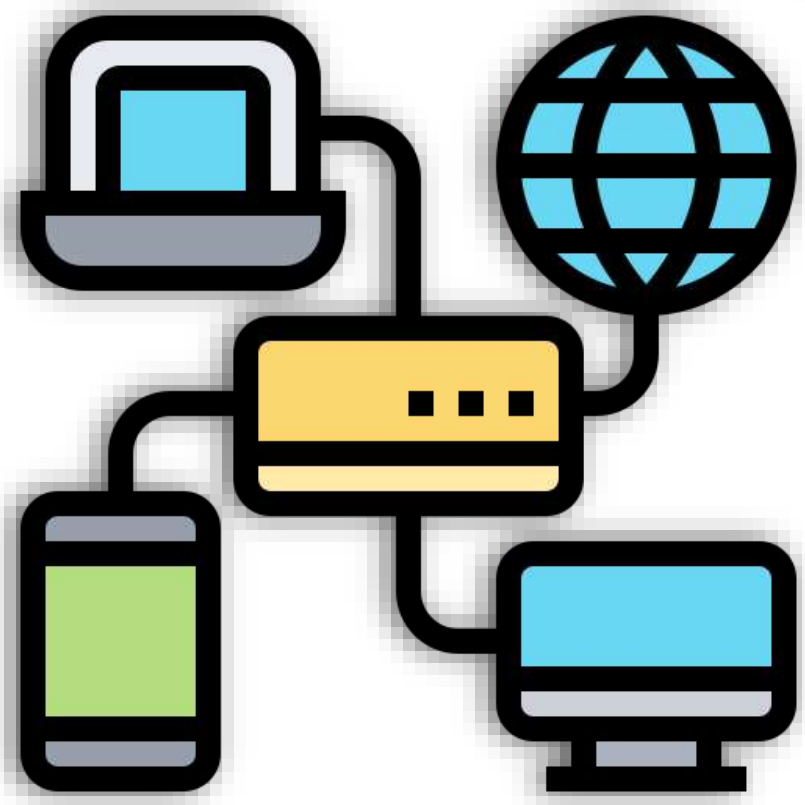


Ramses Recovery System

Teams' Names:

1-**Shehab Gamal Abdelmaksoud**
2-**Mahmoud Reda Mohamed**
3-**Mahmoud Usama Sayed**
4-**Amr Mohamed Abdelfattah**

Table of Contents:

1. Introduction :

In recent months, the unexpected service outage that occurred in **Ramses Central Office** highlighted the critical need for robust redundancy and fast recovery mechanisms within telecommunication infrastructures. The incident demonstrated how a single point of failure can affect large geographical areas and disrupt essential services for thousands of users.

This real-world failure inspired our team to develop a comprehensive Recovery and Backup System as the core idea for our graduation project. Rather than building the project on theoretical concepts alone, we decided to simulate an actual central office environment, complete with a primary site and a fully functional backup site that can take over during emergencies or system failures.

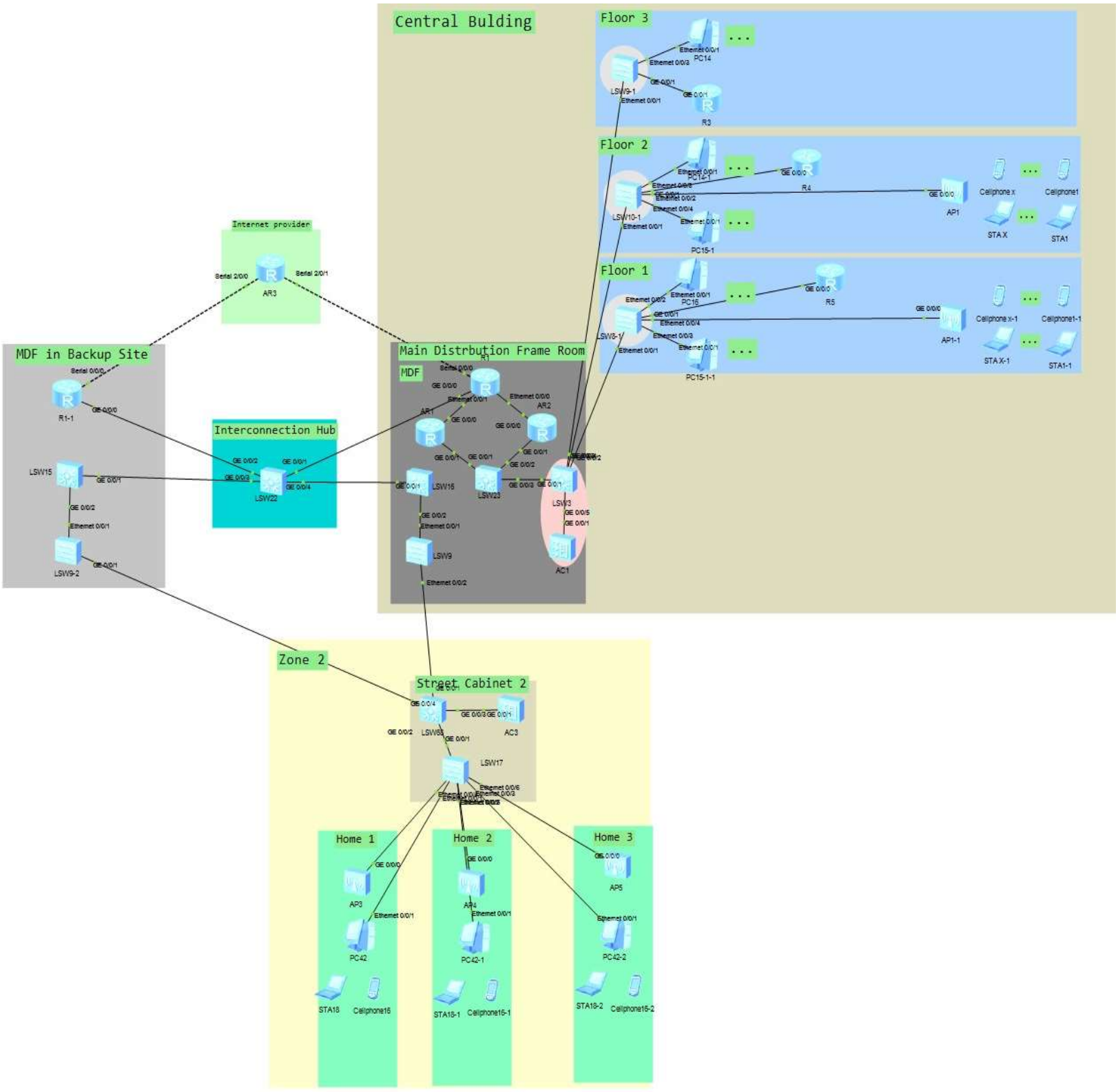
To make the simulation more realistic, we designed the network as if it were serving real residential areas. The network was divided into several Zones, each representing a separate distribution region similar to actual telecom street cabinets. Inside every zone, we created three independent home networks, allowing us to model real scenarios such as service distribution, fault isolation, **DHCP** allocation, routing convergence, **VRRP** failover, and more.

Throughout the project, we implemented all the technologies and skills we learned during the **HCIA** and **HCIP** training tracks. These included **VLAN** segmentation, **OSPF** routing, **VRRP** high availability, **DHCP** deployment, **NAT** configuration, wireless **AC/AP** management, and **RSTP**—ensuring that our simulated environment reflects professional telecom standards.

This documentation presents the complete design, implementation steps, configurations, and operational behavior of the system. It also includes the reasoning behind our architectural choices and highlights how our design achieves resilience, scalability, and reliability similar to a real-world central office deployment.

Our goal is to deliver a project that not only demonstrates academic knowledge but also provides a practical, industry-level model for central office recovery systems.

2.Topology :


Central Bulding
Floor 3
PC14
LSW9-1
R3
Floor 2
PC14-1
R4
LSW10-1
AP1
Cellphone x
Cellphone1
STA X
STA1
PC15-1
Floor 1
PC15
R5
LSW8-1
AP1-1
Cellphone x-1
Cellphone1-1
STA X-1
STA1-1
PC15-1-1
Internet provider
AR3
Serial 2/0/0
Serial 2/0/1
MDF in Backup Site
R1-1
LSW15
LSW9-2
Interconnection Hub
LSW22
Main Distrbution Frame Room
MDF
R1
AR1
AR2
LSW16
LSW23
LSW3
AC1
LSW9
Zone 2
Street Cabinet 2
LSW5
AC3
LSW17
Home 1
AP3
PC42
STA18
Cellphone16
Home 2
AP4
PC42-1
STA18-1
Cellphone16-1
Home 3
AP5
PC42-2
STA18-2
Cellphone16-2

3. Executive Summary:

This Document provides a complete, accurate, and overview of the final implemented network for **Ramses Central**, reflecting the configurations deployed across routers, switches, wireless controllers, and access points. The network delivers Internet distribution from the **central uplink** to:

- ✓ Three floors (Floor1–Floor3)
- ✓ Residential homes (Home1–Home3, Zone1–Zone3)

High-availability is achieved using **VRRP**, dynamic routing via **OSPF**, structured **VLAN** segmentation, and **DHCP-based IP addressing**. This document captures the final operational state after deployment.

---

4. Project Scope:

This document covers:

- ❖ Physical & logical topology
- ❖ VRRP
- ❖ VLAN and IP addressing scheme
- ❖ Routing protocols configuration (OSPF)
- ❖ Switching architecture (trunking, access, RSTP)
- ❖ Wireless architecture (AC + APs)
- ❖ DHCP design
- ❖ Telnet, AAA, and management
- ❖ NAT and internet access design
- ❖ Recommendations

---

5. Network Topology Overview :

The network consists of the following core components:

5.1 Physical Topology :

- **Internet Provider** (AR3) which is acting as the source of internet.
- **Main Distribution Frame (MDF)** hosts AR2 (primary building router), AC1 (wireless controller), and several distribution switches.
- **Building Floors** (1–3) are served via VLAN-based segmentation through LSW23, LSW3, LSW8-1, LSW10-1, and LSW9-1,
- **Central Uplink** connects to AR3 and R1-1 via Serial PPP links.
- **Backup Main Distribution Frame (BMDF)** R1-1 will automatically be the master, once the main router R1 failed,
  and **Wi-Fi APs** (area_1, area_2, AP1-1, AP1) are managed centrally by AC1.
- **Homes in (Zone1–Zone3)** are connected via LSW16, LSW15, and other access switches.

---

6. Device Inventory:

6.1 Routers (Huawei AR Series):

- **AR3** – Serial link, NAT, OSPF, PPP links
- **AR2** – Main building router (VLAN termination, VRRP, DHCP)
- **R1 (AR Router)** – Home network gateway (DHCP, VRRP)
- **R1-1** – VRRP backup for R1

6.2 Wireless Infrastructure :

Building floors:

- **AC1 (Huawei AC6005)** – Central WLAN controller
- **APs** – area_1, area_2, AP1, AP1-1.

Homes :

- **AC3** with (AP3, AP4, AP5).

6.3 Switching Infrastructure :

• LSW23 & LSW3 – Main Distribution Switches

These switches handle most of the VLAN trunking and inter-floor connectivity. They distribute VLANs 31–33 to the floor switches and ensure stable links between MDF devices.

• LSW8-1, LSW10-1, LSW9-1 – Floor Access Switches

Each switch serves one of the building floors:

- LSW8-1 → Floor 1 (VLAN 31)
- LSW10-1 → Floor 2 (VLAN 32)
- LSW9-1 → Floor 3 (VLAN 33)

They provide access ports for PCs and forward traffic to the distribution layer.

• LSW22, LSW16, LSW15, LSW9, LSW9-2 – Home Distribution (Zones 1–3)

These switches form the L2 distribution for the home networks.
They carry VLANs 21–23 for Home1, Home2, Home3 and connect to the different zones.
Some of these switches also participate in **RSTP root/backup roles.**

Roles:

- **LSW22** → Primary RSTP Root Bridge
- **LSW16** → Secondary Root
- The rest (LSW15, LSW9, LSW9-2) → Access/Distribution for home networks

• LSW68 – Zone 2 Aggregation Switch

This switch handles VLANs 21, 22, 23 .
It provides DHCP for Zone2 and acts as the main L2 aggregation point for residential connections.

• LSW17 – Access Switch for Zone 2

Provides the final access connections for homes inside Zone2.
It delivers VLANs 21, 22, and 23 to end devices and links back to LSW68.

7. VLAN & IP Addressing Scheme

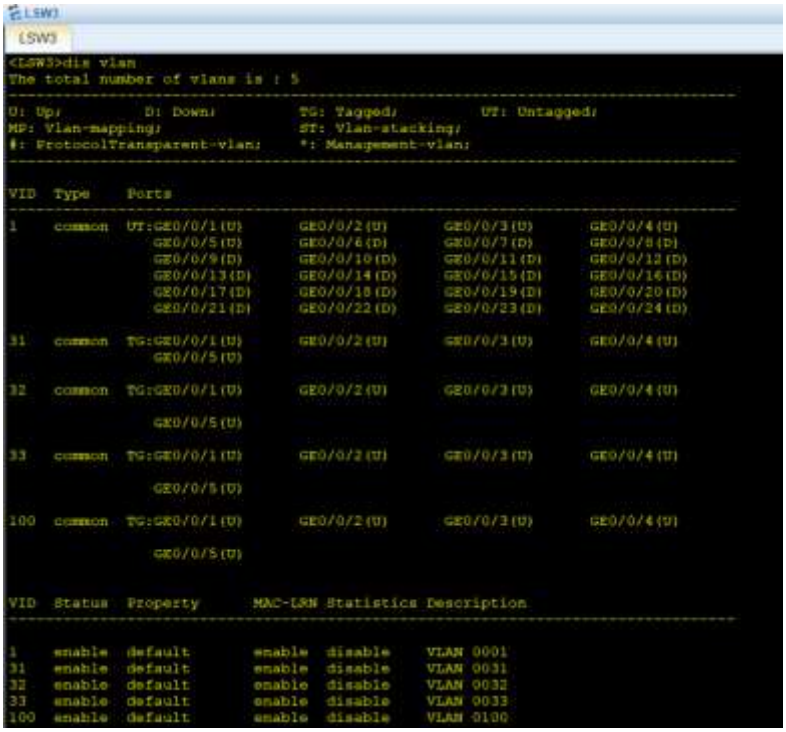
7.1 VLAN Allocation:

VLAN	Purpose	Description
31	Floor 1	PCs, wired devices
32	Floor 2	PCs, wired devices + WLAN SSID
33	Floor 3	PCs, wired devices
21, 22, 23	Home Distribution	Home1/Home2/Home3 segregation
100	Building WLAN Management	AC–AP CAPWAP management
150	Zone 2 WLAN Management	AC–AP CAPWAP management

1.This screenshot shows the VLAN setup on LSW3, which serves the building floors. The switch includes VLANs **31, 32, and 33**, dedicated to Floor1, Floor2, and Floor3. Additionally, VLAN **100** is configured as the WLAN management VLAN used for AC/AP communication.

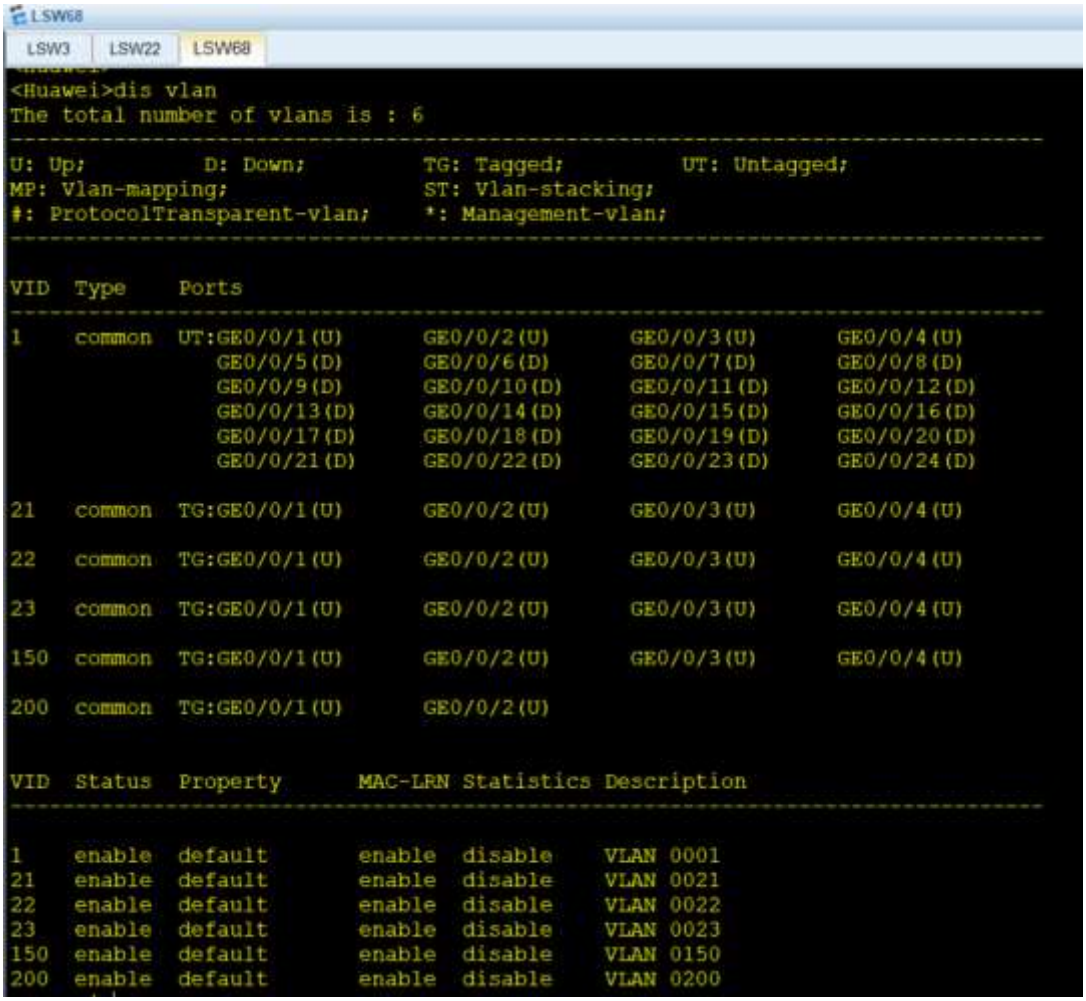
The uplink interfaces (GE0/0/1–GE0/0/4) are tagged for all floor VLANs, confirming proper trunking toward the MDF. Access ports for each floor are untagged in their respective VLANs, which ensures correct mapping of end-user devices to their floor networks.

This output confirms that the switch is correctly segmenting traffic per floor and supporting wireless management as designed.



2.This screenshot shows the VLAN configuration on switch LSW68, which is part of the Zone distribution layer.
Along with the standard VLANs **21, 22, and 23** (Home1–Home3) and VLAN **200** (Zone2 backhaul), the switch also includes **VLAN 150**, which is used as an auxiliary/service VLAN for AC/AP communication where required.

All VLANs appear in an *enabled* state, confirming that segmentation is fully active on the switch. The presence of tagged uplinks on GE0/0/1–GE0/0/4 indicates proper trunk configuration toward upper-layer switches, ensuring clean VLAN forwarding between the zone and the central MDF.
This verifies that VLAN provisioning on LSW68 is correct and aligned with the project's design.



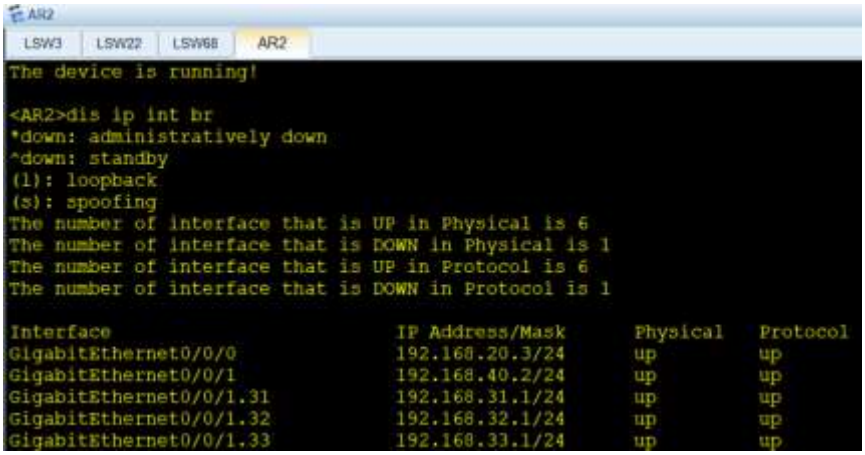
7.2 IP Subnetting:

Subnet	Usage	Gateway
192.168.10.0/24	Core uplink segment	192.168.10.254 (VRRP)
192.168.20.0/24	MDF internal	192.168.20.3
192.168.30.0/24	Distribution	192.168.30.1
192.168.40.0/24	Internal building backbone	192.168.40.254 (VRRP)
192.168.31.0/24	Floor 1	192.168.31.1
192.168.32.0/24	Floor 2	192.168.32.1
192.168.33.0/24	Floor 3	192.168.33.1
192.168.1.0/24	Home 1	192.168.1.1
192.168.2.0/24	Home 2	192.168.2.1
192.168.3.0/24	Home 3	192.168.3.1
192.168.100.0/24	Building WLAN Management	192.168.100.1
192.168.200.0/24	Zone2 subnet	192.168.200.1
192.168.150.0/24	Zone 2 WLAN Management	192.168.150.1

1. This screenshot shows the IP addressing configuration on AR2, the main building router.
AR2 interfaces are configured as follows:

- **192.168.20.3/24** – Internal MDF network
- **192.168.40.2/24** – Building backbone network (VRRP enabled)
- **192.168.31.1 / 32.1 / 33.1** – Floor 1, Floor 2, Floor 3 gateways

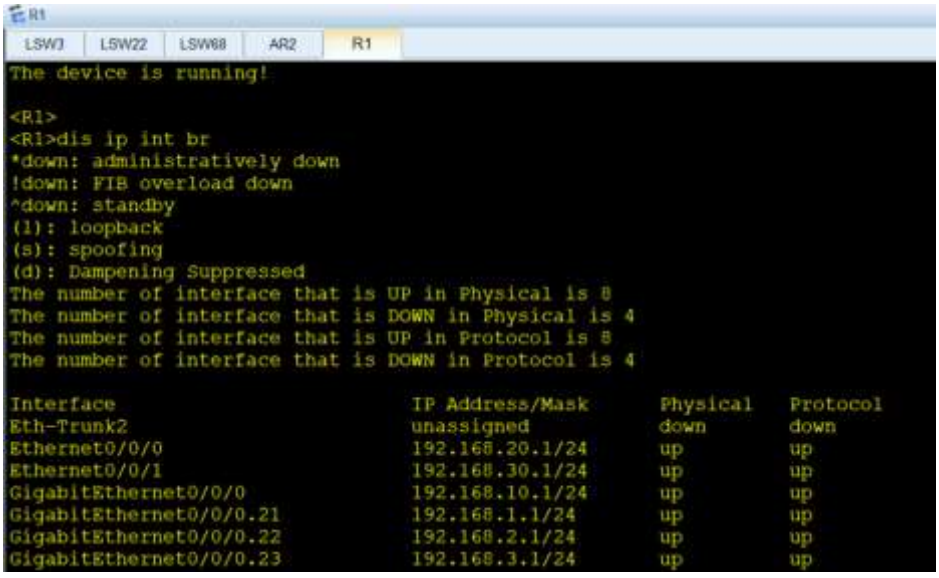
All floor subinterfaces (vlanif31, vlanif32, vlanif33) are UP, confirming that AR2 is providing both routing and DHCP services for all building floors.
The configuration ensures full inter-VLAN routing and stable OSPF participation.



2. This screenshot shows the IP addressing layout on R1, the primary Home Gateway router.
R1 handles multiple network segments:

- **192.168.20.1/24** – MDF internal communication
- **192.168.30.1/24** – distribution layer
- **192.168.10.1/24** – core link toward AR3
- **192.168.1.x / 2.x / 3.x** – Home1, Home2, Home3 subinterfaces for DHCP and routing

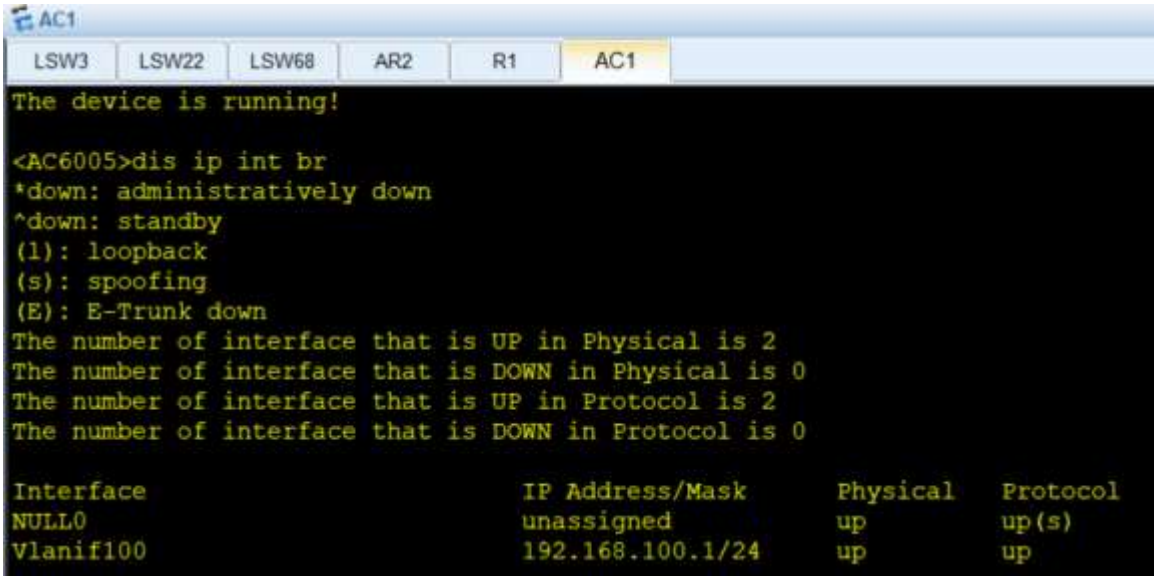
All subinterfaces (.21, .22, .23) are UP, confirming proper tagging for VLANs 21–23 and ensuring that R1 is correctly delivering gateway and DHCP services to the home networks.



3. This screenshot shows the IP addressing configuration on AC1.

The AC controller is assigned the management IP **192.168.100.1/24** on **vlanif100**, which is the dedicated WLAN management VLAN used for CAPWAP communication with all Access Points.

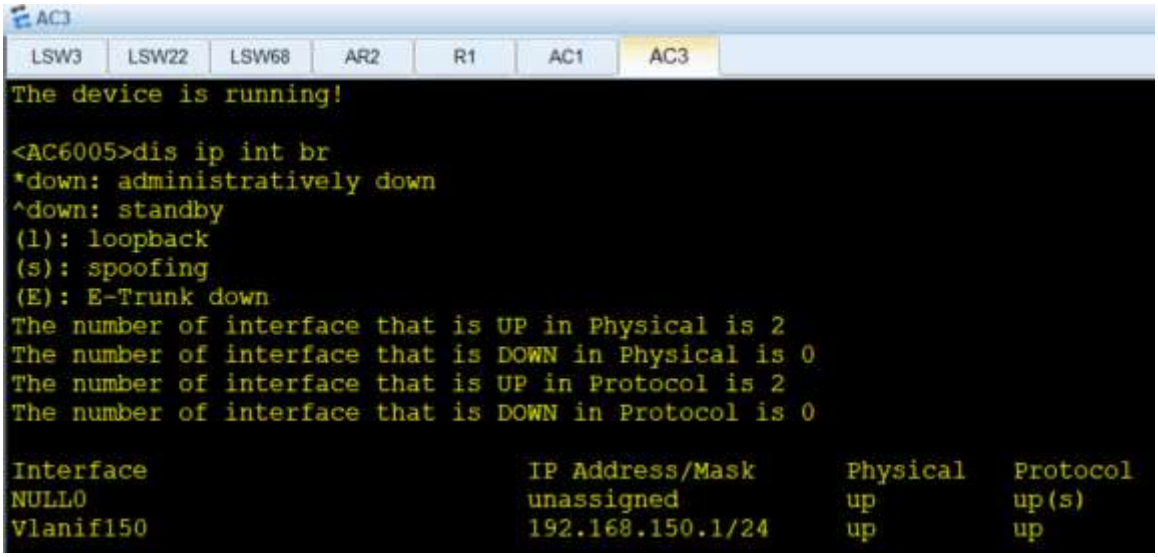
Both the physical and protocol states are UP, confirming that the controller is fully reachable through VLAN 100 and actively managing connected APs.



4. This screenshot displays the IP configuration on AC3, where vlanif150 (192.168.150.1/24) is active.

VLAN 150 serves as an additional service/management VLAN used for AP provisioning and control-plane communication.

The interface is shown as UP, indicating that AC3 is operational and participating in wireless infrastructure management over this VLAN.



8. Routing Architecture :

8.1 VRRP High Availability

Virtual Router Redundancy Protocol (**VRRP**) is implemented to ensure continuous gateway availability and seamless failover between primary and backup routers. This mechanism prevents service disruption during router or link failure.

VRRP Objectives

- Provide a redundant gateway for critical subnets.
- Enable automatic failover with minimal packet loss.
- Increase network stability across core and distribution layers.

VRRP Deployment Summary

VRRP	Subnet	Virtual IP	Master Device	Backup Device	Purpose
1	192.168.10.0/24	192.168.10.254	R1 (Priority 150)	R1-1 (Priority 90)	Core uplink redundancy
2	192.168.40.0/24	192.168.40.254	AR2 (Priority 150)	AR1 (Priority 90)	Building backbone redundancy

Failover Behavior

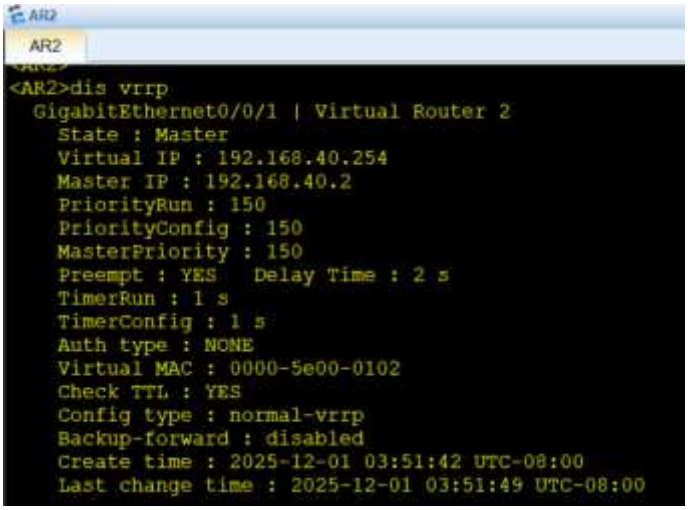
- VRRP Master advertises the virtual IP and MAC.
- Backup router listens for VRRP advertisements.
- Backup takes over as Master within seconds if advertisements stop.

Benefits

- Zero reconfiguration required for users.
- High reliability for floors, home networks, and wireless infrastructure.
- Supports scalable and resilient architecture.

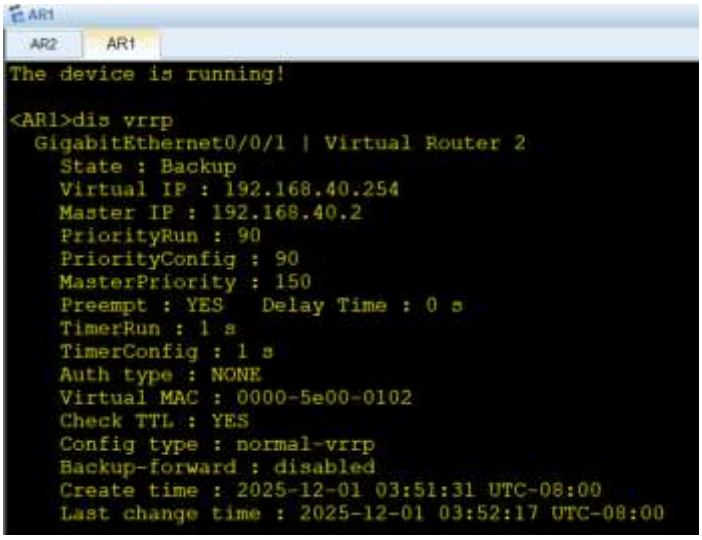
1. This screenshot shows the VRRP state on AR2, acting as the Master router for Virtual Router 2 on subnet 192.168.40.0/24.
AR2 holds the **highest priority value (150)**, which allows it to take the Master role.
The virtual IP **192.168.40.254** and virtual MAC **0000-5e00-0102** are correctly assigned.

With **preemption enabled**, AR2 automatically assumes Master role whenever it becomes available.
The interface and state information verify that AR2 is actively forwarding traffic as the primary gateway for the building backbone.



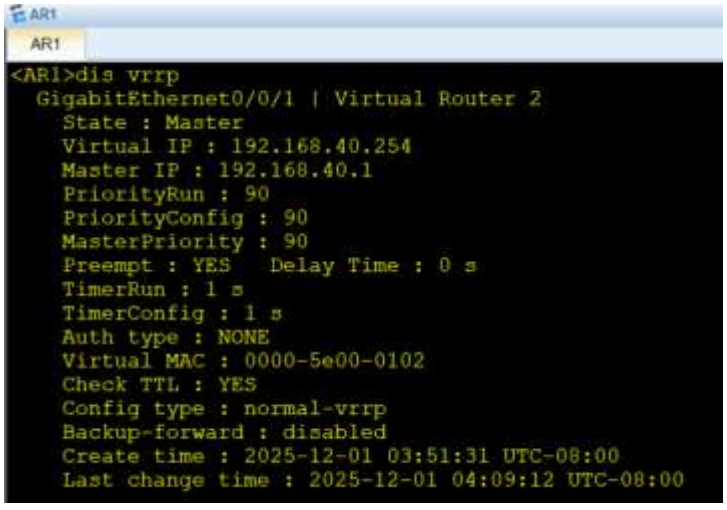
2. This screenshot displays the VRRP state on AR1 while AR2 is still active.
Here, AR1 correctly appears as **Backup**, with a lower priority value (**90**) than AR2's 150.
AR1 is monitoring AR2's advertisements and is ready to take over if the Master fails.

The virtual IP (**192.168.40.254**) is shared with AR2, ensuring seamless failover without requiring any change on the client side.
The configuration verifies that redundancy is functioning correctly, with AR1 on standby as a hot-backup router.



3.This screenshot shows AR1 taking over as the Master router after the failure or shutdown of AR2.
Once AR2 stopped sending VRRP hello messages, AR1 immediately transitioned from Backup to Master, using the same virtual IP (**192.168.40.254**) and virtual MAC.

This demonstrates VRRP's fast failover capability and confirms that redundancy works exactly as designed.
The consistent gateway IP ensures zero impact on user connectivity during router failure, highlighting the reliability of the implemented high-availability architecture



8.2 OSPF (Area 0)

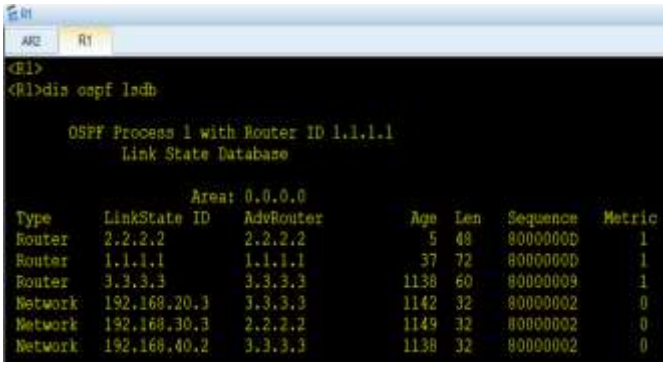
Routers AR2, R1, and AR3 participate in OSPF Process 1:

- AR3 advertises WAN/PPP subnets (10.0.12.0/30, 10.0.13.0/30)
- R1 and AR2 advertise building and home networks
- Default routes propagated via default-route-advertise

Router	Router-ID	OSPF Area	Advertised Networks	Role / Description
AR3	— (default)	**Area 0.0.0.1**	10.0.12.0/30 10.0.13.0/30	- WAN/PPP router - Injects default route into OSPF - Connects internal network to the upstream provider
R1	1.1.1.1	**Area 0.0.0.0**	192.168.10.0/24 192.168.20.0/24 192.168.30.0/24 192.168.40.0/24	- Main internal router - Advertises all building subnets - Primary VRRP gateway for 192.168.10.0/24
AR2	3.3.3.3	**Area 0.0.0.0**	192.168.10.0/24 192.168.20.0/24 192.168.30.0/24 192.168.40.0/24	- Building router - VLAN gateway for floors - VRRP master for 192.168.40.0/24 backbone
AR1	2.2.2.2	**Area 0.0.0.0**	192.168.10.0/24 192.168.20.0/24 192.168.30.0/24 192.168.40.0/24	- Backup router - VRRP backup for AR2 - Takes over routing if AR2 fails

1. This screenshot shows the OSPF Link-State Database on R1, which operates in Area 0 with Router ID 1.1.1.1.
The LSDB contains router LSAs for all participating routers:

- **1.1.1.1** (R1)
- **2.2.2.2** (AR1)
- **3.3.3.3** (AR2)

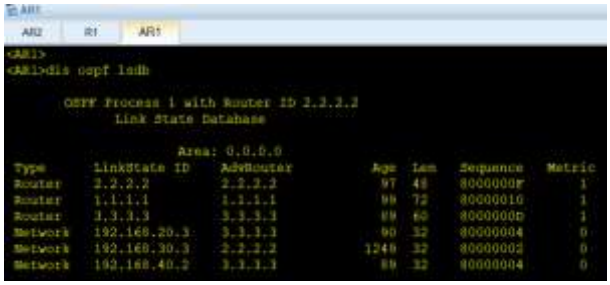


Additionally, R1 has learned network LSAs for the key subnets advertised inside Area 0, including:

- **192.168.20.3** — MDF internal network
- **192.168.30.3** — distribution network
- **192.168.40.2** — building backbone network

This confirms that R1 has full visibility of all routers and networks inside Area 0, proving that OSPF adjacency and LSA exchange are functioning correctly.

2. This screenshot displays the OSPF LSDB on AR1, identified by Router ID 2.2.2.2.
The router successfully learns all router LSAs (1.1.1.1, 2.2.2.2, 3.3.3.3), which proves stable OSPF neighbor relationships.

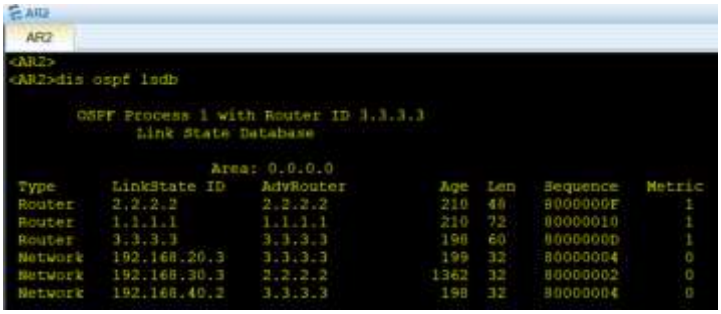


The network LSAs show the exact same subnets seen on R1:

- **192.168.20.3**
- **192.168.30.3**
- **192.168.40.2**

The matching LSDB contents confirm consistent link-state information across the entire OSPF domain and validate proper synchronization between AR1 and the rest of the routers.

3. This screenshot shows the OSPF LSDB for AR2, using Router ID 3.3.3.3.
AR2 has learned all router LSAs for the OSPF domain and is advertising its own information to the other routers.



AR2 also holds network LSAs for the primary building networks:

- **192.168.20.3** — MDF network via GE0/0/0
- **192.168.30.3** — distribution network
- **192.168.40.2** — VRRP backbone network

Since AR2 has identical LSDB entries to R1 and AR1, this demonstrates full OSPF convergence across the domain, ensuring consistent routing and stable inter-VLAN connectivity throughout the network

9. DHCP Architecture :

The DHCP architecture in this project is designed to automatically assign IP addresses across all service areas, including building floors, residential home networks, wireless infrastructure, and Zone 2. Each network segment receives a dedicated DHCP pool to ensure proper isolation, easy management, and accurate address distribution.

9.1 DHCP for Building Floors (AR2):

AR2 is responsible for supplying DHCP to the three building floors.
Each floor operates in its own VLAN and has a separate IP subnet:

Floor	VLAN	Subnet	Gateway
Floor 1	31	192.168.31.0/24	192.168.31.1
Floor 2	32	192.168.32.0/24	192.168.32.1
Floor 3	33	192.168.33.0/24	192.168.33.1

AR2 assigns IP addresses, DNS information, and default gateways to all devices connected to these floors.
This ensures structured network separation and stable communication between floors and the core.

9.2 DHCP for Home Networks (R1):

R1 provides DHCP services for Home1, Home2, and Home3 within the different Zones.
Each home is mapped to a unique VLAN and subnet:

Home	VLAN	Subnet	Gateway
Home 1	21	192.168.1.0/24	192.168.1.1
Home 2	22	192.168.2.0/24	192.168.2.1
Home 3	23	192.168.3.0/24	192.168.3.1

This design mirrors how telecom street cabinets distribute services to households, ensuring each home operates independently and securely.

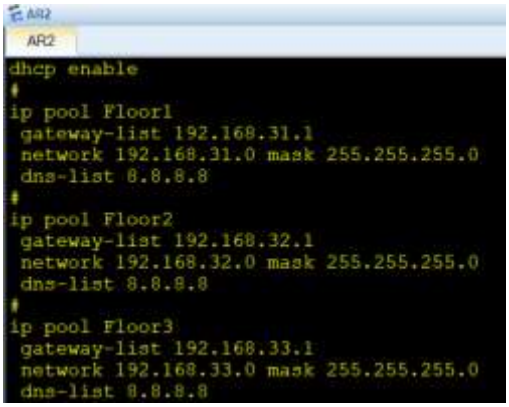
9.3 DHCP for WLAN Management (AC1):

The wireless controller AC1 manages DHCP for the Building WLAN Management VLAN (VLAN 100), and AC2 manages DHCP for the Homes WLAN Management (VLAN 150)
This pool assigns IPs to Access Points for CAPWAP communication with the controller, ensuring stable wireless provisioning and centralized control.

- All DHCP pools include gateway, DNS, and standard /24 addressing.

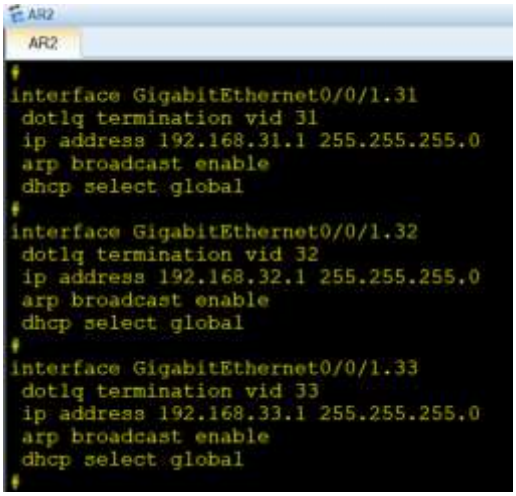
1. DHCP Pools for Floors

This screenshot shows the creation of the DHCP pools for the three building floors (Floor1, Floor2, Floor3). Each pool defines the gateway, network range, and DNS server to automatically assign IP addresses to devices in each floor.



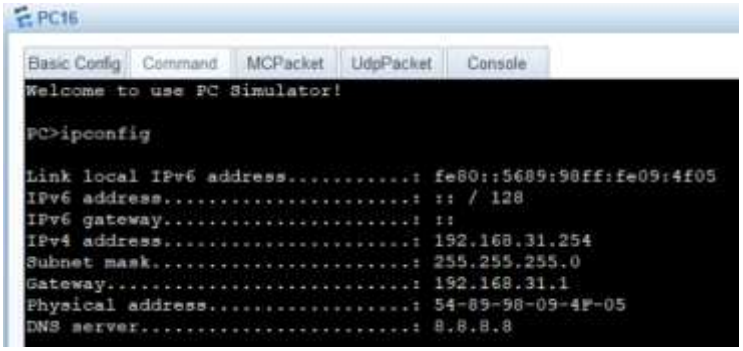
2.Sub-Interfaces for the Three Floors

Here we configured the sub-interfaces on AR2 for VLANs 31, 32, and 33. Each sub-interface corresponds to a specific floor and enables DHCP service delivery to devices within that VLAN.



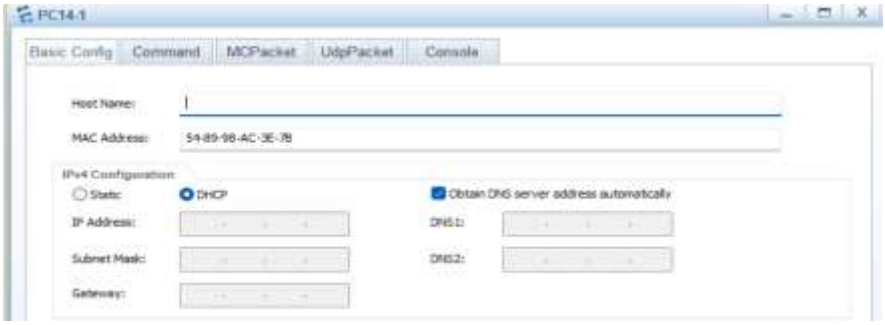
3.Device in Floor 1

This device on Floor 1 successfully received an IP address from the DHCP pool of VLAN 31, confirming that DHCP is functioning correctly for this floor.



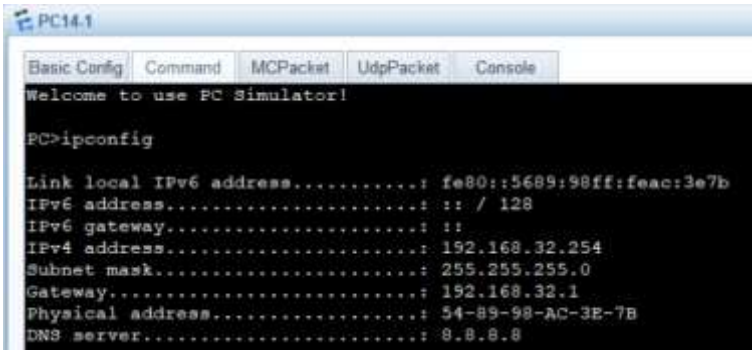
4.Selecting DHCP Mode on Devices

Before testing DHCP, the device must be set to obtain its IPv4 configuration dynamically (DHCP) instead of static, so it can request an IP address from the router automatically.



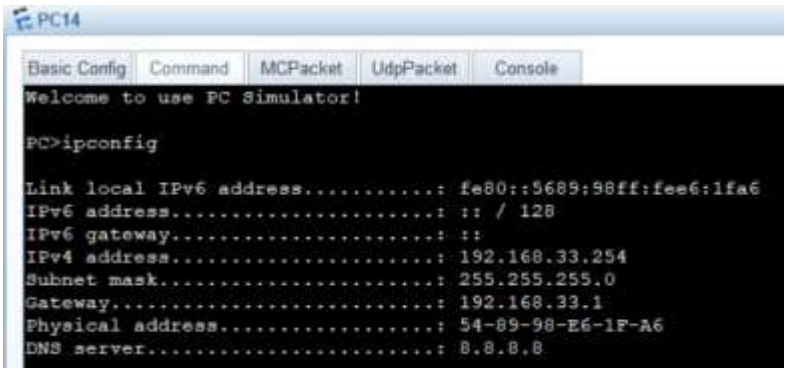
5. Device in Floor 2

The device on Floor 2 received its IP address from the DHCP pool associated with VLAN 32, including the correct gateway and DNS settings.



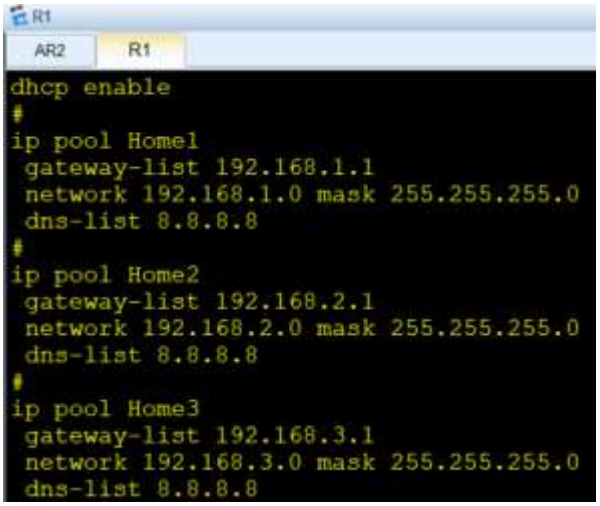
6.Device in Floor 3

The device on Floor 3 successfully obtained an IP address from the DHCP pool for VLAN 33, confirming the proper operation of DHCP for all building floors.



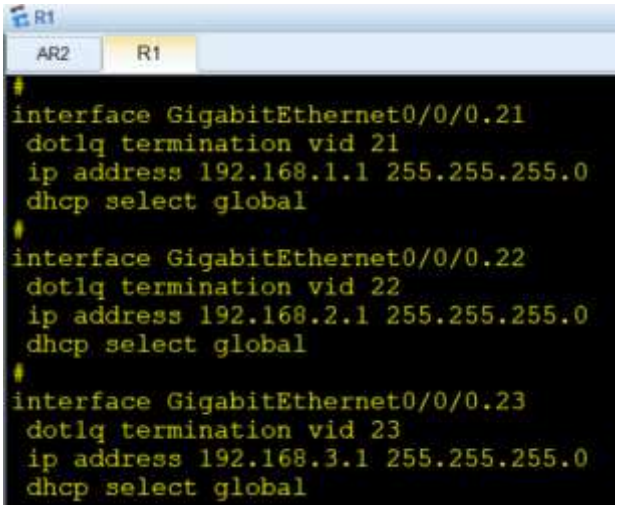
7. DHCP Pools for Homes

This screenshot shows the creation of DHCP pools for the three home networks (Home1, Home2, Home3). Each home is isolated under its own VLAN (21, 22, 23), and each pool provides gateway, subnet, and DNS settings.



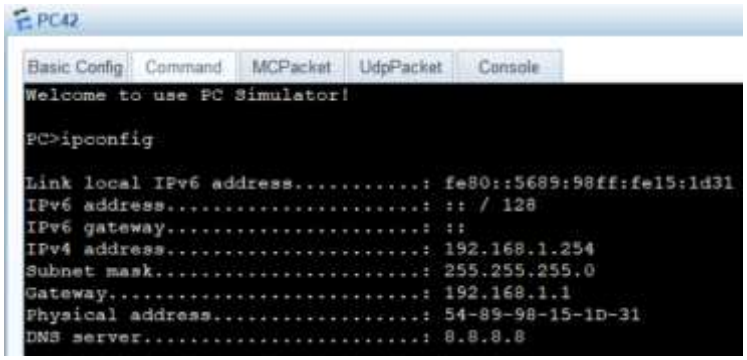
8. Sub-Interfaces for the Three Homes

Here we configured sub-interfaces on R1 for VLANs 21, 22, and 23. These sub-interfaces deliver DHCP services to the three home networks independently.



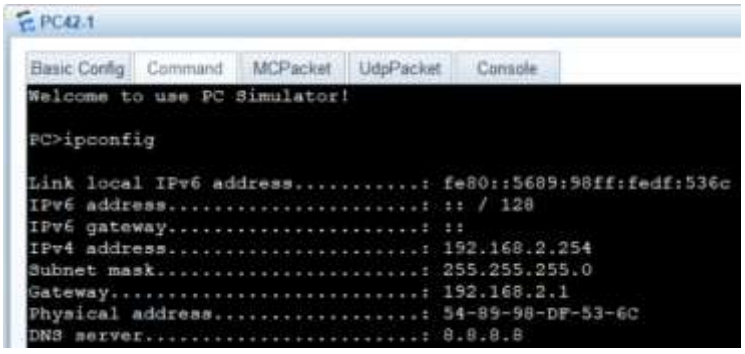
9. Home 1 – DHCP Assignment

The device in Home 1 received its IP address from the 192.168.1.0/24 DHCP pool, proving that DHCP is working correctly on VLAN 21.



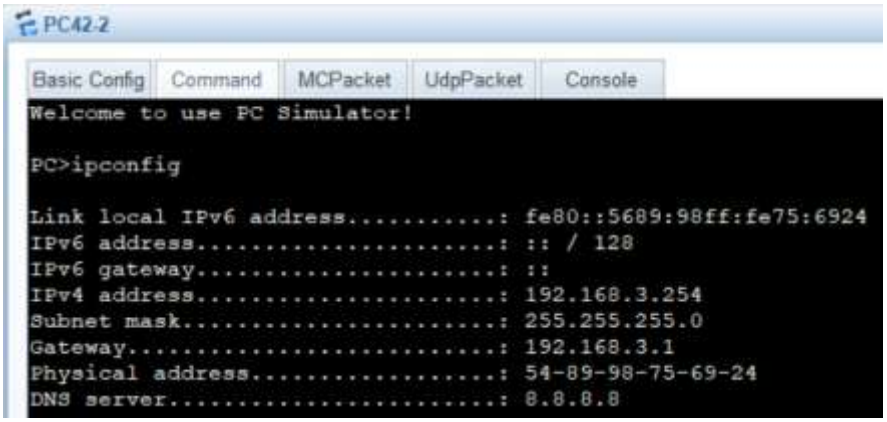
10. Home 2 – DHCP Assignment

The device in Home 2 automatically obtained an IP address from the 192.168.2.0/24 DHCP pool, showing successful DHCP service on VLAN 22**.**



11. Home 3 – DHCP Assignment

The device in Home 3 obtained an IP address from the 192.168.3.0/24 DHCP pool, confirming proper DHCP operation for VLAN 23.



10. Switching Architecture :

The network uses a hierarchical switching layout:

10.1 Trunking :

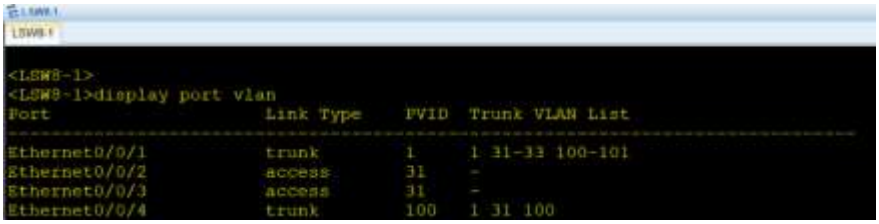
All distribution switches propagate VLANs 31–33 and 21–23 depending on their role. Trunks include VLAN100 where APs are connected.

10.2 Access Layer :

- Floor switches (LSW8-1, LSW10-1, LSW9-1) map access ports to VLAN 31/32/33 respectively.
- Street Cabinet switches map ports to VLANs 21–23 for home distribution.
- Zone2 uses VLAN 200 for service delivery.

1. This screenshot confirms the access layer setup for **SW8-1 (Floor 1 Switch)**.

- Ports **GE0/0/2** and **GE0/0/3** operate as **access ports** mapped to **VLAN 31**, serving end devices on Floor 1.
- Ports **GE0/0/1** and **GE0/0/4** are **trunk ports** carrying VLANs **31–33** and **100**, forwarding traffic upward to the distribution layer.

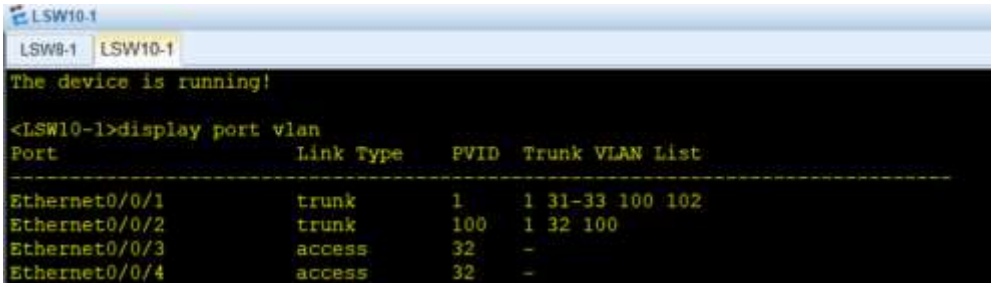


This matches the design where floor switches map access ports to VLAN 31/32/33 and trunks carry all building VLANs.

2. This switch handles **SW10-1 (Floor 2 Switch)** connectivity:

- Access ports **GE0/0/3** and **GE0/0/4** belong to **VLAN 32**, serving wired users.
- Trunk ports carry VLAN **31–33**, **100**, and additional service VLANs.

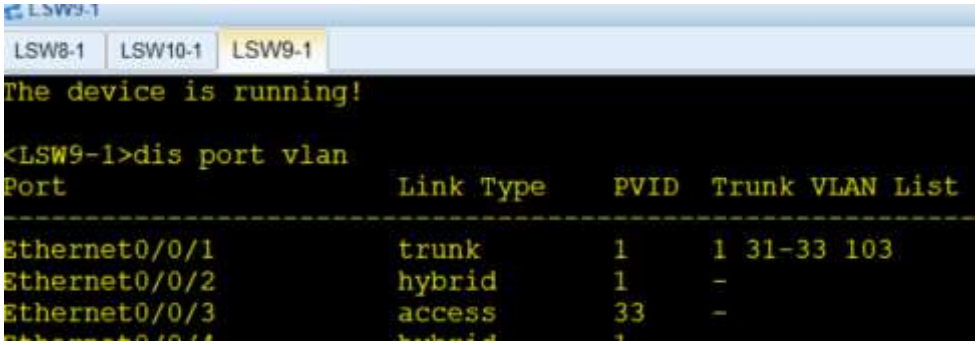
This aligns with the Access Layer design for floors.



3. The screenshot shows **SW9-1 (Floor 3 Switch)** :

- **GE0/0/3** as an **access port** in **VLAN 33** for Floor 3 devices.
- **GE0/0/1** acting as a **trunk** carrying all floor VLANs (31–33).

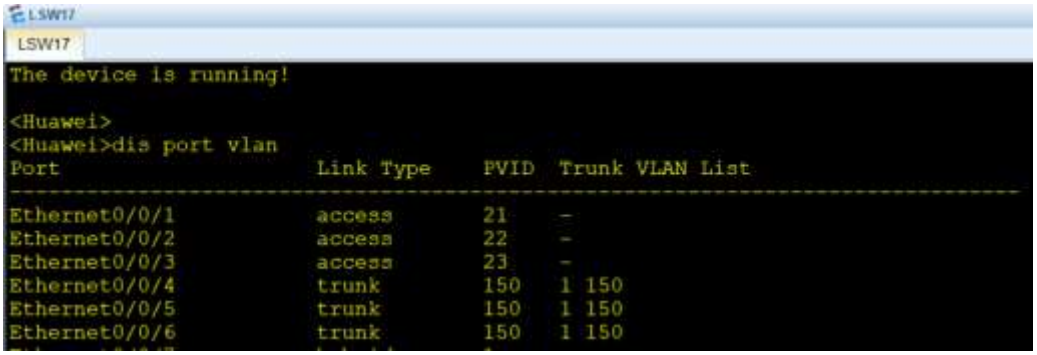
This supports the requirement of mapping each floor to its corresponding VLAN.



4. This **SW17 (Street Cabinet / Zone Aggregation)** is part of the *street cabinet.*

- Access ports **GE0/0/1–3** are mapped to VLANs **21, 22, and 23** for Home1–Home3.
- Trunk links carry VLANs **21–23** and **VLAN 200** for Zone2.

This matches the design where street cabinets map access ports to VLANs 21–23 and Zone 2 uses VLAN 200.



11. Wireless Architecture:

11.1 AC1 Controller (AC6005)

- Management IP: **192.168.100.1/24**
- CAPWAP Source: vlanif100
- SSID: **wlan-net**
- Security: WPA/WPA2 PSK (a1234567)
- User traffic bridged into **VLAN 32** (Floor 2)
- User traffic bridged into **VLAN 31** (Floor 1)

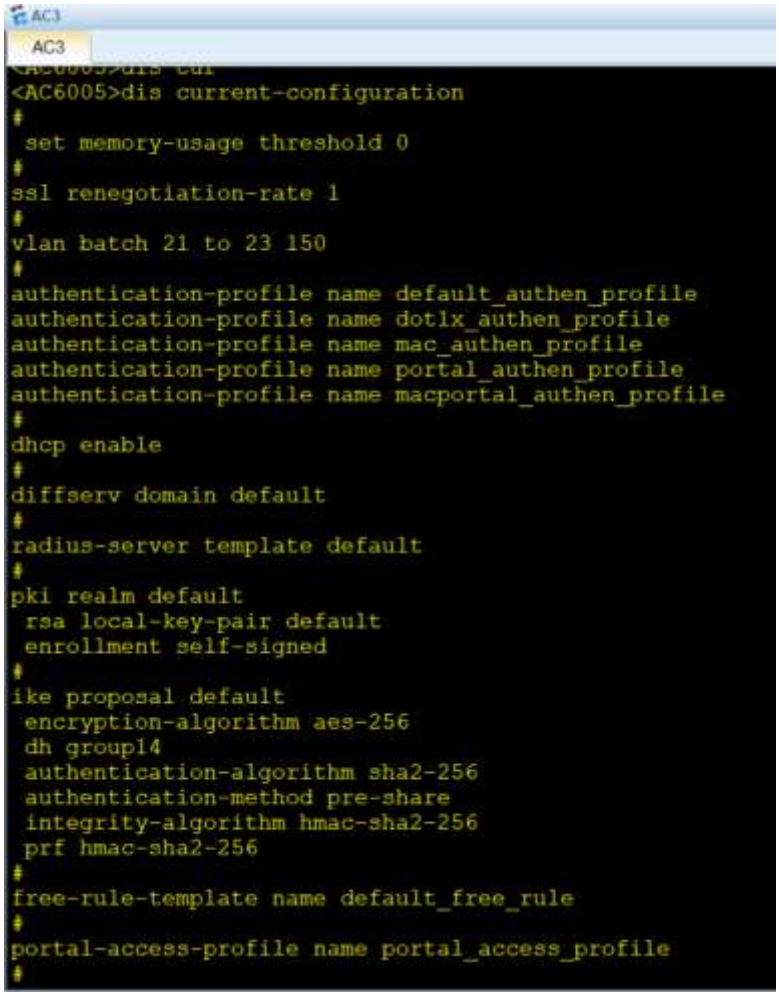
11.2 Access Points

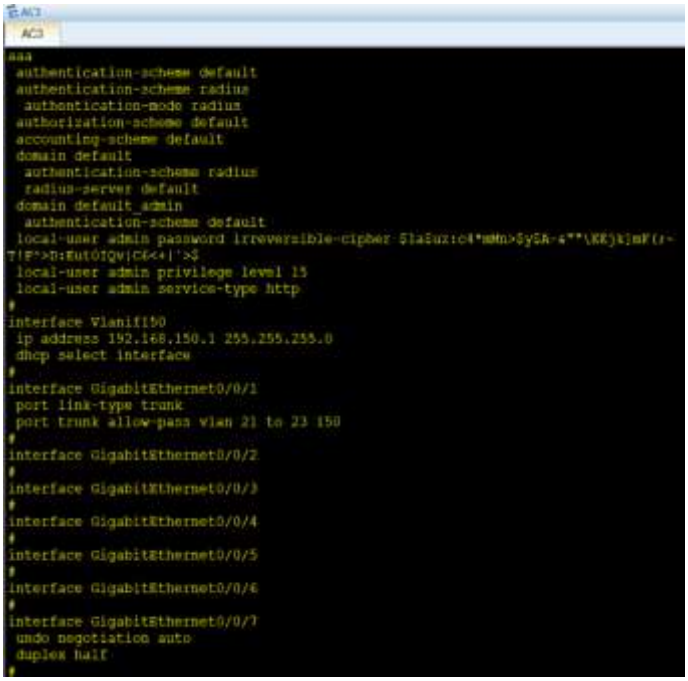
APs are centrally provisioned via AC1:

- AP1 area_1 (floor1 coverage)
- AP2 area_2 (floor1 coverage)

1. AC3 – Global WLAN & Authentication Configuration

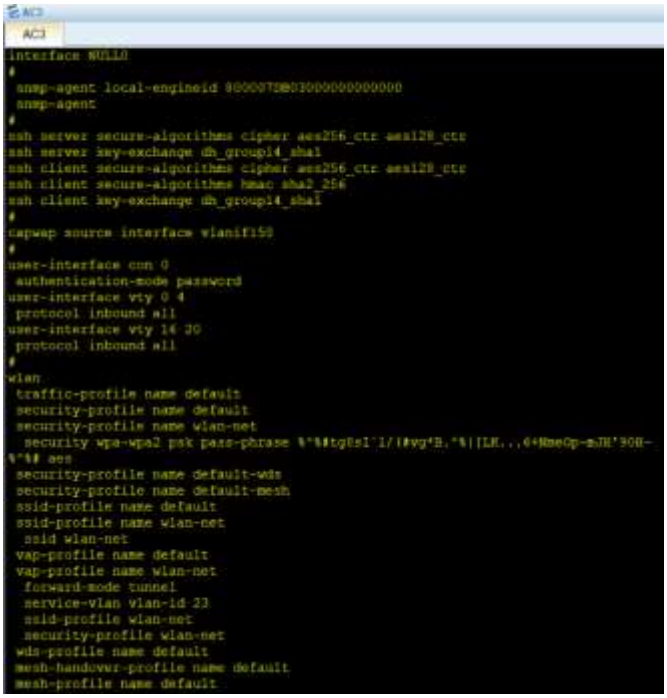
This screenshot shows the initial configuration of the **AC6005 Wireless Controller (AC3)**.
It includes VLAN creation for wireless services, AAA authentication profiles, RADIUS template, PKI setup, and IKE security parameters. These settings prepare the AC for secure management, AP provisioning, and encrypted control channels.





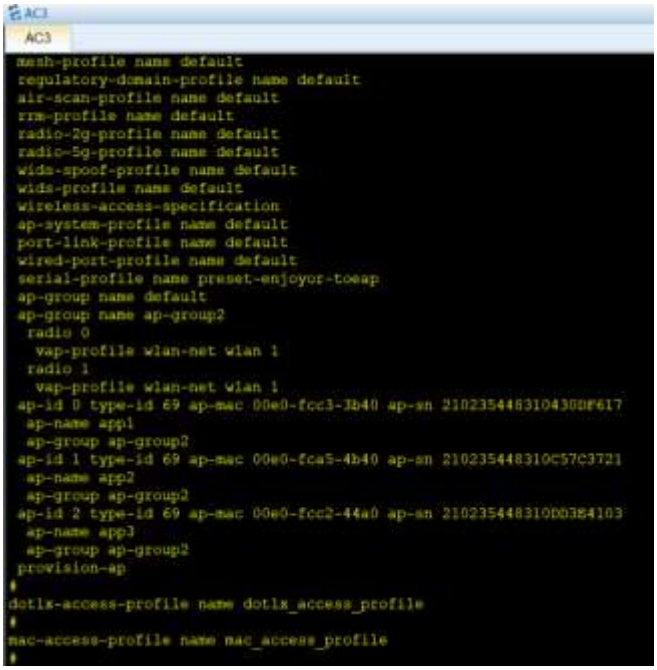
2. AC3 – Management VLAN, AAA, and Uplink Configuration

Here, VLANIF150 is configured with IP **192.168.150.1/24**, serving as the **CAPWAP management interface** used for AP discovery and control.
AAA is enabled with local admin access, and port GE0/0/1 is configured as a **trunk** carrying VLANs **21–23 and 150** toward the street cabinet, ensuring wireless management traffic reaches the APs.



3. AC3 – CAPWAP and WLAN SSID Settings

This screenshot confirms that **CAPWAP source interface = VLANIF150**, enabling APs to join the controller.
SSH is configured for secure remote management.
The WLAN SSID **“wlan-net”** is created with WPA/WPA2-PSK security, and the VAP is mapped to **VLAN 23** for tunneling user traffic through AC3.

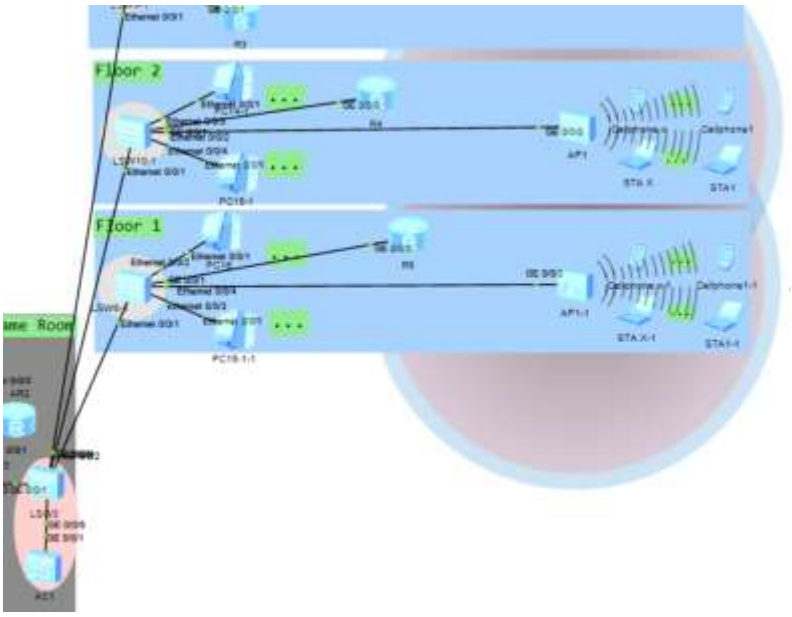


4. AC3 – AP Group Configuration & AP Registration

This screenshot shows AP grouping and provisioning.
APs are automatically discovered and added to **ap-group2**, where both 2.4GHz and 5GHz radios broadcast the “wlan-net” SSID.
Each AP (app1, app2, app3) has its radio and service profiles applied, confirming correct AP registration and provisioning inside Zone 2 homes.

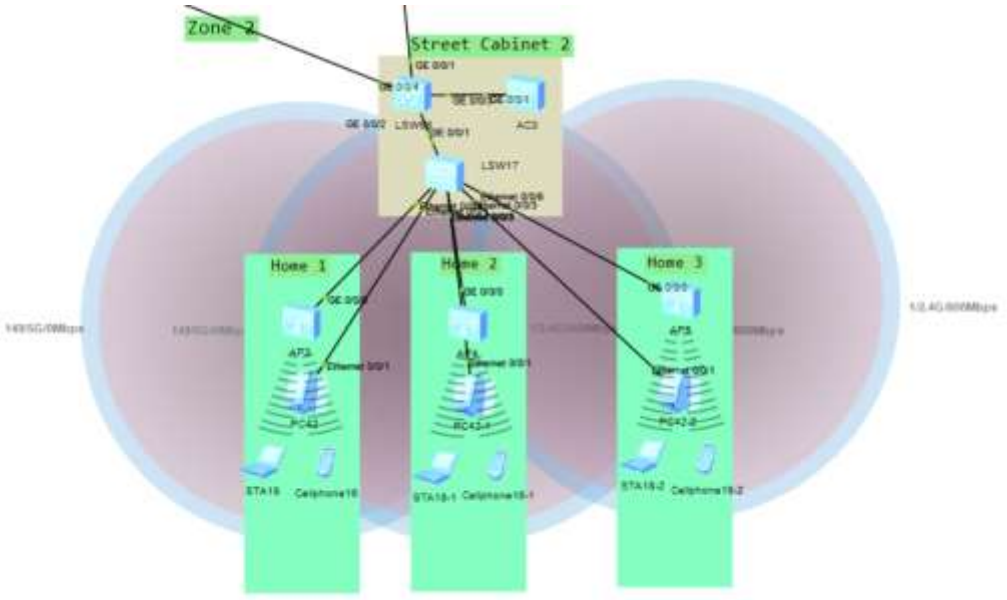
5. Wireless Coverage – Building Floors

This image illustrates the Wi-Fi deployment on Floor 1 and Floor 2.
AP1-1 (Floor 1) and AP1 (Floor 2) broadcast the same SSID “wlan-net,” providing seamless wireless coverage inside the building area.
Traffic is bridged into VLANs 31 and 32, matching the wired segmentation for each floor.



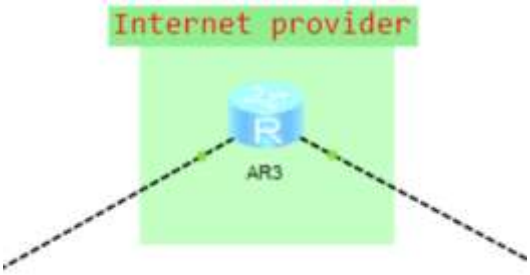
6. Wireless Coverage – Home Zone Architecture

This topology image shows the wireless coverage inside **Home1, Home2 and Home3**. Each home contains an AP providing Wi-Fi access for multiple devices (PCs, laptops, mobile phones).
Traffic from all APs is forwarded through VLAN150 toward AC3, where user authentication and SSID control are managed centrally.



12. NAT & ACL :

The NAT implementation in this project is configured on **AR3**, which acts as the upstream router responsible for providing Internet access to the internal networks. An address group is used for public IP assignment, and an ACL is applied to control which internal networks are translated.



12.1 NAT Overview (AR3):

AR3 performs **source NAT (outbound NAT)** for the internal home networks.
A public **address group** is assigned to the NAT process, allowing internal private IPs to be translated into the public IP **203.0.113.100**.

- Converts internal private IP ranges into a single public IP address.
- Ensures secure and controlled access to the Internet.
- Applied specifically on interface **GigabitEthernet0/0/0**, which connects AR3 to the external network.

12.2 ACL Controlling NAT Traffic :

NAT translation is restricted using **ACL 2000**, which defines exactly which internal networks are allowed to access the Internet.

Networks Allowed by the ACL

- **192.168.1.0/24** → Home 1
- **192.168.2.0/24** → Home 2

Only traffic from these subnets is matched and translated through NAT.

1. ACL Configuration (Traffic Selection)

The ACL (number 2000) defines which internal networks are allowed to use NAT for internet access.
From the screenshot:

```
#
acl number 2000
 rule 5 permit source 192.168.1.0 0.0.0.255
 rule 10 permit source 192.168.2.0 0.0.0.255
#
```

- **Rule 5** permits traffic from **192.168.1.0/24**
- **Rule 10** permits traffic from **192.168.2.0/24**

- This means NAT will only apply to users in **Home1** and **Home2** networks.

2. NAT Address Group

The NAT address-group assigns the public IP address used for translation:

- **Public IP: 203.0.113.100**

```
#
 nat address-group 1 203.0.113.100 203.0.113.100
#
```

- This is the external IP the internal users will appear as when accessing the internet.

3. NAT on the WAN Interface

NAT outbound is applied on:

- **Interface:** GigabitEthernet0/0/0
- Using **ACL 2000** and **-group 1**

```
#
interface GigabitEthernet0/0/0
 nat outbound 2000 address-group 1
#
```

- This means any traffic that matches ACL 2000 leaving this interface is translated to the public IP **203.0.113.100**.

---

13. Telnet & AAA :

- Basic AAA with local users deployed across all devices
- **Telnet enabled on devices in Building floors** → May be disabled and replaced with SSH

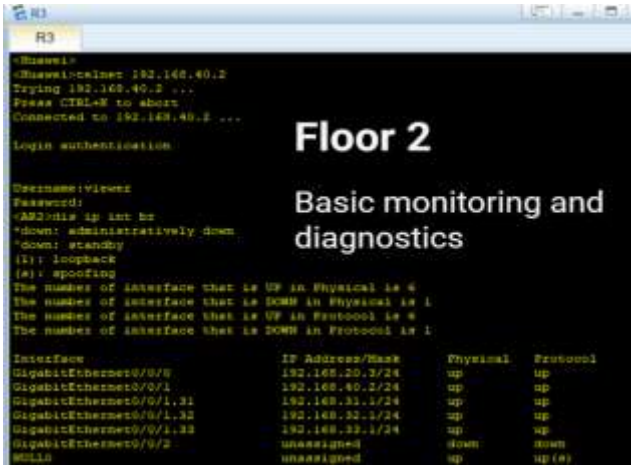
Detailed Explanation:

Telnet access has been configured with distinct privilege levels for each floor to enforce role separation and limit management scope:

- **Floor 3** — Telnet privilege **level 15** (full admin)
- **Floor 2** — Telnet privilege **level 1** (limited user)
- **Floor 1** — Telnet privilege **level 0** (no command execution)

- **Level 15 (Floor 3)**

They have full administrative privileges over permitted devices. They can view and modify configuration, manage routing protocols, VRRP, DHCP pools, and perform troubleshooting tasks. This level is intended for senior engineers or on-site administrators responsible for recovery actions and critical changes.



- **Level 1 (Floor 2)**

Level 1 users can perform basic monitoring and limited operational commands (for example: show commands, basic diagnostics). They cannot change critical configuration or restart services. This level suits junior technicians or local support staff who need visibility but not control.

- **Level 0 (Floor 1)**

Level 0 is effectively minimal/no access — users can connect but are not permitted to execute commands. This can be used for read-only monitoring sessions that are strictly controlled or as a placeholder for endpoints that should

14. PPP Links (Point-to-Point Protocol)

AR3 operates as the central uplink router, providing two PPP connections for the WAN-side communication. These links use the subnets **10.0.12.0/30** and **10.0.13.0/30**, forming the backbone for route exchange and upstream connectivity.

PPP on R1 and R1-1 (Core Routers) :

R1 and its backup router R1-1 both run PPP on all serial interfaces.
This unified configuration ensures:

- Seamless link establishment
- Reliable communication with AR3
- Consistent OSPF route advertisement
- Smooth failover when shifting between main and backup routers

Even though R1 and R1-1 have multiple PPP-enabled serial interfaces, only the active paths—determined by routing and OSPF—are used at a given time. The additional PPP interfaces provide flexibility for redundancy, simulational accuracy, and potential future expansion.

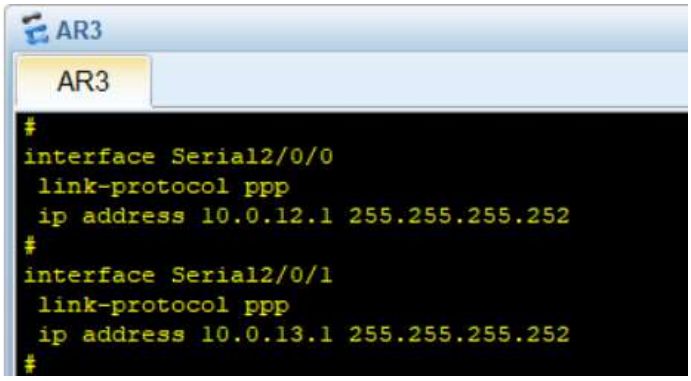
Why PPP Was Chosen

- Stable WAN encapsulation: Specially designed for point-to-point telecom links.
- Error detection & link monitoring: Ensures clean and reliable communication.
- OSPF-friendly: Ideal for carrying dynamic routing updates.
- Redundancy support: Works smoothly with R1 and R1-1 failover scenarios
-

1. This screenshot shows AR3 uses two serial interfaces, each configured with PPP encapsulation and assigned point-to-point IP addresses:

- **Serial 2/0/0**
  - Protocol: PPP
  - IP Address: **10.0.12.1 /30**
- **Serial 2/0/1**
  - Protocol: PPP
  - IP Address: **10.0.13.1 /30**

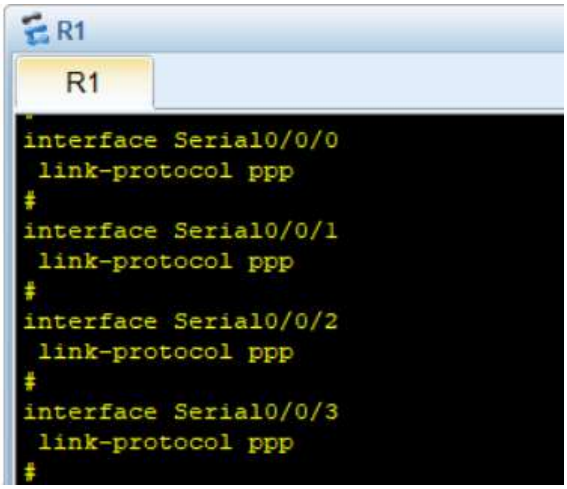
These interfaces form the WAN links toward R1.



2.This screenshot shows R1 has multiple serial interfaces configured for PPP, acting as the central router in the WAN:

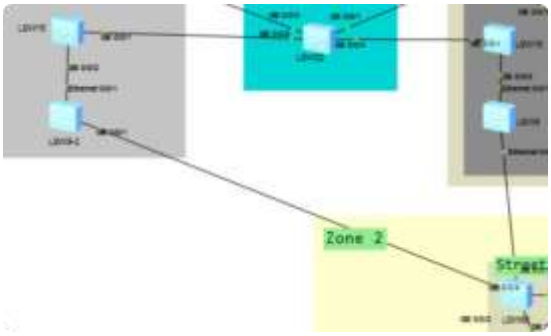
- **Serial 0/0/0 — PPP enabled**
- **Serial 0/0/1 — PPP enabled**
- **Serial 0/0/2 — PPP enabled**
- **Serial 0/0/3 — PPP enabled**

Each interface establishes PPP sessions with neighboring routers, ensuring stable point-to-point communication across the WAN.



---

15. Spanning Tree Architecture (RSTP) :



Rapid Spanning Tree Protocol (RSTP – IEEE 802.1w) is deployed across the home distribution and Zone2 switching infrastructure to ensure a loop-free Layer-2 topology. This provides fast convergence and prevents broadcast loops across VLANs 21, 22, 23.

15.1 Root Bridge & Priority Design

RSTP priorities were configured to enforce deterministic Root Bridge behavior:

Switch	STP Mode	Priority	Role
LSW22	RSTP	**4096**	**Primary Root Bridge**
LSW16	RSTP	8192	Secondary Root Bridge
LSW15	RSTP	16384	Distribution Tier
LSW9	RSTP	12288	Distribution Tier
LSW9-2	RSTP	20480	Access Aggregation
LSW68	RSTP	24576	Zone2 Aggregation

LSW22 holds the lowest priority, making it the **Root Bridge** for the RSTP domain.
LSW16 serves as the backup root, maintaining high availability.

15.2 VLANs Participating in RSTP

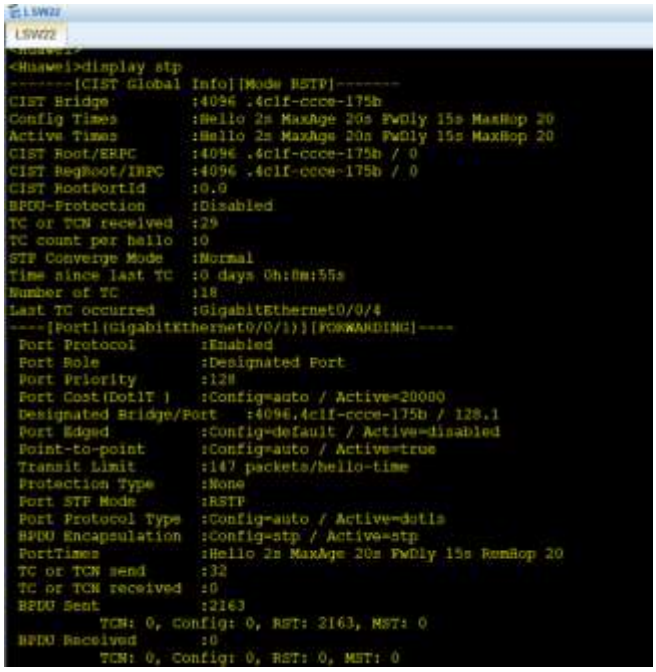
RSTP protects the following VLANs across the home/Zone2 domain:

VLAN	Purpose
21	Home 1 Distribution zone 2
22	Home 2 Distribution zone 2
23	Home 3 Distribution zone 2
200	Zone2 / Residential Backhaul
-----	The rest of zones are the same

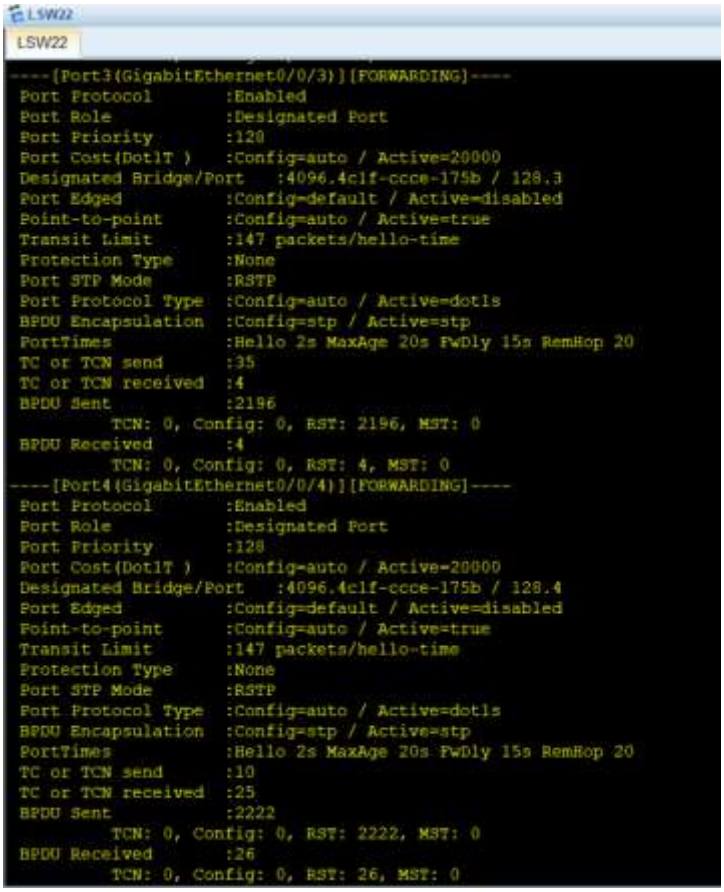
15.3 Convergence Behavior :

- All RSTP-enabled switches exchange BPDUs to elect forwarding/blocking paths.
- **RSTP** provides rapid recovery (typically < 1 second) when link failures occur.
- Multi-uplink paths between LSW22, LSW16, LSW15, LSW9, LSW9-2, and LSW68 are protected to prevent Layer-2 loops.

1. **This screenshot shows** the global RSTP status on switch LSW22, confirming that RSTP is enabled, the bridge is stable, and the switch is exchanging BPDUs normally. It also shows that the last topology change occurred on interface GE0/0/4.



2. This screenshot shows the RSTP port details for interfaces GE0/0/2 and GE0/0/3, where both ports are operating as Designated Ports in the Forwarding state. The ports are confirmed as point-to-point links, actively sending BPDUs with no errors.



3. This screenshot shows the RSTP status for interface GE0/0/4, which is also functioning as a Designated Port in the Forwarding state. BPDU exchange is active, indicating healthy connectivity and loop-free operation on this link.

16. Future Enhancements :

1. Disable Telnet everywhere, enforce SSH only.

2. **Implement SNMPv3** for secure monitoring.

3. Centralize AAA using RADIUS if available.

5. Implement **MSTP** if VLAN scaling expands beyond the current range.

6. Introduce firewalling between Home networks and building networks.

7.Network Automation.

---

17. Conclusion :

The development of this recovery-based central office simulation allowed us to translate theoretical knowledge into a fully functional and realistic network infrastructure. Inspired by the real outage at Ramses Central, our project demonstrated how redundancy, proper design, and professional configuration practices can significantly reduce downtime and improve service continuity.

By building a complete model of a primary central office with a fully operational backup site, along with multiple zoning areas that simulate residential networks, we successfully recreated the essential components of a real telecom environment. This hands-on approach enabled us to apply every concept learned throughout the HCIA and HCIP tracks—including routing, switching, high availability, wireless management, VLAN segmentation, and RSTP optimization—within a practical, measurable scenario.

The system we designed not only fulfills the academic requirements of our graduation project but also reflects industry-level standards for resilience and performance. The zones, homes, floor networks, VRRP services, OSPF routing, and AC-controlled wireless structure all worked together to create a robust infrastructure capable of handling failures and maintaining continuity.

Overall, this project strengthened our technical understanding, improved our troubleshooting and design skills, and provided us with a realistic perspective on how large-scale networks operate. With further enhancements—such as automation, monitoring integration, and security hardening—the model can evolve into an even more comprehensive representation of a modern, high-availability telecom system.
