Enterprise Campus Network Simulation

Lab 5 — Enterprise Network Services Implementation

Author: Julfri Caguiat
CCNA | Security+ | CS | MIS

Date: February 14, 2026

Lab Documentation

Table of Contents

1. Executive Summary

Lab 5 focuses on the **implementation of core enterprise network services and features** in a simulated multi-layer campus network. The lab leverages a variety of devices including **routers, L3 and L2 switches, servers, and end-user devices** to model a realistic enterprise environment.

Key activities in this lab included:

- **Network Infrastructure Configuration:** Deploying VLANs, inter-VLAN routing, EtherChannels (L2 & L3 using PAgP and LACP), HSRP for gateway redundancy, STP / Rapid PVST+ for loop prevention, and PPP with CHAP for WAN links (used instead of eBGP due to Packet Tracer limitations).

- **Network Management & Monitoring:** Configuring **NTP**, and implementing **Syslog** and **SNMP v2c** traps with limited functionality due to Packet Tracer constraints.

- **Security & Access Control:** Limited to **PortFast** and **BPDU Guard**; Access Control Lists (ACLs) were implemented to enforce least-privilege access by restricting inter-VLAN traffic between user and IT networks while also providing foundational permissions for NAT/PAT operations.
- **Enterprise Services:** Deploying **DHCP** and **DNS** on lab servers, and enabling CDP / LLDP for neighbor discovery.

While **wireless integration (WLC / LWAP) and advanced security features** are prepared, they are reserved for upcoming labs. This lab provides practical experience in configuring **core, distribution, and access layers** of an enterprise network, ensuring redundancy, operational visibility, and foundational service management.

The lab outcomes provide a solid base for **future expansions**, including wireless deployment, comprehensive ACLs, and enhanced security, aligning with real-world enterprise best practices.

2. Lab Objectives / Scope

The objective of Lab 5 is to implement and validate **core enterprise network services** and foundational network management functionalities in a simulated campus environment. This lab focuses on practical configuration, verification, and awareness of simulator limitations while providing a controlled environment to test enterprise-grade protocols and services.

2.1 Objectives

1. **Infrastructure Configuration**
    - Deploy VLANs and configure **inter-VLAN routing** for traffic segmentation.
    - Implement **HSRP** for gateway redundancy.
    - Configure **EtherChannels** (L2 & L3) using **PAgP** and **LACP** for link aggregation.
    - Apply **STP / Rapid PVST+** to prevent network loops.
    - Set up **PPP with CHAP authentication** for WAN connectivity (used as a workaround for eBGP limitations).
2. **Security & Access Control**
    - Enable **PortFast** and **BPDU Guard** on access layer ports.
    - Implement **ACLs** for NAT/PAT as required by the lab topology.
3. **Enterprise Services**
    - Configure **DHCP** on the router (to be migrated to a dedicated server in the next lab).
    - Configure **DNS** on a dedicated lab server.
    - Enable **CDP / LLDP** for device discovery and topology verification.
4. **Network Services Implementation**
    - Configure **NTP** for time synchronization across routers and switches.
    - Implement **Syslog** for centralized logging of network events.
    - Deploy **SNMP v2c** for basic network monitoring using community strings.

2.2 Simulation Limitations Awareness

- **eBGP / BGP full functionality** – While eBGP neighbor relationships can be successfully established, the simulation does **not allow configuration of a default route to the ISP**, preventing a fully functional BGP session. PPP with CHAP was used as a reliable workaround.

- **SNMP** – Only **community string configuration** is supported; SNMP traps and alerting functionality are not fully operational in the simulator.

- **Syslog severity levels** – The platform supports only **debugging-level logs**; finer-grained severity levels such as informational, warning, or critical are unavailable.

- **VRRP** – Not supported.

- **DNS-server configuration on routers** – Routers cannot act as authoritative DNS servers; dedicated server deployment is required for lab functionality.

- **NTP** – External Internet NTP sources inaccessible; Edge-01 functions as the authoritative internal time source for the simulated network.

2.3 Scope

- **Included:** Core, distribution, and access layer configuration; VLANs; routing protocols; basic monitoring (SNMP, Syslog); DHCP on router; DNS on dedicated server; PPP WAN links; HSRP; EtherChannel; STP / Rapid PVST+.

- **Excluded / Deferred:** Full AAA server integration; advanced ACLs and security hardening; full SNMP trap functionality; migration of DHCP to dedicated server; full Internet NTP synchronization.

3. Network Topology

3.1 Topology Diagram

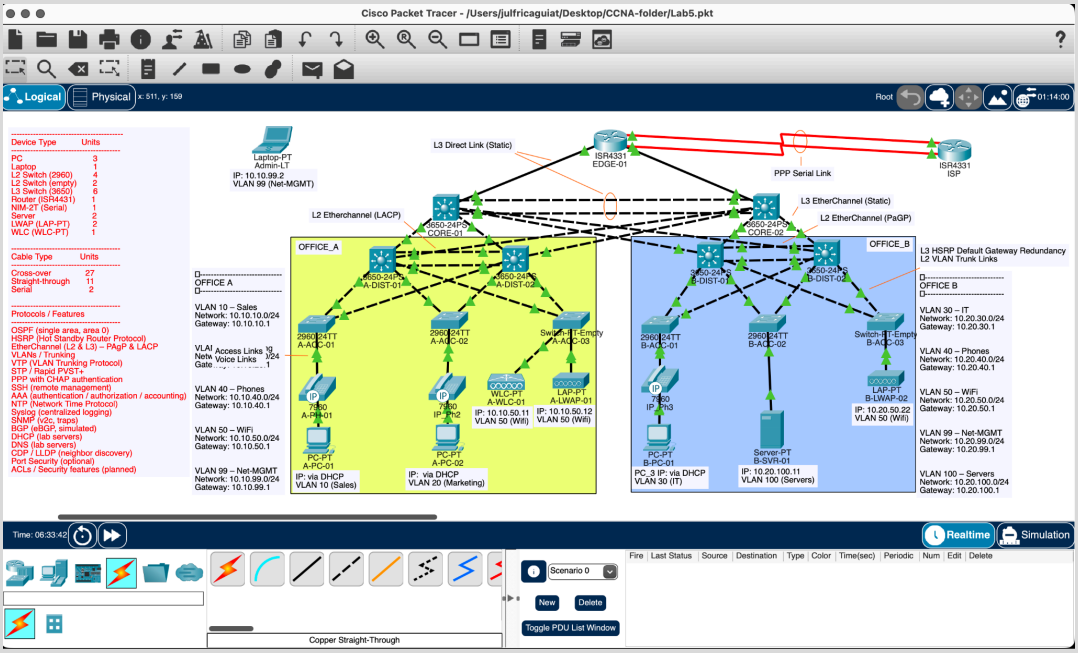


Figure 1 – Enterprise Campus Network Topology (Lab 5)
The diagram illustrates the full lab setup including Core, Distribution, Access, and Edge layers, WAN links, VLAN segmentation, and service devices. All links and device roles are clearly labeled to replicate the environment in Packet Tracer.

3.1 Topological Flow

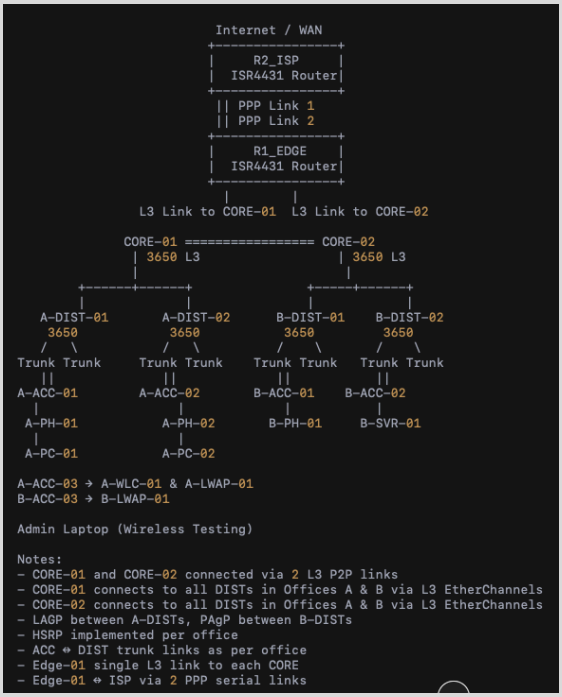


Figure 2 – Enterprise Campus Network Topological Flow (Lab 5)
Shows the logical flow of Core, Distribution, and Access layers, Edge connectivity, redundancy, and device mapping for both offices.

4. Addressing & VLAN Strategy

The enterprise campus network follows a hierarchical private addressing structure based on RFC1918, with site-based allocation—Office A uses 10.10.0.0/16 and Office B uses 10.20.0.0/16—further segmented into subnets for Sales, Marketing, IT, Phones, Wi-Fi, Management, and Servers, reserving lower addresses for static infrastructure and higher addresses for dynamic end devices to maintain separation and organized network traffic.

4.1 Enterprise VLAN Addressing and Subnet Allocation Plan

VLAN ADDRESSING & SUBNET ALLOCATION TABLE

VLAN ID	Name / Function	Subnet / Prefix	Site / Location	Notes / Usage
10	Sales	10.10.10.0/24	Office A	User VLAN
20	Marketing	10.10.20.0/24	Office A	User VLAN
30	IT	10.20.30.0/24	Office B	User VLAN
40	Phones	10.10.40.0/24	Office A	VoIP VLAN
40	Phones	10.20.40.0/24	Office B	VoIP VLAN
50	Wi-Fi	10.10.50.0/24	Office A	WLAN Users / APs
50	Wi-Fi	10.20.50.0/24	Office B	WLAN Users / APs
99	Network Management	10.10.99.0/24	Office A	Device Mgmt / Admin PCs / Trunks
99	Network Management	10.20.99.0/24	Office B	Device Mgmt / Admin PCs / Trunks
100	Servers	10.20.100.0/24	Office B	Services VLAN / Future L3 area

- Addressing Schema Overview
  - Site-Based Allocation:
    - Office A: 10.10.0.0/16
    - Office B: 10.20.0.0/16
  - All VLANs currently operate in single OSPF area 0.

4.2 Loopback & Router IDs

Purpose: Loopback addresses provide stable router IDs for OSPF, management access, and monitoring.

- Addressing LogicEdge Router:
  - R1 uses a unique /32 loopback to separate WAN-facing interfaces from the internal router ID.
  - Core Layer: CORE-01 and CORE-02 use dedicated /32 loopbacks for router ID and management.
  - Distribution Layer: Each distribution switch has its own /32 loopback to serve as a stable OSPF
  - router ID, independent of physical interface changes.

LOOPBACK & ROUTER IP ASSIGNMENT TABLE

Device	Layer	Loopback IP	Purpose / Notes
CORE-01	Core	10.255.255.1	Router ID & Management
CORE-02	Core	10.255.255.2	Router ID & Management
EDGE-01	Edge	10.255.255.3	Router ID & Management / WAN separation
A-DIST-01	Distribution	10.255.255.11	Router ID for OSPF
A-DIST-02	Distribution	10.255.255.12	Router ID for OSPF

B-DIST-01	Distribution	10.255.255.21	Router ID for OSPF
B-DIST-02	Distribution	10.255.255.22	Router ID for OSPF

—-

4.3 SVI IP Assignment – L3 Switching Design

- Addressing Logic – SVI Design:
  - Each site follows an area summary:
    - Office A → 10.10.0.0/16
    - Office B → 10.20.0.0/16
  - The first 20 IP addresses are reserved for critical infrastructure, including:
  - HSRP virtual and standby gateways
  - Distribution switches
  - Wireless LAN controllers
  - Access points
  - Firewalls
  - Printers
  - Monitoring tools
  - DHCP scopes begin at .21 to ensure predictable static addressing and simplify operational management.
  - VLAN 99 and VLAN 100 remain static-only networks to enhance security and prevent unauthorized device assignment.
  - VLAN 50 is designated for wireless services. Infrastructure components including the WLC,
  - LWAPs, and administrative devices use static IP addressing for consistent management and monitoring, while wireless clients are dynamically assigned addresses via DHCP to enable flexible and scalable connectivity.

SVI ASSIGNMENT TABLE

Site	VLAN	Name / Purpose	Subnet	Default Gateway	IP Allocation	Notes
Office A	10	Sales	10.10.10.0/24	10.10.10.1	DHCP (.21–.254)	First 20 IPs reserved
Office A	20	Marketing	10.10.20.0/24	10.10.20.1	DHCP (.21–.254)	—
Office B	30	IT	10.20.30.0/24	10.20.30.1	DHCP (.21–.254)	—
Office A	40	Voice (VoIP)	10.10.40.0/24	10.10.40.1	DHCP (.21–.254)	IP phones
Office B	40	Voice (VoIP)	10.20.40.0/24	10.20.40.1	DHCP (.21–.254)	IP phones
Office A	50	Wi-Fi / WLAN	10.10.50.0/24	10.10.50.1	DHCP (.21–.254)	Wireless clients
Office B	50	Wi-Fi / WLAN	10.20.50.0/24	10.20.50.1	DHCP (.21–.254)	Wireless clients
Office A	99	Network Management	10.10.99.0/24	10.10.99.1	Static	Infrastructure devices
Office B	99	Network Management	10.20.99.0/24	10.20.99.1	Static	Infrastructure devices
Office B	100	Servers	10.20.100.0/24	10.20.100.1	Static	Server farm

—-

4.4 Infrastructure Management IP Assignment — VLAN 99

- Addressing Logic – Management VLAN Design:
  - VLAN 99 is dedicated exclusively to network infrastructure management, providing secure administrative access to distribution and access layer switches.
  - Default Gateway – HSRP virtual IPs serve as the default gateway for each site:
    - Office A VIP: 10.10.99.1
    - Office B VIP: 10.20.99.
      This ensures gateway redundancy while maintaining uninterrupted management connectivity during failover events.
  - Core and Edge Devices – Core switches and the edge router are managed using loopback

interfaces rather than VLAN 99. This design improves stability for routing protocols and allows consistent reachability independent of physical interface states.

- Administrative Access – The Admin-LT workstation resides in VLAN 99 and is authorized to manage infrastructure devices across both offices.

IP ASSIGNMENT TABLE (VLAN 99 - Net-MGMT)

Device	Interface / SVI	IP Address	Role / Purpose	Default Gateway
Admin-LT	Wireless	10.10.99.2	Enterprise management workstation (Office A)	10.10.99.1
EDGE-01	Loopback0	10.255.255.3	Edge router Router ID and management	–
CORE-01	Loopback0	10.255.255.1	Core Router ID and management	–
CORE-02	Loopback0	10.255.255.2	Core Router ID and management	–
A-DIST-01	VLAN 99	10.10.99.11	Active distribution switch (Office A)	10.10.99.1
A-DIST-02	VLAN 99	10.10.99.12	Standby distribution switch (Office A)	10.10.99.1
B-DIST-01	VLAN 99	10.20.99.21	Active distribution switch (Office B)	10.20.99.1
B-DIST-02	VLAN 99	10.20.99.22	Standby distribution switch (Office B)	10.20.99.1
A-ACC-01	VLAN 99	10.10.99.31	Access switch (Office A)	10.10.99.1
A-ACC-02	VLAN 99	10.10.99.32	Access switch (Office A)	10.10.99.1
A-ACC-03	VLAN 99	10.10.99.33	Access switch – wireless aggregation (Office A)	10.10.99.1
B-ACC-01	VLAN 99	10.20.99.31	Access switch (Office B)	10.20.99.1
B-ACC-02	VLAN 99	10.20.99.32	Access switch (Office B)	10.20.99.1
B-ACC-03	VLAN 99	10.20.99.33	Access switch – wireless aggregation (Office B)	10.20.99.1

—–

4.5 VLAN-to-Device Mapping Summary

VLAN to DEVICE MAPPING TABLE

VLAN	Name / Purpose	Subnet	Primary Devices	Gateway	Site
10	Sales	10.10.10.0/24	User PCs, printers	10.10.10.1	Office A
20	Marketing	10.10.20.0/24	User PCs	10.10.20.1	Office A
30	IT	10.20.30.0/24	IT workstations, admin devices	10.20.30.1	Office B
40	Voice	10.10.40.0/24 / 10.20.40.0/24	IP phones	x.x.40.1	Both
50	Wi-Fi	10.10.50.0/24 / 10.20.50.0/24	Wireless clients (DHCP), WLC, LWAPs, Admin-LT (static)	x.x.50.1	Both
99	Network Management	10.10.99.0/24 / 10.20.99.0/24	Switches, infrastructure devices, Admin-LT	x.x.99.1	Both
100	Servers	10.20.100.0/24	Application servers, future services	10.20.100.1	Office B

Note: VLAN segmentation separates user, voice, wireless, server, and management traffic to improve security, reduce broadcast domains, and support scalable Layer 3 routing.

5. Device Inventory (Lab Assets)

Purpose: Displays all deployed devices along with their respective cable types.

5.1 Devices

DEPLOYED DEVICES TAB;E

Device Type	Units	Location	Notes
PC	3	Office A & B	End-user VLAN testing
Laptop	1	–	Network management / WiFi testing
L2 Switch (Cisco 2960)	4	2 per office	Access switches
L2 Switch (Empty)	2	1 per office	Access switches for WLC & LWAPs
PT-SWITCH-NM-1CE Module	7	A-ACC-03 / B-ACC-02	4 in A-ACC-03, 3 in B-ACC-02 for WLC & LWAPs
L3 Switch (Cisco 3650)	2	Core	Backbone switches
Distribution Switch (Cisco 3650)	4	2 per office	HSRP & EtherChannel
Router (Cisco ISR4431)	2	EDGE / WAN	R1: backbone, R2_ISP: WAN simulation
NIM-2T Serial Module	2	ISR4431	Installed for Serial PPP WAN links
Server	1	Office B	DNS server
LWAP (LAP-PT)	2	1 per office	Wireless APs for Wi-Fi VLAN testing
WLC (WLC-PT)	1	Office A	Wireless LAN Controller

5.2 Cables

CABLES UTILIZED

Cable Type	Units	Location / Notes
Cross-over	28	Device-to-device connections
Straight-through	13	PC-to-switch / switch-to-router
Serial	2	PPP WAN links

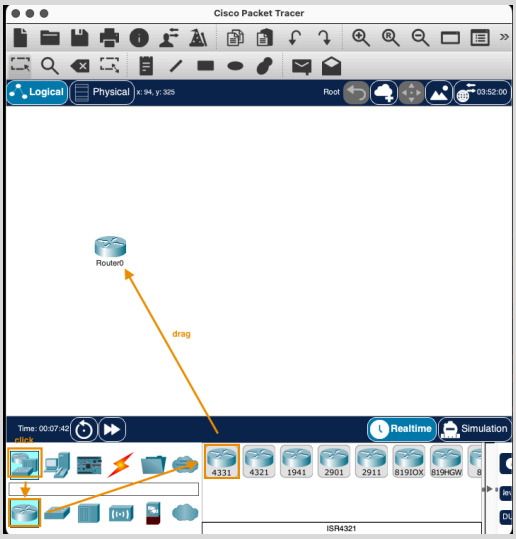
6. Device Deployment & Initial Setup

Purpose: Selection, foundational configuration and connectivity of all network devices guide, ensuring they are correctly installed, powered, and accessible for subsequent network implementation and testing.

6.1 Device Deployment on Packet Tracer Platform

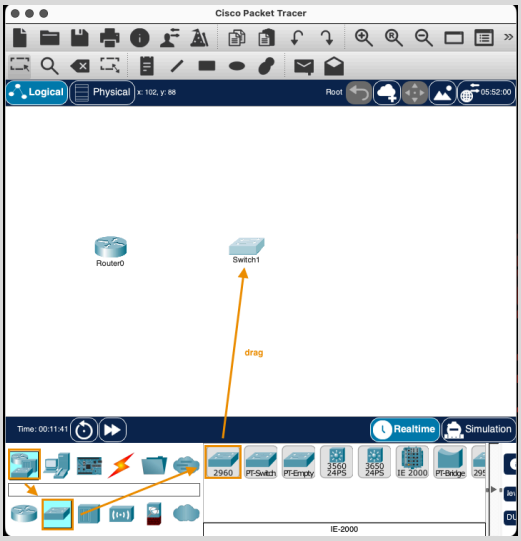
Router:

1. Click on Network Devices icon
2. Click on Routers icon
3. Select Model (click or drag/drop)



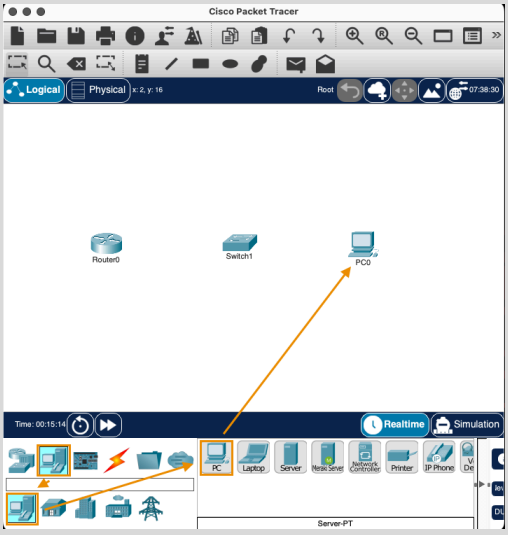
Switch:

1 Click on Network Devices icon
2. Click on Switches icon
3. Select Model (click or drag/drop)



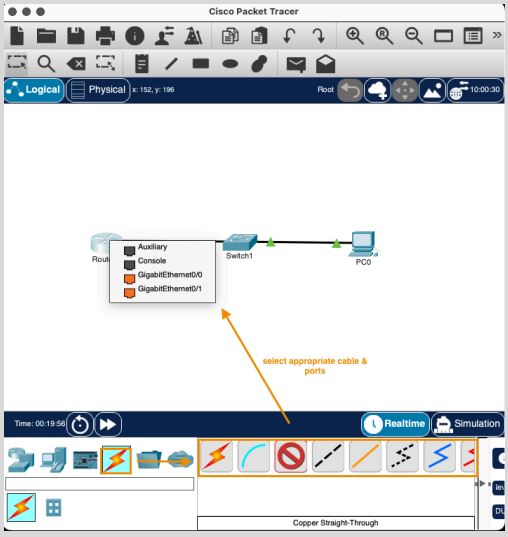
End Device:

1. Click on End Devices icon
2. Select PC (click or drag/drop)



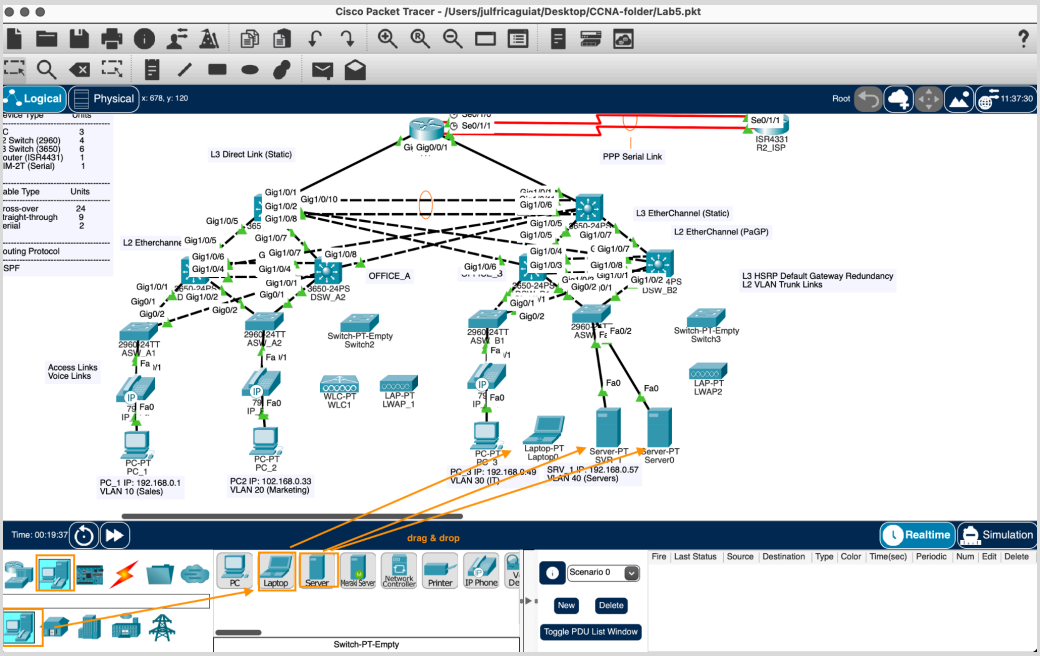
Cable:

1 Click on Connections icon
2. Select Type (click or drag/drop)
3. Select Ports



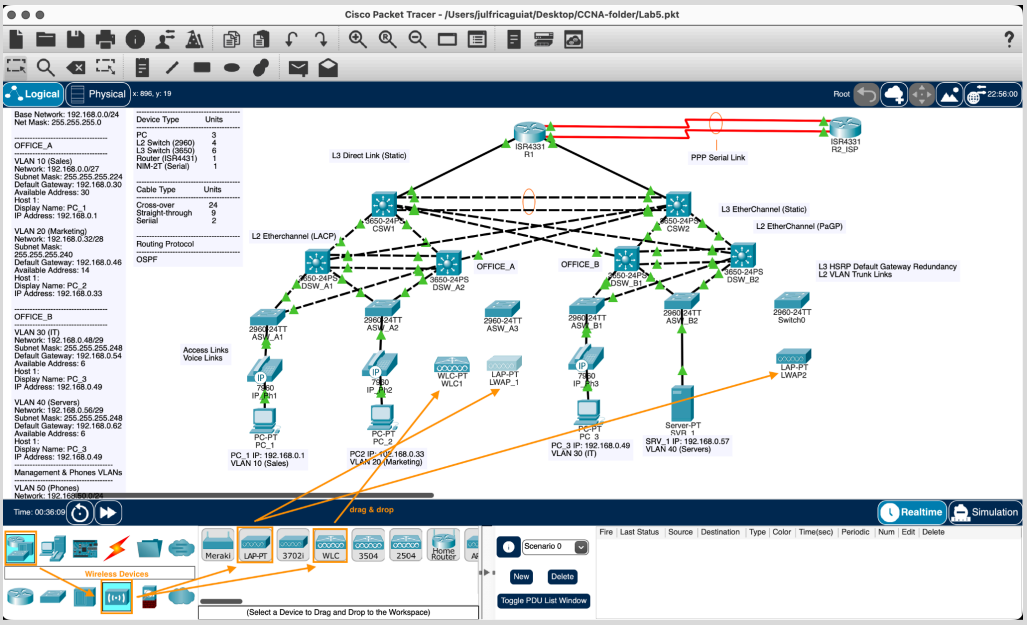
Servers & Laptop:

1. Click on End DEvice
2. Select devices (click or drag/drop)



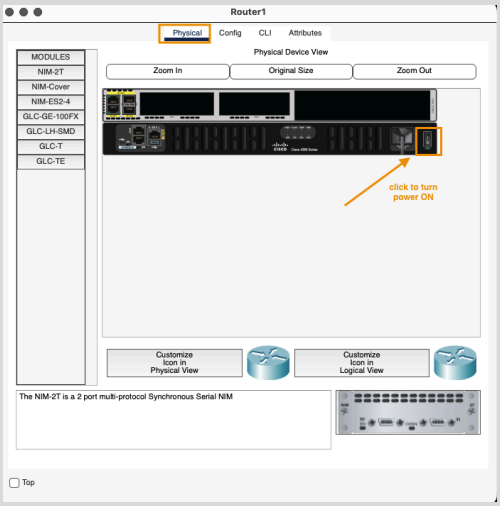
Wireless Devices:

1. Click on End DEvice
2. Click on Wireless Device icon
3. Select devices (click or drag/drop)

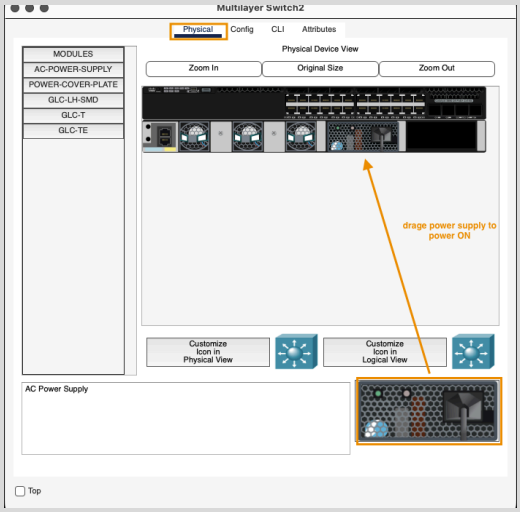


6.2 Powering On Devices

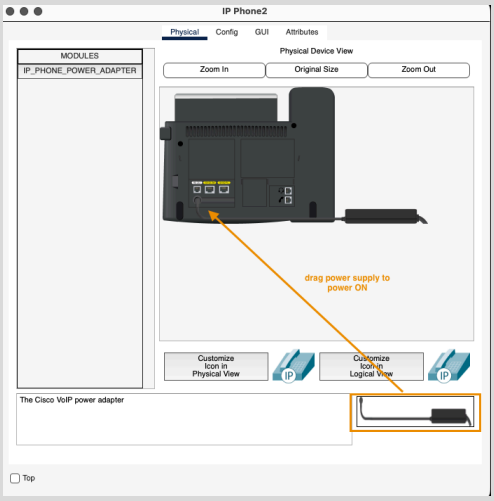
Router: Turn power switch to ON



L3 (Multi-Layer) Switch: Drag/drop power supply

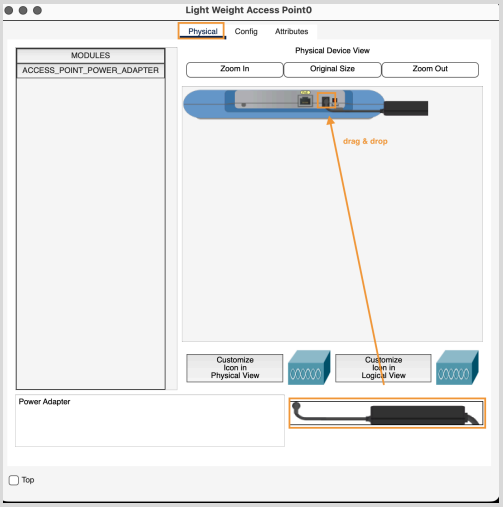


IP Phones: Drag/drop power cord

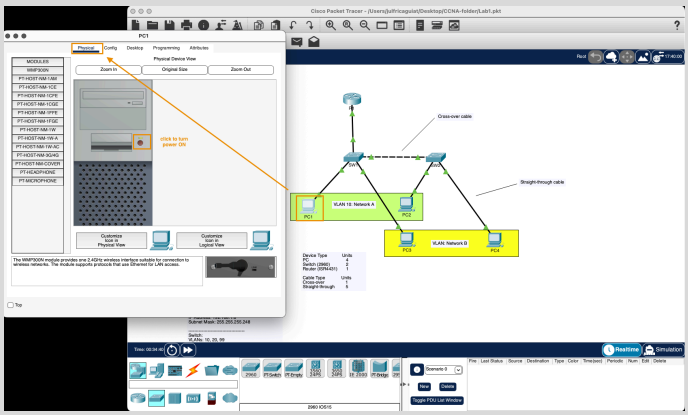


WLC: Turn power switch to ON

LWAP: Drag/drop power cord

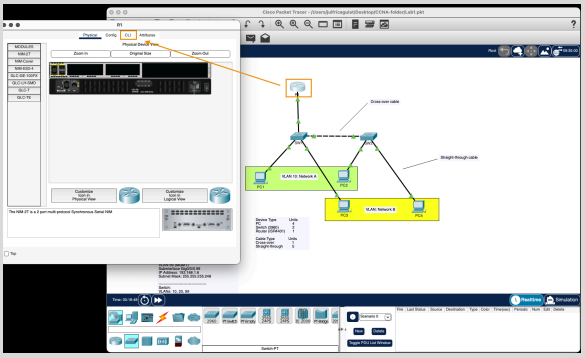


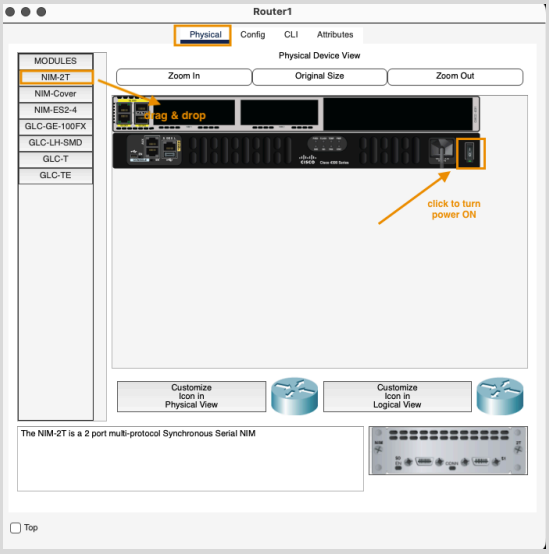
PC: push power button ON



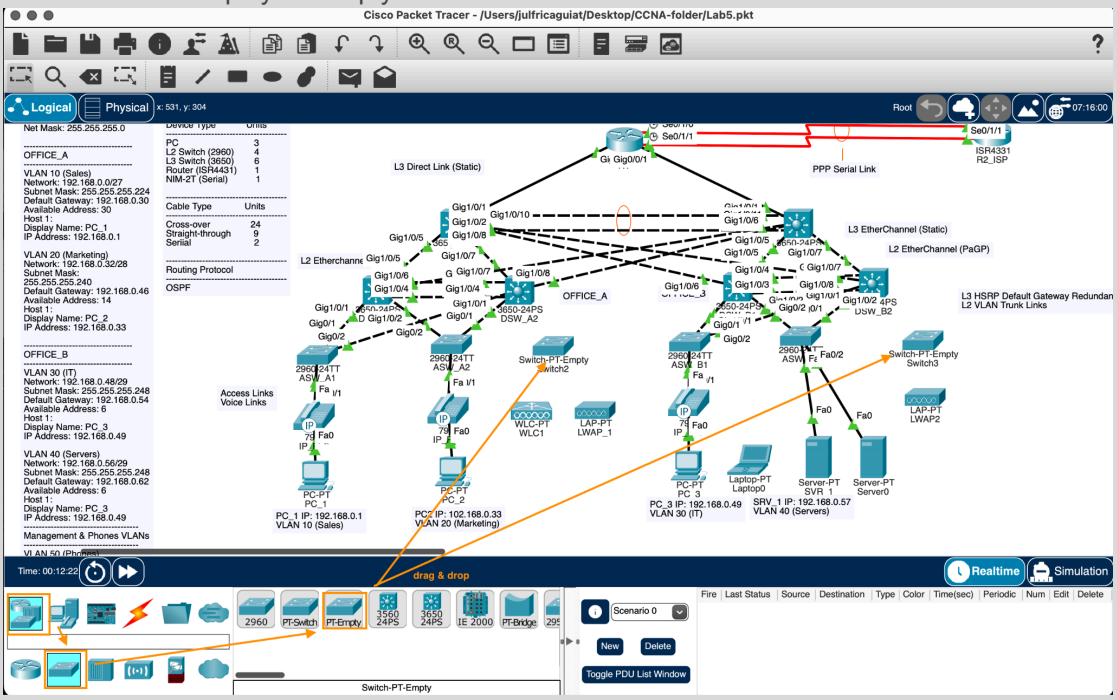
6.3 Installing Modules to Devices

- Router **NIM-2T Serial Module** (for Serial Link)
    - Installation
    1. Turn power switch to OFF
    2. Drag/drop NIM-2T Serial Module to selected slot
    3. Turn power switch to ON



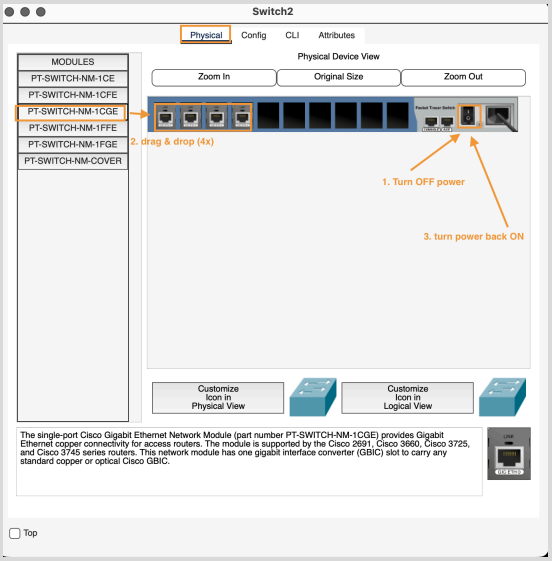


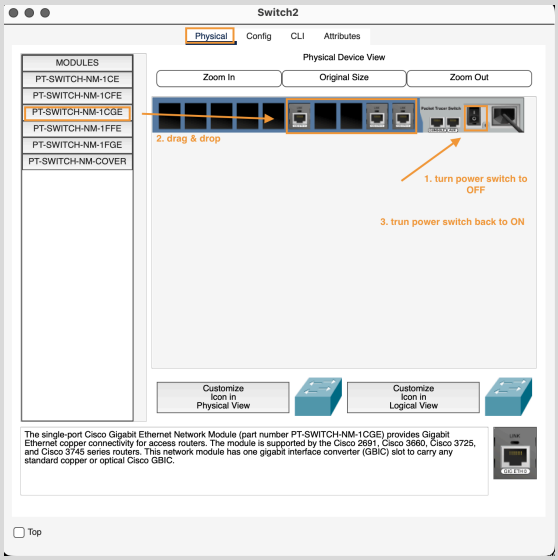
- L2 Empty Switch **PT-SWITCH-NM-1CE Module** (Gigabit Ethernet Ports):
    - Deploy L2 Empty Switch



- Installation:

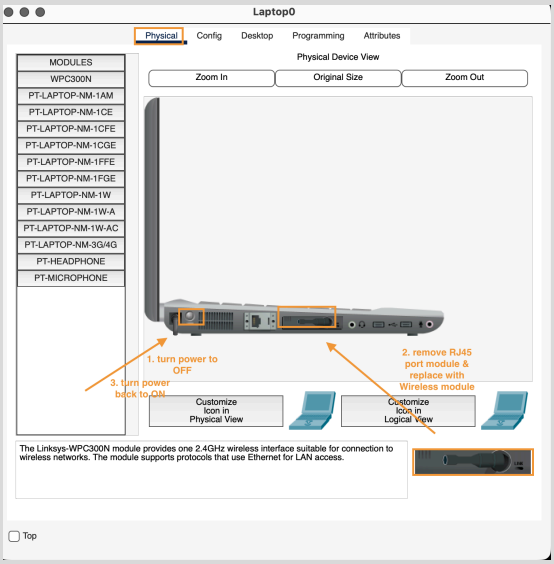
1. Turn power switch to OFF
2. Drag/drop PT-SWITCH-NM-1CE Module to selected slots
3. Turn power switch to ON





- Laptop **Linksys-WPC300N module** (for wireless connectivity)
  - Installation:

1. Turn power button OFF
2. Remove existing module to be replaced
3. Drag/drop Linksys-WPC300N module
4. Turn power button to ON



Note: Refer to Lab1 for initial device configurations. Click the link below:

- Link to Packet Tracer Labs

7. Protocols & Technologies Implemented

Purpose: Summarizes all network protocols and technologies deployed to enable connectivity, redundancy, security, and management across the enterprise network.

ENTERPRISE PROTOCOL & TECHNOLOGY MATRIX

Category	Protocol / Technology	Purpose	Deployment Scope
Dynamic Routing	OSPF (Single Area – Area 0)	Provides fast convergence and dynamic route exchange across the enterprise	Core, Distribution, Edge
Gateway Redundancy	HSRP	Ensures highly available default gateways for all VLANs	Distribution
Link Aggregation	Layer 3 EtherChannel (Static)	Increases bandwidth and removes single points of failure between routed devices	Core ↔ Distribution
Link Aggregation	LACP / PAgP	Provides resilient switch interconnections	Distribution
Network Segmentation	VLANs & 802.1Q Trunking	Separates user, voice, wireless, server, and management traffic	Access & Distribution
Layer 2 Stability	Rapid PVST+	Prevents switching loops and enables rapid convergence	Enterprise switching domain
WAN Connectivity	PPP with CHAP	Authenticated point-to-point connectivity to simulated ISP	Edge
Address Translation	NAT / PAT	Enables internal networks to communicate externally	Edge
Inter-VLAN Routing	Switch Virtual Interfaces (SVIs)	Acts as default gateways for VLAN traffic	Distribution
Infrastructure Management	SSH	Secure remote device administration	Enterprise
Infrastructure Management	AAA (Local)	Provides controlled administrative access	Infrastructure devices
Time Synchronization	NTP	Maintains consistent timestamps for logs and monitoring	Infrastructure
Monitoring	SNMPv2c	Supports device monitoring (limited Packet Tracer functionality)	Infrastructure
Logging	Syslog	Centralized event logging for operational visibility	Infrastructure
IP Services	DHCP (Router-based → server migration next)	Dynamically assigns addresses to client devices	Edge (temporary design)
IP Services	DNS (Dedicated Server)	Provides hostname resolution for the enterprise	Office B
Neighbor Discovery	CDP / LLDP	Assists with topology validation and troubleshooting	Enterprise

The enterprise lab implements a hierarchical campus design leveraging dynamic routing, gateway redundancy, network segmentation, and centralized management services to emulate a production-style infrastructure.

8. Network Configuration / Implementation

Purpose: Document the full network implementation, including configuration commands applied at each stage to establish connectivity, services, and redundancy across the enterprise network.

———

8.1 **Phase 1 — Core Backbone Deployment**
Purpose: Establish the routed backbone that all downstream layers depend on.

- **Implementation Stages:**

    1. **Redundant Core Links** – Dual Layer 3 point-to-point connections were configured between CORE-01 and CORE-02 to provide backbone redundancy and support fast convergence.

    2. **Core-to-Distribution Layer 3 EtherChannels** – Layer 3 port-channels were implemented between the core and distribution switches to deliver increased bandwidth and eliminate single points of failure.

    3. **Core-to-Edge Transit Links** – Dedicated Layer 3 transit networks were established from each core switch to the edge router (R1) to enable upstream connectivity and path resiliency.

    4. **Loopback Interfaces and OSPF Configuration** – /32 loopback interfaces were assigned on core, distribution, and edge devices to serve as stable router IDs. OSPF was reinitialized (from the previous lab) and deployed in a single-area design (Area 0). Transit and loopback networks were advertised, and loopback interfaces were configured as passive.

—-
Stage 1: Redundant Core Links

CORE BACKBONE LINKS TABLE

Link	Device A	Interface A	IP A	Device B	Interface B	IP B	Subnet	Type	Purpose
CORE-01 ↔ CORE-02 (Primary)	CORE-01	Gi1/0/1	10.255.30.1	CORE-02	Gi1/0/1	10.255.30.2	/30	L3 P2P	Primary core redundancy
CORE-01 ↔ CORE-02 (Backup)	CORE-01	Gi1/0/2	10.255.30.5	CORE-02	Gi1/0/2	10.255.30.6	/30	L3 P2P	Secondary core path

REDUNDANT CORE LINKS CONFIGURATION:

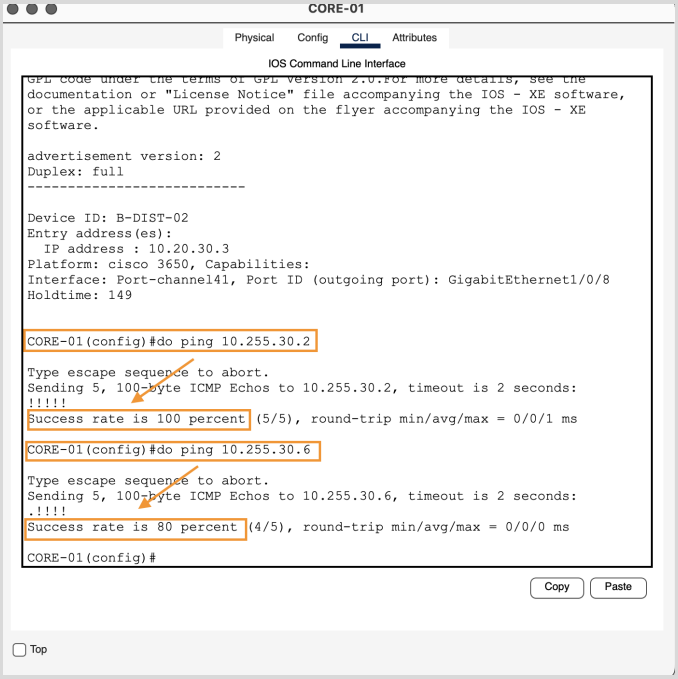
- **CORE-01 to CORE-02**

```
interface g1/0/1
 description L3 P2P to CORE-02 (Primary)
 ip address 10.255.30.1 255.255.255.252
 no shutdown
 exit

interface g1/0/2
 description L3 P2P to CORE-02 (Backup)
 ip address 10.255.30.5 255.255.255.252
 no shutdown
 exit
```

- **CORE-02 to CORE-01**

```
interface g1/0/1
 description L3 P2P to CORE-01 (Primary)
 ip address 10.255.30.2 255.255.255.252
 no shutdown
 exit

interface g1/0/2
 description L3 P2P to CORE-01 (Backup)
 ip address 10.255.30.6 255.255.255.252
 no shutdown
 exit
```

Verification:
Ping CORE-02 from CORE-01 on both links
`ping 10.255.30.2, ping 10.255.30.6`



—-

Stage 2: Core-to-Distribution Layer 3 EtherChannels

ENTERPRISE TRANSIT / P2P LINKS – IP ASSIGNMENT TABLE

Device A	Physical Int	Port-Channel	IP Address	Device B	Physical Int	Port-Channel	IP Address	Subnet	Notes
CORE-01	Gi1/0/5	Po10	10.255.10.1	A-DIST-01	Gi1/0/5	Po10	10.255.10.2	10.255.10.0/30	Office A
CORE-02	Gi1/0/6	Po11	10.255.10.5	A-DIST-01	Gi1/0/6	Po11	10.255.10.6	10.255.10.4/30	Office A
CORE-01	Gi1/0/7	Po20	10.255.10.9	A-DIST-02	Gi1/0/7	Po20	10.255.10.10	10.255.10.8/30	Office A
CORE-02	Gi1/0/8	Po21	10.255.10.13	A-DIST-02	Gi1/0/8	Po21	10.255.10.14	10.255.10.12/30	Office A
CORE-02	Gi1/0/5	Po30	10.255.20.1	B-DIST-01	Gi1/0/5	Po30	10.255.20.2	10.255.20.0/30	Office B
CORE-01	Gi1/0/6	Po31	10.255.20.5	B-DIST-01	Gi1/0/6	Po31	10.255.20.6	10.255.20.4/30	Office B
CORE-02	Gi1/0/7	Po40	10.255.20.9	B-DIST-02	Gi1/0/7	Po40	10.255.20.10	10.255.20.8/30	Office B
CORE-01	Gi1/0/8	Po41	10.255.20.13	B-DIST-02	Gi1/0/8	Po41	10.255.20.14	10.255.20.12/30	Office B

CORE-TO-DISTRIBUTION ETHERCHANNELS CONFIGURATION:

- **CORE-01 to A-DIST-01/02 & B-DIST-01/02**

```
! 1. Assign physical interfaces to port-channel
interface g1/0/5
 description link to A-DIST-01
 no switchport
 channel-group 10 mode on
 no shutdown
 exit

! 2. Assign L3 IPs to port-channel interface
interface Port-channel10
 description L3 EChannel to A-DIST-01
 ip address 10.255.10.1 255.255.255.252
 no shutdown
 exit

--
interface g1/0/7
 description link to A-DIST-02
 no switchport
 channel-group 20 mode on
 no shutdown
 exit

interface Port-channel20
 description L3 EChannel to A-DIST-02
 ip address 10.255.10.9 255.255.255.252
 no shutdown
 exit

--
interface g1/0/6
 description link to B-DIST-01
 no switchport
 channel-group 31 mode on
 no shutdown
 exit

interface Port-channel31
 description L3 EChannel to B-DIST-01
 ip address 10.255.20.5 255.255.255.252
 no shutdown
 exit
--
interface g1/0/8
 description link to B-DIST-02
 no switchport
 channel-group 41 mode on
 no shutdown
 exit

interface Port-channel41
 description L3 EChannel to B-DIST-02
 ip address 10.255.20.13 255.255.255.252
 no shutdown
 exit
```

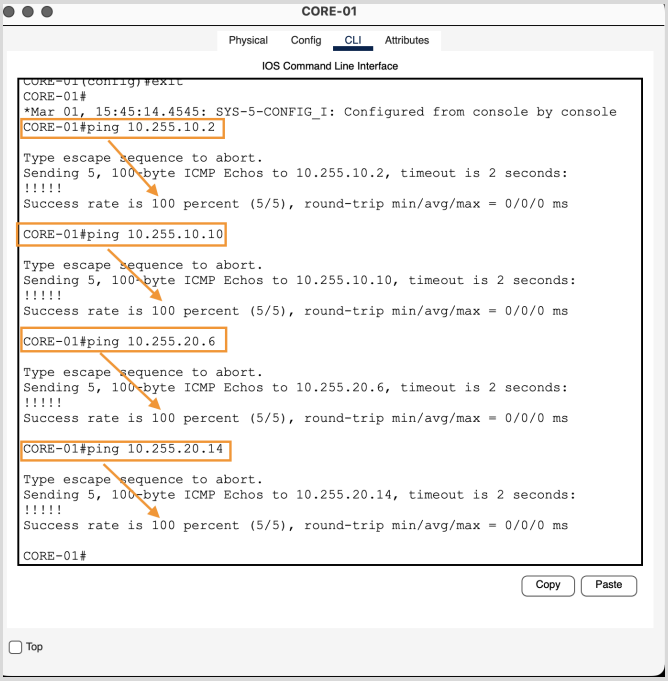
- **CORE-02 to to A-DIST-01/02 & B-DIST-01/02**

```
! 1. Assign physical interfaces to port-channels
interface range g1/0/6
 description link to A-DIST-01
 no switchport
 channel-group 11 mode on
 no shutdown
 exit

! 2. Assign L3 IPs to Port-Channel Interface
interface Port-channel11
 description L3 EChannel to A-DIST-01
 ip address 10.255.10.5 255.255.255.252
 no shutdown
 exit

--
interface range g1/0/8
 description link to A-DIST-02
 no switchport
 channel-group 21 mode on
 no shutdown
 exit

interface Port-channe21
 description L3 EChannel to A-DIST-02
 ip address 10.255.10.13 255.255.255.252
 no shutdown
 exit

--
interface range g1/0/5
 description link to B-DIST-01
 no switchport
 channel-group 30 mode on
 no shutdown
 exit

interface Port-channel30
 description L3 EChannel to B-DIST-01
 ip address 10.255.20.1 255.255.255.252
 no shutdown
 exit

--
interface range g1/0/7
 description link to B-DIST-02
 no switchport
 channel-group 40 mode on
 no shutdown
 exit

interface Port-channel40
 description L3 EChannel to B-DIST-02
 ip address 10.255.20.9 255.255.255.252
 no shutdown
 exit
```

Verification:

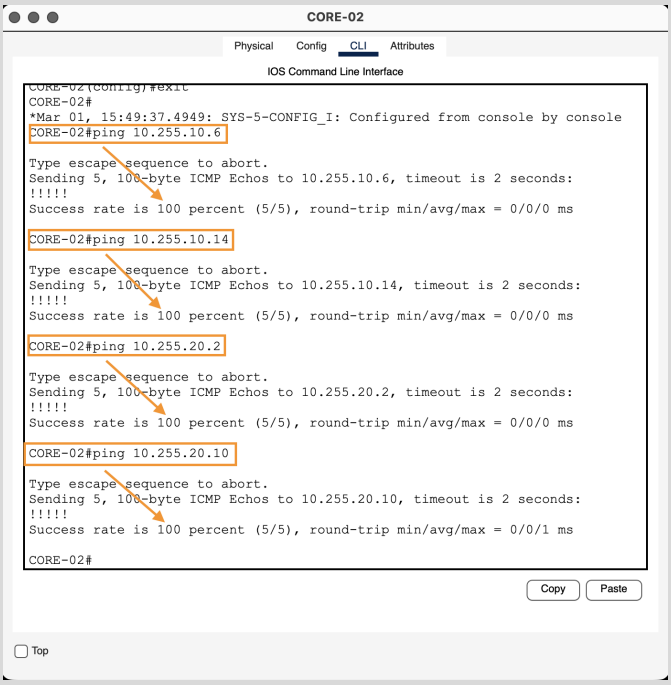
Ping A-DIST-01, A-DIST-02, B-DIST-01, B-DIST-02 from CORE-01

`ping 10.255.10.2` (A-DIST--01)
`ping 10.255.10.10` (A-DIST-02)
`ping 10.255.20.6` (B-DIST--01)
`ping 10.255.20.14` (B-DIST-02)



Ping A-DIST-01, A-DIST-02, B-DIST-01, B-DIST-02 from CORE-02

`ping 10.255.10.6` (A-DIST--01)
`ping 10.255.10.14` (A-DIST-02)
`ping 10.255.20.2` (B-DIST--01)
`ping 10.255.20.10` (B-DIST-02)



—-

Stage 3: Core-to-Edge Transit Links

EDGE TRANSIT LINKS TABLE

Link	Device A	Interface A	IP A	Device B	Interface B	IP B	Subnet	Type	Purpose
CORE-01 ↔ EDGE-01	CORE-01	Gi1/0/10	10.255.31.1	EDGE-01	Gi0/0/0	10.255.31.2	/30	L3 Transit	Primary edge path
CORE-02 ↔ EDGE-01	CORE-02	Gi1/0/11	10.255.31.5	EDGE-01	Gi0/0/1	10.255.31.6	/30	L3 Transit	Backup edge path

CORE-TO-EDGE TRANSIT LINKS CONFIGURATION:

- **CORE-01 to EDGE-01**

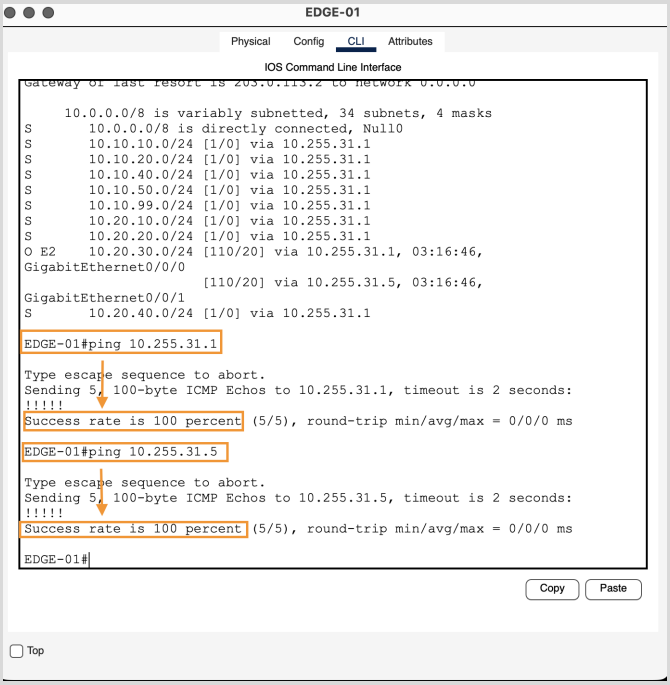
```
interface Gi1/0/10
 description L3 P2P to EDGE-01
 ip address 10.255.31.1 255.255.255.252
 no shutdown
 exit
```

- **CORE-02 to EDGE-01**

```
interface Gi1/0/11
 description L3 P2P to EDGE-01
 ip address 10.255.31.5 255.255.255.252
 no shutdown
 exit
```

Verification:
Ping CORE-01 & CORE-02 from EDGE-01

```
ping 10.255.31.1
ping 10.255.31.5
```



—

Stage 4: Loopback Interfaces and OSPF

LOOPBACK INTERFACE ADDRESSING (Router ID Allocation) TABLE

Device	Loopback Interface	IP Address	Purpose / Notes
CORE-01	Loopback0	10.255.255.1	OSPF Router ID, management
CORE-02	Loopback0	10.255.255.2	OSPF Router ID, management
A-DIST-01	Loopback0	10.255.255.11	OSPF Router ID
A-DIST-02	Loopback0	10.255.255.12	OSPF Router ID
B-DIST-01	Loopback0	10.255.255.21	OSPF Router ID
B-DIST-02	Loopback0	10.255.255.22	OSPF Router ID
EDGE-01	Loopback0	10.255.255.254	OSPF Router ID / management

LOOPBACK INTERFACES & OSPF CONFIGURATION:

- **CORE-01**

```
! Assign Loopback for Management / OSPF Router ID
interface Loopback0
 ip address 10.255.255.1 255.255.255.255
 no shutdown

! Delete old OSPF process (delete configuration from previous lab)
no router ospf 10

! Create new OSPF process
router ospf 10

! Set router id
 router-id 10.255.255.1

! Advertise networks to neighbors in area 0
 network 10.255.10.0 0.0.0.255 area 0
 network 10.255.20.0 0.0.0.255 area 0
 network 10.255.30.0 0.0.0.255 area 0
 network 10.255.31.0 0.0.0.255 area 0

! Advertise loopback address
 network 10.255.255.1 0.0.0.0 area 0

! Set loopback to passive-interface
 passive-interface loopback0
 exit

! Configure CORE-01 to CORE-02 links as P2P
interface range gi1/0/1-2
 ip ospf network point-to-point
 exit

! Configure CORE-01 to DISTs P2P links as P2P
interface range gi1/0/5-8
 ip ospf network point-to-point
 exit
```

! Configure CORE-1 to EDGE-01 link as P2P
```
interface gi1/0/10
 ip ospf network point-to-point
 exit
```

! Save running-config to startup config
```
do write memory
```

- **CORE-02**

```
interface Loopback0
 ip address 10.255.255.2 255.255.255.255
 no shutdown
 exit

no router ospf 10

router ospf 10
 router-id 10.255.255.2

 network 10.255.10.0 0.0.0.255 area 0
 network 10.255.20.0 0.0.0.255 area 0
 network 10.255.30.0 0.0.0.255 area 0
 network 10.255.31.0 0.0.0.255 area 0

 network 10.255.255.2 0.0.0.0 area 0
 passive-interface loopback0
 exit

interface range gi1/0/1-2
 ip ospf network point-to-point
 exit

interface range gi1/0/5-8
 ip ospf network point-to-point
 exit

interface gi1/0/11
 ip ospf network point-to-point
 exit
```

- **A-DIST-01**

```
interface Loopback0
 ip address 10.255.255.11 255.255.255.255
 no shutdown
 exit

no router ospf 10
router ospf 10
 router-id 10.255.255.11

 network 10.255.10.0 0.0.0.255 area 0

 network 10.255.255.11 0.0.0.0 area 0
 passive-interface loopback0
 exit

interface range g1/0/5-6
 ip ospf network point-to-point
 exit
```

- **A-DIST-02**

```
interface Loopback0
 ip address 10.255.255.12 255.255.255.255
 no shutdown
 exit

no router ospf 10

router ospf 10
 router-id 10.255.255.12

 network 10.255.10.0 0.0.0.255 area 0

 network 10.255.255.12 0.0.0.0 area 0
 passive-interface loopback0
 exit

interface range g1/0/7-8
 ip ospf network point-to-point
 exit
```

- **B-DIST-01**

```
interface Loopback0
 ip address 10.255.255.21 255.255.255.255
 no shutdown
 exit

no router ospf 10

router ospf 10
 router-id 10.255.255.21

 network 10.255.20.0 0.0.0.255 area 0

 network 10.255.255.21 0.0.0.0 area 0
 passive-interface loopback0
 exit

interface range g1/0/5-6
 ip ospf network point-to-point
 exit
```

- **B-DIST-02**

```
interface Loopback0
 ip address 10.255.255.22 255.255.255.255
 no shutdown
 exit

no router ospf 10

router ospf 10
 router-id 10.255.255.22

 network 10.255.20.0 0.0.0.255 area 0

 network 10.255.255.22 0.0.0.0 area 0
 passive-interface loopback0
 exit
```

```
interface range g1/0/7-8
 ip ospf network point-to-point
 exit
```

- **EDGE-01**

ip routing

```
interface Loopback0
 ip address 10.255.255.254 255.255.255.255
 no shutdown
 exit
```

! Default Route toward ISP

```
ip route 0.0.0.0 0.0.0.0 203.0.113.2
ip route 0.0.0.0 0.0.0.0 203.0.113.6 5     ! Floating static route (backup)

no router ospf 10

router ospf 10
 router-id 10.255.255.254

 network 10.255.31.0 0.0.0.255 area 0
 network 10.255.255.254 0.0.0.0 area 0
 passive-interface loopback0
 exit

interface range gi0/0/0-1
 ip ospf network point-to-point
 exit
```

! Advertise default route

```
router ospf 10
 default-information originate
 exit
```

———

8.2 Phase 2 — Campus Fabric Deployment

Purpose: Build a resilient switching architecture before introducing gateways.

- **Implementation Stages:**

    1. **Distribution Interconnects** – EtherChannels were configured between distribution switches to support redundancy and load balancing. (LACP in Office A, PAgP in Office B.)

    2. **Distribution < – > Access Trunking** – Redundant 802.1Q trunk links were established from each access switch to both distribution switches.

    3. **VLAN Deployment** – Enterprise VLANs were provisioned to segment user, voice, wireless, server, and management traffic. (VTP domains: OfficeA, Office B))

    4. **Spanning Tree Optimization** – Rapid PVST+ was tuned with the distribution layer acting as the root bridge to stabilize Layer 2 convergence.

—-

Stage 1: Distribution Interconnects (LACP / PaGP)

LACP L2-EtherChannel (IEEE 802.3ad)

- Aggregate parallel trunk links between distribution switches using LACP for redundancy and higher bandwidth.
- Port-Channels configured as trunks, carrying VLANs 10, 20, 40, 50, and 99.
- Native VLAN is 99 for management.

OFFICE A:

- **A-DIST-01 (set to active):**

```
! L2 EtherChannel A-DSW-01to A-DIST-02 (LACP)
interface range gigabitEthernet1/0/3 - 4
 description L2-channel Po1 member
 channel-group 1 mode active
 exit

! Configure Port-Channel interface for DSW channel
interface po1
 description L2-channel to A-DIST-02 (LACP)
 sw mode trunk
 sw trunk native vlan 99
 sw trunk allowed vlan 10,20,40,50,99
 sw nonegotiate
 exit
```

- **A-DIST-02 (set to active or passive):**

```
interface range gigabitEthernet1/0/3 - 4
 description L2-channel Po1 member
 channel-group 1 mode active
 exit

interface po1
 description L2-channel to A-DIST-01 (LACP)
 sw mode trunk
 sw trunk native vlan 99
 sw trunk allowed vlan 10,20,40,50,99
 sw nonegotiate
 exit
```

(PaGP L2-EtherChannel - Cisco Proprietary)

- Aggregate parallel trunk links between distribution switches using PaGP for redundancy and higher bandwidth.
- Port-Channels configured as trunks, carrying VLANs 30, 40, 50, 99, and 100.
- Native VLAN is 99 for management.

OFFICE B:

- **B-DIST-01 (set to desirable):**

```
interface range gigabitEthernet1/0/3 - 4
 description L2-channel Po1 member
 channel-group 1 mode desirable
 no shutdown
 exit
```

```
interface port-channel 1
 description L2-channel to B-DIST-02 (PaGP)
 switchport mode trunk
 switchport trunk native vlan 99
 switchport trunk allowed vlan 30,40,50,99,100
 switchport nonegotiate
 exit
```

- **B-DIST-02 (set to auto or desirable):**

```
interface range gigabitEthernet1/0/3 - 4
 description L2-channel Po1 member
 channel-group 1 mode desirable
 no shut
 exit

interface port-channel 1
 description L2-channel to B-DIST-01 (PaGP)
 switchport mode trunk
 switchport trunk native vlan 99
 switchport trunk allowed vlan 30,40,50,99,100
 switchport nonegotiate
 exit
```

—-

Stage 2: Distribution < – > Access Trunking

- Separates management traffic from user and voice VLANs, improving security and control.
- Ensures trunk negotiation and untagged traffic are handled consistently across switches.
- Simplifies network management, as all switches use the same native VLAN (VLAN 99) for infrastructure

OFFICE A Distribution Switches:

- **A-DIST-01 → A-ACC-01/02/03 Trunk Links**

```
! Trunks to access switches
interface range gi1/0/1-2, g1/0/7
 description Trunk to A-ACC-01/02/03
 switchport mode trunk
 switchport trunk allowed vlan 10,20,40,50,99
 switchport trunk native vlan 99

 no shutdown
 exit
```

- **A-DIST-02 → A-ACC-01/02/03 Trunk Links**

```
interface range gi1/0/1-2, g1/0/5
 description Trunk to A-ACC-01/02/03
 switchport mode trunk
 switchport trunk allowed vlan 10,20,40,50,99
 switchport trunk native vlan 99

 no shutdown
 exit
```

OFFICE A Access Switches:

- **A-ACC-01 (Sales)**

```
interface gi0/1
 description Trunk to A-DSW-01
 switchport mode trunk
 switchport trunk allowed vlan 10,20,40,50,99
 switchport trunk native vlan 99
 no shutdown
 exit

interface gi0/2
 description Trunk to A-DSW-02
 switchport mode trunk
 switchport trunk allowed vlan 10,20,40,50,99
 switchport trunk native vlan 99

 no shutdown
 exit
```

- **A-ACC-02 (Marketing)**

```
interface gi0/1
 description Trunk to A-DSW-02
 switchport mode trunk
 switchport trunk allowed vlan 10,20,40,50,99
 switchport trunk native vlan 99

 no shutdown
 exit

interface gi0/2
 description Trunk to A-DSW-01
 switchport mode trunk
 switchport trunk allowed vlan 10,20,40,50,99
 switchport trunk native vlan 99

 no shutdown
 exit
```

- **A-ACC-03 (Wi-Fi)**

```
interface gi7/1
 description Trunk to A-DSW-01
 switchport mode trunk
 switchport trunk allowed vlan 10,20,40,50,99
 switchport trunk native vlan 99

 no shutdown
 exit

interface gi5/1
 description Trunk to A-DSW-02
 switchport mode trunk
 switchport trunk allowed vlan 10,20,40,50,99
 switchport trunk native vlan 99

 no shutdown
 exit
```

OFFICE B Distribution Switches:

- **B-DSW-01 → B-ACC-01/02/03 Trunk Links**

```
interface range gi1/0/1-2, g1/0/7
 description Trunk to B-ACC-01/02/03
 switchport mode trunk
 switchport trunk allowed vlan 30,40,50,99,100
 switchport trunk native vlan 99

 no shutdown
 exit
```

- **B-DSW-02 → B-ACC-01/02/03 Trunk Links**

```
interface range gi1/0/1-2, g1/0/5
 description Trunk to B-ACC-01/02/03
 switchport mode trunk
 switchport trunk allowed vlan 30,40,50,99,100
 switchport trunk native vlan 99

 no shutdown
 exit
```

OFFICE B Access Switches:

- **B-ACC-01 (IT)**

```
interface gi0/1
 description Trunk to B-DSW-01
 switchport mode trunk
 switchport trunk allowed vlan 30,40,50,99,100
 switchport trunk native vlan 99

 no shutdown
 exit

interface gi0/2
 description Trunk to B-DSW-02
 switchport mode trunk
 switchport trunk allowed vlan 30,40,50,99,100
 switchport trunk native vlan 99

 no shutdown
 exit
```

- **B-ACC-02 (Servers)**

```
interface gi0/1
 description Trunk to B-DSW-02
 switchport mode trunk
 switchport trunk allowed vlan 30,40,50,99,100
 switchport trunk native vlan 99

 no shutdown
 exit

interface gi0/2
 description Trunk to B-DSW-01
 switchport mode trunk
```

```
 switchport trunk allowed vlan 30,40,50,99,100
 switchport trunk native vlan 99

 no shutdown
 exit
```

- **B-ACC-03 (Wi-Fi)**

```
interface gi5/1
 description Trunk to B-DSW-02
 switchport mode trunk
 switchport trunk allowed vlan 30,40,50,99,100
 switchport trunk native vlan 99

 no shutdown
 exit

interface gi7/1
 description Trunk to B-DSW-01
 switchport mode trunk
 switchport trunk allowed vlan 30,40,50,99,100
 switchport trunk native vlan 99

 no shutdown
 exit
```

—-

Stage 3: VLAN Deployment (VTP)

- VTP propagates VLAN configuration across all switches in the same VTP domain.
- Reduces manual VLAN configuration on each switch, simplifying network management.
- Operates only on trunk links, not access ports.

VLAN DEPLOYMENT CONFIGURATION

OFFICE A:

- **A-DIST-02, A-ACC-01, A-ACC-02 (VTP Clients):**

```
! Configure vtp domain
vtp domain OfficeA

! Configure version
vtp version 2

! Configure Switch as VTP Clients
vtp mode client
```

- **A-DIST-01 (VTP Server):**

```
! Configure domain
vtp domain OfficeA
vtp version 2
vtp mode server

! Create VLANs
vlan 10
 name A-Sales
 exit
vlan 20
 name A-Marketing
 exit
```

```
vlan 40
 name Phones
 exit
vlan 50
 name Wifi
 exit
vlan 99
 name Net-Mgmt
 exit
```

OFFICE B:

- **B-DIST-02, B-ACC-01, B-ACC-02 (VTP Clients):**

```
vtp domain OfficeB
vtp version 2
vtp mode client
```

- **B-DIST-1 (VTP server OFFICE_B: default)**

```
domain OfficeB
vtp version 2
vtp mode server

vlan 30
 name B-IT
 exit
vlan 40
 name Phones
 exit
vlan 50
 name Wifi
 exit
vlan 99
 name Net-Mgmt
 exit
vlan 100
 name B-Servers
 exit
```

—-

Stage 4: Spanning Tree Optimization (Rapid PVST+)

- Rapid PVST Implementation: Enabled rapid-pvst mode on all distribution and access switches to provide fast convergence and minimize network downtime during topology changes.
- PortFast for End Devices: Configured PortFast on interfaces connecting PCs, wireless controllers, and access points to allow immediate transition to forwarding state, reducing boot-up and connection delays.
- BPDU Guard for Access Ports: Enabled BPDU Guard on all PortFast-enabled interfaces to protect the network from accidental or malicious spanning-tree loops caused by unauthorized device connections.
- Targeted Device Application: Applied to all ACCs in both offices, including PCs (A-ACC-01/02, B-ACC-01/02) and wireless devices (A-ACC-03, A-WLC-01, A-LWAP-01, B-LWAP-01), ensuring consistent network protection and stability.

- **All Distribution (DST) & Access (ACC) Switches**

```
! Enable Rapid PVST mode
spanning-tree mode rapid-pvst
```

- A-ACC-01 & 02 / B-ACC-01 & 02 (PCs)

! Enable PortFast + BPDU Guard on end-device facing ports

```
interface range Fa0/1 - 24
  spanning-tree portfast
  spanning-tree bpduguard enable
```

- A-ACC-03 (A-WLC-01 & A-LWAP-01)

```
interface range g0/1, g1/1
  spanning-tree portfast
  spanning-tree bpduguard enable
```

- B-ACC-01 (B-LWAP-01)

interface g0/1

```
  spanning-tree portfast
  spanning-tree bpduguard enable
```

———

8.3 **Phase 3 — Inter-VLAN Routing & Gateway Services**

Purpose: Turn the distribution layer into the campus routing boundary.

- **Implementation Stages:**

1. **Switch Virtual Interface (SVI) Configuration** – SVIs were deployed on distribution switches to enable inter-VLAN routing.

2. **First-Hop Redundancy (HSRP) & STP Root Priority Alignment** – HSRP virtual gateways were implemented on distribution switches to ensure continuous default gateway availability for endpoints. STP root priority was aligned with HSRP active roles to maintain predictable Layer 2 forwarding paths, optimize traffic flow, and minimize convergence during failover events.

3. **OSPF VLAN Advertisement & Summarization** – VLAN networks were summarized at the distribution layer and advertised into Area 0, eliminating the need for redistributed static routes.

—-

Stage 1: Switch Virtual Interface (SVI)

- IP addressing follows a site-based hierarchy (10.10.0.0/16 for Office A and 10.20.0.0/16 for Office B), making subnet identification intuitive and supporting efficient route summarization.
- Gateway addresses are standardized across VLANs to maintain predictable default gateway patterns, simplifying troubleshooting and operational support.
- Infrastructure devices (distribution switches, wireless controllers, and critical network services) use static IP assignments to ensure stability and consistent reachability.
- The addressing model is designed with scalability in mind, allowing additional VLANs or departments to be introduced without requiring major readdressing.

SWITCH VIRTUAL INTERFACE (SVI) ASSIGNMENT TABLE

Device	Role	Office	VLAN / Interface	SVI IP Address	Notes
A-DIST-01	Distribution L3	A	VLAN 10	10.10.10.2/24	SVI for inter-VLAN routing
A-DIST-01	Distribution L3	A	VLAN 20	10.10.20.2/24	SVI for inter-VLAN routing
A-DIST-01	Distribution L3	A	VLAN 50	10.10.50.2/24	SVI for inter-VLAN routing
A-DIST-01	Distribution L3	A	VLAN 99	10.10.99.2/24	SVI for management
A-DIST-02	Distribution L3	A	VLAN 10	10.10.10.3/24	SVI for inter-VLAN routing
A-DIST-02	Distribution L3	A	VLAN 20	10.10.20.3/24	SVI for inter-VLAN routing
A-DIST-02	Distribution L3	A	VLAN 50	10.10.50.3/24	SVI for inter-VLAN routing
A-DIST-02	Distribution L3	A	VLAN 99	10.10.99.3/24	SVI for management
B-DIST-01	Distribution L3	B	VLAN 30	10.20.30.2/24	SVI for inter-VLAN routing
B-DIST-01	Distribution L3	B	VLAN 40	10.20.40.2/24	SVI for inter-VLAN routing
B-DIST-01	Distribution L3	B	VLAN 50	10.20.50.2/24	SVI for inter-VLAN routing
B-DIST-01	Distribution L3	B	VLAN 99	10.20.99.2/24	SVI for management
B-DIST-02	Distribution L3	B	VLAN 30	10.20.30.3/24	SVI for inter-VLAN routing
B-DIST-02	Distribution L3	B	VLAN 40	10.20.40.3/24	SVI for inter-VLAN routing
B-DIST-02	Distribution L3	B	VLAN 50	10.20.50.3/24	SVI for inter-VLAN routing
B-DIST-02	Distribution L3	B	VLAN 99	10.20.99.3/24	SVI for management
A-ACC-01/02/03	Access L2	A	VLAN 99	10.10.99.11–13/24	Management VLAN for ACCs
B-ACC-01/02/03	Access L2	B	VLAN 99	10.20.99.11–13/24	Management VLAN for ACCs

Office A – Distribution Switches:

- **A-DIST-01**

```
! VLAN 10 - A-Sales
interface vlan 10
 description A-Sales
 ip address 10.10.10.2 255.255.255.0
 no shutdown
exit

! VLAN 20 - A-Marketing
interface vlan 20
 description A-Marketing
 ip address 10.10.20.2 255.255.255.0
 no shutdown
exit

! VLAN 40 – A-Phones
interface vlan 40
 description A-Phones
 ip address 10.10.40.2 255.255.255.0
 no shutdown
exit
```

```
! VLAN 50 – A-Wi-Fi
interface vlan 50
description A-Wifi
ip address 10.10.50.2 255.255.255.0
 no shutdown
exit

! VLAN 99 – A-Net-Mgmt
interface vlan 99
description A-Net-Mgmt
 ip address 10.10.99.2 255.255.255.0
 no shutdown
exit
```

- **A-DIST-02**

```
interface vlan 10
 description A-Sales
 ip address 10.10.10.3 255.255.255.0
 no shutdown
exit

interface vlan 20
description A-Marketing
 ip address 10.10.20.3 255.255.255.0
 no shutdown
exit

interface vlan 40
description A-Phones
 ip address 10.10.40.3 255.255.255.0
 no shutdown
exit

interface vlan 50
description A-Wifi
 ip address 10.10.50.3 255.255.255.0
 no shutdown
exit

interface vlan 99
description A-Net-Mgmt
 ip address 10.10.99.3 255.255.255.0
 no shutdown
exit
```

Office A – Access Switches

- **A-ACC-01**

```
interface vlan 10
description A-Sales
 ip address 10.10.10.11 255.255.255.0
 no shutdown
exit

interface vlan 20
description A-Marketing
 ip address 10.10.20.11 255.255.255.0
 no shutdown
exit
```

```
interface vlan 40
description A-Phones
 ip address 10.10.40.11 255.255.255.0
 no shutdown
exit

interface vlan 50
description A-Wifi
 ip address 10.10.50.11 255.255.255.0
 no shutdown
exit

interface vlan 99
 ip address 10.10.99.11 255.255.255.0
description A-Net-Mgmt
 no shutdown
exit
```

- **A-ACC-02**

```
interface vlan 10
 description A-Sales
 ip address 10.10.10.12 255.255.255.0
 no shutdown
 exit

interface vlan 20
 description A-Marketing
 ip address 10.10.20.12 255.255.255.0
 no shutdown
 exit

interface vlan 40
 description A-Phones
 ip address 10.10.40.12 255.255.255.0
 no shutdown
 exit

interface vlan 50
 description A-Wifi
 ip address 10.10.50.12 255.255.255.0
 no shutdown
 exit

interface vlan 99
 description A-Net-Mgmt
 ip address 10.10.99.12 255.255.255.0
 no shutdown
 exit
```

- **A-ACC-03 (Wi-Fi)**

```
interface vlan 10
 description A-Sales
 ip address 10.10.10.13 255.255.255.0
 no shutdown
 exit
```

```
interface vlan 20
 description A-Marketing
 ip address 10.10.20.13 255.255.255.0
 no shutdown
 exit

interface vlan 40
 description A-Phones
 ip address 10.10.40.13 255.255.255.0
 no shutdown
 exit

interface vlan 50
 description A-Wifi
 ip address 10.10.50.13 255.255.255.0
 no shutdown
 exit

interface vlan 99
 description A-Net-Mgmt
 ip address 10.10.99.13 255.255.255.0
 no shutdown
 exit
```

Office B – Distribution Switches

- **B-DIST-01**

```
! VLAN 30 - B-IT
interface vlan 30
 description B-IT
 ip address 10.20.30.2 255.255.255.0
 no shutdown
 exit

interface vlan 40
 description B-Phones
 ip address 10.20.40.2 255.255.255.0
 no shutdown
 exit

interface vlan 50
 description B-Wifi
 ip address 10.20.50.2 255.255.255.0
 no shutdown
 exit

interface vlan 99
 description B-Net-Mgmt
 ip address 10.20.99.2 255.255.255.0
 no shutdown
 exit

! VLAN 100 - B-Servers
interface vlan 100
 description B-Servers
 ip address 10.20.100.2 255.255.255.0
 no shutdown
 exit
```

- **B-DIST-02**

```
interface vlan 30
 description B-IT
 ip address 10.20.30.3 255.255.255.0
 no shutdown
 exit

interface vlan 40
 description B-Phones
 ip address 10.20.40.3 255.255.255.0
 no shutdown
 exit

interface vlan 50
 description B-Wifi
 ip address 10.20.50.3 255.255.255.0
 no shutdown
 exit

interface vlan 99
 description B-Net-Mgmt
 ip address 10.20.99.3 255.255.255.0
 no shutdown
 exit

interface vlan 100
 description B-Servers
 ip address 10.20.100.3 255.255.255.0
 no shutdown
 exit
```

Office B – Access Switches

- **B-ACC-01**

```
interface vlan 30
 description B-IT
 ip address 10.20.30.11 255.255.255.0
 no shutdown
 exit

interface vlan 40
 description B-Phones
 ip address 10.20.40.11 255.255.255.0
 no shutdown
 exit

interface vlan 50
 description B-WiFi
 ip address 10.20.50.11 255.255.255.0
 no shutdown
 exit

interface vlan 99
 description B-Net-Mgmt
 ip address 10.20.99.11 255.255.255.0
 no shutdown
 exit
```

```
interface vlan 100
 description B-Servers
 ip address 10.20.100.11 255.255.255.0
 no shutdown
 exit
```

- **B-ACC-02**

```
interface vlan 30
 description B-IT Users
 ip address 10.20.30.12 255.255.255.0
 no shutdown
 exit

interface vlan 40
 description B-Phones
 ip address 10.20.40.12 255.255.255.0
 no shutdown
 exit

interface vlan 50
 description B-WiFi
 ip address 10.20.50.12 255.255.255.0
 no shutdown
 exit

interface vlan 99
 description B-Net-Mgmt
 ip address 10.20.99.12 255.255.255.0
 no shutdown
 exit

interface vlan 100
 description B-Servers
 ip address 10.20.100.12 255.255.255.0
 no shutdown
 exit
```

- **B-ACC-03 (Wi-Fi)**

```
interface vlan 30
 description B-IT
 ip address 10.20.30.13 255.255.255.0
 no shutdown
 exit

interface vlan 40
 description B-Phones
 ip address 10.20.40.13 255.255.255.0
 no shutdown
 exit

interface vlan 50
 description B-WiFi
 ip address 10.20.50.13 255.255.255.0
 no shutdown
 exit

interface vlan 99
 description B-Net-Mgmt
 ip address 10.20.99.13 255.255.255.0
 no shutdown
```

```
 exit

interface vlan 100
 description B-Servers
 ip address 10.20.100.13 255.255.255.0
 no shutdown
 exit
```

—-

Stage 2: First-Hop Redundancy (HSRP) & STP Root Priority Alignment

- Provides default gateway redundancy for hosts in a VLAN.
- Allows two or more routers/switches to share a single virtual IP address (VIP).
- Ensures high availability: if the active device fails, the standby device automatically takes over.
- Aligns STP root bridge priority with HSRP active roles to maintain optimal traffic paths and prevent suboptimal Layer 2 forwarding.
- Implements load balancing by distributing active HSRP roles across distribution switches, ensuring user VLANs utilize both devices for gateway processing and improving overall network efficiency.

Default Gateway Strategy:

- The HSRP Virtual IP (VIP) will always use the .1 address in each VLAN subnet.

Office A HSRP Design Rules:

- A-DIST-01 = Active for VLAN 10 / VLAN 20
- A-DIST-02 = Active for VLAN 40 / VLAN 50 / VLAN 99

Office B HSRP Design Rules:

- B-DIST-01 = Active for VLAN 30 / VLAN 100
- B-DIST-02 = Active for VLAN 40 / VLAN 50 / VLAN 99

FIRST-HOP REDUNDANCY (HSRP) GATEWAY ASSIGNMENTS TABLE

Device	Role	Office	VLAN / Interface	IP Address	HSRP VIP	HSRP Role	Notes
A-DIST-01	Distribution L3	A	VLAN 10	10.10.10.2/24	10.10.10.1	Active	HSRP Active for VLAN 10/20
A-DIST-01	Distribution L3	A	VLAN 20	10.10.20.2/24	10.10.20.1	Active	HSRP Active for VLAN 10/20
A-DIST-01	Distribution L3	A	VLAN 50	10.10.50.2/24	10.10.50.1	Standby	HSRP Backup for VLAN 50/99
A-DIST-01	Distribution L3	A	VLAN 99	10.10.99.2/24	10.10.99.1	Standby	HSRP Backup for Management VLAN
A-DIST-02	Distribution L3	A	VLAN 10	10.10.10.3/24	10.10.10.1	Standby	HSRP Backup for VLAN 10/20
A-DIST-02	Distribution L3	A	VLAN 20	10.10.20.3/24	10.10.20.1	Standby	HSRP Backup for VLAN 10/20
A-DIST-02	Distribution L3	A	VLAN 50	10.10.50.3/24	10.10.50.1	Active	HSRP Active for VLAN 50/99
A-DIST-02	Distribution L3	A	VLAN 99	10.10.99.3/24	10.10.99.1	Active	HSRP Active for Management VLAN
B-DIST-01	Distribution L3	B	VLAN 30	10.20.30.2/24	10.20.30.1	Standby	HSRP Backup for VLAN 30/40
B-DIST-01	Distribution L3	B	VLAN 40	10.20.40.2/24	10.20.40.1	Standby	HSRP Backup for VLAN 30/40
B-DIST-01	Distribution L3	B	VLAN 50	10.20.50.2/24	10.20.50.1	Standby	HSRP Backup for VLAN 50/99
B-DIST-01	Distribution L3	B	VLAN 99	10.20.99.2/24	10.20.99.1	Standby	HSRP Backup for Management VLAN
B-DIST-02	Distribution L3	B	VLAN 30	10.20.30.3/24	10.20.30.1	Active	HSRP Active for VLAN 30/40
B-DIST-02	Distribution L3	B	VLAN 40	10.20.40.3/24	10.20.40.1	Active	HSRP Active for VLAN 30/40
B-DIST-02	Distribution L3	B	VLAN 50	10.20.50.3/24	10.20.50.1	Active	HSRP Active for VLAN 50/99
B-DIST-02	Distribution L3	B	VLAN 99	10.20.99.3/24	10.20.99.1	Active	HSRP Active for Management VLAN
A-ACC-01/02/03	Access L2	A	VLAN 99	10.10.99.11–13/24	10.10.99.1	n/a	Management VLAN for ACC switches
B-ACC-01/02/03	Access L2	B	VLAN 99	10.20.99.11–13/24	10.20.99.1	n/a	Management VLAN for ACC switches

Note: HSRP uses priority values to determine the Active router. Higher = more preferred. Default is 100. Preemption is enabled with standby <group> preempt.

HSRP & STP ROOT PRIORITY ALIGNMENT CONFIGURATION

OFFICE A:

HSRP Design Rules:

- A-DIST-01 = Active for VLAN 10 / VLAN 20
- A-DIST-02 = Active for VLAN 40 / VLAN 50 / VLAN 99

- **A-DIST-01**

```
!Enable IP routing
ip routing

! VLAN 10 — A-SALES (ACTIVE)
interface vlan 10

 ! Set HSRP version 2
 standby version 2

 ! Configure VIP IP address
 standby 10 ip 10.10.10.1

 ! Configure A-DIST-01 as Active
 standby 10 priority 110

 ! Set A-DIST-01 as Active after failure
 standby 10 preempt

 no shutdown
 exit

! VLAN 20 — A-MKTG (ACTIVE)
interface vlan 20
 standby version 2
 standby 20 ip 10.10.20.1
 standby 20 priority 110
 standby 20 preempt
 no shutdown
 exit

! VLAN 40 — PHONES (STANDBY)
interface vlan 40
 standby version 2
 standby 40 ip 10.10.40.1
 standby 40 priority 100
 no shutdown
 exit

! VLAN 50 — WIFI (STANDBY)
interface vlan 50
 standby version 2
 standby 50 ip 10.10.50.1
 standby 50 priority 100
 no shutdown
 exit
```

! VLAN 99 — Net-MGMT (STANDBY)
```
interface vlan 99
  standby version 2
 standby 99 ip 10.10.99.1
 standby 99 priority 100
 no shutdown
 exit
```

STP Alignment on A-DIST-01 (using Primary Root Designation)

!Align HSRP active with STP root for each VLAN:
```
spanning-tree vlan 10 root primary
spanning-tree vlan 20 root primary

spanning-tree vlan 40 root secondary
spanning-tree vlan 50 root secondary
spanning-tree vlan 99 root secondary
```

- **A-DIST-02**

! Enable IP routing
```
ip routing
```

! VLAN 10 — SALES (STANDBY)
```
interface vlan 10
 standby version 2
 standby 10 ip 10.10.10.1
 standby 10 priority 100
 no shutdown
 exit
```

! VLAN 20 — Net-MKTG (STANDBY)
```
interface vlan 20
 standby version 2
 standby 20 ip 10.10.20.1
 standby 20 priority 100
 no shutdown
 exit
```

! VLAN 40 — PHONES (ACTIVE)
```
interface vlan 40
  standby version 2
  standby 40 ip 10.10.40.1
 standby 40 priority 110
 standby 40 preempt
 no shutdown
 exit
```

! VLAN 50 — WIFI (ACTIVE)
```
interface vlan 50
 standby version 2
 standby 50 ip 10.10.50.1
 standby 50 priority 110
 standby 50 preempt
 no shutdown
 exit
```

```
! VLAN 99 — Net-MGMT (ACTIVE)
interface vlan 99
 standby version 2
 standby 99 ip 10.10.99.1
 standby 99 priority 110
 standby 99 preempt
 no shutdown
 exit
```

STP Alignment on A-DIST-02

```
spanning-tree vlan 10 root secondary
spanning-tree vlan 20 root secondary

spanning-tree vlan 40 root primary
spanning-tree vlan 50 root primary
spanning-tree vlan 99 root primary
```

OFFICE B:

HSRP Design Rules:

- B-DIST-01 = Active for VLAN 30 / VLAN 100
- B-DIST-02 = Active for VLAN 40 / VLAN 50 / VLAN 99

- **B-DIST-01**

```
ip  routing

! VLAN 30 — IT (ACTIVE)
interface vlan 30
 standby version 2
 standby 30 ip 10.20.30.1
 standby 30 priority 110
 standby 30 preempt
 no shutdown
 exit

! VLAN 100 — SERVERS (ACTIVE)
interface vlan 100
 standby version 2
 standby 100 ip 10.20.100.1
 standby 100 priority 110
 standby 100 preempt
 no shutdown
 exit

! VLAN 40 — PHONES (STANDBY)
interface vlan 40
 standby version 2
 standby 40 ip 10.20.40.1
 standby 40 priority 100
 no shutdown
 exit

! VLAN 50 — WIFI (STANDBY)
interface vlan 50
 standby version 2
 standby 50 ip 10.20.50.1
 standby 50 priority 100
 no shutdown
 exit
```

```
! VLAN 99 — Net-MGMT (STANDBY)
interface vlan 99
 standby version 2
 standby 99 ip 10.20.99.1
 standby 99 priority 100
 no shutdown
 exit
```

STP Alignment on B-DIST-01 (using Lower Bridge Priority Assignment)

```
spanning-tree vlan 30 priority 4096   ! Active = STP Root
spanning-tree vlan 100 priority 4096  ! Active = STP Root

spanning-tree vlan 40 priority 8192   ! Standby = STP Backup
spanning-tree vlan 50 priority 8192   ! Standby = STP Backup
spanning-tree vlan 99 priority 8192   ! Standby = STP Backup
```

- **B-DIST-02**

```
ip routing

! VLAN 30 — IT (STANDBY)
interface vlan 30
 standby version 2
 standby 30 ip 10.20.30.1
 standby 30 priority 100
 no shutdown
 exit

! VLAN 100 — SERVERS (STANDBY)
interface vlan 100
 standby version 2
 standby 100 ip 10.20.100.1
 standby 100 priority 100
 no shutdown
 exit

! VLAN 40 — PHONES (ACTIVE)
interface vlan 40
 standby version 2
 standby 40 ip 10.20.40.1
 standby 40 priority 110
 standby 40 preempt
 no shutdown
 exit

! VLAN 50 — WIFI (ACTIVE)
interface vlan 50
 standby version 2
 standby 50 ip 10.20.50.1
 standby 50 priority 110
 standby 50 preempt
 no shutdown
 exit
```

! VLAN 99 — MGMT (ACTIVE)
```
interface vlan 99
 standby version 2
 standby 99 ip 10.20.99.1
 standby 99 priority 110
 standby 99 preempt
 no shutdown
 exit
```

STP Alignment on B-DIST-02

```
spanning-tree vlan 30 priority 8192   ! Standby = STP Backup
spanning-tree vlan 100 priority 8192  ! Standby = STP Backup

spanning-tree vlan 40 priority 4096   ! Active = STP Root
spanning-tree vlan 50 priority 4096   ! Active = STP Root
spanning-tree vlan 99 priority 4096   ! Active = STP Root
```

—-

Stage 3: OSPF VLAN Advertisement & Summarization

- Aggregates all user, voice, Wi-Fi, and management VLANs into a single route to reduce routing table size.
- Provides efficient route advertisement while maintaining logical separation between sites.

VLAN NETWORK SUMMARIZATION – OSPF AREA 0

Office	Summary Network	Subnet Mask	Wildcard Mask	Advertised By
Office A	10.10.0.0	/16	0.0.255.255	A-DIST-01 / A-DIST-02
Office B	10.20.0.0	/16	0.0.255.255	B-DIST-01 / B-DIST-02

OSPF VLAN ADVERTISEMENT & SUMMARIZATION CONFIGURATION

Office A:

- **A-DIST-01**

! Router config mode
```
router ospf 10
```

! Summarize all Office A VLAN networks and advertise into OSPF Area 0
```
network 10.10.0.0 0.0.255.255 area 0
```

! Configure SVIs as passive to advertise networks without forming unnecessary adjacencies
```
passive-interface default
```

! Enable OSPF on Port-Channels to establish neighbor adjacencies
```
no passive-interface Port-channel10
no passive-interface Port-channel11
exit
```

- **A-DIST-02**

```
router ospf 10
 network 10.10.0.0 0.0.255.255 area 0
 passive-interface default
 no passive-interface Port-channel20
 no passive-interface Port-channel21
 exit
```

Office B:

- **B-DIST-01**

```
router ospf 10
 network 10.20.0.0 0.0.255.255 area 0
 passive-interface default
 no passive-interface Port-channel30
 no passive-interface Port-channel31
 exit
```

- **B-DIST-02**

```
router ospf 10
 network 10.20.0.0 0.0.255.255 area 0
 passive-interface default
 no passive-interface Port-channel40
 no passive-interface Port-channel41
 exit
```

—-

8.4 **Phase 4 — WAN Edge Deployment (PPP w/ CHAP Authentication)**

Purpose: Extend enterprise routing beyond the campus.

- **Implementation:**
    - **PPP Serial Connectivity –** Redundant PPP links were established between the edge router and the simulated ISP.
    - **CHAP Authentication** – Mutual authentication was implemented to secure WAN adjacencies.
    - **Default Route Propagation –** The edge router originated the default route into OSPF, enabling upstream reachability for internal networks.
    - **Deployment Summary:**
        - Redundant WAN links provide failover if the primary link goes down.
        - DCE side (R1) provides the clock for both primary and backup serial links.
        - HLDC provides framing and reliable data transmission over point-to-point serial links.

EDGE-01 & ISP (R2) IP ASSIGNMENT TABLE

Link	EDGE-01 Interface	EDGE IP	ISP Interface	EDGE-01 IP	Subnet	DCE/DTE
Primary	S0/0/0	203.0.113.1	S0/0/0	203.0.113.2	255.255.255.252	EDGE-01 = DCE
Backup	S0/0/1	203.0.113.5	S0/0/1	203.0.113.6	255.255.255.252	EDGE-01 = DCE

PPP W/ CHAP CONFIGURATION

- **EDGE-01 (DCE)**

```
! Create CHAP credentials (username must match neighbor's hostname)
username ISP password p@ss123                    ! R2_ISP hostname and password

! Configure interface
interface s0/1/0
 description Links to ISP (Primary)
 encapsulation ppp
 ppp authentication chap
 ip address 203.0.113.1 255.255.255.252
 clock rate 64000
 no shutdown
 exit

interface s0/1/1
 encapsulation ppp
 description Links to ISP (Backup)
 ppp authentication chap
 ip address 203.0.113.5 255.255.255.252
 clock rate 64000
 no shutdown
 exit
```

- **ISP (DTE)**

```
! Create CHAP credentials (username must match neighbor's hostname)
username EDGE-01 password p@ss123                ! R1 hostname and password

interface s0/1/0
 description Link to EDGE-01 (Primary)
 encapsulation ppp
 ppp authentication chap
 ip address 203.0.113.2 255.255.255.252
 no shutdown
 exit

interface s0/1/1
 description Link to EDGE-01 (Backup)
 encapsulation ppp
 ppp authentication chap
 ip address 203.0.113.6 255.255.255.252
 no shutdown
 exit

! Link 1 to be Primary Path
ip route 0.0.0.0 0.0.0.0 203.0.113.1             ! Link 1 (Primary)
ip route 0.0.0.0 0.0.0.0 203.0.113.5 5           ! Floating Static Route - AD set to 5 (Backup)
```

8.5 **Phase 5 — Access Layer & End Device Integration**

Purpose: Ensure proper VLAN segmentation and reliable endpoint connectivity at the access layer, enabling secure, organized, and efficient communication for all end devices.

- Traffic Segmentation: Data (PCs) and voice (IP phones) are placed in separate VLANs for security and QoS optimization.
- Voice VLAN Tagging: IP phones tag voice traffic using the configured voice VLAN, while connected PCs use the assigned data VLAN.
- Port-Level Clarity: Each access port is explicitly assigned VLAN membership to reduce misconfiguration and improve manageability.
- Edge Optimization: spanning-tree portfast is enabled on end-device ports to reduce convergence delay.

CONFIGURATION

Office A:

END DEVICE PORT CONNECTIONS TABLE

End Device	Connected To	Switch Port	VLAN	Notes
A-PH-01	A-ACC-01	Fa0/1	40 (A-Phones)	IP via DHCP
A-PC-01	A-PH-01	Fa0	10 (A-Sales)	
A-PH-02	A-ACC-02	Fa0/1	40 (A-Phones)	IP via DHCP
A-PC-02	A-PH-02	Fa0	20 (A-Marketing)	
A-WLC-01	A-ACC-03	Gi0/0	50 (Wi-Fi)	Static IP
A-LWAP-01	A-ACC-03	Gi1/1	50 (Wi-Fi)	Static IP

Note: Phones act as access devices for PCs, using voice VLAN for phones and data VLAN for PC.

- **A-ACC-01**

```
interface fa0/1
 description A-PH-01 Sales PC+PH
 switchport mode access
 switchport access vlan 10                    ! Data VLAN for PC
 switchport voice vlan 40                     ! Voice VLAN for phone
 spanning-tree portfast
 no shutdown
 exit
```

- **A-ACC-02**

```
interface fa0/1
 description A-PH-02 Mktg PC+PH
 switchport mode access
 switchport access vlan 20                    ! Data VLAN for PC
 switchport voice vlan 40                     ! Voice VLAN for phone
 spanning-tree portfast
 no shutdown
 exit
```

- **A-ACC-03**

```
interface gi1/1
 description A-WLC-01
 switchport mode access
 switchport access vlan 50                    ! Wifi VLAN
 spanning-tree portfast
 no shutdown
 exit

interface gi1/1
 description A-LWAP-01
 switchport mode access
 switchport access vlan 50                    ! Wifi VLAN
 spanning-tree portfast
 no shutdown
 exit
```

Office B

END DEVICE PORT CONNECTIONS TABLE

End Device	Connected To	Switch Port	VLAN	Notes
B-PH-01	B-ACC-01	Fa0/1	40 (B-Phones)	IP via DHCP
B-PC-01	B-PH-01	Fa0	30 (B-IT)	Connected through phone
B-SVR-01	B-ACC-02	Fa0/1	100 (B-Servers)	Static IP
Admin-L	WiFi	Wireless	99 (Admin/WiFi)	Static IP
B-LWAP-01	A-ACC-03	Gi0/1	50 (Wi-Fi)	Static IP

Note: Laptop is wireless — no physical switchport required.

- **B-ACC-01**

```
interface fa0/1
 description B-PH-01 IT PC+PH
 switchport mode access
 switchport access vlan 30
 switchport voice vlan 40
 spanning-tree portfast
 exit
```

- **B-ACC-02**

```
interface fa0/1
 description B-SVR-01
 switchport mode access
 switchport access vlan 100
 spanning-tree portfast
```

- **B-ACC-03**

```
interface gi0/1
 description B-LWAP-01
 switchport mode access
 switchport access vlan 50
 spanning-tree portfast
```

END-DEVICE STATIC IP ASSIGNMENT TABLE

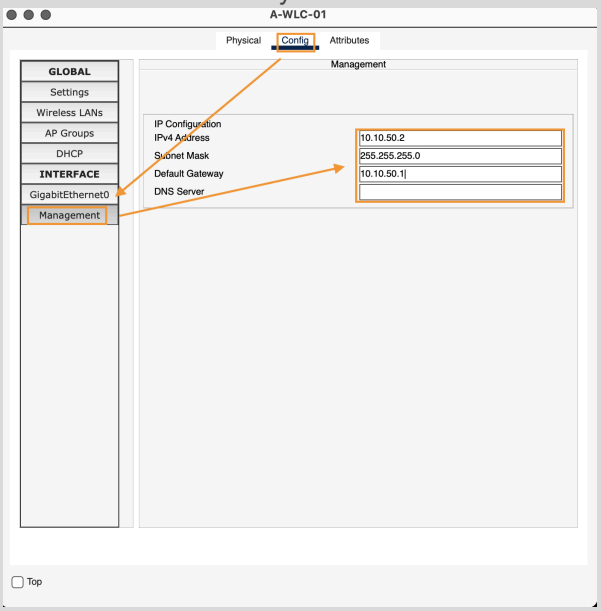
VLAN	VLAN Name	Device	IP Address	Default Gateway	Location / Notes	Excluded from DHCP
50	Wi-Fi	A-WLC-01	10.10.50.2	10.10.50.1	Office A (A-ACC-03)	Yes
99	Net-Mgmt	Admin-LT	10.10.99.2	10.10.99.1	Core / Dist / Access Switches	Yes
100	B-Servers	B-SRV-01	10.20.100.2	10.20.100.1	Office B (B-DIST)	Yes

Static IP Configuration on End-Devices:

A-WLC-01

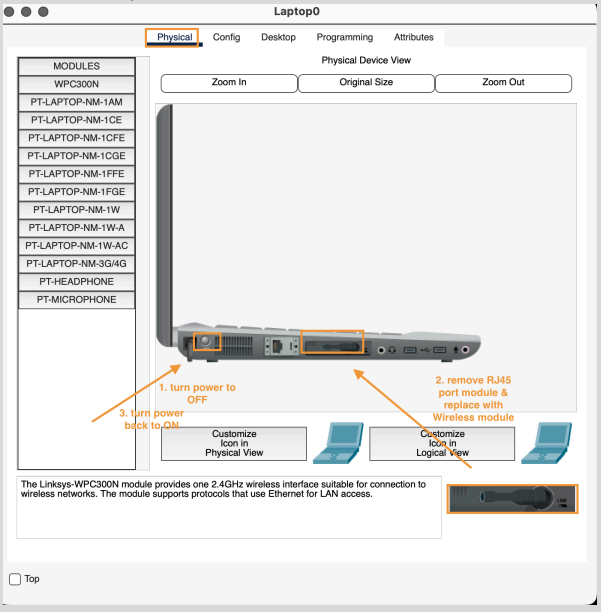
Navigate to Manage

IPv4 Address: 10.10.50.2
Subnet Mask: 255.255.255.0
Default Gateway: 10.10.50.1

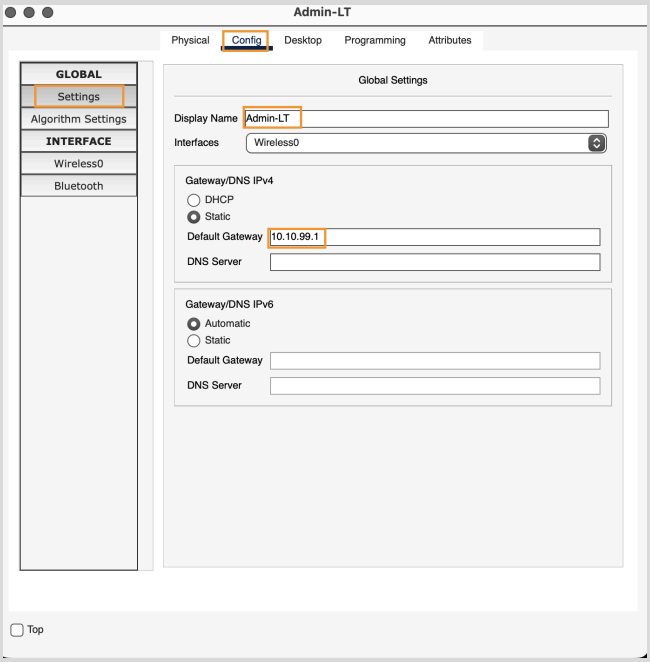


Admin-LT

1. Replace NIC Ethernet module with Wireless module

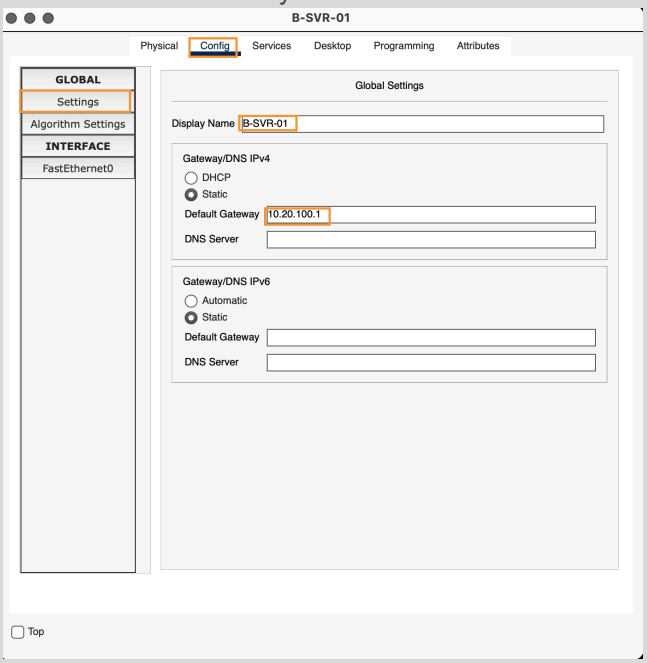


2. Navigate to Settings
   Click on Static radio button
   Default Gateway: 10.10.99.2

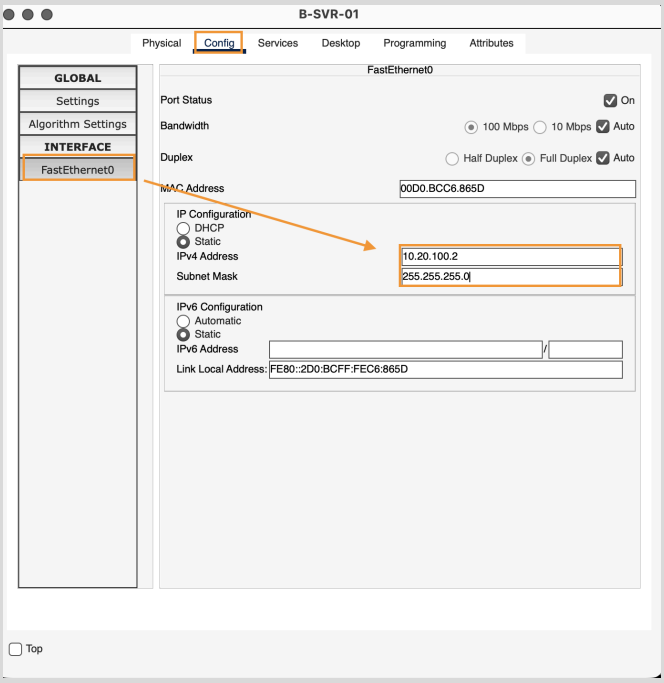


B-SRV-01

1. Navigate to Settings
   Click on Static radio button
   Default Gateway: 10.20.100.1



2. Navigate to FastEthernet0
Click on Static radio button
IPv4 Address: 10.20.100.2
Subnet Mask 255.255.255.0



8.6 **Phase 6 — Infrastructure Services Deployment**

Purpose: Provide operational visibility and time consistency across the network.

- **Services:**

1. **NAT / PAT** – EDGE-01 performs NAT (Network Address Translation) and PAT (Port Address Translation) for internal hosts, enabling private IP networks to communicate with external networks while maintaining security and conserving public IP addresses.

2. **Network Time Protocol (NTP)** – EDGE-01 serves as the NTP server, and all core, distribution, and access switches are configured as NTP clients to ensure synchronized time across the network.

3. **Syslog** – EDGE-01 acts as the centralized syslog server, collecting logs from all network devices for monitoring, auditing, and troubleshooting purposes.

4. **Simple Network Management Protocol (SNMP)** – EDGE-01 is configured as the SNMP manager, while all network devices run SNMP agents, allowing centralized monitoring of device performance, status, and alerts.

5. **Secure Remote Access (SSH / AAA)** – SSH is enabled on all network devices for encrypted remote management. AAA is configured on the core and distribution switches with EDGE-01 as the RADIUS/AAA server, providing authentication, authorization, and accounting for administrative access.

—-

1. NAT / PAT

- Allows internal IPv4 networks (LANs behind CSWs) to access external networks (simulated Internet).
- Translates private IP addresses to a public IP (or a single lab IP) for outbound traffic.
- Provides redundancy and ensures that internal hosts don't need public IPs.

EDGE NAT INTERFACE ASSIGNMENT & ROLE TABLE

Device	Interface	Role	IP Address / Subnet	Notes
EDGE-01	Gi0/0/0	NAT Inside	10.255.31.2/30	Connected to CORE-1 (LAN, Office A/B via COREs)
EDGE-01	Gi0/0/1	NAT Inside	10.255.31.6/30	Connected to CORE-2 (LAN, Office B/A via COREs)
EDGE-01	s0/1/0	NAT Outside	203.0.113.1/30	Connected to ISP (R2)
EDGE-01	s0/1/1	NAT Outside	203.0.113.5/30	Connected to ISP (R2) - backup

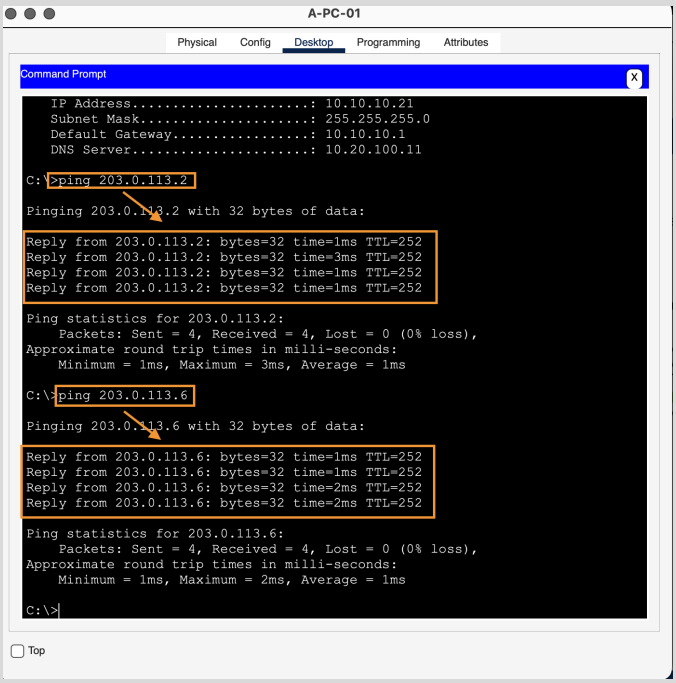
CONFIGURATION

- **EDGE-01 (Edge Router)**

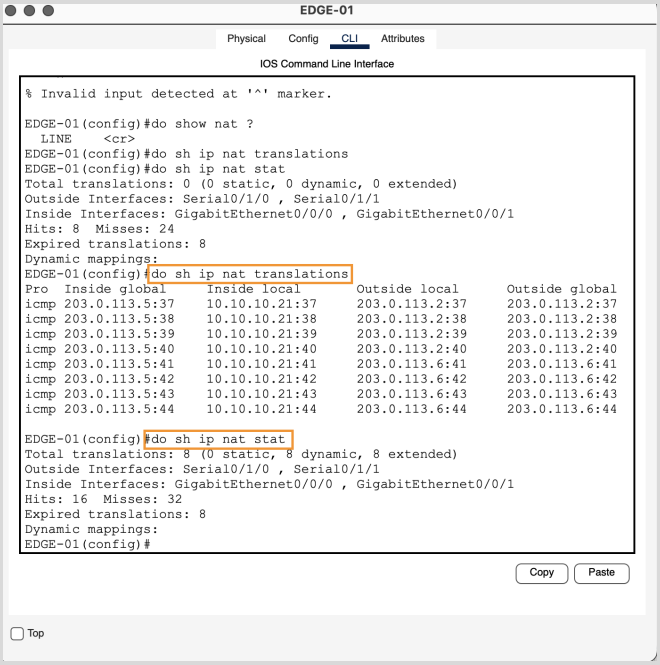
```
! Configure inside interfaces (LAN-facing)
interface g0/0/0
ip nat inside
 no shutdown
 exit

interface g0/0/1
 ip nat inside
 no shutdown
 exit

! Configure outside interface (WAN-facing)
interface s0/1/0
 ip nat outside
 no shutdown
 exit

interface s0/1/1
 ip nat outside
 no shutdown
 exit

! Define ACL: the internal networks to be translated
access-list 1 permit 10.10.0.0 0.0.255.255              !10.10.0.0/16
access-list 1 permit 10.20.0.0 0.0.255.255


! Define NAT overload / PAT (1 public IP for multiple private IPs)
ip nat inside source list 1 interface s0/1/0 overload
ip nat inside source list 1 interface s0/1/1 overload
```

Verification:
Ping ISP (R2), verify NAT translations, & check NAT statistics

`ping 203.0.113.2`
`ping 203.0.113.6` (backup)



`do show ip nat translations`
`do show ip nat statistics`



—-

2. Network Time Protocol (NTP)

- Logs correlate correctly across Syslog, SNMP, and security tools
- Certificates and authentication remain valid
- Troubleshooting timelines are accurate
- Network devices share a trusted time source

NTP ROLE REFERENCES TABLE

Device	Role	NTP Source / Peer	Stratum	Notes / Authentication
EDGE-01	Internal Time Master	Syncs to Internet NTP	3	ntp server <external> key 10; authoritative for enterprise
CORE-01	NTP Client	EDGE-01 Loopback	4	Authenticated (key 10)
CORE-02	NTP Client	EDGE-01 Loopback	4	Authenticated (key 10)
DISTR-01	NTP Client	CORE-01 / CORE-02	5	Redundant upstreams
DISTR-02	NTP Client	CORE-01 / CORE-02	5	Redundant upstreams
A-ACC-01	NTP Client	DISTR-01 / DISTR-02	6	Access layer devices
A-ACC-02	NTP Client	DISTR-01 / DISTR-02	6	Access layer devices
WLC / Servers	NTP Client	DISTR-01 / DISTR-02	6	Access / Server devices

CONFIGURATION

- **EDGE-01** (NTP Master)

! Set accurate clock (if not synching form external time servers)

```
clock set <hh:mm:ss> <Month> <date> <year>                    ! Priv Exec mode
clock timezone <NAME ex. EST> <OFFSET-from-UTC ex. -5>        ! Global Config mode
```

! Enable NTP authentication

```
ntp authenticate
```

! Create authentication key

```
ntp authentication-key 10 md5 passNTP
```

! Trust the key

```
ntp trusted-key 10
```

! Make EDGE authoritative, Stratum 3

```
ntp master 3
```

! Source NTP from a loopback

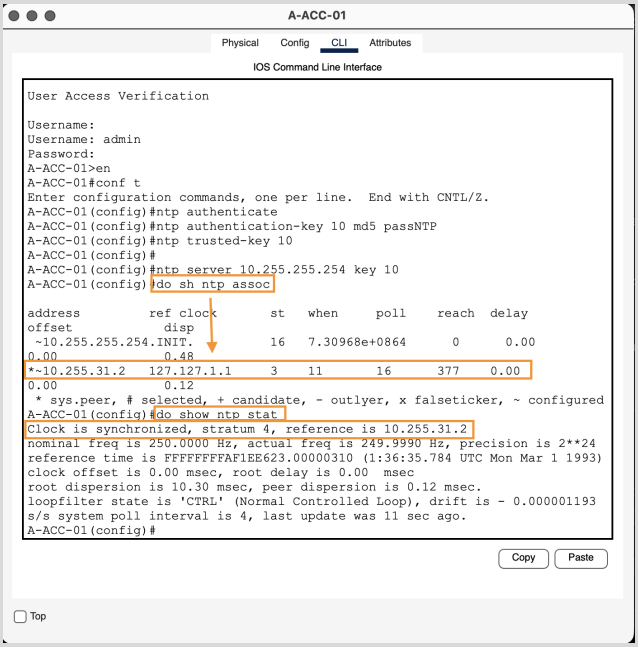
```
ntp source loopback0      ! not supported by Packet Tracer
```

- **CORE-01, CORE-02, DISTs, & ACCs** (Servers, & WLC if supported)

```
ntp authenticate
ntp authentication-key 10 md5 passNTP
ntp trusted-key 10

ntp server 10.255.255.254 key 10     !EDGE-01 loopback address (server)
```

Verification:

```
show ntp association          ! *~ shows successful peering w/ ntp server (EDGE-01)
show ntp status               ! Verifies successful clock synchronized
```



Notes:

Typical Internet Time Hierarchy (Stratum Levels):

- Stratum 0 → Atomic clocks / GPS devices
- Stratum 1 → Public time servers
- Stratum 2 → ISPs
- Stratum 3 → Enterprise networks

Real-World Best Practices:

- Always configure multiple external NTP sources for redundancy.
- Use authentication keys for security.

Example External NTP Servers:

```
ntp server time.google.com
ntp server time.cloudflare.com
ntp server pool.ntp.org
```

—-

3 & 4. Syslog & SNMP (Centralized Logging & Monitoring)

- Syslog: Collects event messages from devices (routers, switches, firewalls) into a centralized server. Logs are stored chronologically and can be filtered by severity.
- SNMP Traps: Event-driven notifications sent to a management station when certain conditions occur (e.g., interface down, high CPU usage). Provides real-time alerts.
- Edge-01 acts as both syslog server and SNMP trap receiver in this lab setup.
- Suitable for monitoring core, distribution, access layers, WLCs, and servers.

SYSLOG & SNMP DEVICE ROLES & SETTINGS

Device	Role	Syslog Destination	SNMP Trap Destination	Community / Key	Notes
EDGE-01	Syslog & SNMP Server	Local storage	Receives traps	CCNA-LAB-STR	Lab “collector”
CORE-01/02	Client	10.255.255.254	10.255.255.254	CCNA-LAB-STR	Log events & send traps
DIST / ACCs	Client	10.255.255.254	10.255.255.254	CCNA-LAB-STR	Log events & send traps
WLC / Servers	Client (if CLI available)	10.255.255.254	10.255.255.254	CCNA-LAB-STR	Optional in lab

SYSLOG SEVERITY LEVELS

Level	Name	Description
0	Emergency	System unusable
1	Alert	Immediate action required
2	Critical	Critical conditions
3	Error	Error conditions
4	Warning	Warning conditions
5	Notice	Normal but significant events
6	Informational	Informational messages
7	Debugging	Debug messages

Note: Packet Tracer does not support severity filtering. Commands referencing severity are included for real-world context only.

CONFIGURATION

- **EDGE-01 (Syslog Server-Collector)**

! Enable logging on the router itself (optional)
```
logging on
```

! Set severity level for console messages
```
logging console <warning>                                    ! severity setting not supported by PT
```

! Enable timestamp in logs
```
service timestamps log datetime msec <localtime> !localtime not supported
```

! Configure memory buffer for local log storage
```
logging buffered 4096 <informational>                        ! severity setting not supported
```

! Enable syslog server capability
```
logging host 10.255.255.254                                  ! point router logs to itself
logging trap <informational>                                 ! PT limitation; debugging available but not set
```

- **EDGE-01 (SNMP Manager)**

! Define SNMP community string (RO read-only for monitoring)
```
snmp-server community CCNA-LAB-STR RO
```

! Enable SNMP traps for critical events
```
snmp-server enable traps                                    !not supported
snmp-server host 10.255.255.254 version 2c CCNA-LAB-STR     !not supported
```

! Specify which traps (interface, config changes, CPU, etc.)
```
snmp-server enable traps snmp authentication linkup linkdown    !not supported
snmp-server enable traps config                                 ! not supported
```

- **COREs, DISTs, ACCs** - EDGE-01 (already configured).

! Syslog Forwarding to EDGE-01
```
logging host 10.255.255.254
```

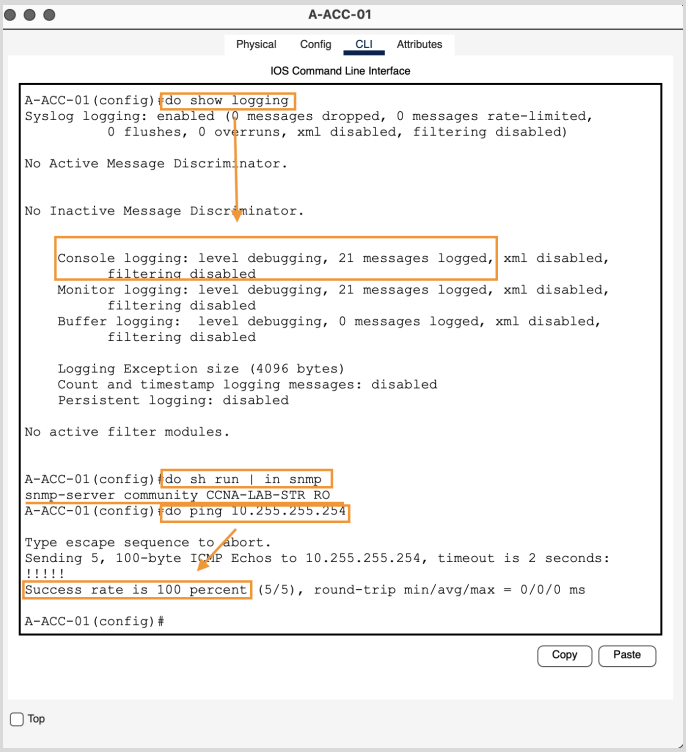
! Configure severity for traps (PT limitation)
```
logging trap <informational>                    ! debugging available but not set
```

! Timestamp and buffer for local logs
```
service timestamps log datetime msec <localtime> !localtime     !not supported
logging buffered 4096
```

SNMP Agent Configuration
```
snmp-server community CCNA-LAB-STR RO
```

Verification:

```
show logging                    ! Displays locally stored logs
show logging | include <IP>     ! not supported
ping 10.255.255.254             ! Confirm connectivity to syslog server
show snmp                       ! not supported
```



Notes:

1. Edge-01 collects logs from all network devices and stores them locally.
2. SNMP traps are sent immediately to Edge-01 for selected critical events.
3. Monitoring workflow:
   - Console: warnings & errors visible immediately
   - Syslog: detailed logs stored for audit or troubleshooting
   - SNMP traps: alert admins in real-time if configured in a monitoring tool

⚠️ Packet Tracer Limitations Encountered

Feature	Status
Syslog severity selection	Not supported
SNMP traps	Not supported
SNMP manager host	Not supported
Timestamp localtime	Not supported

—-

5. Secure Remote Access (SSH / AAA / Privilege-level Configuration)

- AAA & Local Users – Provides centralized authentication, authorization, and (where supported) accounting for device access. Privilege levels enforce role-based command access.
- SSH Access – Secures remote management by encrypting login and session traffic. SSH source is tied to Loopback0 for consistent identity.
- Privilege Levels – Admin accounts (level 15) have full configuration rights; engr accounts (level 7) are limited to monitoring and troubleshooting commands.
- VTY Lines & Timeouts – All VTY sessions are restricted to SSH only, with idle timeouts and synchronous logging to prevent accidental input disruption.
- Banners – MOTD and login banners notify users of authorized access restrictions and monitoring for compliance and security awareness.

SSH, AAA, & PRIVILEGE LEVEL CONFIGURATION TABLE

Device	Role	AAA Supported	Local Users / Privilege	SSH Version	VTY Access	Notes
EDGE-01	Edge Router	Yes	admin (15), engr (7)	2	0–4	Loopback0 as SSH source; privilege-based access; full AAA enabled
CORE-01/02	Core L3	Yes	admin (15), engr (7)	2	0–4	Full AAA, privilege level for monitoring & troubleshooting
A-DIST-01/02	Distribution L3	Yes	admin (15), engr (7)	2	0–4	Full AAA; privilege-based access; monitoring commands only for engr
B-DIST-01/02	Distribution L3	Yes	admin (15), engr (7)	2	0–4	Full AAA; privilege-based access; monitoring commands only for engr
A-ACC-01/02 /03	Access L2	No	admin (15), engr (7)	2	0–4	AAA not supported; local user authentication; SSH only; privilege 15 for admin
B-ACC-01/02 /03	Access L2	No	admin (15), engr (7)	2	0–4	AAA not supported; local user authentication; SSH only; privilege 15 for admin

OFFICE A SSH REFERENCE TABLE — VLAN 99 (10.10.99.0/25)

Device	Management Interface	SSH IP Address	Gateway	Role
Admin-LT	NIC	10.10.99.2	10.10.99.1	Primary management workstation
A-DIST-01	VLAN 99	10.10.99.11	10.10.99.1	Distribution (Active Gateway)
A-DIST-02	VLAN 99	10.10.99.12	10.10.99.1	Distribution (Standby)
A-ACC-01	VLAN 99	10.10.99.31	10.10.99.1	Access switch
A-ACC-02	VLAN 99	10.10.99.32	10.10.99.1	Access switch
A-ACC-03	VLAN 99	10.10.99.33	10.10.99.1	Wireless aggregation

OFFICE B SSH REFERENCE TABLE — VLAN 99 (10.20.99.0/25)

Device	Management Interface	SSH IP Address	Gateway	Role
B-DIST-01	VLAN 99	**10.20.99.21**	10.20.99.1	Distribution (Active Gateway)
B-DIST-02	VLAN 99	10.20.99.22	10.20.99.1	Distribution (Standby)
B-ACC-01	VLAN 99	10.20.99.31	10.20.99.1	Access switch
B-ACC-02	VLAN 99	10.20.99.32	10.20.99.1	Access switch
B-ACC-03	VLAN 99	10.20.99.33	10.20.99.1	Wireless aggregation

CISCO IOS 16 PRIVILEGE LEVELS 0–15:

Level	Default Access
0	Very limited—only basic commands like logout, enable, disable
1	User EXEC mode – normal login, basic show commands
2–14	Custom levels – you can configure which commands are allowed
15	Full administrative access – same as enable mode, can configure everything

CONFIGURATION

- **EDGE-01; All CORE & DISTRIBUTION Switches**

! Enable AAA on the device
```
aaa new-model
```

! Use local user database for SSH login
```
aaa authentication login default local
```

! Assign privilege level from local user account
```
aaa authorization exec default local
```

! Log all EXEC sessions (login/logout) for auditing
```
aaa accounting exec default start-stop group system
```
! NOT SUPPORTED

! Create credential for admin (full access)
```
username admin privilege 15 secret passAdmin
```

! Create credential for user (limited access)
```
username engr privilege 7 secret passEngr
```

! Create password for Privilege Exec mode authorization
```
enable secret passEnable
```

```
! Domain Name required for SSH key generation
ip domain-name ccna-lab.local

! Generate RSA key for SSH
crypto key generate rsa modulus 2048

! Use SSH version 2 (secure)
ip ssh version 2

! SSH timeout for idle attempts
ip ssh time-out 60

! Max login retries
ip ssh authentication-retries 3

! VTY Line Configuration (SSH access for lines 0 - 4)
line vty 0 4

 ! Use AAA local users for login
 login authentication default

! Only allow SSH (disable Telnet)
 transport input ssh

! Ensure correct privilege assigned per user
 privilege level 15

! Prevent messages from interrupting typing
 logging synchronous

! Disconnect idle session after 10 minutes
 exec-timeout 10 0

 ! Use Loopback0 as the SSH source interface for consistent device identity
 ip ssh source-interface loopback0                                  ! NOT SUPPORTED
 exit

! Optional Banner
banner motd #
**********************************************
*      Authorized Access Only!                *
*      All activity is logged.                *
**********************************************
#

! Optional Login message

banner login #
**********************************************
*      Welcome!                                *
*      All activity is logged.                *
**********************************************
#
```

```
! Privilege Level 7 Configuration – engr user only authorized to monitoring commands
privilege exec level 7 show running-config
privilege exec level 7 show startup-config
privilege exec level 7 show interfaces
privilege exec level 7 show ip interface brief
privilege exec level 7 show vlan
privilege exec level 7 show mac address-table
privilege exec level 7 show ip route
privilege exec level 7 show version
privilege exec level 7 show logging

! engr user limited to basic troubleshooting function
privilege exec level 7 ping
privilege exec level 7 traceroute
```

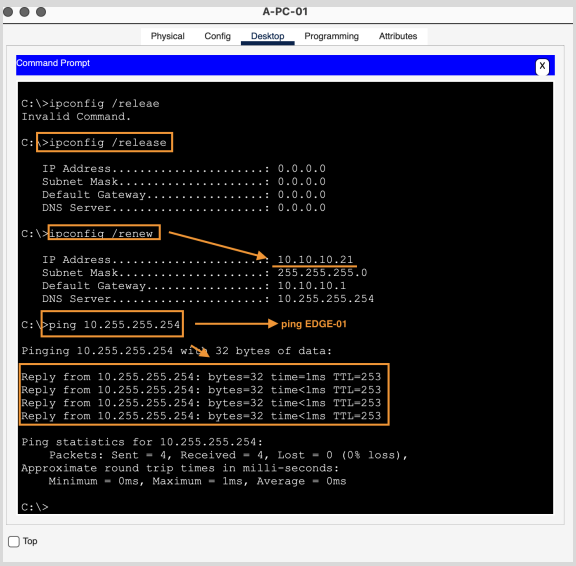
- **A-ACC-01 & 02 / B-ACC-01 & 02**

```
aaa new-model
aaa authentication login default local
aaa authorization exec default local              ! NOT SUPPORTED on ACCs

username admin privilege 15 secret passAdmin
username engr  privilege 7  secret passEngr
enable secret passEn

ip domain-name ccna-lab.local
crypto key generate rsa modulus general-keys 2048
ip ssh version 2
ip ssh time-out 60
ip ssh authentication-retries 3

line vty 0 4
 login authentication default
 transport input ssh
 privilege level 15
 logging synchronous
 exec-timeout 10 0

banner motd #                          ! only motd  /  login banner - NOT SUPPORTED in ACCs
**********************************************
*      Authorized Access Only!                *
*      All activity is logged.                *
**********************************************
#

privilege exec level 7 show running-config
privilege exec level 7 show startup-config
privilege exec level 7 show interfaces
privilege exec level 7 show ip interface brief
privilege exec level 7 show vlan
privilege exec level 7 show mac address-table
privilege exec level 7 show ip route
privilege exec level 7 show version
privilege exec level 7 show logging

privilege exec level 7 ping
privilege exec level 7 traceroute
```

- **A-ACC-03 & A-ACC-03** (aaa authentication not supported on L2 Empty Switch)

```
username admin privilege 15 secret passAdmin
username engr  privilege 7  secret passEngr
enable secret passEnable

ip domain-name ccna-lab.local
crypto key generate rsa modulus 2048
ip ssh version 2
ip ssh time-out 60
ip ssh authentication-retries 3

line vty 0 4
 login local                          ! AAA authentication not supported
 transport input ssh
 privilege level 15
 logging synchronous
 exec-timeout 10 0

banner motd #
**********************************************
*      Authorized Access Only!                *
*      All activity is logged.                *
**********************************************
#

privilege exec level 7 show running-config
privilege exec level 7 show startup-config
privilege exec level 7 show interfaces
privilege exec level 7 show ip interface brief
privilege exec level 7 show vlan
privilege exec level 7 show mac address-table
privilege exec level 7 show ip route
privilege exec level 7 show version
privilege exec level 7 show logging

privilege exec level 7 ping
privilege exec level 7 traceroute
```

Validation:
Verify SSH connectivity to EDGE-01
`ssh -l admin 10.255.255.254`



Key Points from Comments

1. AAA Section – controls who can log in, what privilege they get, and logging/accounting of activity.
2. Local Users – privilege 15 = full, privilege 7 = restricted.
3. Domain Name / RSA – needed for SSH key generation; without it, SSH won't work.
4. VTY Lines – tie SSH login to AAA, assign privileges, limit transport to SSH only.
5. Privilege 7 Commands – define exactly what limited users can do.

Notes / Best Practices

1. username netadmin privilege 15 → Full admin account
2. username engineer privilege 7 → Daily engineer account (limit commands if desired)
3. aaa new-model → AAA now handles all authentication
4. crypto key generate rsa 2048 → Needed for SSH; RSA 1024 works too, but 2048 is more secure
5. line vty 0 4 → Restricts login to SSH only (transport input ssh)
6. exec-timeout 10 0 → Auto logout after 10 min of inactivity

_____

8.7 Phase 7 — Enterprise Network Services

Purpose: Deliver services consumed by endpoints.

- **Services:**

    1. **DHCP Deployment -** Currently hosted on the router, with planned migration to a dedicated server.

    2. **DNS Services – Centralized DNS was deployed within the services VLAN.**

    3. **Wireless Infrastructure Staging – Wireless components were integrated into the topology to support future WLAN deployment.**

—-

1:DHCP (Dynamic Host Configuration Protocol) Deployment

DHCP Addressing Strategy

- The first 20 IP addresses in each VLAN are excluded from DHCP and reserved for static infrastructure devices (servers, WLCs, APs, phones, management systems).
- The default-router always points to the HSRP Virtual IP (VIP) for gateway consistency and failover.
- The DNS server is set to 10.255.255.254 (EDGE-01 Loopback0).
- Lease customization is not supported in Packet Tracer.

IP Allocation Model

- End-user devices receive dynamic IP addresses from the DHCP pool outside the reserved static range.
- Infrastructure devices use static IPs for reliability and predictable management.
- This design separates dynamic clients from critical infrastructure, improving operational stability and scalability.

DHCP & STATIC DEVICE ADDRESSING TABLE

VLAN	Name / Purpose	Available Hosts	Device	IP Address	Source	Default Gateway	Location / Switches	Notes
10	Sales – User VLAN	254	A-PC-01	10.10.10.x	DHCP	10.10.10.1	Office A (A-DIST / A-ACC-SALES)	DHCP pool starts at .11
20	Marketing – User VLAN	254	A-PC-02	10.10.20.x	DHCP	10.10.20.1	Office A (A-DIST / A-ACC-MKTG)	DHCP pool starts at .11
30	IT – User VLAN	254	B-PC-01	10.20.30.x	DHCP	10.20.30.1	Office B (B-DIST / B-ACC-IT)	DHCP pool starts at .11
40	Phones – VoIP VLAN	254	A-PH-01	10.10.40.x	DHCP	10.10.40.1	Office A / B (All Phones Access)	DHCP pool starts at .11
40	Phones – VoIP VLAN	254	A-PH-02	10.10.40.x	DHCP	10.10.40.1	Office A / B (All Phones Access)	DHCP pool starts at .11
40	Phones – VoIP VLAN	254	B-PH-01	10.20.40.x	DHCP	10.20.40.1	Office B (B-ACC-Phones)	DHCP pool starts at .11
50	Wi-Fi – WLAN VLAN	254	A-WLC-01	10.10.50.2	Static	10.10.50.1	Office A (A-ACC-Wi-Fi)	Excluded from DHCP
50	Wi-Fi – WLAN VLAN	254	A-LWAP011	10.10.50.3	Static	10.10.50.1	Office A (A-ACC-Wi-Fi)	Excluded from DHCP
50	Wi-Fi – WLAN VLAN	254	B-LWAP-01	10.20.50.4	Static	10.20.50.1	Office B (B-ACC-Wi-Fi)	Excluded from DHCP
99	Network Mgmt – Device Mgmt	254	Admin-LT	10.10.99.2	Static	10.10.99.1	Core / Dist / Access Switches	For management & trunk mgmt
100	Servers – Services VLAN	254	B-SRV-01	10.20.100.2	Static	10.20.100.1	Office B (B-DIST / Server Farm)	

CONFIGURATION

OFFICE A

- **EDGE-01**

! VLAN 10 – A-Sales (PCs)
! Exclude reserved IP addresses (gateway, infrastructure devices, static hosts)
```
ip dhcp excluded-address 10.10.10.1 10.10.10.20
```

! Create DHCP pool for VLAN 10 – Office A Sales
```
ip dhcp pool VLAN10_A_SALES
```

! Define the subnet for this VLAN
```
network 10.10.10.0 255.255.255.0
```

```
! Default gateway assigned to clients (HSRP VIP)
 default-router 10.10.10.1

 ! Provide domain name to DHCP clients
 domain-name ccna-lab.local

 ! DNS server for name resolution
 dns-server 10.255.255.254

 exit

! VLAN 20 – A-Marketing (PCs)
ip dhcp excluded-address 10.10.20.1 10.10.20.20
ip dhcp pool VLAN20_A_MARKETING
 network 10.10.20.0 255.255.255.0
 default-router 10.10.20.1
 domain-name ccna-lab.local
 dns-server 10.255.255.254
 exit

! VLAN 40 – Phones
ip dhcp excluded-address 10.10.40.1 10.10.40.20
ip dhcp pool VLAN40_A_PHONES
 network 10.10.40.0 255.255.255.0
 default-router 10.10.40.1
 domain-name ccna-lab.local
 dns-server 10.255.255.254
 exit

! VLAN 50 – Wi-Fi
ip dhcp excluded-address 10.10.50.1 10.10.50.20
ip dhcp pool VLAN50_A_WIFI
 network 10.10.50.0 255.255.255.0
 default-router 10.10.50.1
 domain-name ccna-lab.local
 dns-server 10.255.255.254
 exit
```

OFFICE B

- **EDGE-01**

```
! VLAN 30 – B-IT (PCs)
ip dhcp excluded-address 10.20.30.1 10.20.30.20
ip dhcp pool VLAN30_B_IT
 network 10.20.30.0 255.255.255.0
 default-router 10.20.30.1
 domain-name ccna-lab.local
 dns-server 10.255.255.254
 exit

! VLAN 40 – Phones
ip dhcp excluded-address 10.20.40.1 10.20.40.20
ip dhcp pool VLAN40_B_PHONES
 network 10.20.40.0 255.255.255.0
 default-router 10.20.40.1
 domain-name ccna-lab.local
 dns-server 10.255.255.254
 exit
```

! VLAN 50 – Wi-Fi
```
ip dhcp excluded-address 10.20.50.1 10.20.50.20
ip dhcp pool VLAN50_B_WIFI
 network 10.20.50.0 255.255.255.0
 default-router 10.20.50.1
 domain-name ccna-lab.local
 dns-server 10.255.255.254
 exit
```

Notes:

- Excluded addresses: First 20 IPs in each VLAN are reserved for static devices (servers, WLCs, phones, management PCs).
- Default-router: Always points to the VLAN SVI of the active HSRP router.
- DNS-server: Points to EDGE-01 Loopback0 (10.255.255.254).
- `Lease` not supported by Packet Tracer

CONFIGURE: IP helper-addresses on the active HSRP SVI interfaces

- **Office A – Distribution Switches (A-DIST-01 / A-DIST-02)**

! VLAN 10 – A-Sales (PCs)
```
interface vlan 10
 ip helper-address 10.255.255.254
 no shutdown
 exit
```

! VLAN 20 – A-Marketing (PCs)
```
interface vlan 20
 ip helper-address 10.255.255.254
 no shutdown
 exit
```

! VLAN 40 – Phones
```
interface vlan 40
 ip helper-address 10.255.255.254
 no shutdown
 exit
```

! VLAN 50 – Wi-Fi / WLAN
```
interface vlan 50
 ip helper-address 10.255.255.254
 no shutdown
 exit
```

Office B – Distribution Switches (B-DIST-01 / B-DIST-02)

! VLAN 30 – B-IT (PCs)
```
interface vlan 30
 ip helper-address 10.255.255.254
 no shutdown
 exit
```

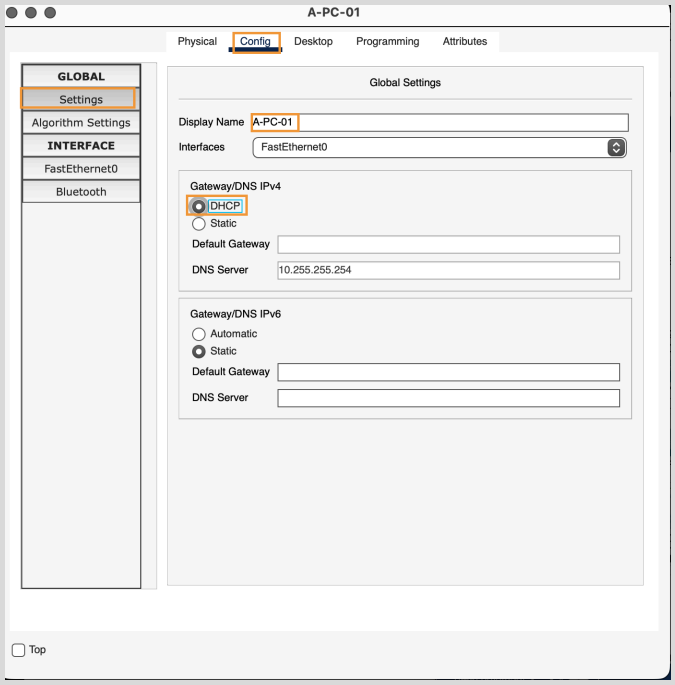
! VLAN 40 – Phones
```
interface vlan 40
 ip helper-address 10.255.255.254
 no shutdown
 exit
```

```
! VLAN 50 – Wi-Fi / WLAN
interface vlan 50
 ip helper-address 10.255.255.254
 no shutdown
 exit
```

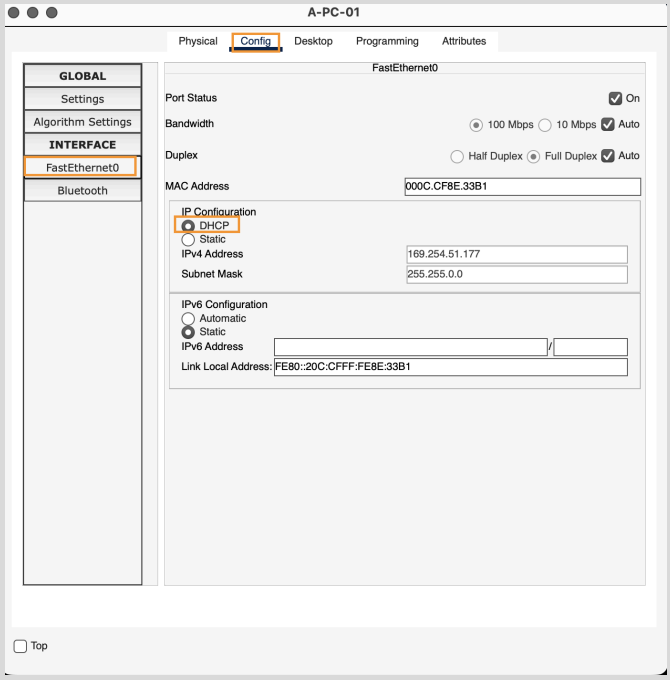
Verification:

A-PC-01:

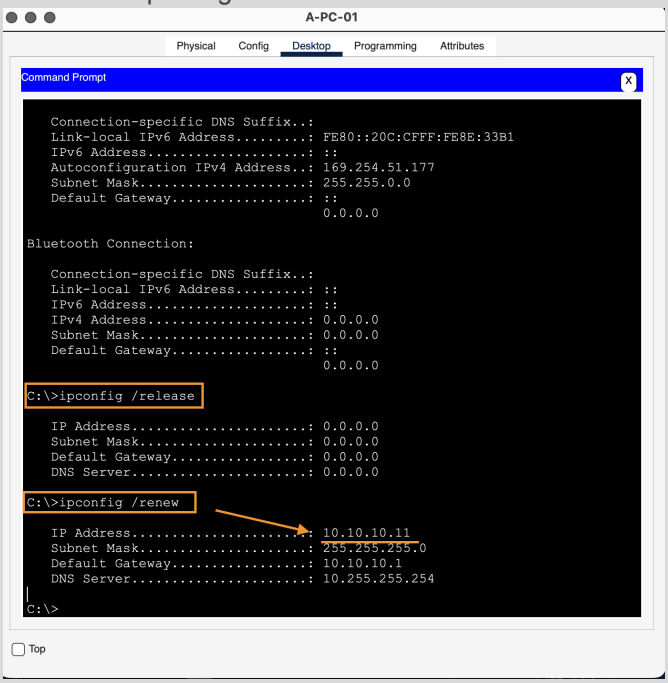
1. Navigate to **Config**
2. Click **DHCP** radio button



3. Click **FastEthernet0** on the side menu bar
4. Click **DHCP** radio button



5. Navigate to Desktop > CMD Terminal
6. run ipconfig /release
7. run ipconfig /renew



⚠TROUBLESHOOTING: DHCP Lease Instability — Conflict Identification & Scope Hardening

Diagnosed an intermittent DHCP failure where an endpoint repeatedly lost its assigned IP address despite successful initial lease allocation.

Identified an overlapping DHCP scope as the root cause and stabilized address assignment by reserving infrastructure ranges and forcing lease renewal.

Problem: A-PC-01 intermittently dropped its DHCP-assigned IP address within VLAN 10, resulting in loss of gateway reachability and management network connectivity.

Initial Hypothesis: Suspected an IP address conflict caused by overlap between dynamically assigned addresses and statically configured infrastructure components such as:

- VLAN SVI
- HSRP Virtual IP
- Network devices

Diagnostic Methodology:

On A-PC-01

Client Validation

- ipconfig
- ipconfig /release
- ipconfig /renew

Checked Global & Interface settings and confirmed the issue was DHCP related

On EDGE-01 (DHCP Server)

- show run | include dhcp
- show ip dhcp binding

Observed that the lease remained bound to the client MAC despite connectivity drops.

Key Findings: 1. Packet Tracer maintains persistent DHCP bindings mapped to MAC addresses. clear ip dhcp binding command is not supported.
2. Clearing the Layer 2 MAC table does not remove DHCP leases.

Root Cause: The VLAN 10 SVI (10.10.10.11) resided inside the DHCP allocation pool, introducing the risk of duplicate addressing and lease instability.

Remediation Strategy: 1. Update EDGE-01 DHCP excluded addresses – Hardened the DHCP scope by reserving infrastructure space (first 20 IP addresses).
2. Forced a new lease by modifying the endpoint MAC address and renewing the client configuration.

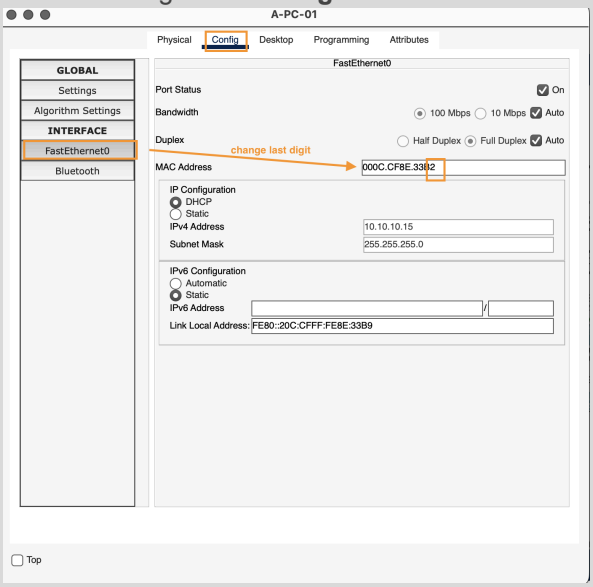
🛠️ **! —-APPLY FIX—-----**

1. Update DHCP Pools on EDGE-01 (DHCP Server)

- **EDGE-01**

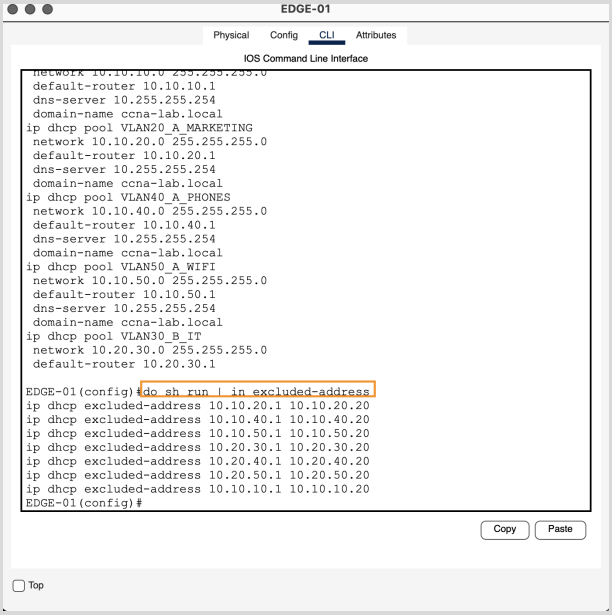
```
ip dhcp excluded-address 10.10.10.1 10.10.10.20
ip dhcp excluded-address 10.10.20.1 10.10.20.20
ip dhcp excluded-address 10.10.40.1 10.10.40.20
ip dhcp excluded-address 10.10.50.1 10.10.50.20

ip dhcp excluded-address 10.20.30.1 10.20.30.20
ip dhcp excluded-address 10.20.40.1 10.20.40.20
ip dhcp excluded-address 10.20.50.1 10.20.50.20
```

2. Changed the MAC address of A-PC-01 to force a new DHCP lease.
   a. Navigate to **Config**
   b. Click **FastEthernet0** on side menu bar
   c. Change the **last digit of the MAC address**

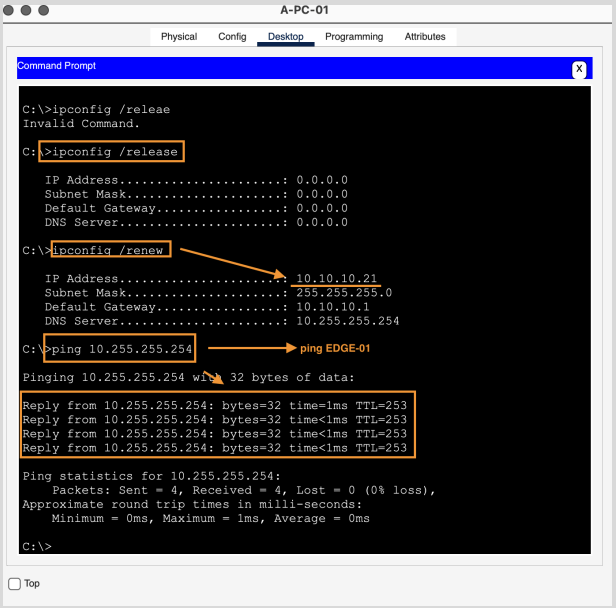


Verification:

Check EDGE-01configuration
run: `show running-config | include excluded-address`

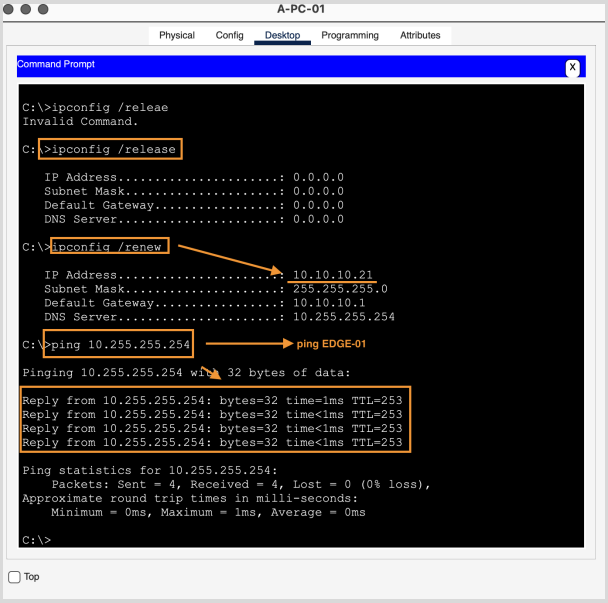


Ping EDGE-01 (DHCP Server) form A-PC-01
`ping 10.255.255.254`



Renew IP Address lease from DHCP Server

```
ipconfig /release
ipconfig /renew
```



—-

2: DNS Services (Implemented on dedicated server)

Function: Provides name resolution by translating human-readable domain names (e.g., ccna-lab.local or www.ccna-lab.com) into IP addresses, allowing devices to locate and communicate with network resources without requiring users to remember numeric IP addresses.

⚠️DNS Service Failure – EDGE-01 (Packet Tracer Limitation)

Problem: Attempting to enable DNS service on EDGE-01 using: EDGE-01(config)# `ip dns server`

Result: `% Invalid input detected at '^' marker.` The command is not recognized by the device.

Initial Hypothesis: The ip dns server feature may not be supported in Cisco Packet Tracer, depending on the router model and IOS image being emulated.

Diagnostic Methodology: Context Help Verification executed: EDGE-01(config)# `ip ?`

Observed available DNS-related options:

```
ip domain
ip domain-lookup
ip domain-name
ip name-server
ip host
```

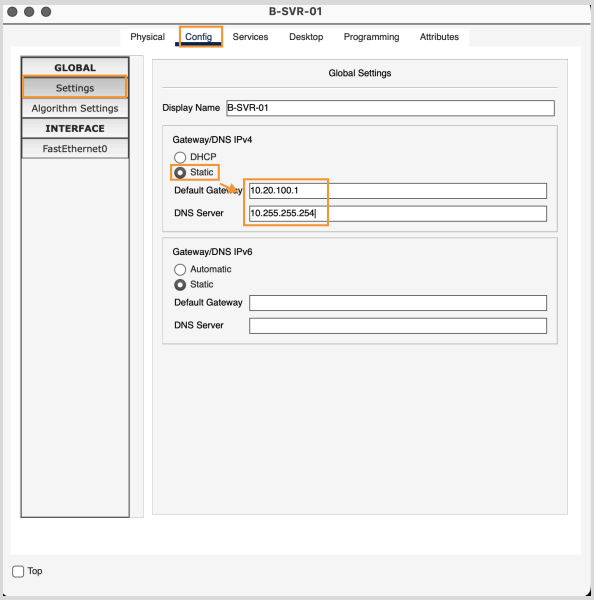
Key Finding: The expected command:`ip dns server` does not appear in the command tree, confirming the feature is unavailable on this platform.

Root Cause: Platform limitation within Packet Tracer. The router image being used does not support DNS server functionality.

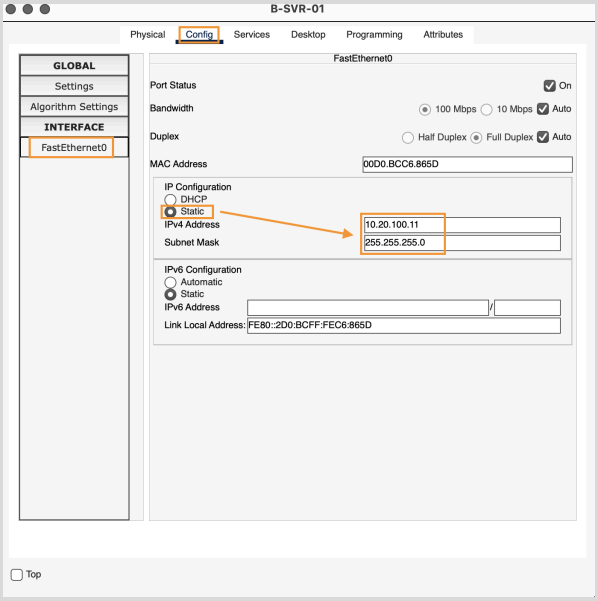
Remediation Strategy: Design Decision: Deploy a dedicated DNS server instead of hosting DNS on the edge router. Selected Device: **B-SVR-01**

🛠️ ! —-APPLY FIX—-----

Configure B-SVR-01 (Server 1)
Default Gateway: `10.20.100.1`
DNS Server: `10.255.255.254`



IP Address: `10.20.100.11`
Subnet Mask: `255.255.255.0`



DNS DATA DATABASE ENTRIES:

CORE INFRASTRUCTURE (loopback addresses)

Hostname	FQDN	IP Address
edge-01	edge-01.ccna-lab.local	10.255.255.254
core-01	core-01.ccna-lab.local	10.255.255.1
core-02	core-02.ccna-lab.local	10.255.255.2
ssh-gateway		10.255.255.254

DISTRIBUTION SWITCHES (Management VLAN)

Hostname	FQDN	IP
a-dist-01	a-dist-01.ccna-lab.local	10.10.99.11
a-dist-02	a-dist-02.ccna-lab.local	10.10.99.12
b-dist-01	b-dist-01.ccna-lab.local	10.20.99.21
b-dist-02	b-dist-02.ccna-lab.local	10.20.99.22

ACCESS SWITCHES

Hostname	FQDN	IP
a-acc-01	a-acc-01.ccna-lab.local	10.10.99.31
a-acc-02	a-acc-02.ccna-lab.local	10.10.99.32
a-acc-03	a-acc-03.ccna-lab.local	10.10.99.33
b-acc-01	b-acc-01.ccna-lab.local	10.20.99.31
b-acc-02	b-acc-02.ccna-lab.local	10.20.99.32
b-acc-03	b-acc-03.ccna-lab.local	10.20.99.33

CRITICAL SERVERS

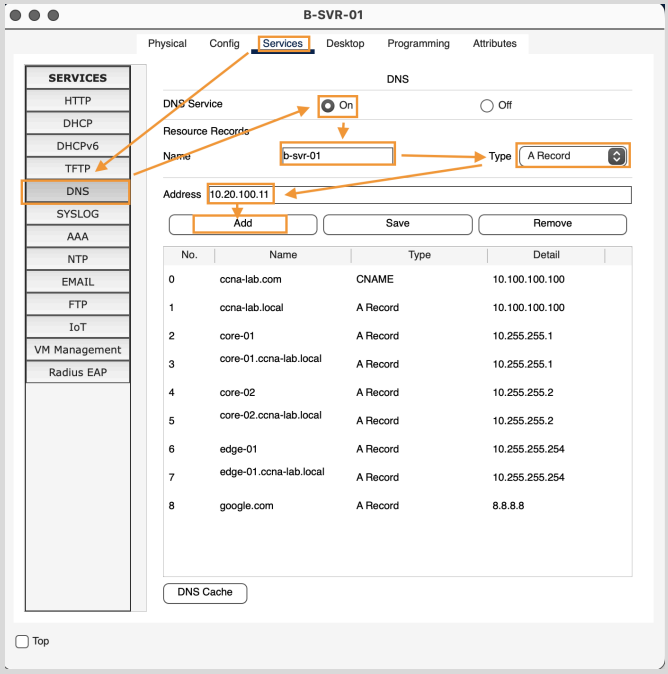
Hostname	FQDN	IP
b-svr-01	b-svr-01.ccna-lab.local	10.20.100.11
dns-svr	dns-svr.ccna-lab.local	10.20.100.11
dhcp-svr	dhcp-svr.ccna-lab.local	–

ADMIN WORKSTATION

Hostname	FQDN	IP
admin-lt	admin-lt.ccna-lab.local	10.10.99.2

Data Entry into DNS server:

1. Click **Services** tab
2. Click on **DNS** on the side menu
3. Click on **DNS Service** radio button
4. Enter **entity name**
5. Select **Type** of record (A = IPv4, AAAA = IPv6, etc)
6. Enter **IP Address**
7. Click **Add**



3: Wireless Infrastructure Staging

Purpose: Prepare the wireless infrastructure for integration into the network, ensuring initial IP assignment and connectivity for management and endpoint devices. Full wireless deployment will be completed in the next lab phase.

Implementation Notes:

- Wireless devices were staged and assigned IP addresses during the access layer and end-device configuration phase.
- Initial connectivity was verified to ensure devices are reachable on their respective VLANs.
- Full wireless deployment, including WLC-LWAP association and SSID configuration, will be performed in the subsequent lab.

WIRELESS DEVICES & IP ASSIGNMENTS

Device	Role	Office	VLAN	IP Address	Notes
A-WLC-01	Wireless Controller	A	50	10.10.50.11	Static IP, Wi-Fi management
A-LWAP-01	Lightweight AP	A	50	10.10.50.12	Static IP, staged
B-LWAP-01	Lightweight AP	B	50	10.20.50.22	Static IP, staged
Admin-LT	Wireless Admin	A/B	99	10.10.99.2 / 10.20.99.2	Static IP, management laptop

___

8.8 Phase 8 — Security Baseline

Function: Establish a secure foundation for the network by enforcing access controls, protecting management access, and mitigating Layer 2 and inter-VLAN risks.

- **Implemented Controls:**
  - **PortFast & BPDU Guard –** Enabled on edge and access ports during Rapid PVST+ deployment to prevent loops and mitigate accidental topology changes.
  - **Secure Management Access –** VLAN 99 was used for device management; SSH access and AAA policies were implemented to secure administrative sessions.
  - **Foundational ACLs for NAT/PAT –** Controlled traffic flows between internal and external networks, providing an initial layer of protection for network resources while enabling NAT/PAT functionality.
  - **Access Control Lists (ACLs)** – Extended Named ACLs were deployed on redundant distribution switches to enforce least-privilege access between VLANs:
    - ACLs applied inbound on source VLAN SVIs to block Sales (VLAN 10) and Marketing (VLAN 20) from accessing IT resources (VLAN 30)
    - Wildcard masks precisely define source and destination subnets, permitting all other traffic.
    - Applied as close to the source as possible for efficiency and consistency across redundant paths.

ACL CONFIGURATION

- **All Distribution Switches (DIST)**

```
! Create extended ACL to block Sales & Marketing from reaching IT
ip access-list extended BLOCK_OUTGOING_TO_IT
  deny ip 192.168.0.0 0.0.0.31 192.168.0.48 0.0.0.7   ! Sales → IT
  deny ip 192.168.0.32 0.0.0.15 192.168.0.48 0.0.0.7  ! Marketing → IT
  permit ip any any                                   ! Allow all other traffic

! Apply ACL inbound on source VLAN SVIs for filtering before routing
interface vlan 10
  ip access-group BLOCK_OUTGOING_TO_IT  in
  exit
interface vlan 20
  ip access-group BLOCK_OUTGOING_TO_IT  in
  exit
```

___

8.9 Phase 9 — Save Configuration

Purpose: Ensure all device configurations are written to non-volatile memory to prevent loss after reload or power interruption.

- **On Each Configured Device**

```
write memory
```

or

```
! IOS Standard
copy running-config startup-config
```

9. Troubleshooting & Issue Resolution

Purpose: Document challenges encountered during implementation and the strategies used to resolve them, ensuring a smoother deployment process in future labs.

- **Issues & Resolutions:**
    - **VRRP Limitation:** Attempted to implement VRRP for first-hop redundancy, but it failed because Packet Tracer does not support VRRP. HSRP was used instead.
    - **End-Device Connectivity:** Initially, A-PC-01 could not ping EDGE-01. The issue was that EDGE-01 lacked a route back to VLAN 10. Originally, static routes were redistributed into OSPF, but a better solution was implemented by summarizing VLAN networks on distribution switches and advertising them into OSPF.
    - **DNS Router Implementation:** DNS could not be implemented on EDGE-01 due to Packet Tracer limitations, so a dedicated server was used for name resolution.
    - **DHCP Binding Management:** Deleting DHCP bindings is unsupported in Packet Tracer. To assign a new IP to a device, its MBGP Connectivity
    - AC address was changed to trigger a new DHCP lease.
    - **eBGP Connectivity:** eBGP was attempted between EDGE-01 and R2_ISP, but full adjacency and route exchange could not be achieved. The solution was to revert to the previous lab configuration using **PPP with CHAP** for WAN connectivity.

Note: All troubleshooting solutions were applied after the respective protocols and services were implemented, ensuring that the network remained functional and consistent with lab objectives.

10. Essential Verification (Show) Commands

Purpose: Provide a single reference table of essential commands to quickly verify network configuration, connectivity, and service functionality across the lab.

VERIFICATION (SHOW COMMANDS) TABLE

Category	Command	Purpose / What it Shows
VLAN & Access Ports	show vlan brief	Confirms VLAN creation and port assignments
VLAN & Access Ports	show interfaces switchport	Verifies access VLAN and voice VLAN per port
Trunks & Native VLAN	show interfaces trunk	Verifies trunk links and allowed VLANs
EtherChannel	show etherchannel summary	Confirms LACP/PAgP bundle status
Spanning Tree	show spanning-tree vlan <id>	Shows root bridge and port roles
HSRP	show standby brief	Confirms Active/Standby routers & VIPs
Layer 3 EtherChannel	show ip interface brief	Verifies routed port-channel IP and status
PPP w/ CHAP	show interfaces serial <id>	Confirms PPP encapsulation and LCP status
OSPF	show ip ospf neighbor	Verifies OSPF adjacency FULL
OSPF	show ip route ospf	Displays OSPF-learned routes
NAT / PAT	show ip nat translations	Shows active NAT/PAT translations
Routing / Failover	show ip route	Confirms primary/backup default route
ACLs	show access-lists	Quick view of ACL rules and hit counts
NTP	show ntp status	Verifies NTP synchronization
Syslog	show logging	Confirms log messages are being collected
SNMP	show snmp	Checks SNMP operational status
SSH / AAA	show ssh	Displays connected SSH sessions and version

11. Design Decisions & Operational Impact

Operational Impact

The implemented architecture enhances network resilience, scalability, and administrative control. HSRP at the distribution layer ensures gateway redundancy, minimizing user disruption during device or link failures. Layer 3 EtherChannels between core and distribution switches increase bandwidth while providing link-level fault tolerance.

The use of single-area OSPF simplifies routing management and accelerates convergence within the current lab scope, while maintaining flexibility for future multi-area expansion. VLAN segmentation improves security and broadcast domain control, reducing unnecessary traffic and limiting lateral movement between departments.

Structured IP addressing (10.10.0.0/16 for Office A and 10.20.0.0/16 for Office B) enhances route summarization potential and simplifies troubleshooting. Centralized logging and service integration (DNS, DHCP, Syslog) improve operational visibility and administrative efficiency.

Overall, the design balances simplicity and redundancy, providing a stable foundation that supports future wireless integration, security enhancements, and scalability improvements.

12. Encountered Limitations (Packet Tracer Environment)

12. Limitations

Purpose: Documents the functional limitations encountered in Cisco Packet Tracer during lab implementation to clarify simulation constraints and distinguish them from real-world Cisco IOS capabilities.

While this lab was designed to simulate a production-style enterprise network, several functional and feature limitations were encountered due to constraints within Cisco Packet Tracer. The following limitations were identified during implementation:

12.1 First-Hop Redundancy Protocol (FHRP) Support

- VRRP (Virtual Router Redundancy Protocol) is not supported.
- Only HSRP (Hot Standby Router Protocol) is available.

Impact: Limited ability to demonstrate vendor-neutral redundancy configurations.

12.2 AAA (Authentication, Authorization, Accounting)

- Basic AAA functionality is supported.
- Accounting features are not supported
- No TACACS+ capability.

Impact: Cannot fully simulate centralized enterprise authentication and logging policies.

12.3 eBGP (External Border Gateway Protocol)

- eBGP peering is technically implementable.
- However, advanced path attributes, policy manipulation, and real-world ISP behavior simulation are limited.

Impact: eBGP can demonstrate basic adjacency and route exchange, but not full production-level Internet edge behavior.

12.4 NTP (Network Time Protocol)

- Devices can be configured for NTP.
- No integration capability with external/public time sources.

Impact: Time synchronization can be simulated internally, but realistic enterprise time distribution cannot be fully modeled.

12.5 DNS Services

- DNS server functionality is not fully implementable on routers.
- Name resolution features are limited compared to real IOS or server-based DNS.

Impact: Cannot demonstrate enterprise DNS architecture or redundancy.

12.6 Syslog

- Basic syslog configuration is supported.
- Limited log depth, filtering, and severity customization.
- No realistic integration with external SIEM platforms (e.g., Splunk, Wazuh).

Impact: Logging can be demonstrated conceptually but lacks production-grade observability depth.

12.7 SNMP (Simple Network Management Protocol)

- SNMP configuration is available.
- Limited trap functionality and monitoring depth.
- No realistic NMS (Network Management System) integration.

Impact: Monitoring and alerting simulation is constrained.

12.8 Service Source-Interface Limitations

- `source-interface loopback0` not supported.

Impact: Cannot dedicated source simulation hardening practice.

Overall Assessment

Despite these limitations, Packet Tracer remains an effective platform for:

- Core routing and switching fundamentals
- Layer 2/Layer 3 design validation
- High availability concepts (HSRP, EtherChannel)
- OSPF and basic BGP implementation
- Structured IP addressing and enterprise topology modeling

The limitations identified above were acknowledged during design and were mitigated where possible through architectural adjustments.

13. Lessons Learned

Purpose: Capture insights and key takeaways from the lab, highlighting practical challenges, troubleshooting experiences, and best practices to inform future network designs and implementations.

- **Key Lessons and Insights**
    - **Network Design and Layering:** Implementing a phased approach—starting from core, distribution, access, then end devices—ensured a stable, testable, and scalable network. Proper VLAN segmentation and voice/data separation reduced misconfigurations and simplified troubleshooting.
    - **Routing and Redundancy**: HSRP configuration with aligned STP root priorities provided seamless gateway failover, while summarizing VLAN networks in OSPF was a more efficient solution than redistributing static routes, enhancing routing efficiency and reducing configuration complexity.
    - **Protocol Limitations in Packet Tracer:** Certain protocols such as VRRP, eBGP, AAA accounting, and external NTP sources could not be fully implemented. Workarounds—like using static routes, VLAN summarization, or dedicated servers—highlighted the need to adapt lab designs to simulator constraints.
    - **Management and Monitoring:** Enabling NTP, Syslog, SNMP, and SSH/AAA improved operational visibility, centralized logging, and secure administrative access. Assigning VLAN 99 as the management VLAN ensured separation of management traffic from user and voice VLANs.
    - **Troubleshooting and Validation:** Hands-on verification of VLANs, EtherChannels, HSRP, STP, ACLs, NAT/PAT, and PPP links highlighted the importance of step-by-step testing. Issues such as unreachable end devices or misconfigured routes reinforced the need for careful documentation and iterative problem-solving.
    - **Simulator Awareness:** Working within Packet Tracer’s limitations reinforced an understanding of real-world network behavior versus simulation constraints, preparing for practical deployment considerations in physical or production environments.
- **‘Aha’ Moments**
    - **DHCP Handling in Packet Tracer:** Adjusting DHCP allocations via MAC address changes was necessary because deleting DHCP bindings is unsupported in Packet Tracer.
    - **OSPF & Routing Optimization:** Summarizing VLAN networks for OSPF advertisement provided a simpler and more efficient solution than redistributing individual static routes.
    - **Management & Security Practices:** Using VLAN 99 as a dedicated management VLAN improves security and simplifies device administration.
    - **Layer 2 & First-Hop Redundancy Alignment:** Aligning HSRP active roles with STP root priorities optimizes Layer 2 traffic flow and failover behavior.

14. Future Improvements / Next Lab Outline

14. Lab 6 Tasks

Purpose: Extend the current network lab by implementing advanced services, full wireless deployment, and security hardening.

14.1 Wireless Infrastructure Completion

- Fully deploy Wireless LAN Controllers (WLC) and Lightweight Access Points (LWAPs).
- Configure SSIDs, VLAN mapping, and wireless security (WPA2/WPA3).
- Test wireless connectivity for end devices (Admin-LT, laptops, mobile devices).

14.2 Security Hardening

- Implement ACLs to control access between VLANs and limit unnecessary traffic.
- Enable device hardening on switches and routers (disable unused ports, secure management protocols).
- Configure DHCP snooping, Dynamic ARP Inspection, and IP source guard.

14.3 Server Relocation & Service Integration

- Relocate lab servers to their designated VLANs.
- Integrate servers with DNS, DHCP, and NTP services in a structured manner.

14.4. Network Monitoring & Logging

- Expand centralized syslog and SNMP monitoring to include newly added wireless devices.
- Validate alerting and logging functionality for events such as interface flaps, HSRP failovers, and unauthorized access attempts.

14.5. Redundancy and Failover Testing

- Simulate link and device failures to confirm HSRP, OSPF, and EtherChannel redundancy.
- Test PPP failover to ISP links and confirm floating static routes function correctly.

14.6. Documentation & Lessons Learned

- Update the lab documentation with wireless configurations, ACLs, and monitoring settings.
- Record any operational issues, troubleshooting steps, and “aha moments” for future reference.