3         349         0x8000002b 0x00d0cb
192.168.10.2    1.3.1.3         349         0x8000002c 0x003d68
192.168.40.3    1.2.1.2         346         0x80000009 0x003477
192.168.30.2    1.3.1.3         344         0x8000002d 0x005e32
R2Branch#
```

Figure 2.24: OSPF database of branch router.

Access Points Configuration

We made use of WPA2-PSK for security encryption for both staff and customer use at each access point.

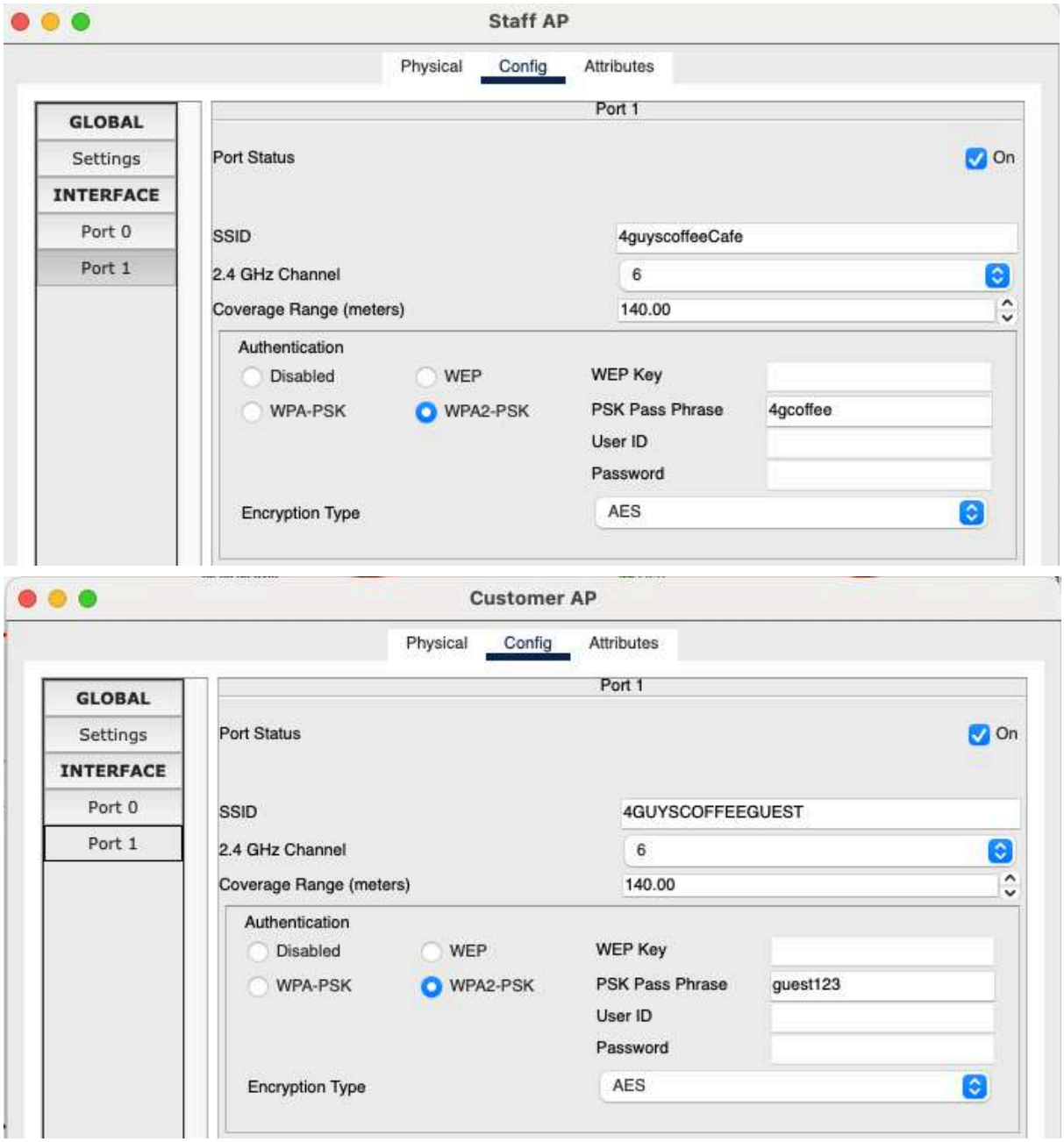


Figure 2.25-2.26: APs configuration for branch cafes with WPA2-passkey.

Connectivity

Connectivity between different VLANs

HQ LAN

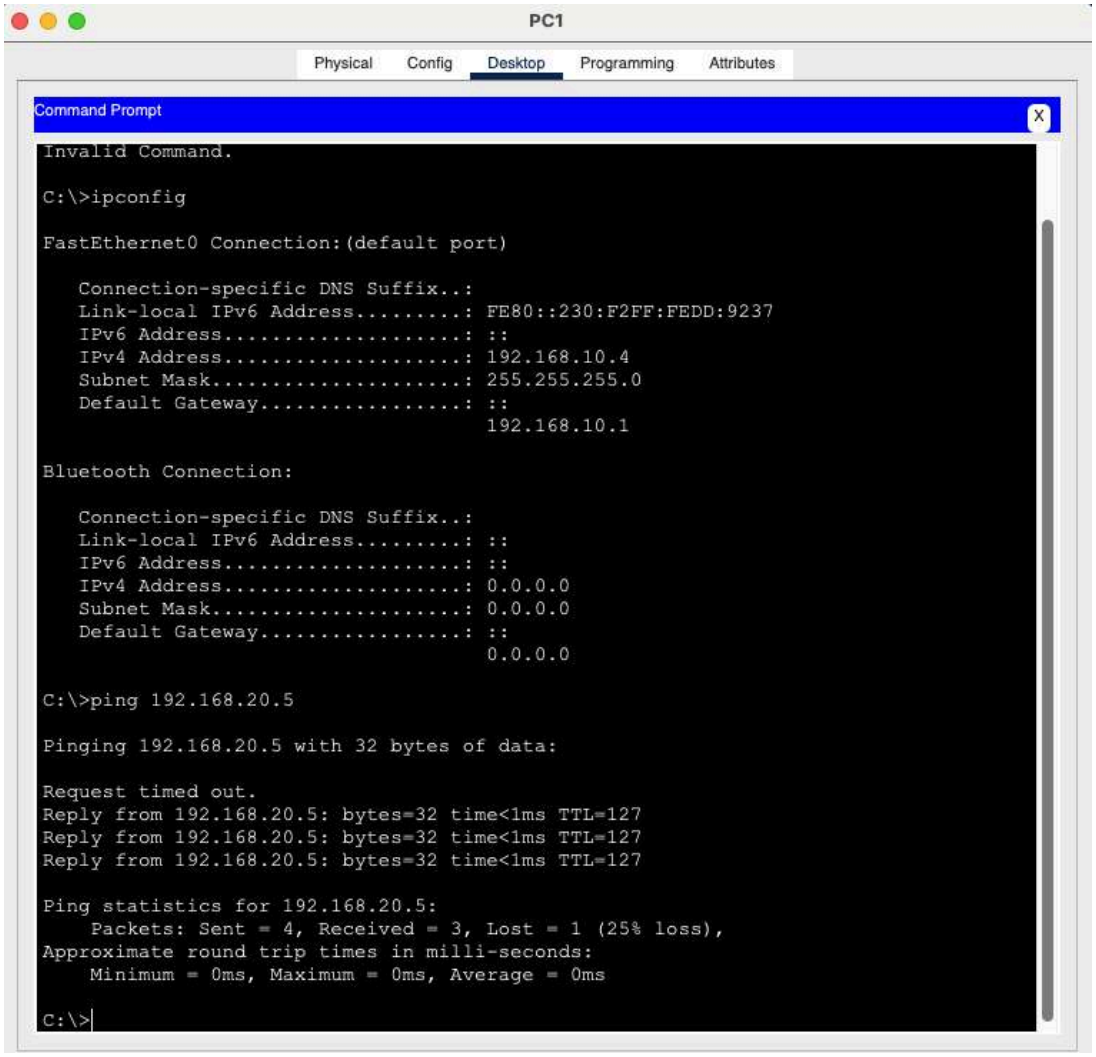


Figure 2.27: Pinging from a PC in Technology, VLAN 10 to a PC in HR, VLAN 20.

Branch LAN

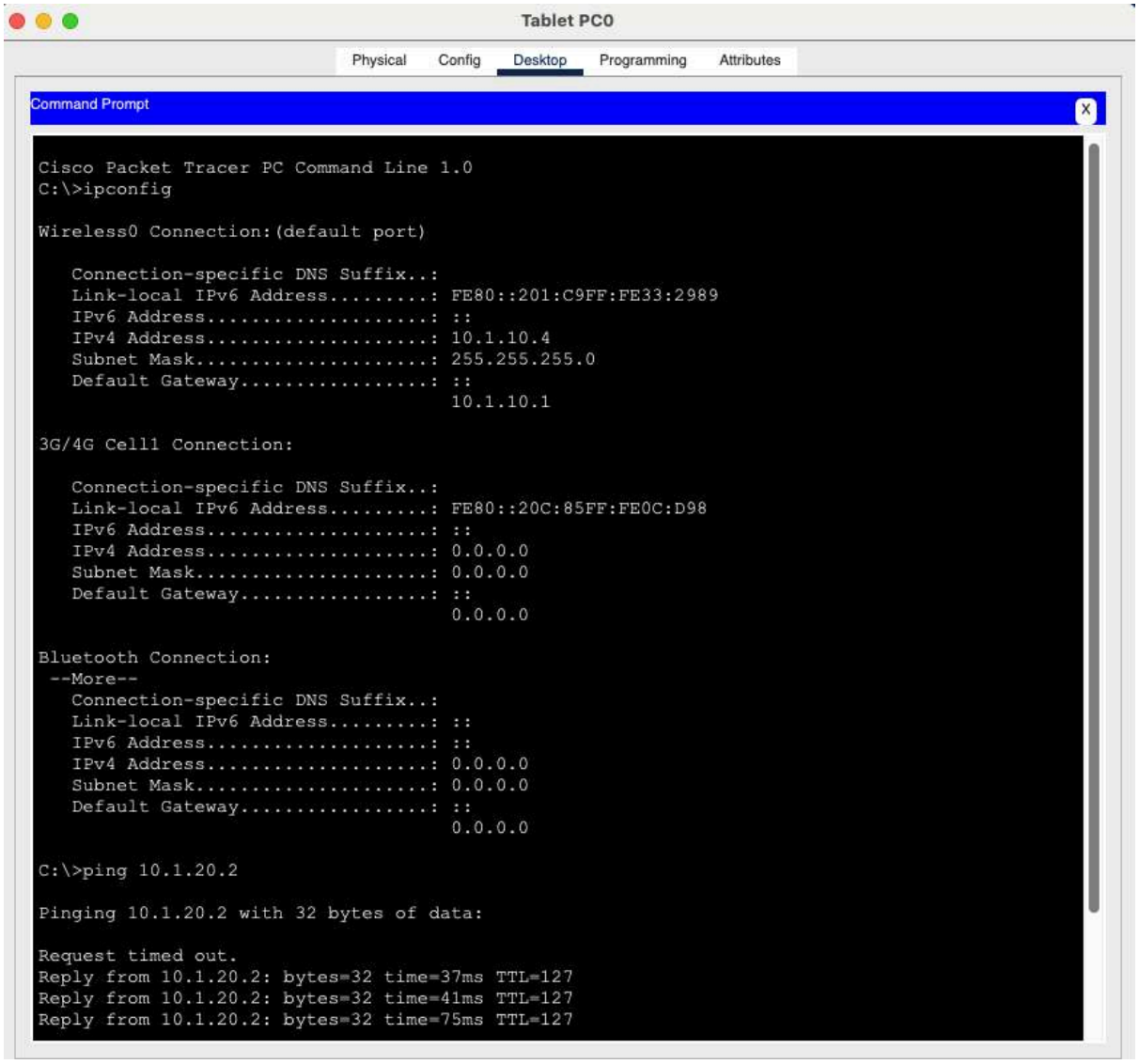


Figure 2.28: Pinging from a tablet connected to the staff AP, VLAN 10, to a customer laptop connected to the customer AP, VLAN 20.

Connectivity across LANs

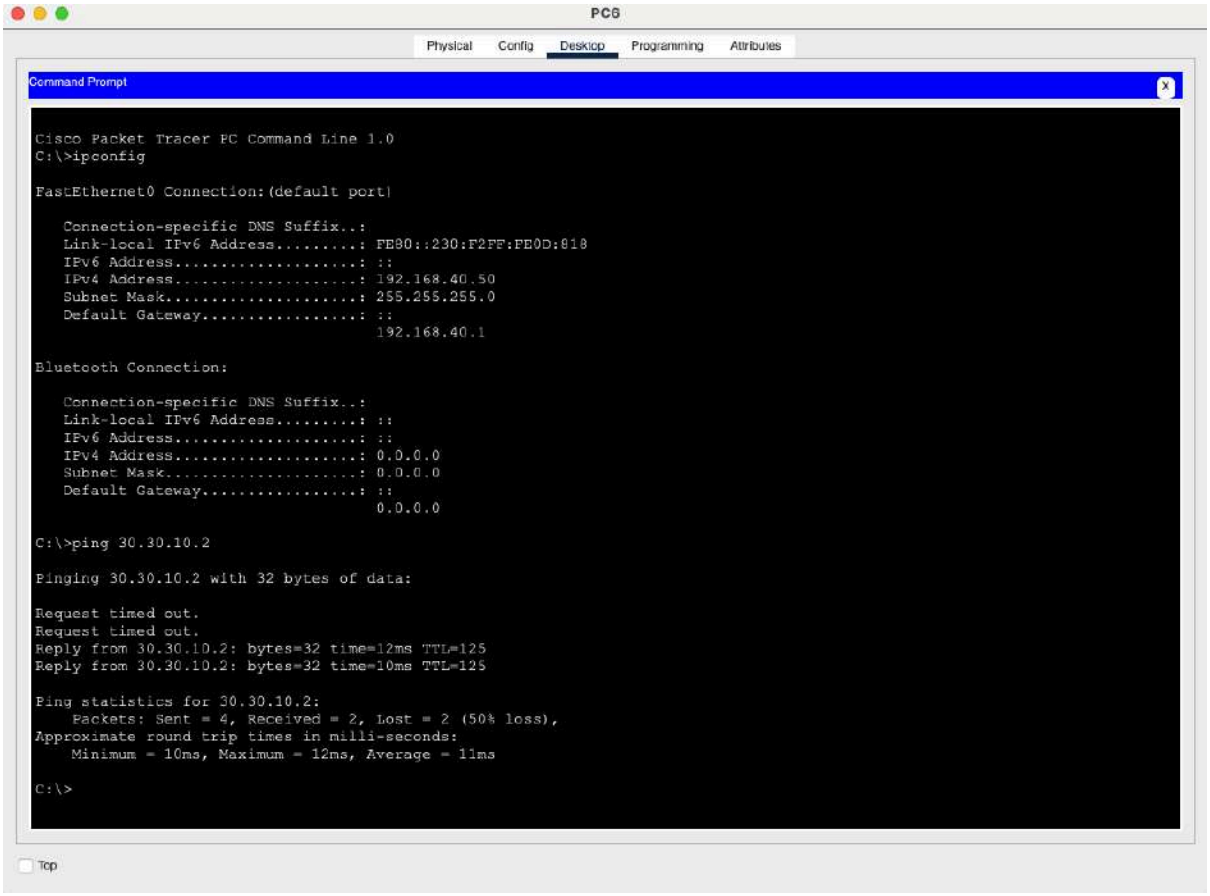


Figure 2.29: Pinging from HQ to Orchard Branch's PC.

Site-to-site VPN

Configuration of VPN

VPN Configuration

Step 1: Check if they have the security package installed in one of the geographical routers:
show version

Step 2: Install the package if it shows disabled
license boot module c2900 technology-package securityk9

Step 3: Create an extended access list to permit traffic to the specific interface of the branch.
access-list 100 permit ip 192.168.0.0 0.0.255.255 10.1.0.0 0.0.255.255

Step 4: Create the IPsec tunnel and bind to interface
crypto isakmp policy 10
encryption aes 256
authentication pre-share
group 5
exit
crypto isakmp key vpn address 10.30.10.14
crypto ipsec transform-set VPN-P2 esp-aes esp-sha-hmac
crypto map VPN-MAP 10 ipsec-isakmp
description VPN connection to R3
set peer 10.30.10.14
set transform-set VPN-P2
match address 100
exit
interface se0/0/0
crypto map VPN-MAP

Step 5: Repeat for the other branch router.

Figure 2.30: VPN tunnel configuration between 2 sites.

```
Technology Package License Information for Module:'c2900'

-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      securityk9    Evaluation    securityk9
uc            disable       None          None
data          disable       None          None

Configuration register is 0x2102


WAN#
```

Figure 2.31: Security package installed - 'Evaluation'.

```
WAN#show ac
WAN#show access-lists
Extended IP access list 100
    10 permit ip 192.168.0.0 0.0.255.255 10.1.0.0 0.0.255.255
Extended IP access list 150
    10 permit ip 192.168.0.0 0.0.255.255 30.30.0.0 0.0.255.255 (1 match(es))

WAN#
```

Figure 2.32: Access List verification for VPN.

VPN verification

```
WAN#
WAN#
WAN#
WAN#sh cry
WAN#sh crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: VPN-MAP2, local addr 10.30.10.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.0.0/255.255.0.0/0/0)
   remote  ident (addr/mask/prot/port): (30.30.0.0/255.255.0.0/0/0)
   current_peer 20.20.20.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 11, #pkts encrypt: 11, #pkts digest: 0
   #pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 1, #recv errors 0

     local crypto endpt.: 10.30.10.2, remote crypto endpt.:20.20.20.1
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0xEE5B9B9C(3998981020)

     inbound esp sas:
      spi: 0xBE16AC84(3189156996)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2000, flow_id: FPGA:1, crypto map: VPN-MAP2
        sa timing: remaining key lifetime (k/sec): (4525504/2619)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xEE5B9B9C(3998981020)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2001, flow_id: FPGA:1, crypto map: VPN-MAP2
        sa timing: remaining key lifetime (k/sec): (4525504/2619)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:
```

Figure 2.33: Verification that a tunnel has been formed between the two sites and packets are encrypted after a successful ping.

Summary

Our network infrastructure utilises a 3-tier hierarchical design for the headquarters and a simpler design for our branch cafes. This tiered approach ensures reliability, scalability, and cost-effectiveness. The core network features a single HQ router, two multilayer switches for VLAN routing and redundancy, and an EtherChannel for optimised bandwidth. We leverage subnets and VLANs to create a multilayered security approach and have implemented OSPF routing for increased network flexibility. To accommodate future growth, we have adopted VLSM with /16 and /24 subnetting for the headquarters and departments. Additionally, we prioritise Layer 2 security with PortFast, BPDUguard,port security, and auto-trunking disabled.

For our WLAN, we utilise a WLC for centralised management, scalability, and enhanced security. The WLC authenticates users with a RADIUS server, requiring login credentials for staff accessing our 4guyscoffeeOfficeNetwork.Secure site-to-site communication is facilitated through IPSec VPNs. Our branch cafes each have a separate router-on-a-stick topology for inter-VLAN connectivity and utilise separate VLANs and networks to provide secure customer Wi-Fi access.