

University of Saint Louis Tuguegarao
School of Architecture, Computing, and Engineering

Networking 2
A10 - NETW 1023

Two-story Co-Working Space Network Plan
Final Project

Submitted by:
AGGABAO, Arvy
CALOSING, Jeanoel
CAMARAUAN, Giann Gioe
CANICULA, Dheeven
PASCUAL, Leah Loraine

May 12, 2026

TABLE OF CONTENTS

PROJECT OVERVIEW.....	4
Project Design Summary.....	4
Overall Floor Plan View.....	5
Network Architecture.....	7
Network Equipment List.....	8
TOPOLOGY AND CABLING SCHEMATICS.....	10
Network Topology.....	10
Server Rack Configuration.....	13
Cable Management.....	14
NETWORK INFRASTRUCTURE.....	16
VLAN Design.....	16
DHCP Design.....	16
Telephony Design.....	17
VTP Configuration.....	17
STP/RSTP Configuration.....	17
Port Assignments.....	18
CWS-CORE-ROUTER (4331).....	18
CWS-CORE-SW (3650).....	18
CWS-ACCESS-F1 (2960).....	18
CWS-ACCESS-F2 (2960).....	19
WLC 3504 Architecture.....	20
Management Interface.....	20
Dynamic Interfaces.....	21
Wireless Design.....	21
Access Point (AP) Groups.....	22
CONFIG DOCUMENTATION.....	22
Core-RT (ISR 4331).....	22
Core-SW (Catalyst 3650).....	24
Server-PT DHCP.....	29
Access Switch Ground Floor (Catalyst 2960).....	30
Access Switch Second Floor (Catalyst 2960).....	34
CME-R (2811).....	38
WLC-3504.....	40
CCTV Setups (DHCP Config).....	46
IP Phone DHCP Config.....	47
LAPs DHCP Config.....	48
Reception Computer (Daisy-chained Connectivity).....	49
TEST DOCUMENTATION.....	50
Ping Test.....	50
IP Phone Calling Test.....	51

Wireless Devices Connecting Test.....	52
VLAN Config Screenshots.....	52
DHCP Config Screenshots.....	54
Spanning Tree Config Screenshots.....	54
VLAN Trunking Protocol Config Screenshots.....	57
Access Control List Screenshot.....	58

PROJECT OVERVIEW

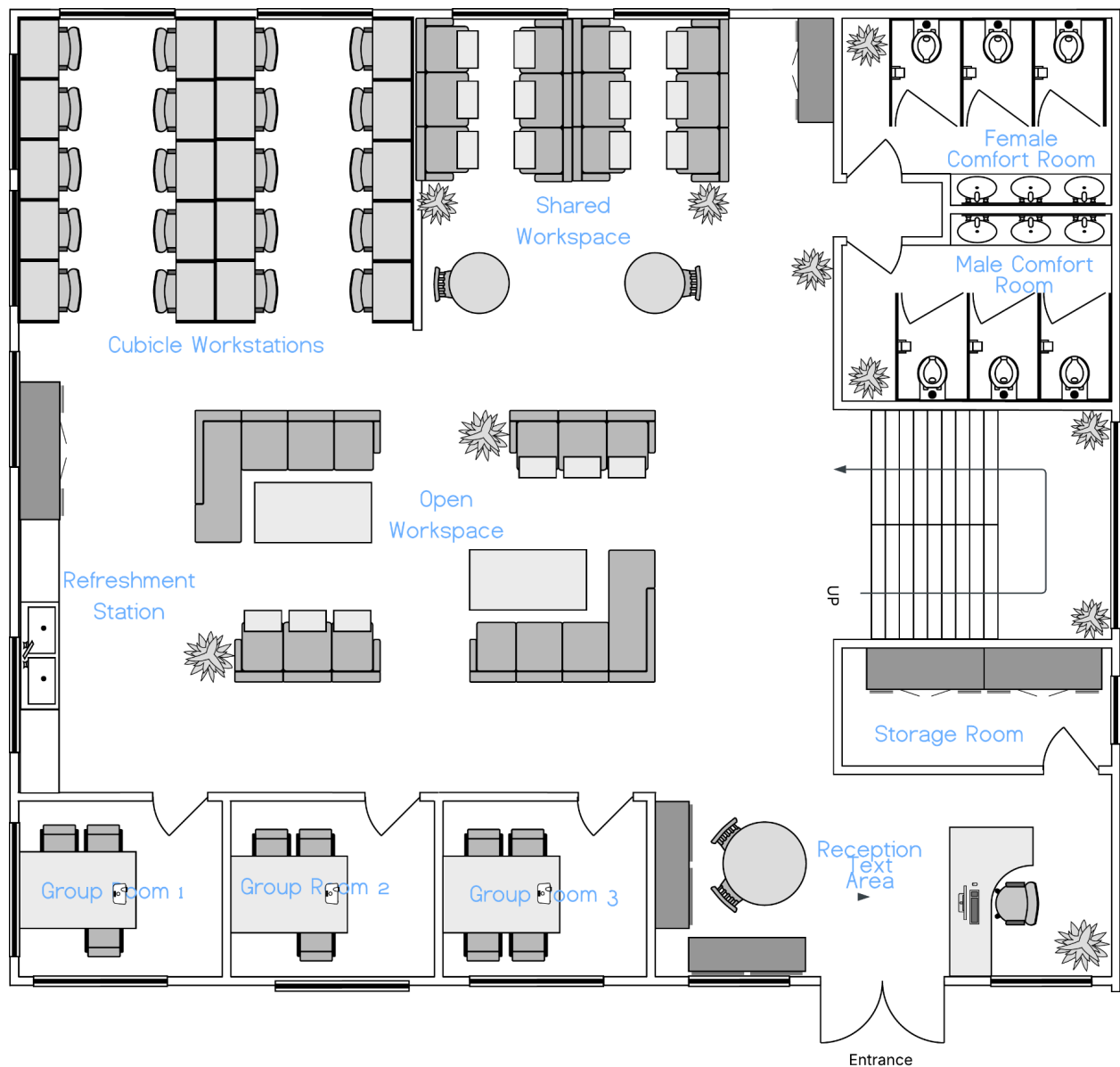
Project Design Summary

This project presents a two-tier network architecture designed for a medium-sized co-working space. The topology consists of a single core router, one Layer 3 core switch, and two access switches serving separate floors. The design balances configuration simplicity with core networking requirements, ensuring reliable connectivity for multiple independent customers and staff.

To minimize network hops and simplify troubleshooting, all centralized services, including the Wireless LAN Controller (WLC), DHCP server, Cisco Unified Communications Manager Express (CME) telephony router, NVR, and server room PC, connects directly to the core switch. The core switch also manages inter-VLAN routing via Switch Virtual Interfaces (SVIs), providing logical isolation between different user groups.

At the access layer, floor switches link to the core via trunks, utilizing Spanning Tree Protocol (STP) to prevent network loops. At the network edge, the router implements dual-ISP failover to maintain continuous internet access during provider outages. Furthermore, Access Control Lists (ACLs) are configured to secure the internal server room from unauthorized external traffic.

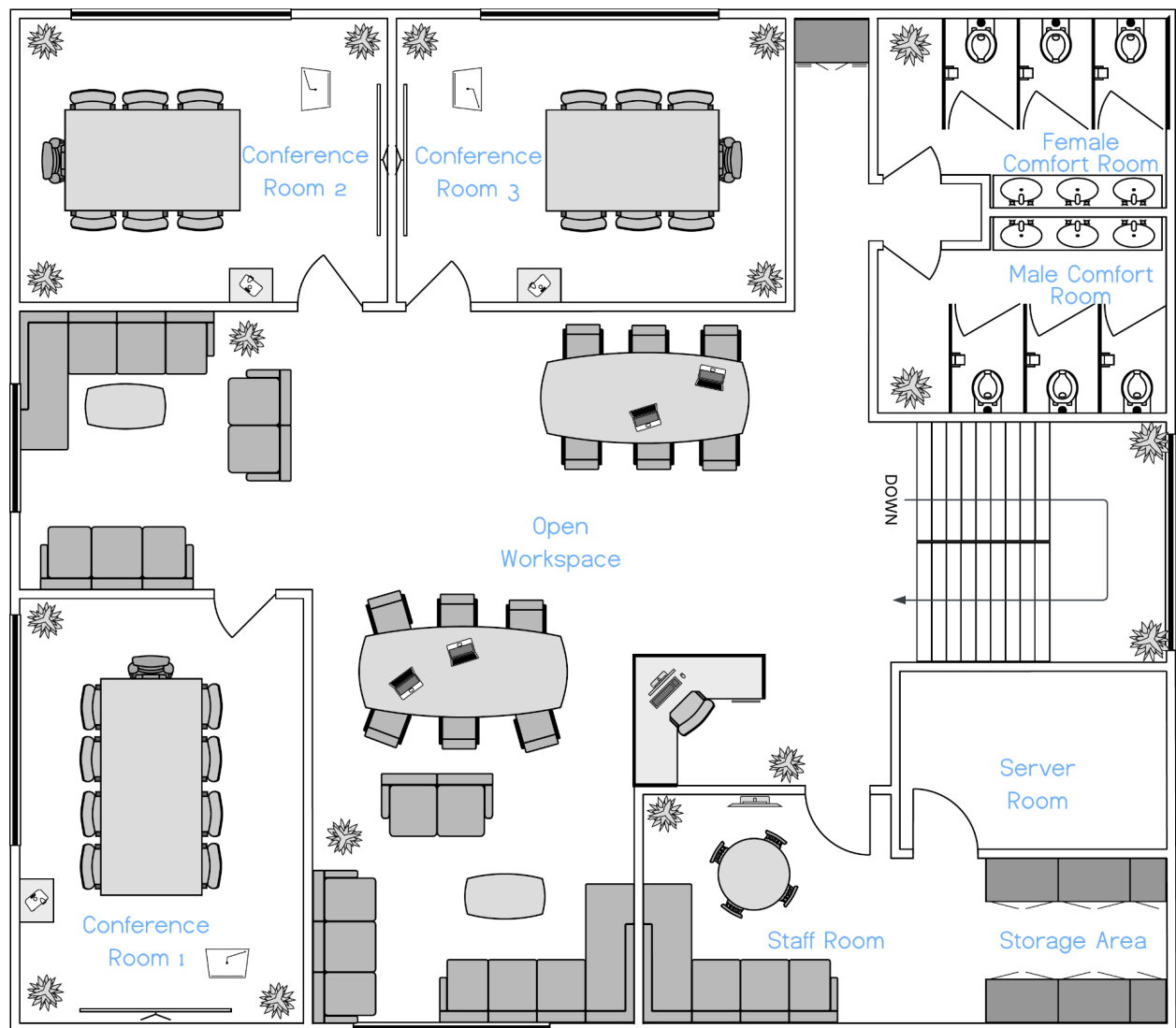
Overall Floor Plan View



FIRST FLOOR PLAN

Figure 1. Co-Working Space Ground Floor Plan

Figure 1 shows the Ground Floor Plan of the Co-Working Space. The ground floor is accessible through the main entrance and contains a shared workspace and an open workspace to accommodate different working preferences. It also includes three Group Rooms for small-team collaborations, a Reception Area near the entrance, a Refreshment Station, a Storage Room, and Comfort Rooms for male and female occupants.



SECOND FLOOR PLAN

Figure 2. Co-Working Space Second Floor Plan

Figure 2 shows the Second Floor Plan of the Co-Working Space. This floor is oriented toward more formal settings, housing three conference rooms, an open workspace at the center, and comfort rooms for males and females. It also includes the staff room, a dedicated space for employees to work and coordinate, and the server room, the central hub of the network infrastructure that hosts the core networking equipment supporting the entire establishment.

Network Architecture

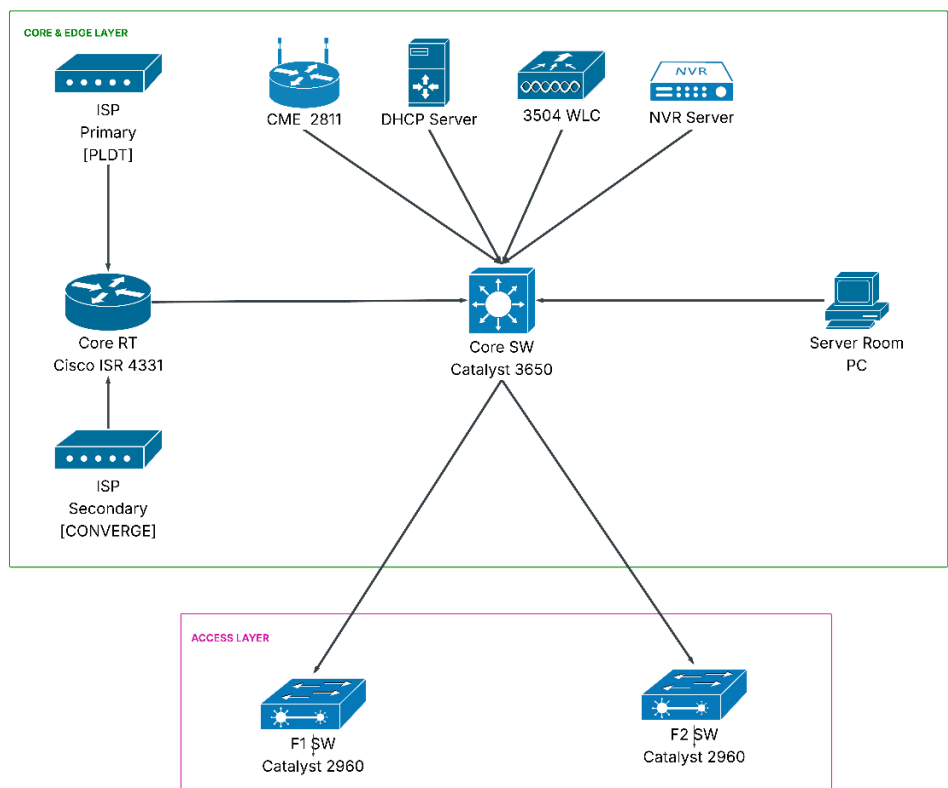


Figure 3. Two-Tier Model Network Architecture

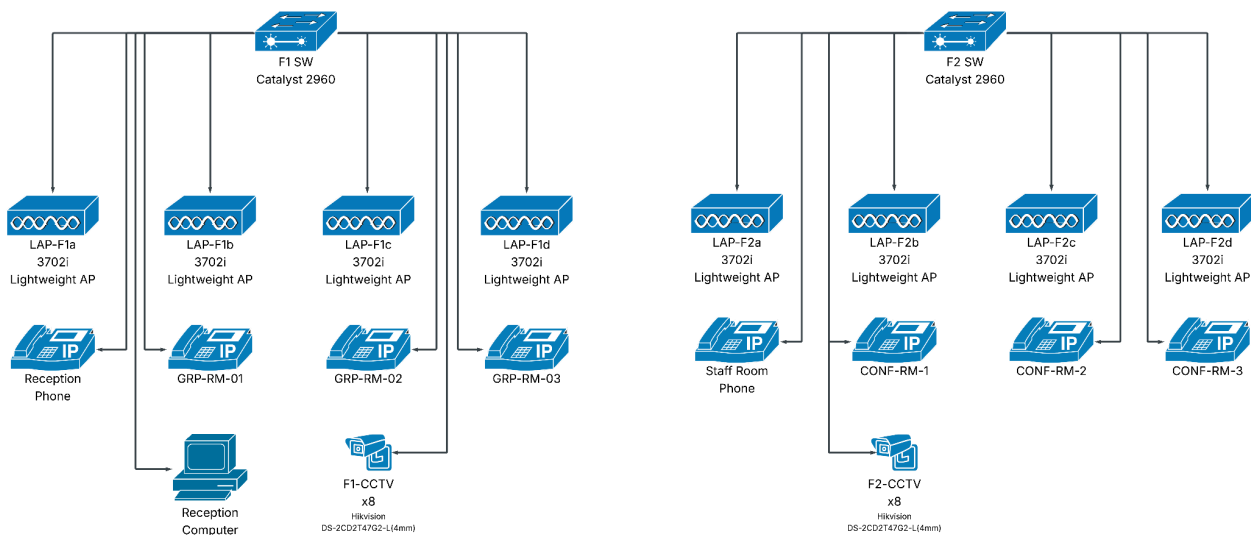


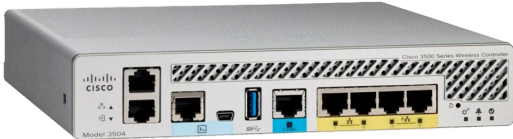
Figure 4. Access Layer Connections

Figure 3 illustrates a Two-Tier Model Network Architecture, a collapsed-core design in which the Catalyst 3650 simultaneously handles core switching and distribution functions. The core and edge layers

sit at the top. The Cisco ISR 4331 router serves as the edge device, dual-homed to two ISPs (PLDT as the primary and CONVERGE as the secondary), providing WAN redundancy. It connects to the Catalyst 3650 via the /30 point-to-point link. The 3650 acts as the collapsed core/distribution switch, handling all inter-VLAN routing and DHCP relay for upstream devices. CME 2811, DHCP Server, 3504 WLC, NVR Server, and Server Room PC all connect to the 3650 on a management VLAN (/24).

The Access Layer consists of two Catalyst 2960 switches per floor, both uplinked to the Core 3650. Figure 4 illustrates the Access Layer Connections; two Catalyst 2960 switches serve each floor. The ground-floor switch (F1 SW) connects to the ground-floor security cameras, the reception phone and computer (reception area), and 4 lightweight access points. The second floor (F2) hosts the staff room, server room, three conference rooms, and its own set of cameras. IP phones on each floor register to the CME 2811. Group/conference rooms endpoints are Cisco IP phones and the 16 total Hikvision DS-2CD2T47G2-L cameras (8 per floor) are streamed to the NVR server on a dedicated surveillance VLAN 50 (/24).

Network Equipment List

Device	Model (PT)	Image	Qty
Core Router	Cisco ISR4331		1
L3 Core Switch	Catalyst 3650 24PS		1
Access Switch	Catalyst 2960		2
WLC	Cisco 3504		1

Lightweight AP	Cisco Aironet 3702i		8
CME Router	Cisco 2811		1
NVR	Cisco Catalyst 9200L-24P-4 G		1
Desktop PC	Generic PCs		2

IP Phone	Cisco Desk Phone 9871		8
CCTV Camera	Hikvision DS-2CD2T47 G2-L(4mm)		16

TOPOLOGY AND CABLING SCHEMATICS

Network Topology

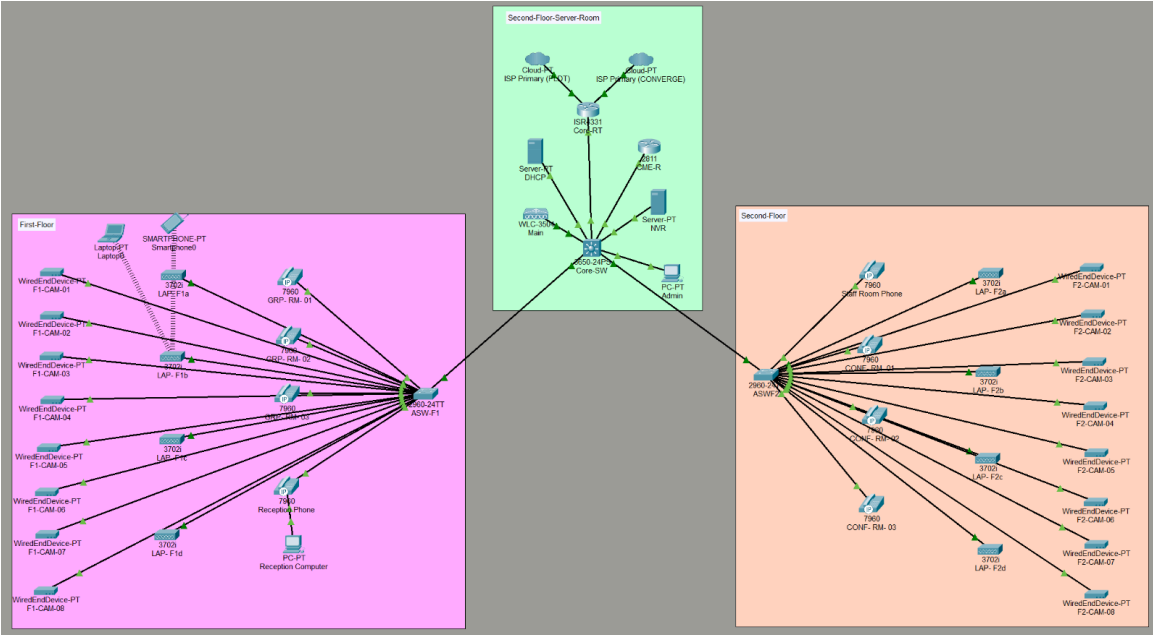


Figure 5a. CWS Full Network Topology



Figure 5b. CWS Ground Floor

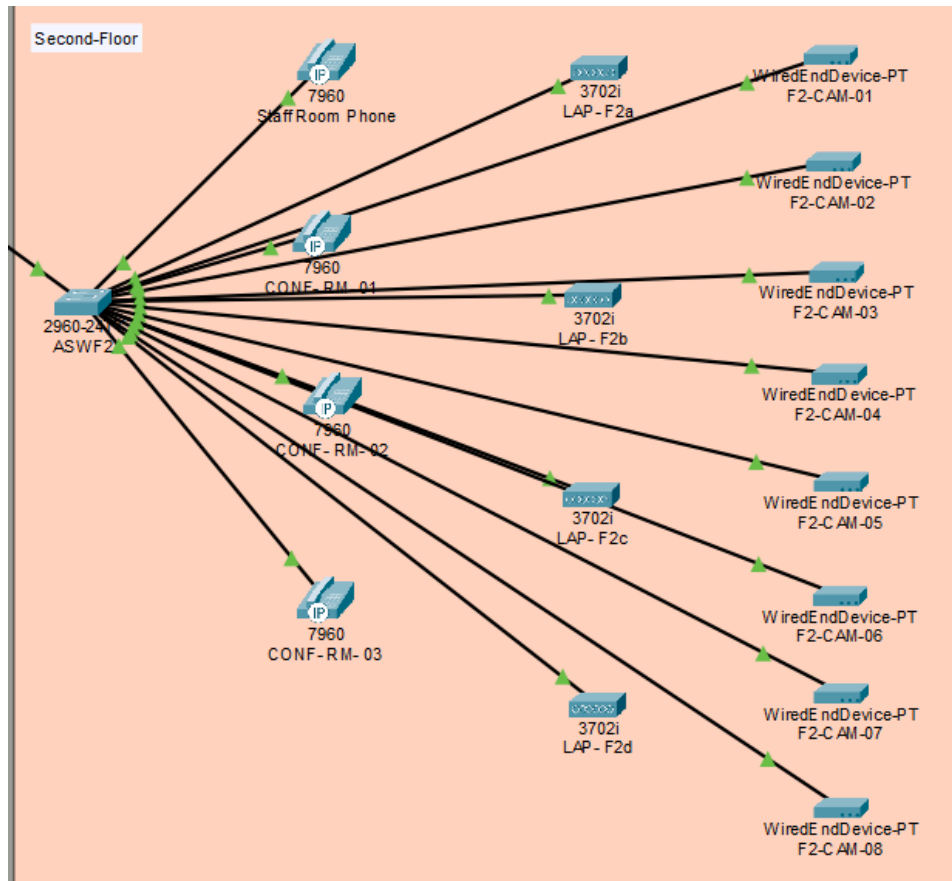


Figure 5c. CWS Second Floor

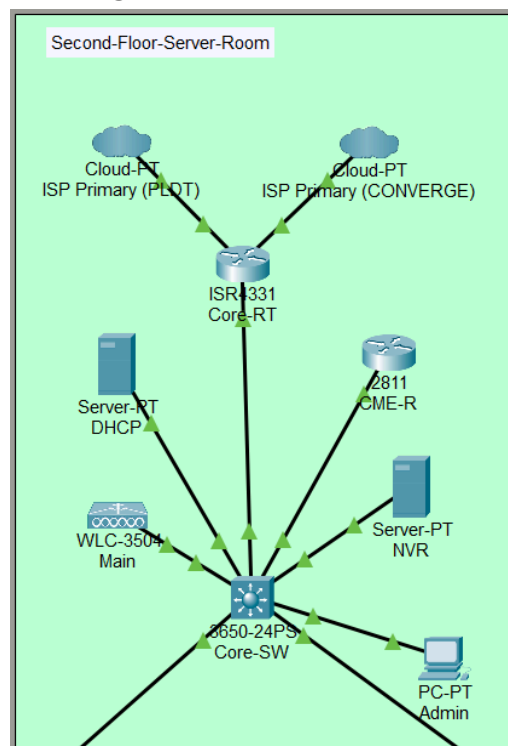


Figure 5d. CWS Server Room

Server Rack Configuration

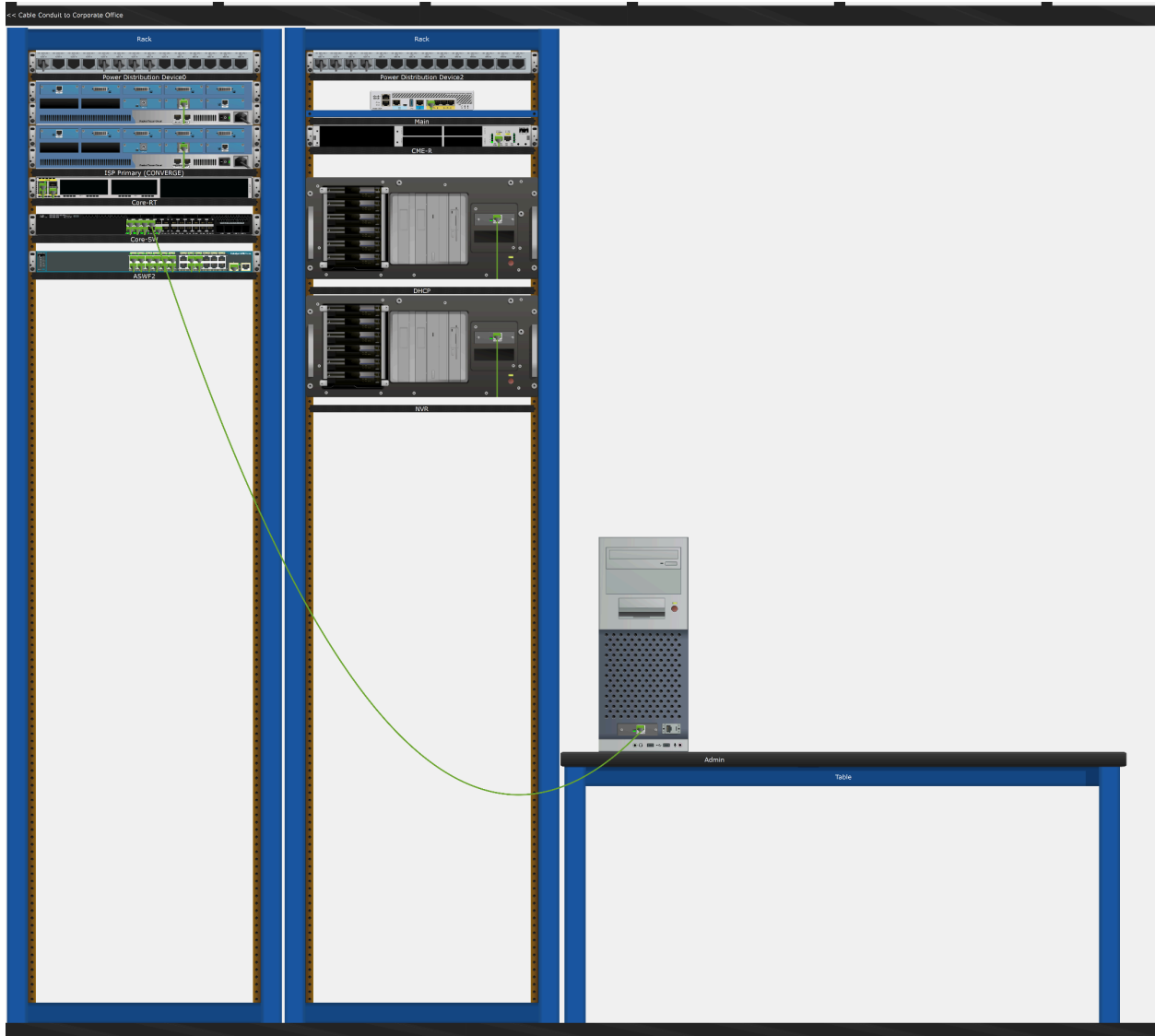
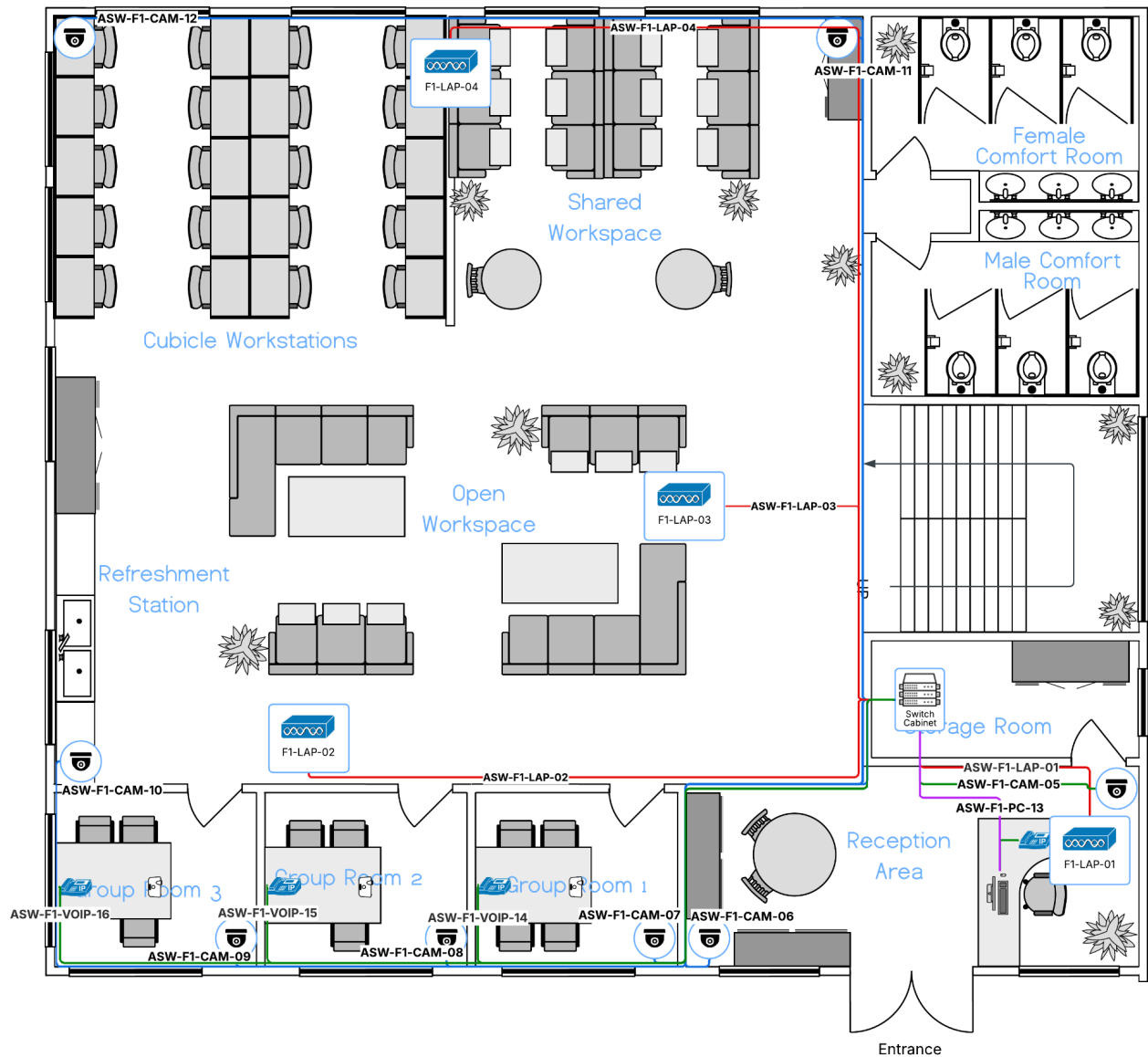


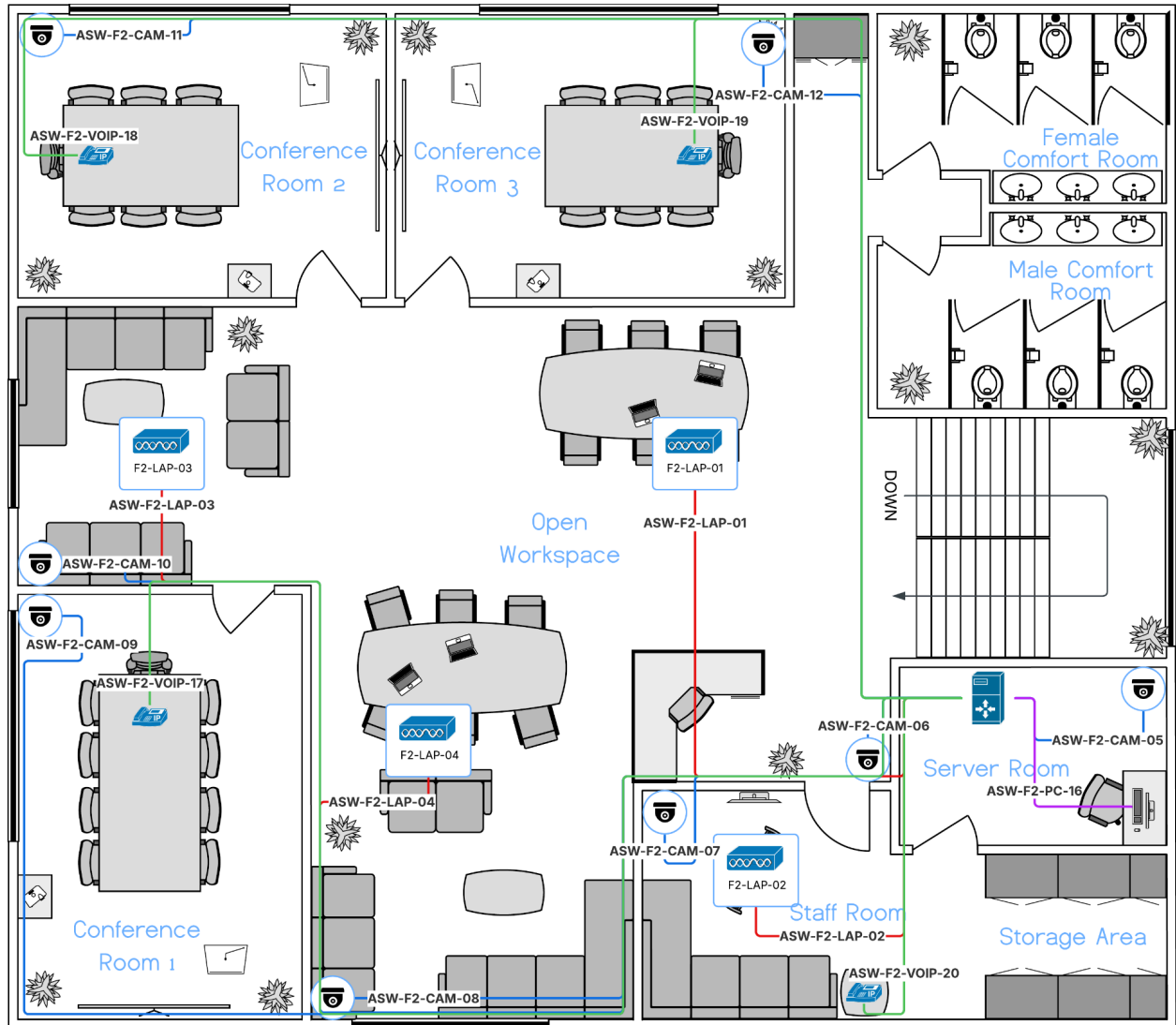
Figure 6. Server Rack Structure

Cable Management



FIRST FLOOR PLAN

Figure 7. CWS Cabling Plan for Ground Floor



SECOND FLOOR PLAN

Figure 8. Cabling Plan for Second Floor

For our cabling design, we used an indoor Cat6 cable throughout the network infrastructure to ensure high-speed, reliable performance for daily operations. And to keep our system organized and easy to maintain, our physical and logical network administration aligns with the core principles of ISO/IEC 14763-2. Our labeling follows a simple human-readable naming structure, formatted as *Layer-Floor-Equipment-ID*, allowing us to quickly identify and troubleshoot any devices that would fail during operation

NETWORK INFRASTRUCTURE

VLAN Design

ID	Name	CIDR	SVI	Mask
10	MANAGEMENT	10.0.10.0/24	10.0.10.1	255.255.255.0
20	STAFF_GLOBAL	10.0.20.0/24	10.0.20.1	255.255.255.0
31	CWS_FLOOR_1	10.0.31.0/24	10.0.31.1	255.255.255.0
32	CWS_FLOOR_2	10.0.32.0/24	10.0.32.1	255.255.255.0
40	VOICE	10.0.40.0/24	10.0.40.1	255.255.255.0
50	IOT_CCTV	10.0.50.0/24	10.0.50.1	255.255.255.0

The following are the assignments of each VLAN Configuration:

- **VLAN 10** - Used for managing all infrastructure. This includes switches, routers, a wireless LAN controller, and the call manager express.
- **VLAN 20** - Used for all CWS Staff on all floors
- **VLAN 31** - Used for customers connected to the Ground Floor's LAPs
- **VLAN 32** - Used for customers connected to the Second Floor's LAPs
- **VLAN 40** - Used for IP Phones
- **VLAN 50** - Used for all the IP Cameras in the workplace

DHCP Design

DHCP is split between two devices based on what each can support in Packet Tracer. **Server-PT** (10.0.20.21, VLAN 20) handles all non-voice pools via its Services GUI:

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Masks	Max Users
STAFF_POOL	10.0.20.1	8.8.8.8	10.0.20.31	255.255.255.0	200
CWS_F1_POOL	10.0.31.1	8.8.8.8	10.0.31.11	255.255.255.0	200
CWS_F2_POOL	10.0.32.1	8.8.8.8	10.0.32.11	255.255.255.0	200
IOT_CCTV_POOL	10.0.50.1	8.8.8.8	10.0.50.21	255.255.255.0	200

CME-2811 (10.0.40.5, VLAN 40) handles the VOICE_POOL only via CLI. It includes “option 150,” which points to itself, telling IP phones where to download the config and register via SCCP.

MGMT_POOL (VLAN 10, for LAPs) stays on the Core 3650 CLI. Server-PT's GUI does not support “option 43”, which is required for LAPs to automatically discover and join the WLC via CAPWAP. This is the only pool that remains on the switch.

The Core 3650 SVIs use an **IP helper-address** to relay DHCP requests to the correct server:

- **VLAN 10** - served locally by Core 3650 (MGMT_POOL with option 43)
- **VLAN 20, 31, 32, 50** - “ip helper-address 10.0.20.21” (Server-PT)
- **VLAN 40** - “ip helper-address 10.0.40.5” (CME-2811)

Telephony Design

A Cisco 2811 router acts as the Call Manager Express (CME) server. All 8 IP phones across both floors register to this single CME instance, enabling native inter-floor calls without any dial-peer configuration.

Floor 1 phones extensions 1001, 1002, 1003, 1004

Floor 2 phones extensions 2001, 2002, 2003, 2004

Phones receive their IP from the CME's own VOICE_POOL. “option 150” in that pool points to “10.0.40.5” (the CME itself), directing phones to register via SCCP on port 2000.

VTP Configuration

VTP allows VLANs to be created once on the Core 3650 and automatically propagated to both access switches over trunk links. This eliminates the need to manually create VLANs on each switch.

Device	Model	VTP Role	Domain	Version
CWS-CORE-SW	Catalyst 3650	Server	CWS_NET	2
CWS-ACCESS-F1	Catalyst 2960	Client	CWS_NET	2
CWS-ACCESS-F2	Catalyst 2960	Client	CWS_NET	2

STP/RSTP Configuration

RSTP (IEEE 802.1w) manages loop prevention. The Core 3650 is the manually designated root bridge for all VLANs via a lowered priority.

Device	STP Role	Priority	Notes
CWS-CORE-SW	Root Bridge	4096	Lowest priority. Always becomes the root for all VLANs
CWS-ACCESS-F1	Non-Root	32768	Default priority
CWS-ACCESS-F2	Non-Root	32768	Default priority

PortFast is enabled on all end-device access ports (LAPs, CCTVs, phones, PCs, NVR, Server-PT, CME). This skips the STP listening and learning states, so devices can communicate immediately on link-up without waiting 30 seconds. In addition, BPDU Guard is enabled on all end-device ports, along with PortFast. If a switch is accidentally plugged into an end-device port and sends BPDU frames, BPDU Guard immediately shuts down that port (err-disabled state) to protect the STP topology.

Port Assignments***CWS-CORE-ROUTER (4331)***

Port	Connected To	Mode	Configuration
G0/0	ISP (Primary)	Routed	203.0.113.2/30 (RFC 5737) NAT Outside Administrative Distance (AD) = 1
G0/1	ISP (Failover)	Routed	198.51.100.2/30 (RFC 5737) NAT Outside Administrative Distance (AD) = 10
G0/2	CWS-CORE-SW	Routed	10.0.0.1/30 NAT Inside

CWS-CORE-SW (3650)

Port	Connected To	Mode	Configuration
G1/0/1	CWS-ROUTER	Routed	10.0.0.2/30
G1/0/2	CWS-ACCESS-F1	Trunk	VLAN 10,20,31,40,50
G1/0/3	CWS-ACCESS-F2	Trunk	VLAN 10,20,32,40,50
G1/0/4	DHCP Server	Access	VLAN 20 Static IP: 10.0.20.21
G1/0/5	CME Router	Access	VLAN 40 Static IP: 10.0.40.5
G1/0/6	NVR Server	Access	VLAN 50 Static IP: 10.0.50.10
G1/0/7	Server Room PC	Access	VLAN 20 Static IP: 10.0.20.20
G1/0/10	WLC 3504	Trunk	VLAN 10,20,31,32 Native VLAN 10

CWS-ACCESS-F1 (2960)

Port	Connected To	Mode	Configuration
G0/1	CWS-CORE-SW	Trunk	VLAN 10,20,31,40,50 (Uplink Connection)
Fa0/1	LAP-F1a (3702i)	Trunk	Native VLAN 10 Allowed VLANs 10, 20, 31 Trunk Portfast
Fa0/2	LAP-F1b (3702i)	Trunk	Native VLAN 10

			Allowed VLANs 10, 20, 31 Trunk Portfast
Fa0/3	LAP-F1c (3702i)	Trunk	Native VLAN 10 Allowed VLANs 10, 20, 31 Trunk Portfast
Fa0/4	LAP-F1d (3702i)	Trunk	Native VLAN 10 Allowed VLANs 10, 20, 31 Trunk Portfast
Fa0/5-12	CCTV Cameras F1 (8x)	Access	VLAN 50 Portfast Enabled BPDU Guard Enabled Port Security Max 1
Fa0/13	Front Desk PC with IP Phone	Multi-VLAN Access	Daisy Chained PC and IP Phone Data VLAN 20 Voice VLAN 40 Port Security Max 3
Fa0/14	Group Room 1 IP Phone	Access	Data VLAN 20 Voice VLAN 40 Port Security Max 2
Fa0/15	Group Room 2 IP Phone	Access	Data VLAN 20 Voice VLAN 40 Port Security Max 2
Fa0/16	Group Room 3 IP Phone	Access	Data VLAN 20 Voice VLAN 40 Port Security Max 3
Fa0/17-24	-	-	<i>Reserved</i>

CWS-ACCESS-F2 (2960)

Port	Connected To	Mode	Configuration
G0/1	CWS-CORE-SW	Trunk	VLAN 10,20,31,40,50 (Uplink Connection)
Fa0/1	LAP-F2a (3702i)	Trunk	Native VLAN 10 Allowed VLANs 10, 20, 31 Trunk Portfast
Fa0/2	LAP-F2b (3702i)	Trunk	Native VLAN 10 Allowed VLANs 10, 20, 31 Trunk Portfast
Fa0/3	LAP-F2c (3702i)	Trunk	Native VLAN 10 Allowed VLANs 10, 20, 31

			Trunk Portfast
Fa0/4	LAP-F2d (3702i)	Trunk	Native VLAN 10 Allowed VLANs 10, 20, 31 Trunk Portfast
Fa0/5-12	CCTV Cameras F1 (8x)	Access	VLAN 50 Portfast Enabled BPDU Guard Enabled Port Security Max 1
Fa0/13-14	-	-	Reserved
Fa0/15	Conference Room 1 IP Phone	Access	Data VLAN 20 Voice VLAN 40 Port Security Max 2
Fa0/16	Conference Room 2 IP Phone	Access	Data VLAN 20 Voice VLAN 40 Port Security Max 2
Fa0/17	Conference Room 3 IP Phone	Access	Data VLAN 20 Voice VLAN 40 Port Security Max 2
Fa0/18	Staff Room IP Phone	Access	Data VLAN 20 Voice VLAN 40 Port Security Max 2
Fa0/19-24	-	-	<i>Reserved</i>

WLC 3504 Architecture

Management Interface

Handles all WLC control plane traffic via CAPWAP tunnel termination from LAPs, GUI access, and AP management

Parameter	Value
Interface Name	management
VLAN ID	10
IP Address	10.0.10.10
Subnet Mask	255.255.255.0
Default Gateway	10.0.10.1
Primary DHCP Server	10.0.10.1
Physical Port	Port 1 (connected to CWS-CORE-SW G1/0/10)

Dynamic Interfaces

Dynamic interfaces are the WLC-side exit points for each wireless data VLAN. When a client associates with an SSID, the WLC places that client's traffic onto the matching dynamic interface, which exits tagged with the correct VLAN toward the Core 3650 Switch.

Interface Name	VLAN ID	IP Address	Subnet Mask	Gateway	Primary DHCP Server
staff-iface	20	10.0.20.2	255.255.255.0	10.0.20.21	10.0.20.21
cws-f1-iface	31	10.0.31.2	255.255.255.0	10.0.31.1	10.0.20.21
cws-f2-iface	32	10.0.32.2	255.255.255.0	10.0.32.1	10.0.20.21

All dynamic interfaces point to Server-PT as the Primary DHCP Server. The WLC uses its virtual interface IP (1.1.1.1) as the GIADDR (relay agent address) when forwarding DHCP requests to Server-PT. Also, the trunk port on CWS-CORE-SW G1/0/10 is configured to allow traffic for VLANs 10, 20, 31, and 32. Without VLAN 31 or 32 on that trunk, traffic on the corresponding dynamic interfaces cannot exit the WLC, and wireless clients on those VLANs will be unreachable.

Wireless Design

The 3504 WLC manages all 8 LAPs via CAPWAP tunnels over VLAN 10. Two separate SSIDs are used per floor because Packet Tracer does not support an AP Group interface override with a single shared SSID.

CWS_WIFI_GroundFloor - VLAN 31, served by AP-GROUP-F1 (Floor 1 APs only)

CWS_WIFI_2ndFloor - VLAN 32, served by AP-GROUP-F2 (Floor 2 APs only)

STAFF_WIFI - VLAN 20, global across all APs on both floors

PT Limitation: Packet Tracer does not fully simulate CAPWAP mobility or seamless AP handoff within a floor. This is a known simulator constraint and does not reflect a design error. In a real deployment, the 3504 WLC handles this natively.

Access Point (AP) Groups

1. AP-GROUP-F1 (Floor 1)

Parameter	Value
Group Name	AP-GROUP-F1
WLANs to add	CWS_WIFI_GroundFloor, STAFF_WIFI
APs to assign	LAP-F1a, LAP-F1b, LAP-F1c, LAP-F1d

2. AP-GROUP-F2 (Floor 2)

Parameter	Value
Group Name	AP-GROUP-F2
WLANs to add	CWS_WIFI_2ndFloor, STAFF_WIFI
APs to assign	LAP-F2a, LAP-F2b, LAP-F2c, LAP-F2d

CONFIG DOCUMENTATION

Core-RT (ISR 4331)

Hardening

```
Router>en
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname CWS-ROUTER
CWS-ROUTER(config)#no ip domain-lookup
CWS-ROUTER(config)#ip domain-name cws.local
CWS-ROUTER(config)#service password-encryption
CWS-ROUTER(config)#enable secret cws@2026
CWS-ROUTER(config)#username admin privilege 15 secret cws@2026
CWS-ROUTER(config)#line con 0
CWS-ROUTER(config-line)#login local
CWS-ROUTER(config-line)#exec-timeout 5 0
CWS-ROUTER(config-line)#line vty 0 4
CWS-ROUTER(config-line)#login local
CWS-ROUTER(config-line)#transport input ssh
CWS-ROUTER(config-line)#exec-timeout 5 0
CWS-ROUTER(config-line)#crypto key generate rsa
The name for the keys will be: CWS-ROUTER.cws.local
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

CWS-ROUTER(config)#ip ssh version 2
*Mar 1 0:7:36.173: %SSH-5-ENABLED: SSH 1.99 has been enabled
CWS-ROUTER(config)#banner motd # CWS-NET  AUTHORIZED ACCESS ONLY #
```

WAN and LAN Interfaces

```
CWS-ROUTER(config)#!  
CWS-ROUTER(config)#int g0/0/0  
CWS-ROUTER(config-if)#desc LINK_ISP1_PRIMARY  
CWS-ROUTER(config-if)#ip addr 203.0.113.2 255.255.255.252  
CWS-ROUTER(config-if)#ip nat outside  
CWS-ROUTER(config-if)#no shut  
  
CWS-ROUTER(config-if)#  
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up  
  
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed  
state to up  
  
CWS-ROUTER(config-if)#int g0/0/1  
CWS-ROUTER(config-if)#desc LINK_ISP2_FAILOVER  
CWS-ROUTER(config-if)#ip addr 198.51.100.2 255.255.255.252  
CWS-ROUTER(config-if)#ip nat outside  
CWS-ROUTER(config-if)#no shut  
  
CWS-ROUTER(config-if)#  
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up  
  
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed  
state to up  
  
CWS-ROUTER(config-if)#int g0/0/2  
CWS-ROUTER(config-if)#desc LINK_TO_CWS-CORE-SW  
CWS-ROUTER(config-if)#ip addr 10.0.0.1 255.255.255.252  
CWS-ROUTER(config-if)#ip nat inside  
CWS-ROUTER(config-if)#no shut  
  
CWS-ROUTER(config-if)#  
%LINK-5-CHANGED: Interface GigabitEthernet0/0/2, changed state to up  
  
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/2, changed  
state to up
```

Floating Static Routes

```
CWS-ROUTER(config)#!  
CWS-ROUTER(config)#ip route 0.0.0.0 0.0.0.0 203.0.113.1 1  
CWS-ROUTER(config)#ip route 0.0.0.0 0.0.0.0 198.51.100.1 10  
CWS-ROUTER(config)#ip route 10.0.0.0 255.0.0.0 10.0.0.2  
CWS-ROUTER(config)#!
```

NAT (PAT Overload)

```
CWS-ROUTER(config)#!  
CWS-ROUTER(config)#ip access-list standard NAT_INSIDE  
CWS-ROUTER(config-std-nacl)#permit 10.0.0.0 0.255.255.255  
CWS-ROUTER(config-std-nacl)#ip nat inside source list NAT_INSIDE interface  
^  
% Invalid input detected at '^' marker.  
  
CWS-ROUTER(config-std-nacl)#exit  
CWS-ROUTER(config)#ip nat inside source list NAT_INSIDE interface  
% Incomplete command.  
CWS-ROUTER(config)#ip nat inside source list NAT_INSIDE interface g0/0/0 overload  
CWS-ROUTER(config)#ip nat inside source list NAT_INSIDE interface g0/0/1 overload  
CWS-ROUTER(config)#end  
CWS-ROUTER#  
%SYS-5-CONFIG_I: Configured from console by console  
  
CWS-ROUTER#wr  
Building configuration...  
[OK]
```

Core-SW (Catalyst 3650)

```
Switch>en
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname CWS-CORE-SW
CWS-CORE-SW(config)#no ip domain-lookup
CWS-CORE-SW(config)#ip domain-name cws.local
```

IP Routing + VTP Server + STP Root

```
CWS-CORE-SW(config)#ip routing
CWS-CORE-SW(config)#spanning-tree mode rapid-pvst
CWS-CORE-SW(config)#spanning-tree vlan 10,20,31,32,40,50 priority 4096
CWS-CORE-SW(config)#vtp mode server
Device mode already VTP SERVER.
CWS-CORE-SW(config)#vtp domain CWS_NET
Changing VTP domain name from NULL to CWS_NET
CWS-CORE-SW(config)%%SW_VLAN-6-VTP_DOMAIN_NAME_CHG: VTP domain name changed to CWS_NET.

CWS-CORE-SW(config)#vtp version 2
CWS-CORE-SW(config)#vtp password cws_net123
Setting device VLAN database password to cws_net123
```

VLAN Creation

```
CWS-CORE-SW(config)#vlan 10
CWS-CORE-SW(config-vlan)#name MANAGEMENT
CWS-CORE-SW(config-vlan)#vlan 20
CWS-CORE-SW(config-vlan)#name STAFF_GLOBAL
CWS-CORE-SW(config-vlan)#vlan 31
CWS-CORE-SW(config-vlan)#name CWS_FLOOR_1
CWS-CORE-SW(config-vlan)#vlan 32
CWS-CORE-SW(config-vlan)#name CWS_FLOOR_2
CWS-CORE-SW(config-vlan)#vlan 40
CWS-CORE-SW(config-vlan)#name VOICE
CWS-CORE-SW(config-vlan)#vlan 50
CWS-CORE-SW(config-vlan)#name IOT_CCTV
CWS-CORE-SW(config-vlan)#
```

Routed Port to Router + Default Route

```
CWS-CORE-SW(config-vlan)#int g1/0/1
CWS-CORE-SW(config-if)#desc LINK_TO_CWS-ROUTER
CWS-CORE-SW(config-if)#no switchport
CWS-CORE-SW(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed state to up

CWS-CORE-SW(config-if)#ip addr 10.0.0.2 255.255.255.252
CWS-CORE-SW(config-if)#no shut
CWS-CORE-SW(config-if)#ip route 0.0.0.0 0.0.0.0 10.0.0.1
CWS-CORE-SW(config)#
```

Inter-VLAN Routing and DHCP Relay

```
CWS-CORE-SW(config)#ip access-list extended ACL_IOT_CCTV
CWS-CORE-SW(config-ext-nacl)#no deny ip 10.0.50.0 0.0.0.255 10.0.0.0 0.255.255.255
CWS-CORE-SW(config-ext-nacl)#permit ip host 10.0.50.10 any
CWS-CORE-SW(config-ext-nacl)#deny ip 10.0.50.0 0.0.0.255 10.0.0.0 0.255.255.255
CWS-CORE-SW(config-ext-nacl)#permit ip any any
CWS-CORE-SW(config-ext-nacl)#ip access-list extended ACL_CWS_CLIENTS
CWS-CORE-SW(config-ext-nacl)#deny ip 10.0.31.0 0.0.0.255 10.0.0.0 0.255.255.255
CWS-CORE-SW(config-ext-nacl)#deny ip 10.0.32.0 0.0.0.255 10.0.0.0 0.255.255.255
CWS-CORE-SW(config-ext-nacl)#permit ip any any
CWS-CORE-SW(config-ext-nacl)#int vlan 10
CWS-CORE-SW(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up

CWS-CORE-SW(config-if)#desc MGMT_SVI
CWS-CORE-SW(config-if)#ip addr 10.0.10.1 255.255.255.0
CWS-CORE-SW(config-if)#no shut
CWS-CORE-SW(config-if)#int vlan 20
CWS-CORE-SW(config-if)#
%LINK-5-CHANGED: Interface Vlan20, changed state to up

CWS-CORE-SW(config-if)#desc STAFF_SVI
CWS-CORE-SW(config-if)#ip addr 10.0.20.1 255.255.255.0
CWS-CORE-SW(config-if)#ip helper-address 10.0.20.21
CWS-CORE-SW(config-if)#no shut
CWS-CORE-SW(config-if)#int vlan 31
CWS-CORE-SW(config-if)#
%LINK-5-CHANGED: Interface Vlan31, changed state to up

CWS-CORE-SW(config-if)#desc CWS_F1_SVI
CWS-CORE-SW(config-if)#ip addr 10.0.31.1 255.255.255.0
CWS-CORE-SW(config-if)#ip helper-address 10.0.20.21
CWS-CORE-SW(config-if)#ip access-group ACL_CWS_CLIENTS in
CWS-CORE-SW(config-if)#no shut
CWS-CORE-SW(config-if)#int vlan 32
CWS-CORE-SW(config-if)#
%LINK-5-CHANGED: Interface Vlan32, changed state to up

CWS-CORE-SW(config-if)#desc CWS_F2_SVI
CWS-CORE-SW(config-if)#ip addr 10.0.32.1 255.255.255.0
CWS-CORE-SW(config-if)# ip helper-address 10.0.20.21
CWS-CORE-SW(config-if)#ip access-group ACL_CWS_CLIENTS in
CWS-CORE-SW(config-if)#no shut
CWS-CORE-SW(config-if)#int vlan 40
CWS-CORE-SW(config-if)#
%LINK-5-CHANGED: Interface Vlan40, changed state to up

CWS-CORE-SW(config-if)#desc VOICE_SVI
CWS-CORE-SW(config-if)#ip addr 10.0.40.1 255.255.255.0
CWS-CORE-SW(config-if)#ip helper-address 10.0.40.5
CWS-CORE-SW(config-if)#no shut
CWS-CORE-SW(config-if)#int vlan 50
CWS-CORE-SW(config-if)#
%LINK-5-CHANGED: Interface Vlan50, changed state to up

CWS-CORE-SW(config-if)#desc IOT_CCTV_SVI
CWS-CORE-SW(config-if)#ip addr 10.0.50.1 255.255.255.0
CWS-CORE-SW(config-if)#ip helper-address 10.0.20.21
```

MGMT_POOL — Local DHCP for LAPs Only

```
CWS-CORE-SW(config)#ip dhcp excluded-address 10.0.10.1 10.0.10.20
CWS-CORE-SW(config)#ip dhcp pool MGMT_POOL
CWS-CORE-SW(dhcp-config)#network 10.0.10.0 255.255.255.0
CWS-CORE-SW(dhcp-config)#default-router 10.0.10.1
CWS-CORE-SW(dhcp-config)#dns-server 8.8.8.8
CWS-CORE-SW(dhcp-config)#option 43 ip 10.0.10.10
CWS-CORE-SW(dhcp-config)#
```

Trunk Ports to Access Switches

```
CWS-CORE-SW(config)#int g1/0/2
CWS-CORE-SW(config-if)#desc LINK_TO_CWS-ACCESS-F1
CWS-CORE-SW(config-if)#switchport mode trunk

CWS-CORE-SW(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan31, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan32, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan40, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan50, changed state to up

CWS-CORE-SW(config-if)#
CWS-CORE-SW(config-if)#switchport trunk allowed vlan 10,20,31,40,50
CWS-CORE-SW(config-if)#ip dhcp snooping trust
CWS-CORE-SW(config-if)#no shut
CWS-CORE-SW(config-if)#int g1/0/3
CWS-CORE-SW(config-if)#desc LINK_TO_CWS-ACCESS-F2
CWS-CORE-SW(config-if)#switchport mode trunk

CWS-CORE-SW(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/3, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/3, changed state to up

CWS-CORE-SW(config-if)#switchport trunk allowed vlan 10,20,32,40,50
CWS-CORE-SW(config-if)#ip dhcp snooping trust
CWS-CORE-SW(config-if)#no shut
CWS-CORE-SW(config-if)#
```

WLC Trunk Port

```
CWS-CORE-SW(config-if)#int g1/0/10
CWS-CORE-SW(config-if)#desc LINK_TO_WLC_3504
CWS-CORE-SW(config-if)#switchport trunk encapsulation dot1q
^
% Invalid input detected at '^' marker.

CWS-CORE-SW(config-if)#switchport mode trunk

CWS-CORE-SW(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/10, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/10, changed state to up

CWS-CORE-SW(config-if)#switchport trunk native vlan 10
CWS-CORE-SW(config-if)#switchport trunk allowed vlan 10,20,31,32
CWS-CORE-SW(config-if)#spanning-tree portfast trunk
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION
CWS-CORE-SW(config-if)#ip dhcp snooping trust
CWS-CORE-SW(config-if)#no shut
CWS-CORE-SW(config-if)#
```

Access Ports for Centralized Devices

```
CWS-CORE-SW(config-if)#int g1/0/4
CWS-CORE-SW(config-if)#desc DHCP_SERVER_PT
CWS-CORE-SW(config-if)#switchport mode access
CWS-CORE-SW(config-if)#switchport access vlan 20
CWS-CORE-SW(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION
```

```
%Portfast has been configured on GigabitEthernet1/0/4 but will only
have effect when the interface is in a non-trunking mode.
CWS-CORE-SW(config-if)#spanning-tree bpduguard enable
CWS-CORE-SW(config-if)# ip dhcp snooping trust
CWS-CORE-SW(config-if)#no shut
CWS-CORE-SW(config-if)#int g1/0/5
CWS-CORE-SW(config-if)#desc CME_ROUTER_2811
CWS-CORE-SW(config-if)#switchport mode access
CWS-CORE-SW(config-if)#switchport access vlan 40
CWS-CORE-SW(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION
```

```
%Portfast has been configured on GigabitEthernet1/0/5 but will only
have effect when the interface is in a non-trunking mode.
CWS-CORE-SW(config-if)#spanning-tree bpduguard enable
CWS-CORE-SW(config-if)#ip dhcp snooping trust
CWS-CORE-SW(config-if)#no shut
CWS-CORE-SW(config-if)#int g1/0/6
CWS-CORE-SW(config-if)#desc NVR_SERVER
CWS-CORE-SW(config-if)#switchport mode access
CWS-CORE-SW(config-if)#switchport access vlan 50
CWS-CORE-SW(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION
```

```
%Portfast has been configured on GigabitEthernet1/0/6 but will only
have effect when the interface is in a non-trunking mode.
CWS-CORE-SW(config-if)#spanning-tree bpduguard enable
CWS-CORE-SW(config-if)#switchport port-security maximum 1
CWS-CORE-SW(config-if)#switchport port-security violation shutdown
CWS-CORE-SW(config-if)#switchport port-security
CWS-CORE-SW(config-if)#no shut
CWS-CORE-SW(config-if)#int g1/0/7
CWS-CORE-SW(config-if)#desc SERVER_ROOM_PC
CWS-CORE-SW(config-if)#switchport mode access
CWS-CORE-SW(config-if)#switchport access vlan 20
CWS-CORE-SW(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION
```

```
%Portfast has been configured on GigabitEthernet1/0/7 but will only
have effect when the interface is in a non-trunking mode.
CWS-CORE-SW(config-if)#spanning-tree bpduguard enable
CWS-CORE-SW(config-if)#switchport port-security maximum 1
CWS-CORE-SW(config-if)#switchport port-security violation shutdown
CWS-CORE-SW(config-if)#switchport port-security
CWS-CORE-SW(config-if)#no shut
CWS-CORE-SW(config-if)#
```

DHCP Snooping

```
CWS-CORE-SW(config)#ip dhcp snooping
CWS-CORE-SW(config)#ip dhcp snooping vlan 10,20,31,32,40,50
CWS-CORE-SW(config)#no ip dhcp snooping information option
CWS-CORE-SW(config)#end
CWS-CORE-SW#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
Compressed configuration from 7383 bytes to 3601 bytes[OK]
[OK]
```

Server-PT DHCP

DHCP

Physical
Config
Services
Desktop
Programming
Attributes

IP Configuration
X

IP Configuration

☐ DHCP
☒ Static

IPv4 Address
10.0.20.21

Subnet Mask
255.255.255.0

Default Gateway
10.0.20.1

DNS Server
8.8.8.8

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
IOT_CCTV_POOL	10.0.50.1	8.8.8.8	10.0.50.21	255.255.255.0	200	0.0.0.0	0.0.0.0
CWS_F2_POOL	10.0.32.1	8.8.8.8	10.0.32.11	255.255.255.0	200	0.0.0.0	0.0.0.0
CWS_F1_POOL	10.0.31.1	8.8.8.8	10.0.31.11	255.255.255.0	200	0.0.0.0	0.0.0.0
STAFF_POOL	10.0.20.1	8.8.8.8	10.0.20.31	255.255.255.0	200	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	10.0.20.0	255.255.255.0	512	0.0.0.0	0.0.0.0

Access Switch Ground Floor (Catalyst 2960)

Hardening + VTP + STP + Management IP

```
Switch>en
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
Switch(config)#hostname CWS-ACCESS-F1
CWS-ACCESS-F1(config)#no ip domain-lookup
CWS-ACCESS-F1(config)#ip domain-name cws.local
CWS-ACCESS-F1(config)#vtp mode client
Setting device to VTP CLIENT mode.
CWS-ACCESS-F1(config)#vtp domain CWS_NET
Domain name already set to CWS_NET.
CWS-ACCESS-F1(config)#vtp version 2
Cannot modify version in VTP client mode
CWS-ACCESS-F1(config)#vtp password cws_net123
Setting device VLAN database password to cws_net123
CWS-ACCESS-F1(config)#spanning-tree mode rapid-pvst
CWS-ACCESS-F1(config)#int vlan 10
CWS-ACCESS-F1(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up

CWS-ACCESS-F1(config-if)#ip addr 10.0.10.4 255.255.255.0
CWS-ACCESS-F1(config-if)#no shut
CWS-ACCESS-F1(config-if)#ip default-gateway 10.0.10.1
```

Uplink Trunking

```
CWS-ACCESS-F1(config)#int g0/1
CWS-ACCESS-F1(config-if)#desc UPLINK_TO_CWS-CORE-SW
CWS-ACCESS-F1(config-if)#switchport mode trunk
CWS-ACCESS-F1(config-if)#switchport trunk allowed vlan 10,20,31,40,50
CWS-ACCESS-F1(config-if)#spanning-tree guard loop
^
% Invalid input detected at '^' marker.

CWS-ACCESS-F1(config-if)#ip dhcp snooping trust
CWS-ACCESS-F1(config-if)#no shut
CWS-ACCESS-F1(config-if)#exit
```

LAP Ports — Fa0/1 to Fa0/4

```
CWS-ACCESS-F1(config)#int range fa0/1-4
CWS-ACCESS-F1(config-if-range)#switchport mode trunk
CWS-ACCESS-F1(config-if-range)#switchport trunk native vlan 10
CWS-ACCESS-F1(config-if-range)#switchport trunk allowed vlan 10,20,31
CWS-ACCESS-F1(config-if-range)#spanning-tree portfast trunk
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION
CWS-ACCESS-F1(config-if-range)#no shut
CWS-ACCESS-F1(config-if-range)#exit
CWS-ACCESS-F1(config)#int fa0/1
CWS-ACCESS-F1(config-if)#desc LAP-F1a
CWS-ACCESS-F1(config-if)#int fa0/2
CWS-ACCESS-F1(config-if)#desc LAP-F1b
CWS-ACCESS-F1(config-if)#int fa0/3
CWS-ACCESS-F1(config-if)#desc LAP-F1c
CWS-ACCESS-F1(config-if)#int fa0/4
CWS-ACCESS-F1(config-if)#desc LAP-F1d
```

CCTV Camera Ports — Fa0/5 to Fa0/12

```
CWS-ACCESS-F1(config)#int range fa0/5-12
CWS-ACCESS-F1(config-if-range)#switchport mode access
CWS-ACCESS-F1(config-if-range)#switchport access vlan 50
CWS-ACCESS-F1(config-if-range)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/5 but will only
have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/6 but will only
have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/7 but will only
have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/8 but will only
have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION
```

```

%Portfast has been configured on FastEthernet0/9 but will only
have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/10 but will only
have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/11 but will only
have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/12 but will only
have effect when the interface is in a non-trunking mode.
CWS-ACCESS-F1(config-if-range)#spanning-tree bpduguard enable
CWS-ACCESS-F1(config-if-range)#switchport port-security maximum 1
CWS-ACCESS-F1(config-if-range)#switchport port-security violation shutdown
CWS-ACCESS-F1(config-if-range)#switchport port-security
CWS-ACCESS-F1(config-if-range)#no shut

CWS-ACCESS-F1(config)#int fa0/5
CWS-ACCESS-F1(config-if)#desc CCTV_CAM_F1_01
CWS-ACCESS-F1(config-if)#int fa0/6
CWS-ACCESS-F1(config-if)#desc CCTV_CAM_F1_02
CWS-ACCESS-F1(config-if)#int fa0/7
CWS-ACCESS-F1(config-if)#desc CCTV_CAM_F1_03
CWS-ACCESS-F1(config-if)#int fa0/8
CWS-ACCESS-F1(config-if)#desc CCTV_CAM_F1_04
CWS-ACCESS-F1(config-if)#int fa0/9
CWS-ACCESS-F1(config-if)#desc CCTV_CAM_F1_05
CWS-ACCESS-F1(config-if)#int fa0/10
CWS-ACCESS-F1(config-if)#desc CCTV_CAM_F1_06
CWS-ACCESS-F1(config-if)#int fa0/11
CWS-ACCESS-F1(config-if)#desc CCTV_CAM_F1_07
CWS-ACCESS-F1(config-if)#int fa0/12
CWS-ACCESS-F1(config-if)#desc CCTV_CAM_F1_08

```

Front Desk — Fa0/13 (IP Phone + PC daisy-chain)

```

CWS-ACCESS-F1(config)#int fa0/13
CWS-ACCESS-F1(config-if)#desc FRONT_DESK_PHONE_PC
CWS-ACCESS-F1(config-if)#switchport mode access
CWS-ACCESS-F1(config-if)#switchport access vlan 20
CWS-ACCESS-F1(config-if)#switchport voice vlan 40
CWS-ACCESS-F1(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/13 but will only
have effect when the interface is in a non-trunking mode.
CWS-ACCESS-F1(config-if)#spanning-tree bpduguard enable
CWS-ACCESS-F1(config-if)#switchport port-security maximum 3
CWS-ACCESS-F1(config-if)#switchport port-security violation restrict
CWS-ACCESS-F1(config-if)#switchport port-security
CWS-ACCESS-F1(config-if)#no shut

```

Group Room IP Phones — Fa0/14 to Fa0/16 (Phone only)

```
CWS-ACCESS-F1(config)#int range fa0/14-16
CWS-ACCESS-F1(config-if-range)#switchport mode access
CWS-ACCESS-F1(config-if-range)#switchport access vlan 20
CWS-ACCESS-F1(config-if-range)#switchport voice vlan 40
CWS-ACCESS-F1(config-if-range)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/14 but will only
have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/15 but will only
have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/16 but will only
have effect when the interface is in a non-trunking mode.
CWS-ACCESS-F1(config-if-range)#spanning-tree bpduguard enable
CWS-ACCESS-F1(config-if-range)#switchport port-security maximum 2
CWS-ACCESS-F1(config-if-range)#switchport port-security violation shutdown
CWS-ACCESS-F1(config-if-range)#switchport port-security
CWS-ACCESS-F1(config-if-range)#no shut
CWS-ACCESS-F1(config-if-range)#exit
CWS-ACCESS-F1(config)#int fa0/14
CWS-ACCESS-F1(config-if)#desc PHONE_GROUP_ROOM_1
CWS-ACCESS-F1(config-if)#int fa0/15
CWS-ACCESS-F1(config-if)#desc PHONE_GROUP_ROOM_2
CWS-ACCESS-F1(config-if)#int fa0/16
CWS-ACCESS-F1(config-if)#desc PHONE_GROUP_ROOM_3
```

DHCP Snooping

```
CWS-ACCESS-F1(config)#ip dhcp snooping
CWS-ACCESS-F1(config)#ip dhcp snooping vlan 10,20,31,40,50
CWS-ACCESS-F1(config)#no ip dhcp snooping information option
CWS-ACCESS-F1(config)#end
CWS-ACCESS-F1#
%SYS-5-CONFIG_I: Configured from console by console

CWS-ACCESS-F1#wr
Building configuration...
[OK]
```

Access Switch Second Floor (Catalyst 2960)

Hardening + VTP + STP + Management IP

```
Switch>en
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname CWS-ACCESS-F2
CWS-ACCESS-F2(config)#no ip domain-lookup
CWS-ACCESS-F2(config)#ip domain-name cws.local
CWS-ACCESS-F2(config)#vtp mode client
Setting device to VTP CLIENT mode.
CWS-ACCESS-F2(config)#vtp domain CWS_NET
Domain name already set to CWS_NET.
CWS-ACCESS-F2(config)#vtp version 2
Cannot modify version in VTP client mode
CWS-ACCESS-F2(config)#vtp password cws_net123
Setting device VLAN database password to cws_net123
CWS-ACCESS-F2(config)#spanning-tree mode rapid-pvst
CWS-ACCESS-F2(config)#int vlan 10
CWS-ACCESS-F2(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up

CWS-ACCESS-F2(config-if)#
CWS-ACCESS-F2(config-if)#ip addr 10.0.10.5 255.255.255.0
CWS-ACCESS-F2(config-if)#no shut
CWS-ACCESS-F2(config-if)#ip default-gateway 10.0.10.1
```

Uplink Trunk Port

```
CWS-ACCESS-F2(config)#int g0/1
CWS-ACCESS-F2(config-if)#desc UPLINK_TO_CWS-CORE-SW
CWS-ACCESS-F2(config-if)#switchport mode trunk
CWS-ACCESS-F2(config-if)#switchport trunk allowed vlan 10,20,32,40,50
CWS-ACCESS-F2(config-if)#spanning-tree guard loop
^
% Invalid input detected at '^' marker.

CWS-ACCESS-F2(config-if)#ip dhcp snooping trust
CWS-ACCESS-F2(config-if)#no shut
```

LAP Ports — Fa0/1 to Fa0/4

```
CWS-ACCESS-F2(config)#int range fa0/1-4
CWS-ACCESS-F2(config-if-range)#switchport mode trunk
CWS-ACCESS-F2(config-if-range)#switchport trunk native vlan 10
CWS-ACCESS-F2(config-if-range)#switchport trunk allowed vlan 10,20,32
CWS-ACCESS-F2(config-if-range)#spanning-tree portfast trunk
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION
CWS-ACCESS-F2(config-if-range)#no shut
CWS-ACCESS-F2(config-if-range)#exit
CWS-ACCESS-F2(config)#int fa0/1
CWS-ACCESS-F2(config-if)#desc LAP-F2a
CWS-ACCESS-F2(config-if)#int fa0/2
CWS-ACCESS-F2(config-if)#desc LAP-F2b
CWS-ACCESS-F2(config-if)#int fa0/3
CWS-ACCESS-F2(config-if)#desc LAP-F2c
CWS-ACCESS-F2(config-if)#int fa0/4
CWS-ACCESS-F2(config-if)#desc LAP-F2d
```

CCTV Camera Ports — Fa0/5 to Fa0/12

```
CWS-ACCESS-F2(config)#int range fa0/5-12
CWS-ACCESS-F2(config-if-range)#switchport mode access
CWS-ACCESS-F2(config-if-range)#switchport access vlan 50
CWS-ACCESS-F2(config-if-range)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/5 but will only
have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/6 but will only
have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/7 but will only
have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/8 but will only
have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION
```

%Portfast has been configured on FastEthernet0/8 but will only have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single host. Connecting hubs, concentrators, switches, bridges, etc... to this interface when portfast is enabled, can cause temporary bridging loops. Use with CAUTION

%Portfast has been configured on FastEthernet0/9 but will only have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single host. Connecting hubs, concentrators, switches, bridges, etc... to this interface when portfast is enabled, can cause temporary bridging loops. Use with CAUTION

%Portfast has been configured on FastEthernet0/10 but will only have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single host. Connecting hubs, concentrators, switches, bridges, etc... to this interface when portfast is enabled, can cause temporary bridging loops. Use with CAUTION

%Portfast has been configured on FastEthernet0/11 but will only have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single host. Connecting hubs, concentrators, switches, bridges, etc... to this interface when portfast is enabled, can cause temporary bridging loops. Use with CAUTION

%Portfast has been configured on FastEthernet0/12 but will only have effect when the interface is in a non-trunking mode.
CWS-ACCESS-F2(config-if-range)#spanning-tree bpduguard enable
CWS-ACCESS-F2(config-if-range)#switchport port-security maximum 1
CWS-ACCESS-F2(config-if-range)#switchport port-security violation shutdown
CWS-ACCESS-F2(config-if-range)#switchport port-security
CWS-ACCESS-F2(config-if-range)#no shut
CWS-ACCESS-F2(config-if-range)#exit

```
CWS-ACCESS-F2(config)#int fa0/5
CWS-ACCESS-F2(config-if)#desc CCTV_CAM_F2_01
CWS-ACCESS-F2(config-if)#int fa0/6
CWS-ACCESS-F2(config-if)#desc CCTV_CAM_F2_02
CWS-ACCESS-F2(config-if)#int fa0/7
CWS-ACCESS-F2(config-if)#desc CCTV_CAM_F2_03
CWS-ACCESS-F2(config-if)#int fa0/8
CWS-ACCESS-F2(config-if)#desc CCTV_CAM_F2_04
CWS-ACCESS-F2(config-if)#int fa0/9
CWS-ACCESS-F2(config-if)#desc CCTV_CAM_F2_05
CWS-ACCESS-F2(config-if)#int fa0/10
CWS-ACCESS-F2(config-if)#desc CCTV_CAM_F2_06
CWS-ACCESS-F2(config-if)#int fa0/11
CWS-ACCESS-F2(config-if)#desc CCTV_CAM_F2_07
CWS-ACCESS-F2(config-if)#int fa0/12
CWS-ACCESS-F2(config-if)#desc CCTV_CAM_F2_08
```

Reserved CCTV Slots — Fa0/13 to Fa0/14

```
CWS-ACCESS-F2(config)#int range fa0/13-14
CWS-ACCESS-F2(config-if-range)#switchport mode access
CWS-ACCESS-F2(config-if-range)#switchport access vlan 50
CWS-ACCESS-F2(config-if-range)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/13 but will only
have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/14 but will only
have effect when the interface is in a non-trunking mode.
CWS-ACCESS-F2(config-if-range)#spanning-tree bpduguard enable
CWS-ACCESS-F2(config-if-range)#switchport port-security maximum 1
CWS-ACCESS-F2(config-if-range)#switchport port-security violation shutdown
CWS-ACCESS-F2(config-if-range)# switchport port-security
CWS-ACCESS-F2(config-if-range)# shutdown

%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively
down

%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively
down
CWS-ACCESS-F2(config-if-range)#!
CWS-ACCESS-F2(config-if-range)#int range fa0/13-14
CWS-ACCESS-F2(config-if-range)#desc RESERVED_SLOTS
```

Conference and Staff Room IP Phones — Fa0/15 to Fa0/18

```
CWS-ACCESS-F2(config)#int range fa0/15-18
CWS-ACCESS-F2(config-if-range)#switchport mode access
CWS-ACCESS-F2(config-if-range)#switchport access vlan 20
CWS-ACCESS-F2(config-if-range)#switchport voice vlan 40
CWS-ACCESS-F2(config-if-range)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/15 but will only
have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/16 but will only
have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/17 but will only
have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/18 but will only
have effect when the interface is in a non-trunking mode.
CWS-ACCESS-F2(config-if-range)#spanning-tree bpduguard enable
CWS-ACCESS-F2(config-if-range)#switchport port-security maximum 2
CWS-ACCESS-F2(config-if-range)#switchport port-security violation shutdown
CWS-ACCESS-F2(config-if-range)#switchport port-security
CWS-ACCESS-F2(config-if-range)#no shut
CWS-ACCESS-F2(config-if-range)#exit
```

DHCP Snooping

```
CWS-ACCESS-F2(config)#int fa0/15
CWS-ACCESS-F2(config-if)#desc PHONE_CONF_ROOM_1
CWS-ACCESS-F2(config-if)#int fa0/16
CWS-ACCESS-F2(config-if)#desc PHONE_CONF_ROOM_2
CWS-ACCESS-F2(config-if)#int fa0/17
CWS-ACCESS-F2(config-if)#desc PHONE_CONF_ROOM_3
CWS-ACCESS-F2(config-if)#int fa0/18
CWS-ACCESS-F2(config-if)#desc PHONE_STAFF_ROOM
CWS-ACCESS-F2(config-if)#exit
CWS-ACCESS-F2(config)#ip dhcp snooping
CWS-ACCESS-F2(config)#ip dhcp snooping vlan 10,20,32,40,50
CWS-ACCESS-F2(config)#no ip dhcp snooping information option
CWS-ACCESS-F2(config)#end
CWS-ACCESS-F2#
%SYS-5-CONFIG_I: Configured from console by console

CWS-ACCESS-F2#wr
Building configuration...
[OK]
```

Telephony Service

CME-R (2811)

Interface and Default Route

```
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname CME-2811
CME-2811(config)#no ip domain-lookup
CME-2811(config)#int fa0/0
CME-2811(config-if)#desc LINK_TO_CWS-CORE-SW
CME-2811(config-if)#ip addr 10.0.40.5 255.255.255.0
CME-2811(config-if)#no shut

CME-2811(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

CME-2811(config-if)#ip default-gateway 10.0.40.1
CME-2811(config)#ip route 0.0.0.0 0.0.0.0 10.0.40.1
```

VOICE DHCP Pool

```
CME-2811(config)#ip dhcp excluded-address 10.0.40.1 10.0.40.10
CME-2811(config)#ip dhcp pool VOICE_POOL
CME-2811(dhcp-config)#network 10.0.40.0 255.255.255.0
CME-2811(dhcp-config)#default-router 10.0.40.5
CME-2811(dhcp-config)#option 150 ip 10.0.40.5
CME-2811(dhcp-config)#dns-server 8.8.8.8
```

Telephony Service

```
CME-2811(config)#telephony-service
CME-2811(config-telephony)#max-ephones 10
CME-2811(config-telephony)#max-dn 10
CME-2811(config-telephony)#ip source-address 10.0.40.5 port 2000
CME-2811(config-telephony)#auto assign 1 to 10
```

Directory Numbers (ephone-dn)

```
CME-2811(config-telephony)#ephone-dn 1
CME-2811(config-ephone-dn)#%LINK-3-UPDOWN: Interface ephone_dsp DN 1.1, changed state to up

CME-2811(config-ephone-dn)#number 1001
CME-2811(config-ephone-dn)#ephone-dn 2
CME-2811(config-ephone-dn)#%LINK-3-UPDOWN: Interface ephone_dsp DN 2.1, changed state to up

CME-2811(config-ephone-dn)#number 1002
CME-2811(config-ephone-dn)#ephone-dn 3
CME-2811(config-ephone-dn)#%LINK-3-UPDOWN: Interface ephone_dsp DN 3.1, changed state to up

CME-2811(config-ephone-dn)#number 1003
CME-2811(config-ephone-dn)#ephone-dn 4
CME-2811(config-ephone-dn)#%LINK-3-UPDOWN: Interface ephone_dsp DN 4.1, changed state to up

CME-2811(config-ephone-dn)#number 1004
CME-2811(config-ephone-dn)#ephone-dn 5
CME-2811(config-ephone-dn)#%LINK-3-UPDOWN: Interface ephone_dsp DN 5.1, changed state to up

CME-2811(config-ephone-dn)#number 2001
CME-2811(config-ephone-dn)#ephone-dn 6
CME-2811(config-ephone-dn)#%LINK-3-UPDOWN: Interface ephone_dsp DN 6.1, changed state to up

CME-2811(config-ephone-dn)#number 2002
CME-2811(config-ephone-dn)#ephone-dn 7
CME-2811(config-ephone-dn)#%LINK-3-UPDOWN: Interface ephone_dsp DN 7.1, changed state to up

CME-2811(config-ephone-dn)#number 2003
CME-2811(config-ephone-dn)#ephone-dn 8
CME-2811(config-ephone-dn)#%LINK-3-UPDOWN: Interface ephone_dsp DN 8.1, changed state to up

CME-2811(config-ephone-dn)#number 2004
CME-2811(config-ephone-dn)#end
CME-2811#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
```

WLC-3504

General Dynamic interface Setup

[MONITOR](#) [WLANs](#) [CONTROLLER](#) [WIRELESS](#) [SECURITY](#) [MANAGEMENT](#) [COMMANDS](#) [HELP](#) [FEEDBACK](#)

Interfaces

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management	IPv6 Address
cws-f1-iface	31	10.0.31.2	Dynamic	Disabled	
cws-f2-iface	32	10.0.32.2	Dynamic	Disabled	
management	10	10.0.10.10	Static	Enabled	::/128
staf-iface	20	10.0.20.2	Dynamic	Disabled	
virtual	N/A	1.1.1.1	Static	Not Supported	

cws-f1-iface config

Physical Information

Port Number

Backup Port

Active Port

Enable Dynamic AP Management ☐

Interface Address

VLAN Identifier

IP Address

Netmask

Gateway

DHCP Information

Primary DHCP Server

Secondary DHCP Server

DHCP Proxy Mode ▼

Enable DHCP Option 82 ☐

cws-f2-iface config

Physical Information

Port Number	1
Backup Port	0
Active Port	1
Enable Dynamic AP Management	☐

Interface Address

VLAN Identifier	32
IP Address	10.0.32.2
Netmask	255.255.255.0
Gateway	10.0.32.1

DHCP Information

Primary DHCP Server	10.0.20.21
Secondary DHCP Server	
DHCP Proxy Mode	Global v
Enable DHCP Option 82	☐

management interface config

Physical Information

Port Number	1
Backup Port	0
Active Port	1
Enable Dynamic AP Management	☒

Interface Address

VLAN Identifier	10
IP Address	10.0.10.10
Netmask	255.255.255.0
Gateway	10.0.10.1

DHCP Information

Primary DHCP Server	10.0.10.1
Secondary DHCP Server	
DHCP Proxy Mode	Global v
Enable DHCP Option 82	☐

staff-iface config

Physical Information

Port Number

1

Backup Port

0

Active Port

1

Enable Dynamic AP Management

☐

Interface Address

VLAN Identifier

20

IP Address

10.0.20.2

Netmask

255.255.255.0

Gateway

10.0.20.1

DHCP Information

Primary DHCP Server

10.0.20.21

Secondary DHCP Server

DHCP Proxy Mode

Global

Enable DHCP Option 82

☐

WLAN SETUP

WLANs

Entries 1

Current Filter:

[\[Change Filter\]](#)[\[Clear Filter\]](#)

Create NewGo

☐	WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies	
☐	1	WLAN	STAFF_WIFI	STAFF_WIFI	Enabled	[WPA2][Auth(PSK)]	Remove
☐	2	WLAN	Ground Floor Customer Wifi	CWS_WIFI_GroundFloor	Enabled	[WPA2][Auth(PSK)]	Remove
☐	3	WLAN	2nd Floor Customer Wifi	CWS_WIFI_2ndFloor	Enabled	[WPA2][Auth(PSK)]	Remove

STAFF_WIFI WLAN

GeneralSecurityQoSPolicy-MappingAdvanced

Profile Name

STAFF_WIFI

Type

WLAN

SSID

STAFF_WIFI

Status

☒ Enabled

Security Policies

[WPA2][Auth(PSK)]

(Modifications done under security tab will appear after applying the changes.)

Radio Policy

All

Interface/Interface Group(G)

staf-iface

Multicast Vlan Feature

☐ Enabled

Broadcast SSID

☒ Enabled

NAS-ID

WLANs > Edit 'STAFF_WIFI'

General **Security** **QoS** **Policy-Mapping** **Advanced**

Layer 2 **Layer 3** **AAA Servers**

Fast Transition
Fast Transition ☐

Protected Management Frame
PMF Disabled ▾

WPA+WPA2 Parameters
WPA Policy ☐
WPA2 Policy ☒
WPA2 Encryption ☒ AES ☐ TKIP

Authentication Key Management
802.1X ☐ Enable
CKM ☐ Enable
PSK ☒ Enable
FT 802.1X ☐ Enable
FT PSK ☐ Enable
PSK Format ASCII ▾
••••••••

WLANs > Edit 'STAFF_WIFI'

General **Security** **QoS** **Policy-Mapping** **Advanced**

Scan Defer Time(msecs) 100

FlexConnect
FlexConnect Local Switching ☒ Enabled
FlexConnect Local Auth ☒ Enabled
Learn Client IP Address ☒ Enabled

CWS_WIFI_GroundFloor WLAN

Profile Name Ground Floor Customer Wifi

Type WLAN

SSID CWS_WIFI_GroundFloor

Status ☒ Enabled

Security Policies [WPA2][Auth(PSK)]
(Modifications done under security tab will appear after applying the changes.)

Radio Policy All ▾

Interface/Interface Group(G) cws-f1-iface ▾

Multicast Vlan Feature ☐ Enabled

Broadcast SSID ☒ Enabled

NAS-ID

WLANs > Edit 'Ground Floor Customer Wifi'

GeneralSecurityQoSPolicy-MappingAdvanced

Layer 2Layer 3AAA Servers

Protected Management Frame

PMFDisabled

WPA+WPA2 Parameters

WPA Policy

WPA2 Policy

WPA2 Encryption

WPA2 Encryption

Authentication Key Management

802.1X

CCKM

PSK

FT 802.1X

FT PSK

PSK Format

WPA gtk-randomize State

WLANs > Edit 'Ground Floor Customer Wifi'

GeneralSecurityQoSPolicy-MappingAdvanced

Scan Defer Priority

Scan Defer Time(msecs)

FlexConnect

FlexConnect Local Switching

FlexConnect Local Auth

Learn Client IP Address

Vlan based Central Switching

Central DHCP Processing

CWS_WIFI_2ndFloor WLAN

Profile Name	2nd Floor Customer Wifi
Type	WLAN
SSID	CWS_WIFI_2ndFloor
Status	☒ Enabled
Security Policies	[WPA2][Auth(PSK)] (Modifications done under security tab will appear after applying the changes.)
Radio Policy	All
Interface/Interface Group(G)	cws-f2-lface
Multicast Vlan Feature	☐ Enabled
Broadcast SSID	☒ Enabled
NAS-ID	

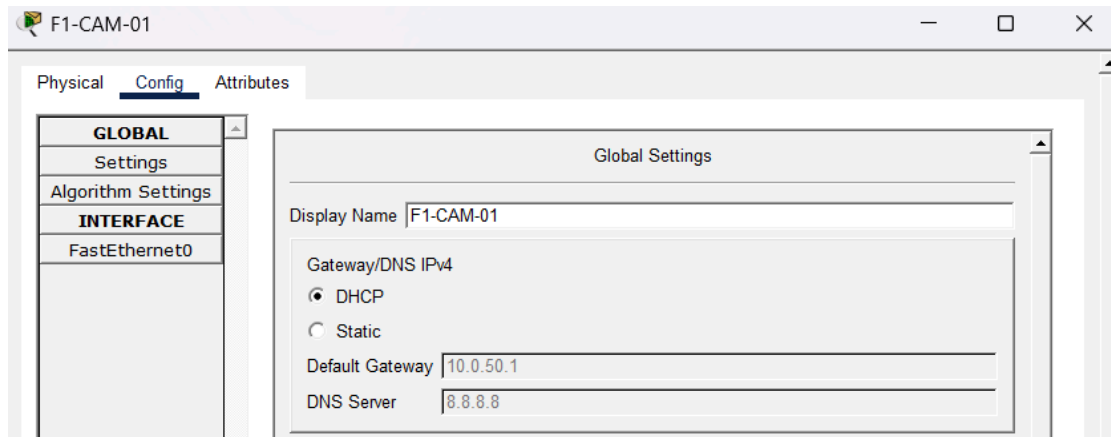
WLANs > Edit '2nd Floor Customer Wifi'

General	Security	QoS	Policy-Mapping	Advanced
Layer 2 Layer 3 AAA Servers				
Protected Management Frame				
PMF		Disabled		
WPA+WPA2 Parameters				
WPA Policy		☐		
WPA2 Policy		☒		
WPA2 Encryption		☒ AES ☐ TKIP		
Authentication Key Management				
802.1X		☐ Enable		
CKKM		☐ Enable		
PSK		☒ Enable		
FT 802.1X		☐ Enable		
FT PSK		☐ Enable		
PSK Format		ASCII		
				
WPA gtk-randomize State 14		Disable		

Scan Defer Time(msecs)	100
FlexConnect	
FlexConnect Local Switching 2	☒ Enabled
FlexConnect Local Auth 12	☒ Enabled
Learn Client IP Address 5	☒ Enabled

CCTV Setups (DHCP Config)

1st Floor



The screenshot shows the configuration window for F1-CAM-01. The window has a title bar with the name 'F1-CAM-01' and standard minimize, maximize, and close buttons. Below the title bar are three tabs: 'Physical', 'Config' (which is selected), and 'Attributes'. On the left side of the 'Config' tab, there is a tree view with the following items: 'GLOBAL' (expanded), 'Settings', 'Algorithm Settings', 'INTERFACE', and 'FastEthernet0'. The main area of the window is titled 'Global Settings' and contains the following fields: 'Display Name' with the value 'F1-CAM-01', 'Gateway/DNS IPv4' section with 'DHCP' selected (indicated by a filled radio button) and 'Static' unselected (indicated by an empty radio button), 'Default Gateway' with the value '10.0.50.1', and 'DNS Server' with the value '8.8.8.8'.

GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0

Global Settings

Display Name: F1-CAM-01

Gateway/DNS IPv4

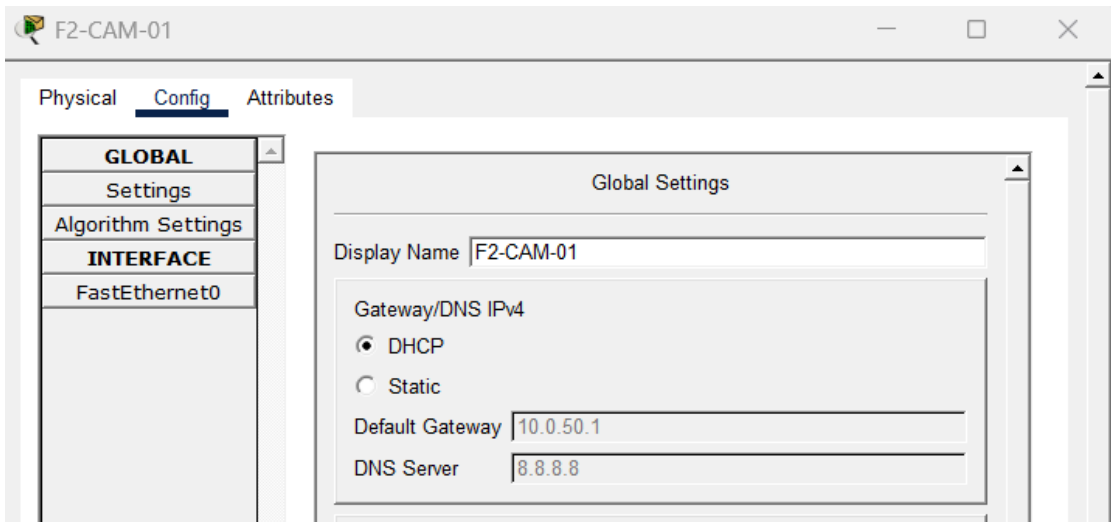
☒ DHCP

☐ Static

Default Gateway: 10.0.50.1

DNS Server: 8.8.8.8

2nd Floor



The screenshot shows the configuration window for F2-CAM-01. The window has a title bar with the name 'F2-CAM-01' and standard minimize, maximize, and close buttons. Below the title bar are three tabs: 'Physical', 'Config' (which is selected), and 'Attributes'. On the left side of the 'Config' tab, there is a tree view with the following items: 'GLOBAL' (expanded), 'Settings', 'Algorithm Settings', 'INTERFACE', and 'FastEthernet0'. The main area of the window is titled 'Global Settings' and contains the following fields: 'Display Name' with the value 'F2-CAM-01', 'Gateway/DNS IPv4' section with 'DHCP' selected (indicated by a filled radio button) and 'Static' unselected (indicated by an empty radio button), 'Default Gateway' with the value '10.0.50.1', and 'DNS Server' with the value '8.8.8.8'.

GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0

Global Settings

Display Name: F2-CAM-01

Gateway/DNS IPv4

☒ DHCP

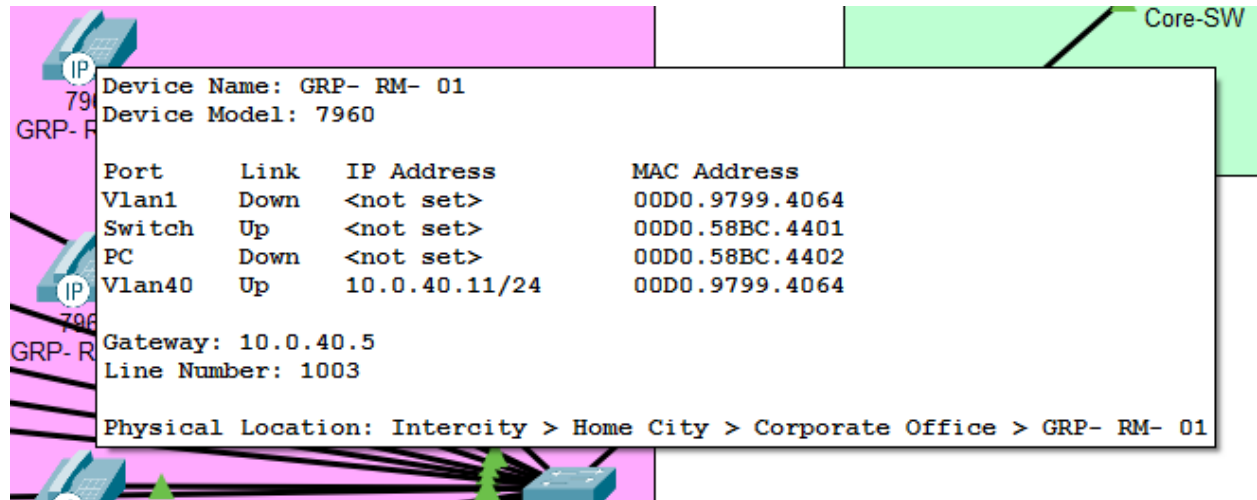
☐ Static

Default Gateway: 10.0.50.1

DNS Server: 8.8.8.8

IP Phone DHCP Config

1st Floor



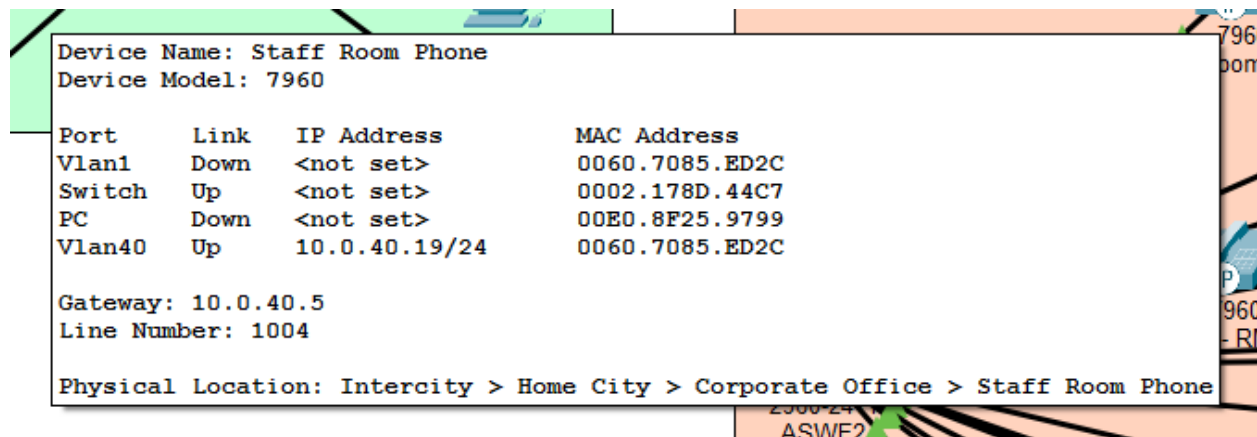
Device Name: GRP- RM- 01
Device Model: 7960

Port	Link	IP Address	MAC Address
Vlan1	Down	<not set>	00D0.9799.4064
Switch	Up	<not set>	00D0.58BC.4401
PC	Down	<not set>	00D0.58BC.4402
Vlan40	Up	10.0.40.11/24	00D0.9799.4064

Gateway: 10.0.40.5
Line Number: 1003

Physical Location: Intercity > Home City > Corporate Office > GRP- RM- 01

2nd Floor



Device Name: Staff Room Phone
Device Model: 7960

Port	Link	IP Address	MAC Address
Vlan1	Down	<not set>	0060.7085.ED2C
Switch	Up	<not set>	0002.178D.44C7
PC	Down	<not set>	00E0.8F25.9799
Vlan40	Up	10.0.40.19/24	0060.7085.ED2C

Gateway: 10.0.40.5
Line Number: 1004

Physical Location: Intercity > Home City > Corporate Office > Staff Room Phone

LAPs DHCP Config

1st Floor

LAP- F1a

Physical **Config** Attributes

GLOBAL
Settings
WLC
INTERFACE
GigabitEthernet0
Dot11Radio0

GigabitEthernet0

Port Status ☒ On

Link Speed ☐ 1000 Mbps ☒ 100 Mbps ☐ 10 Mbps ☒ Auto

Duplex ☐ Half Duplex ☒ Full Duplex ☒ Auto

MAC Address 0060.2FE4.C701

IP Configuration

☒ DHCP

☐ Static

IPv4 Address 10.0.10.26

Subnet Mask 255.255.255.0

2nd Floor

LAP- F2a

Physical **Config** Attributes

GLOBAL
Settings
WLC
INTERFACE
GigabitEthernet0
Dot11Radio0

GigabitEthernet0

Port Status ☒ On

Link Speed ☐ 1000 Mbps ☒ 100 Mbps ☐ 10 Mbps ☒ Auto

Duplex ☐ Half Duplex ☒ Full Duplex ☒ Auto

MAC Address 0000.0C0B.5CC8

IP Configuration

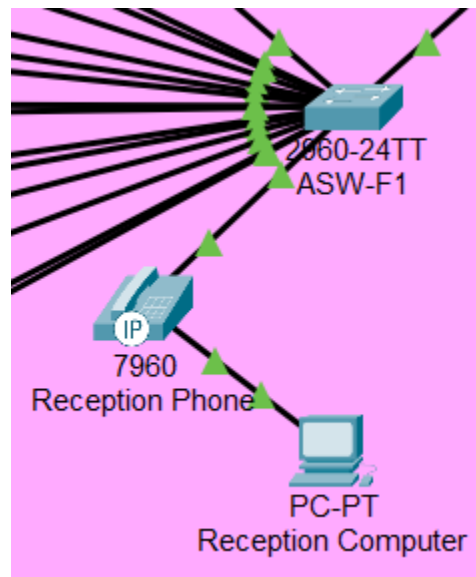
☒ DHCP

☐ Static

IPv4 Address 10.0.10.27

Subnet Mask 255.255.255.0

Reception Computer (Daisy-chained Connectivity)



7960 Reception

Device Name: Reception Phone
Device Model: 7960

Port	Link	IP Address	MAC Address
Vlan1	Down	<not set>	0060.5C62.E575
Switch	Up	<not set>	0060.3E19.A901
PC	Up	<not set>	0060.3E19.A902
Vlan40	Up	10.0.40.18/24	0060.5C62.E575

PC Reception

Gateway: 10.0.40.5
Line Number: 2001

Physical Location: Intercity > Home City > Corporate Office > Reception Phone

Reception Computer

Physical Config **Desktop** Programming Attributes

IP Configuration

☒ DHCP ☐ Static

IPv4 Address: 10.0.20.2

Subnet Mask: 255.255.255.0

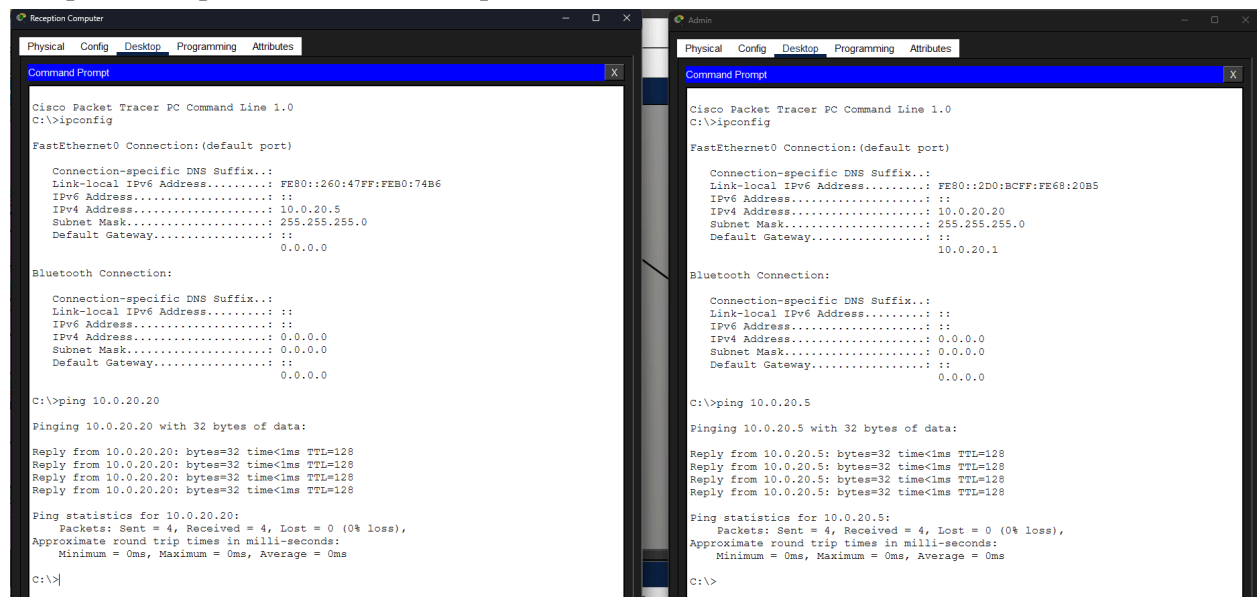
Default Gateway: 0.0.0.0

DNS Server: 8.8.8.8

TEST DOCUMENTATION

Ping Test

Reception Computer and Server Computer



Access Switches to Core Switch

```
CWS-ACCESS-F1#ping 10.0.10.1
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 10.0.10.1, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

```
CWS-ACCESS-F1#
```

```
CWS-ACCESS-F2#ping 10.0.10.1
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 10.0.10.1, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

```
CWS-ACCESS-F2#
```

```
CWS-CORE-SW#ping 10.0.10.4
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 10.0.10.4, timeout is 2 seconds:
```

```
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

```
CWS-CORE-SW#ping 10.0.10.5
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 10.0.10.5, timeout is 2 seconds:
```

```
!!!!!
```

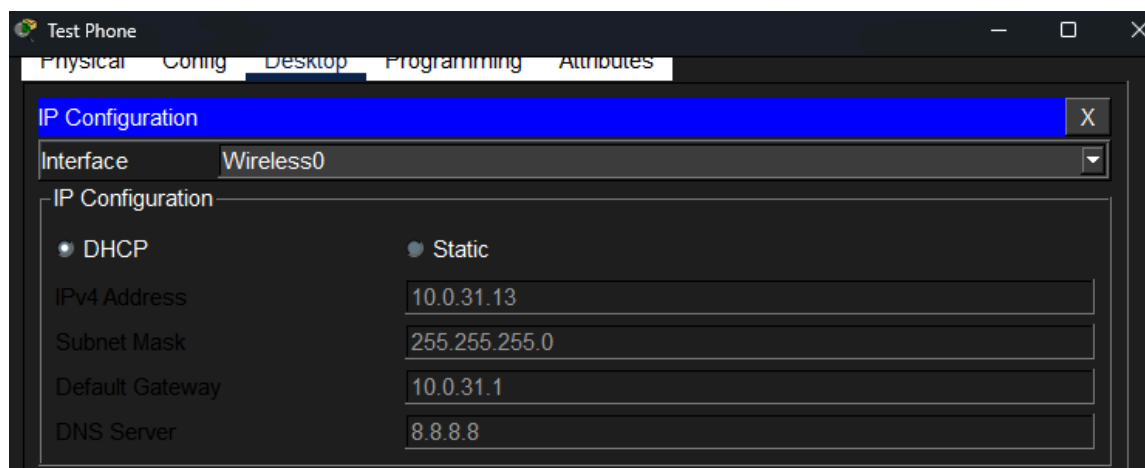
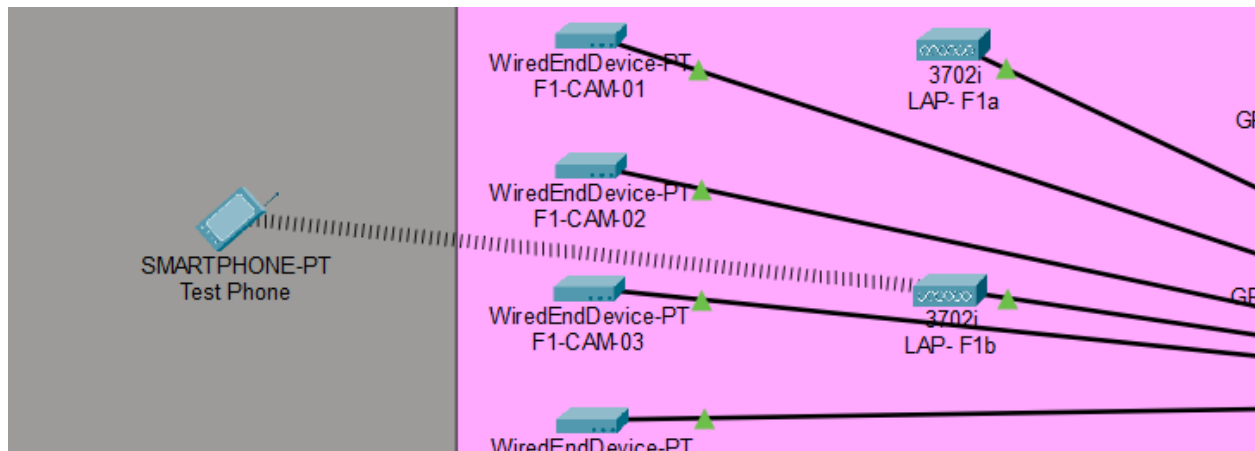
```
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

```
CWS-CORE-SW#
```

IP Phone Calling Test



Wireless Devices Connecting Test



VLAN Config Screenshots

```
CWS-CORE-SW#sh int trunk
Port      Mode      Encapsulation  Status      Native vlan
Gig1/0/2  on        802.1q         trunking    1
Gig1/0/3  on        802.1q         trunking    1
Gig1/0/10 on        802.1q         trunking    10

Port      Vlans allowed on trunk
Gig1/0/2  10,20,31-32,40,50
Gig1/0/3  10,20,31-32,40,50
Gig1/0/10 10,20,31-32

Port      Vlans allowed and active in management domain
Gig1/0/2  10,20,31,32,40,50
Gig1/0/3  10,20,31,32,40,50
Gig1/0/10 10,20,31,32

Port      Vlans in spanning tree forwarding state and not pruned
Gig1/0/2  10,20,31,32,40,50
Gig1/0/3  10,20,31,32,40,50
Gig1/0/10 10,20,31,32
```

```
interface Vlan10
  description MGMT_SVI
  mac-address 00d0.d333.dc01
  ip address 10.0.10.1 255.255.255.0
!
interface Vlan20
  description STAFF_SVI
  mac-address 00d0.d333.dc02
  ip address 10.0.20.1 255.255.255.0
  ip helper-address 10.0.20.21
!
interface Vlan31
  description CWS_F1_SVI
  mac-address 00d0.d333.dc03
  ip address 10.0.31.1 255.255.255.0
  ip helper-address 10.0.20.21
!
interface Vlan32
  description CWS_F2_SVI
  mac-address 00d0.d333.dc04
  ip address 10.0.32.1 255.255.255.0
  ip helper-address 10.0.20.21
!
interface Vlan40
  description VOICE_SVI
  mac-address 00d0.d333.dc05
  ip address 10.0.40.1 255.255.255.0
  ip helper-address 10.0.40.5
!
interface Vlan50
  description IOT_CCTV_SVI
  mac-address 00d0.d333.dc06
  ip address 10.0.50.1 255.255.255.0
  ip helper-address 10.0.20.21
!
```

DHCP Config Screenshots

```

ip dhcp pool MGMT_POOL
 network 10.0.10.0 255.255.255.0
 default-router 10.0.10.1
 option 43 ip 10.0.10.10
 dns-server 8.8.8.8
!
!

ip dhcp pool VOICE_POOL
 network 10.0.40.0 255.255.255.0
 default-router 10.0.40.5
 option 150 ip 10.0.40.5
 dns-server 8.8.8.8
!

```

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User
IOT_CCTV_POOL	10.0.50.1	8.8.8.8	10.0.50.21	255.255.255.0	200
CWS_F2_POOL	10.0.32.1	8.8.8.8	10.0.32.11	255.255.255.0	200
CWS_F1_POOL	10.0.31.1	8.8.8.8	10.0.31.11	255.255.255.0	200
STAFF_POOL	10.0.20.1	8.8.8.8	10.0.20.31	255.255.255.0	200
serverPool	0.0.0.0	0.0.0.0	10.0.20.0	255.255.255.0	512

Spanning Tree Config Screenshots

STP Core Switch

```

CWS-CORE-SW#show span vlan 10
VLAN0010
  Spanning tree enabled protocol rstp
  Root ID    Priority    4106
             Address     00D0.D333.DC62
             This bridge is the root
             Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    4106 (priority 4096 sys-id-ext 10)
             Address     00D0.D333.DC62
             Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 20

Interface      Role Sts Cost      Prio.Nbr Type
-----
Gi1/0/3        Desg FWD 4         128.3    P2p
Gi1/0/2        Desg FWD 4         128.2    P2p
Gi1/0/10       Desg FWD 4         128.10   P2p

```

CWS-CORE-SW#show span vlan 20

VLAN0020

Spanning tree enabled protocol rstp

Root ID Priority 4116
 Address 00D0.D333.DC62
 This bridge is the root
 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 4116 (priority 4096 sys-id-ext 20)
 Address 00D0.D333.DC62
 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
 Aging Time 20

Interface	Role	Sts	Cost	Prio.Nbr	Type
Gi1/0/3	Desg	FWD	4	128.3	P2p
Gi1/0/4	Desg	FWD	19	128.4	P2p
Gi1/0/2	Desg	FWD	4	128.2	P2p
Gi1/0/7	Desg	FWD	19	128.7	P2p
Gi1/0/10	Desg	FWD	4	128.10	P2p

CWS-CORE-SW#show span vlan 31

VLAN0031

Spanning tree enabled protocol rstp

Root ID Priority 4127
 Address 00D0.D333.DC62
 This bridge is the root
 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 4127 (priority 4096 sys-id-ext 31)
 Address 00D0.D333.DC62
 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
 Aging Time 20

Interface	Role	Sts	Cost	Prio.Nbr	Type
Gi1/0/3	Desg	FWD	4	128.3	P2p
Gi1/0/2	Desg	FWD	4	128.2	P2p
Gi1/0/10	Desg	FWD	4	128.10	P2p

CWS-CORE-SW#show span vlan 32

VLAN0032

Spanning tree enabled protocol rstp

Root ID Priority 4128
 Address 00D0.D333.DC62
 This bridge is the root
 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 4128 (priority 4096 sys-id-ext 32)
 Address 00D0.D333.DC62
 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
 Aging Time 20

Interface	Role	Sts	Cost	Prio.Nbr	Type
-----	-----	-----	-----	-----	-----
Gi1/0/3	Desg	FWD	4	128.3	P2p
Gi1/0/2	Desg	FWD	4	128.2	P2p
Gi1/0/10	Desg	FWD	4	128.10	P2p

CWS-CORE-SW#show span vlan 40

VLAN0040

Spanning tree enabled protocol rstp

Root ID Priority 4136
 Address 00D0.D333.DC62
 This bridge is the root
 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 4136 (priority 4096 sys-id-ext 40)
 Address 00D0.D333.DC62
 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
 Aging Time 20

Interface	Role	Sts	Cost	Prio.Nbr	Type
-----	-----	-----	-----	-----	-----
Gi1/0/3	Desg	FWD	4	128.3	P2p
Gi1/0/5	Desg	FWD	19	128.5	P2p
Gi1/0/2	Desg	FWD	4	128.2	P2p

```

CWS-CORE-SW#show span vlan 50
VLAN0050
  Spanning tree enabled protocol rstp
  Root ID      Priority      4146
                Address      00D0.D333.DC62
                This bridge is the root
                Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

  Bridge ID    Priority      4146 (priority 4096 sys-id-ext 50)
                Address      00D0.D333.DC62
                Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
                Aging Time 20

Interface      Role Sts Cost      Prio.Nbr Type
-----
Gi1/0/3        Desg FWD 4        128.3    P2p
Gi1/0/2        Desg FWD 4        128.2    P2p
Gi1/0/6        Desg FWD 19      128.6    P2p

```

VLAN Trunking Protocol Config Screenshots

Core Switch (VTP Server)

```

CWS-CORE-SW#show vtp status
VTP Version capable      : 1 to 2
VTP version running      : 2
VTP Domain Name          : CWS_NET
VTP Pruning Mode         : Disabled
VTP Traps Generation     : Disabled
Device ID                : 00E0.8F0A.6000
Configuration last modified by 0.0.0.0 at 3-1-93 06:42:42
Local updater ID is 10.0.10.1 on interface Vl10 (lowest numbered VLAN interface found)

```

Feature VLAN :

```

-----
VTP Operating Mode       : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs : 11
Configuration Revision   : 123
MD5 digest               : 0xBA 0x62 0x1B 0xC5 0xE9 0x6B 0xC0 0xB9
                        : 0x11 0x37 0xED 0xD8 0x46 0x79 0xB1 0xF1

```

Access Switches (VTP Client)

```
CWS-ACCESS-F1#show vtp status
VTP Version capable      : 1 to 2
VTP version running      : 2
VTP Domain Name          : CWS_NET
VTP Pruning Mode         : Disabled
VTP Traps Generation     : Disabled
Device ID                : 0007.EC89.D000
Configuration last modified by 0.0.0.0 at 3-1-93 06:42:42

Feature VLAN :
-----
VTP Operating Mode       : Client
Maximum VLANs supported locally : 255
Number of existing VLANs : 11
Configuration Revision    : 123
MD5 digest               : 0xBA 0x62 0x1B 0xC5 0xE9 0x6B 0xC0 0xB9
                        : 0x11 0x37 0xED 0xD8 0x46 0x79 0xB1 0xF1

CWS-ACCESS-F2#show vtp status
VTP Version capable      : 1 to 2
VTP version running      : 2
VTP Domain Name          : CWS_NET
VTP Pruning Mode         : Disabled
VTP Traps Generation     : Disabled
Device ID                : 0060.2F7A.8700
Configuration last modified by 0.0.0.0 at 3-1-93 06:42:42

Feature VLAN :
-----
VTP Operating Mode       : Client
Maximum VLANs supported locally : 255
Number of existing VLANs : 11
Configuration Revision    : 123
MD5 digest               : 0xBA 0x62 0x1B 0xC5 0xE9 0x6B 0xC0 0xB9
                        : 0x11 0x37 0xED 0xD8 0x46 0x79 0xB1 0xF1
-----
```

Access Control List Screenshot

```
ip access-list extended ACL_CWS_CLIENTS
deny ip 10.0.31.0 0.0.0.255 10.0.0.0 0.255.255.255
deny ip 10.0.32.0 0.0.0.255 10.0.0.0 0.255.255.255
permit ip any any
ip access-list extended ACL_IOT_CCTV
permit ip 10.0.50.0 0.0.0.255 host 10.0.50.10
permit ip any any
permit ip host 10.0.50.10 any
deny ip 10.0.50.0 0.0.0.255 10.0.0.0 0.255.255.255
```

~ End of Network Plan ~