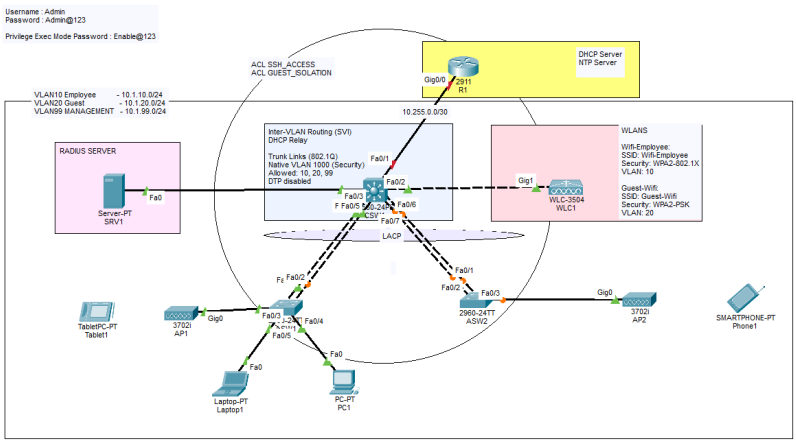
Lab 01: Enterprise Wireless Network

Author : Souaibou BARRY (https://github.com/dineproject)

Topology



Part 1 - Initial Setup

Tasks:

1. Configure the appropriate hostname on each router/switch.

- Router: **R1**
- Core Switch: **CSW1**
- Access Switches: **ASW1**, **ASW2**

2. Configure the enable secret **Enable@123** on each router/switch.

3. Configure the user account **Admin** with secret **Admin@123** on each router/switch. Give the user privilege level 15.

4. Configure the console line to require login with a local user account. Set a **15-minute** inactivity timeout. Enable synchronous logging.

5. Save the configuration on all devices.

Part 2 - VLANs and Layer 2 EtherChannel

Tasks:

1. Use CDP to identify connected ports. Enable port labels: Options → Preferences → Always Show Port Labels in Logical Workspace.

2. Configure a Layer-2 Link Aggregation Group (LAG) between CSW1 and ASW1 using LACP.

- a. Based on CDP discovery, bundle the identified interfaces on both switches
- b. Configure both sides in active mode
- c. Designate the port-channel as PortChannel1

3. Configure a Layer-2 Link Aggregation Group (LAG) between CSW1 and ASW2 using LACP.

- a. Based on CDP discovery, bundle the identified interfaces on both switches
- b. Configure both sides in active mode
- c. Designate the port-channel as PortChannel2

4. Configure 802.1Q trunking on all inter-switch links, including port-channels.

- a. Manually configure trunk mode and disable DTP negotiation
- b. Configure VLAN 1000 as the native VLAN (security best practice)
- c. Restrict trunk to carry only VLANs 10, 20, and 99

5. Implement VLAN management using VTP version 2 in server/client topology.

- a. Configure CSW1 as VTP server with domain name **WirelessLab**
- b. Configure ASW1 and ASW2 as VTP clients
- c. Verify VTP domain synchronization across all switches

6. Create the following VLANs on CSW1 and verify propagation via VTP.

- a. VLAN 10 - Employees (corporate user traffic)
- b. VLAN 20 - Guests (guest wireless traffic)
- c. VLAN 99 - Management (network device management)

7. Between CSW1 and WLC1, configure the trunk.

- a. Configure 802.1Q trunk on CSW1
- b. Disable DTP negotiation
- c. Set native VLAN to 99 (Why?)
- d. Permit VLANs 10, 20, and 99

8. Configure access ports on ASW1 and ASW2 according to the port assignment plan.

- a. Assign VLAN 10 for wired endpoints
- b. Assign VLAN 99 for AP management
- c. Manually configure switchport mode access
- d. Disable DTP on all access ports

9. Implement port security by administratively shutting down all unused interfaces on ASW1 and ASW2.

10. Persist all configurations to NVRAM on all network devices.

Part 3 - IP Addressing and Layer 3 Routing

Tasks:

1. Enable IP routing on CSW1.

2. Configure SVI (Switch Virtual Interface) on CSW1 for inter-VLAN routing.

- a. VLAN 10 (Employees): 10.1.10.1/24
- b. VLAN 20 (Guests): 10.1.20.1/24
- c. VLAN 99 (Management): 10.1.99.1/24

3. Configure loopback interfaces for management and routing stability.

- a. CSW1 Loopback0: 10.255.1.2/32
- b. R1 Loopback0: 10.255.1.1/32

4. Configure the Layer 3 point-to-point link between CSW1 and R1.

- a. On CSW1, convert the interface connected to R1 to a routed port (no switchport)
- b. Assign IP address 10.255.0.2/30 to CSW1
- c. Assign IP address 10.255.0.1/30 to R1

5. Configure a default route on CSW1 pointing to R1 for Internet connectivity.

6. Configure static IP addressing on network devices.

- a. **SRV1:**
  - IP Address: 10.1.10.2
  - Subnet Mask: 255.255.255.0
  - Default Gateway: 10.1.10.1
- b. **WLC1:**
  - IP Address: 10.1.99.2
  - Subnet Mask: 255.255.255.0
  - Default Gateway: 10.1.99.1
- c. **AP1:**
  - IP Address: 10.1.99.3
  - Subnet Mask: 255.255.255.0
  - Default Gateway: 10.1.99.1
- d. **AP2:**
  - IP Address: 10.1.99.4
  - Subnet Mask: 255.255.255.0
  - Default Gateway: 10.1.99.1

7. Verify Layer 3 connectivity.

- a. From CSW1, ping R1 (10.255.0.1)
- b. From CSW1, ping SRV1 (10.1.10.2)
- c. From CSW1, ping WLC1 (10.1.99.2)
- d. From CSW1, ping AP1 (10.1.99.3)
- e. From CSW1, ping AP2 (10.1.99.4)
- f. From SRV1, ping CSW1 SVI (10.1.10.1)

8. Configure routing on R1 to reach internal networks.

- a. From SRV1, ping R1 (10.255.0.1) - Does it work? Analyze why.
- b. Check R1's routing table - Verify if 10.1.0.0/16 route exists
- c. Add a summary route on R1 to reach all internal VLANs: `ip route 10.1.0.0 255.255.0.0 10.255.0.2`
- d. Verify the ping from SRV1 to R1 now succeeds

9. Persist all configurations to NVRAM on all network devices.

Part 4 - DHCP and NTP

Tasks:

1. Configure DHCP excluded addresses on R1 to reserve IPs for static assignments.

- a. Exclude 10.1.10.1 - 10.1.10.9 (VLAN 10)
- b. Exclude 10.1.20.1 - 10.1.20.9 (VLAN 20)

2. Configure DHCP pool for VLAN 10 (Employees) on R1.

- a. Pool name: VLAN10_EMPLOYEES
- b. Network: 10.1.10.0/24
- c. Default gateway: 10.1.10.1
- d. DNS server: 8.8.8.8

3. Configure DHCP pool for VLAN 20 (Guests) on R1.

- a. Pool name: VLAN20_GUESTS
- b. Network: 10.1.20.0/24
- c. Default gateway: 10.1.20.1
- d. DNS server: 8.8.8.8

4. Configure DHCP relay (IP helper-address) on CSW1 for VLANs pointing to R1.

5. Configure R1 as the NTP master server.

- a. Set R1 as NTP master with stratum 1
- b. Configure timezone and clock

6. Configure CSW1, ASW1, and ASW2 as NTP clients.

- a. Point all switches to R1 loopback (10.255.1.1) as NTP server
- b. Configure timezone on all switches

7. Verify DHCP and NTP functionality.

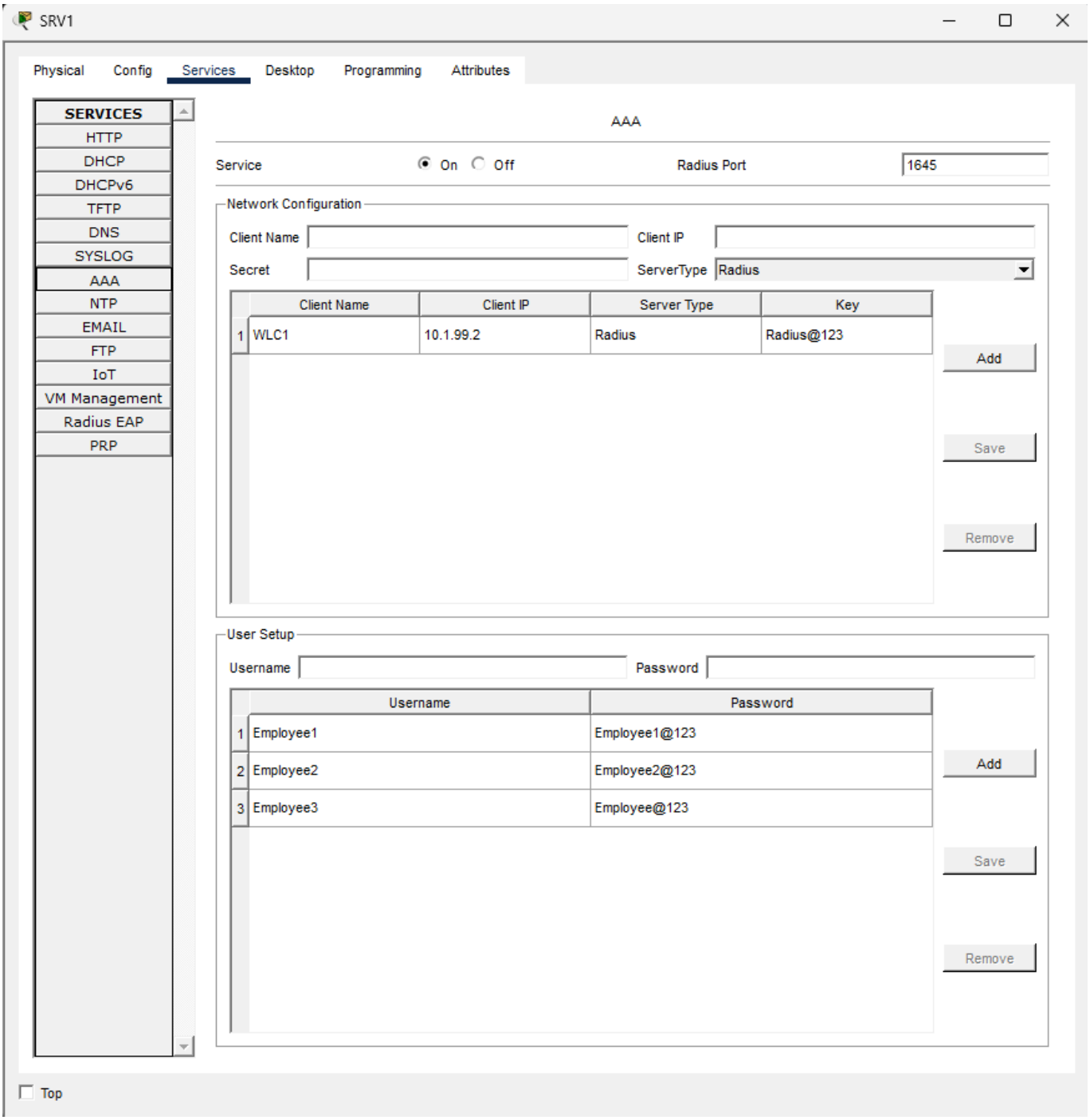
- a. Release and renew IP on a PC - verify it receives DHCP address
- b. Check DHCP bindings on R1
- c. Verify NTP synchronization with `show ntp status` and `show ntp associations`
- d. Check clock synchronization with `show clock`

8. Persist all configurations to NVRAM on all network devices.

Part 5 - Wireless Configuration

Tasks:

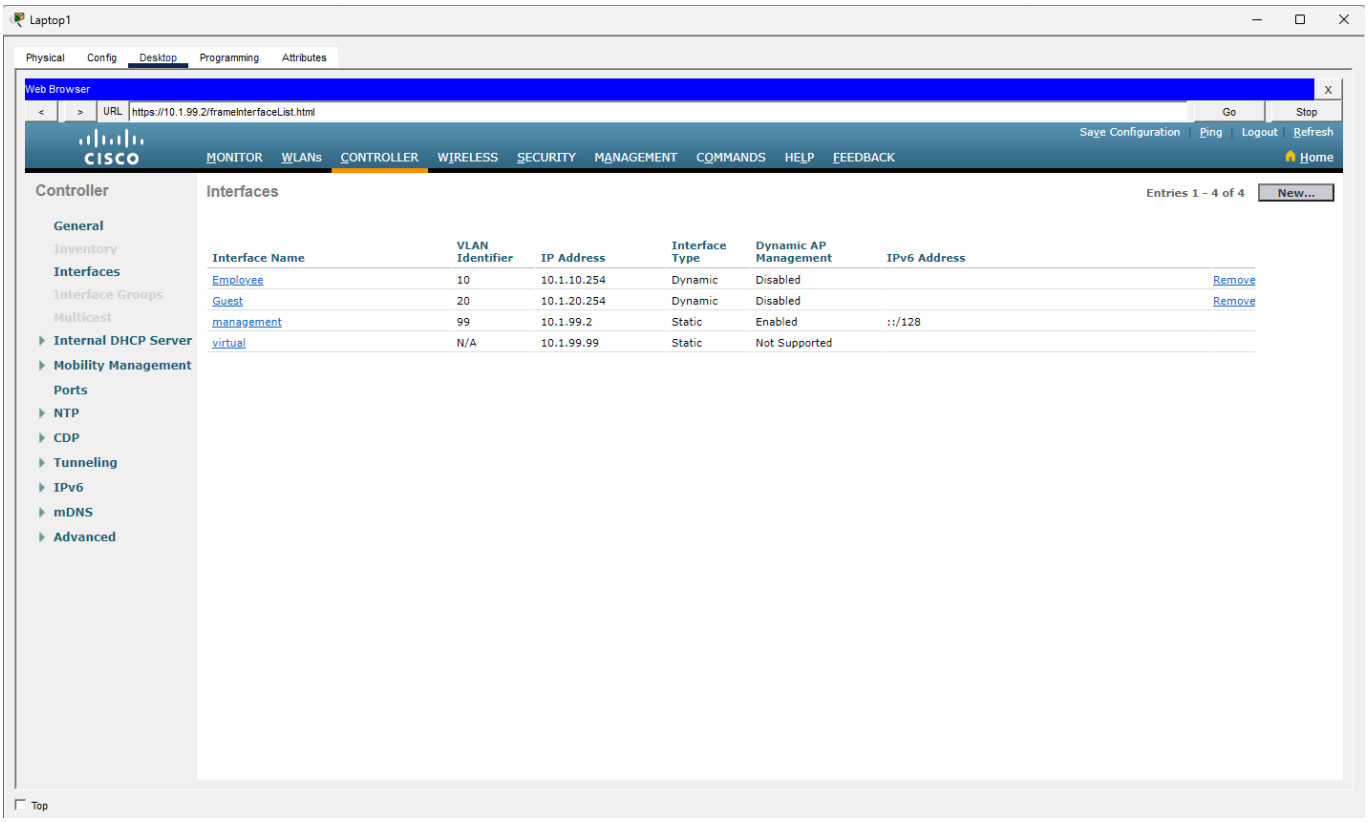
1. Configure RADIUS service on SRV1 for 802.1X authentication. Follow the configuration shown in the screenshot below:

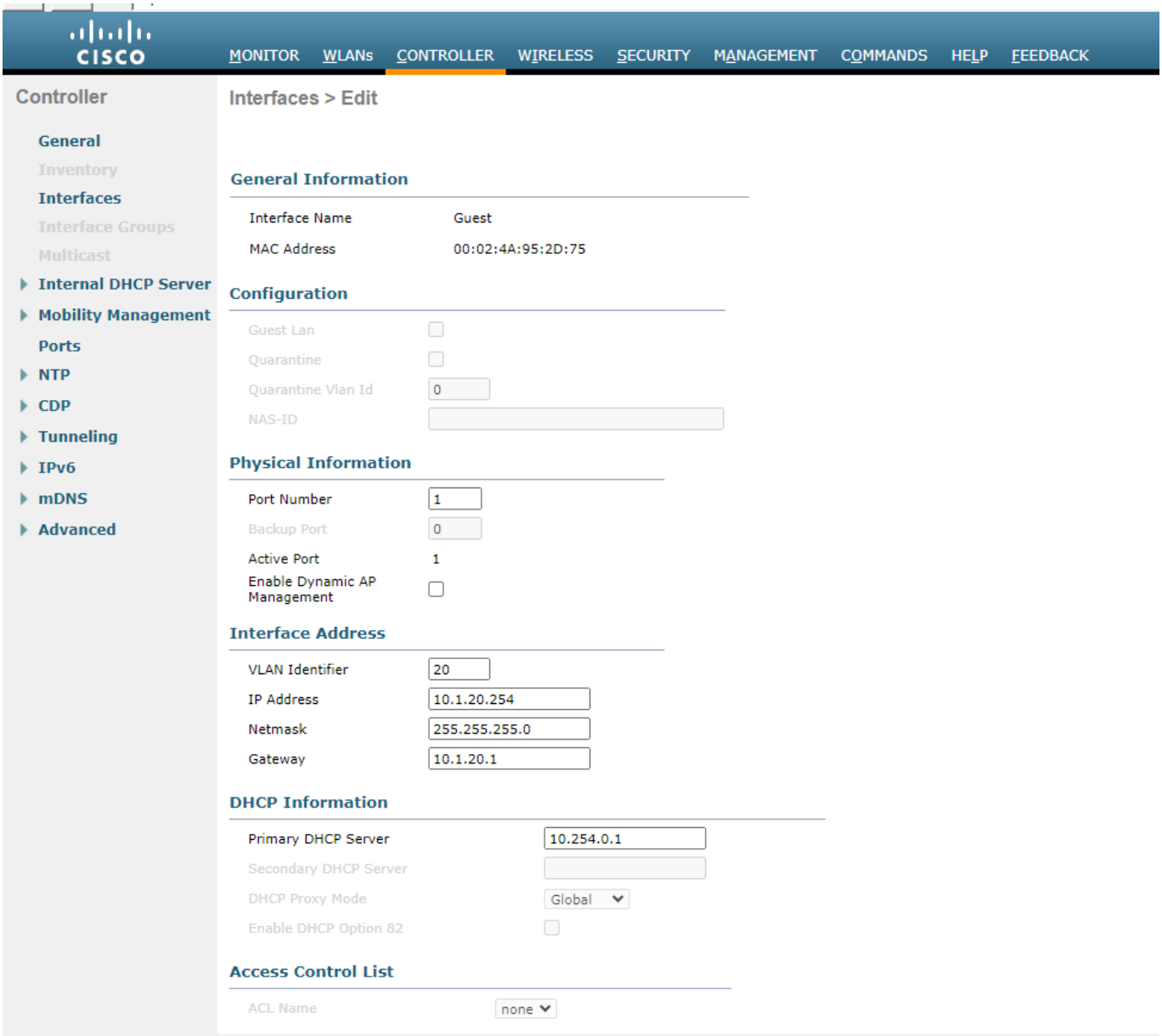


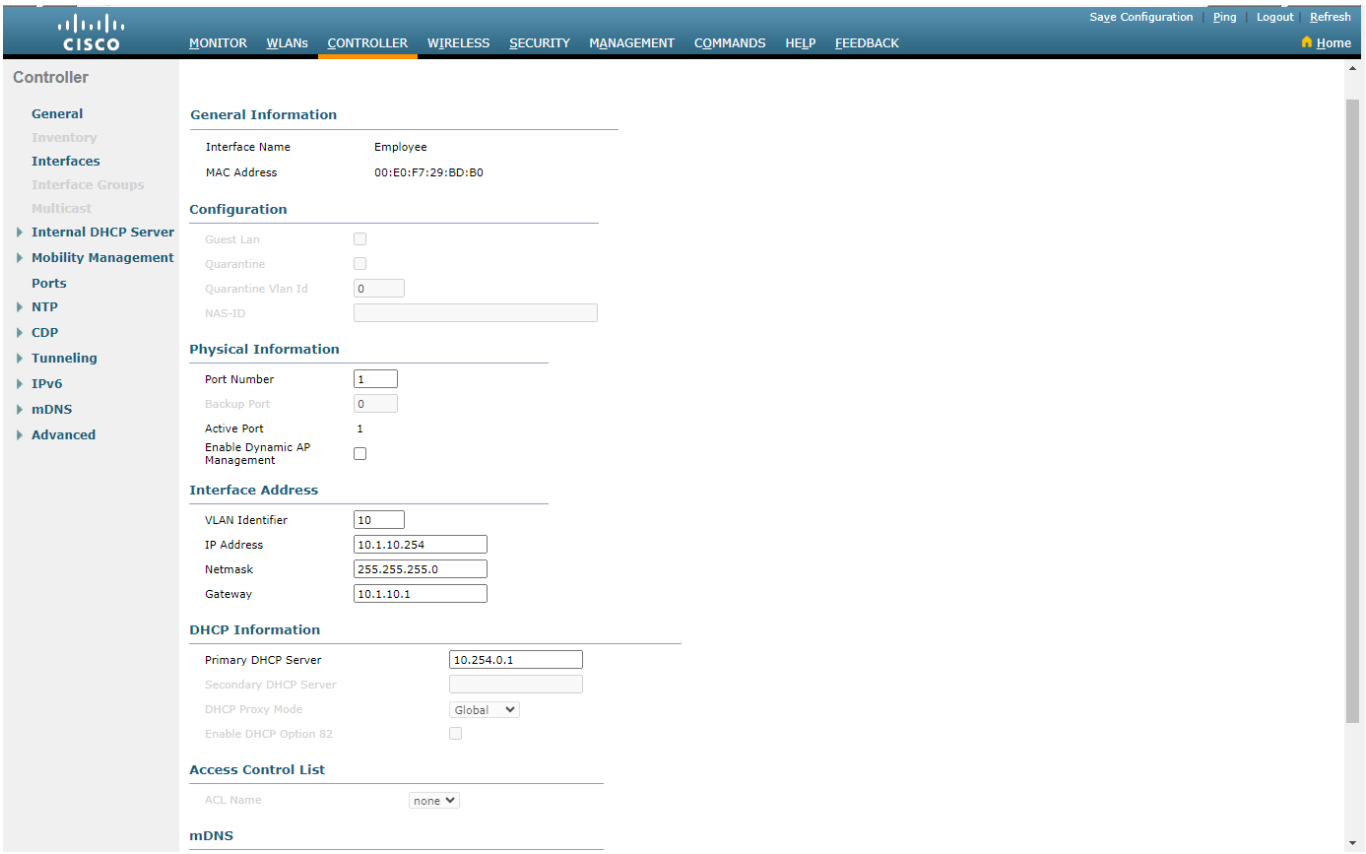
2. Access the WLC1 web interface for initial configuration.

- a. From a PC, open web browser and navigate to: `https://10.1.99.2`
- b. Login with username **Admin** and password **Admin@123**
- c. Navigate through the interface to familiarize yourself with the WLC dashboard

3. Create dynamic interfaces on WLC1 for VLANs. Follow the configuration shown in the screenshots below:


Laptop1
Physical
Config
Desktop
Programming
Attributes
Web Browser
URL
https://10.1.99.2/frameInterfaceList.html
Go
Stop
Save Configuration
Ping
Logout
Refresh
CISCO
MONITOR
WLANs
CONTROLLER
WIRELESS
SECURITY
MANAGEMENT
COMMANDS
HELP
FEEDBACK
Home
Controller
General
Inventory
Interfaces
Interface Groups
Multicast
Internal DHCP Server
Mobility Management
Ports
NTP
CDP
Tunneling
IPv6
mDNS
Advanced
Interfaces
Entries 1 - 4 of 4
New...
Interface Name
VLAN Identifier
IP Address
Interface Type
Dynamic AP Management
IPv6 Address
Employee
10
10.1.10.254
Dynamic
Disabled
Remove
Guest
20
10.1.20.254
Dynamic
Disabled
Remove
management
99
10.1.99.2
Static
Enabled
::/128
virtual
N/A
10.1.99.99
Static
Not Supported
Top


CISCO
MONITOR
WLANs
CONTROLLER
WIRELESS
SECURITY
MANAGEMENT
COMMANDS
HELP
FEEDBACK
Controller
General
Inventory
Interfaces
Interface Groups
Multicast
Internal DHCP Server
Mobility Management
Ports
NTP
CDP
Tunneling
IPv6
mDNS
Advanced
Interfaces > Edit
General Information
Interface Name
Guest
MAC Address
00:02:4A:95:2D:75
Configuration
Guest Lan
Quarantine
Quarantine Vlan Id
0
NAS-ID
Physical Information
Port Number
1
Backup Port
0
Active Port
1
Enable Dynamic AP Management
Interface Address
VLAN Identifier
20
IP Address
10.1.20.254
Netmask
255.255.255.0
Gateway
10.1.20.1
DHCP Information
Primary DHCP Server
10.254.0.1
Secondary DHCP Server
DHCP Proxy Mode
Global
Enable DHCP Option 82
Access Control List
ACL Name
none



4. Create WLANs and assign them to corresponding interfaces. Follow the configuration shown in the screenshots below:

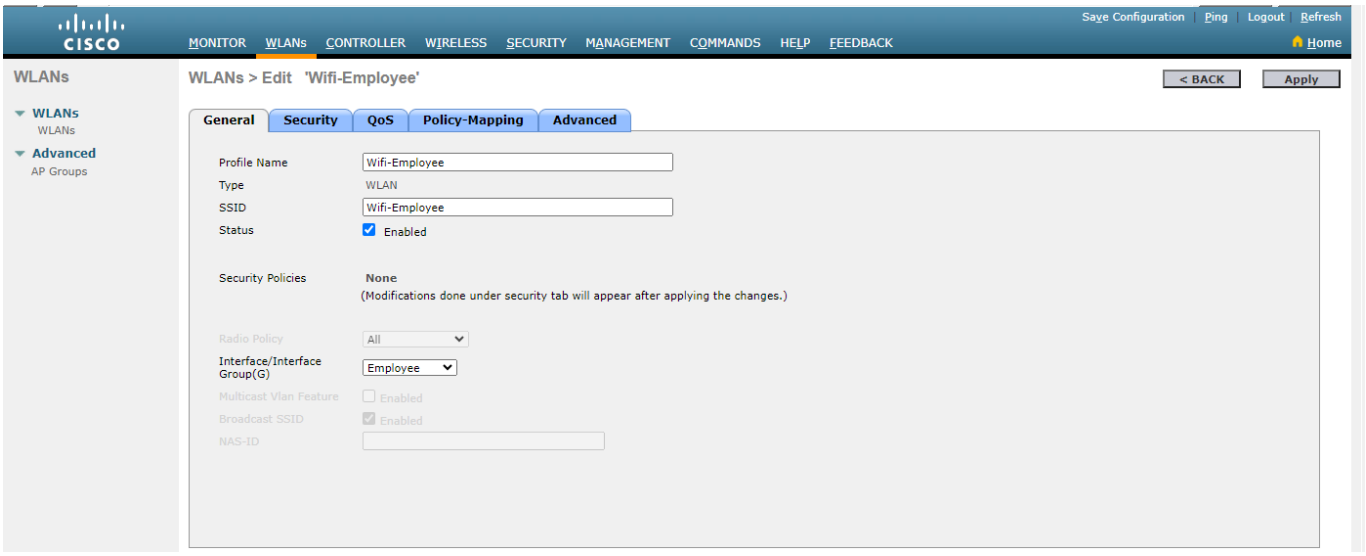
Note: The 802.1X authentication feature for RADIUS is not functional in Packet Tracer for the Employee WLAN. Configure both WLANs using WPA2-PSK instead.

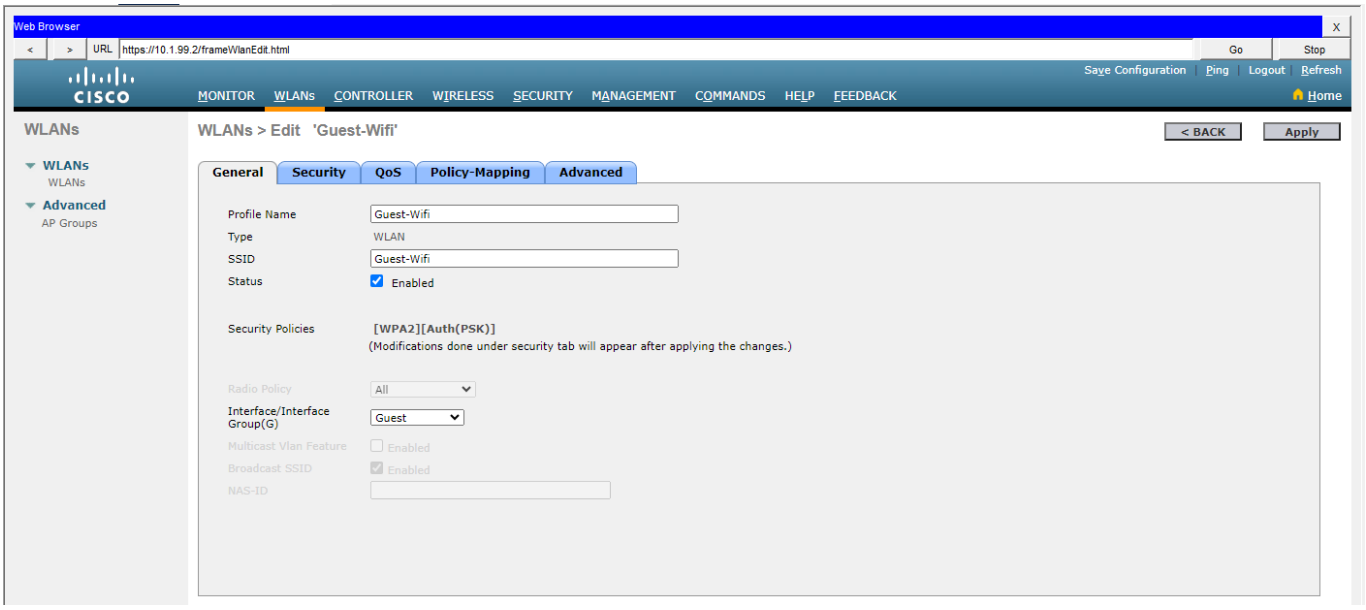
WLAN 1: Wifi-Employee

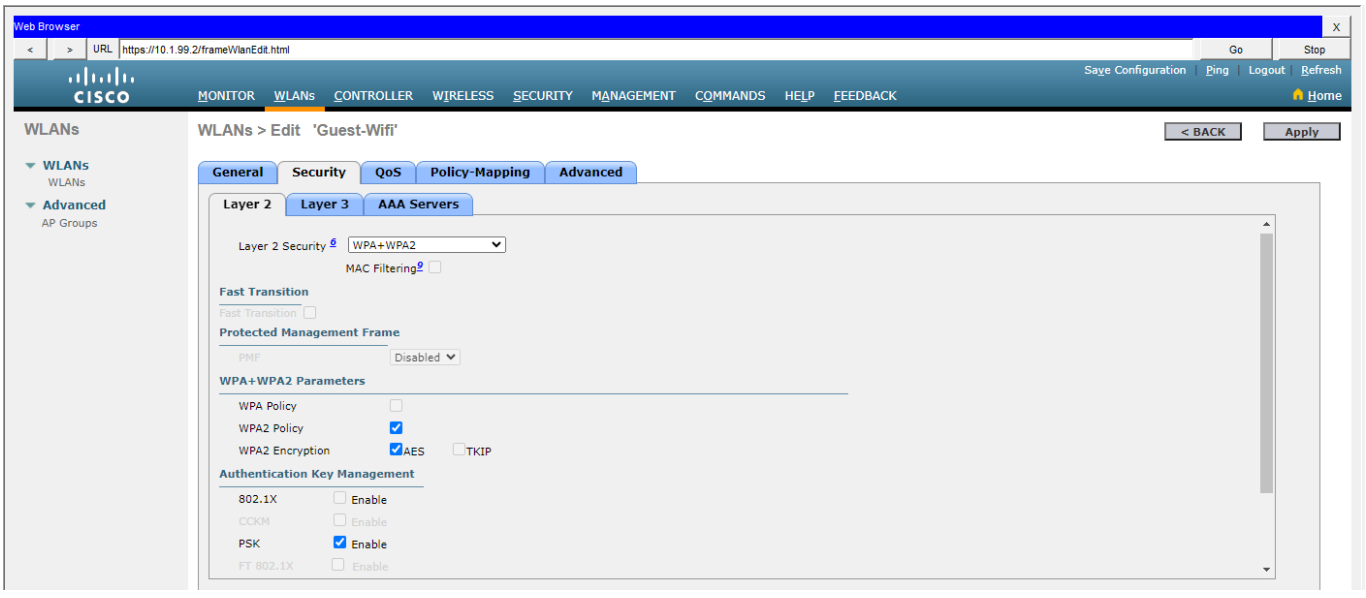
- Profile Name: **Wifi-Employee**
- SSID: **Wifi-Employee**
- Status: **Enabled**
- Interface/Interface Group: **Employee**
- Security: **WPA2-PSK** with password **Employee@123**

WLAN 2: Guest-Wifi

- Profile Name: **Guest-Wifi**
- SSID: **Guest-Wifi**
- Status: **Enabled**
- Interface/Interface Group: **Guest**
- Security: **WPA2-PSK** with password **Guest@123**

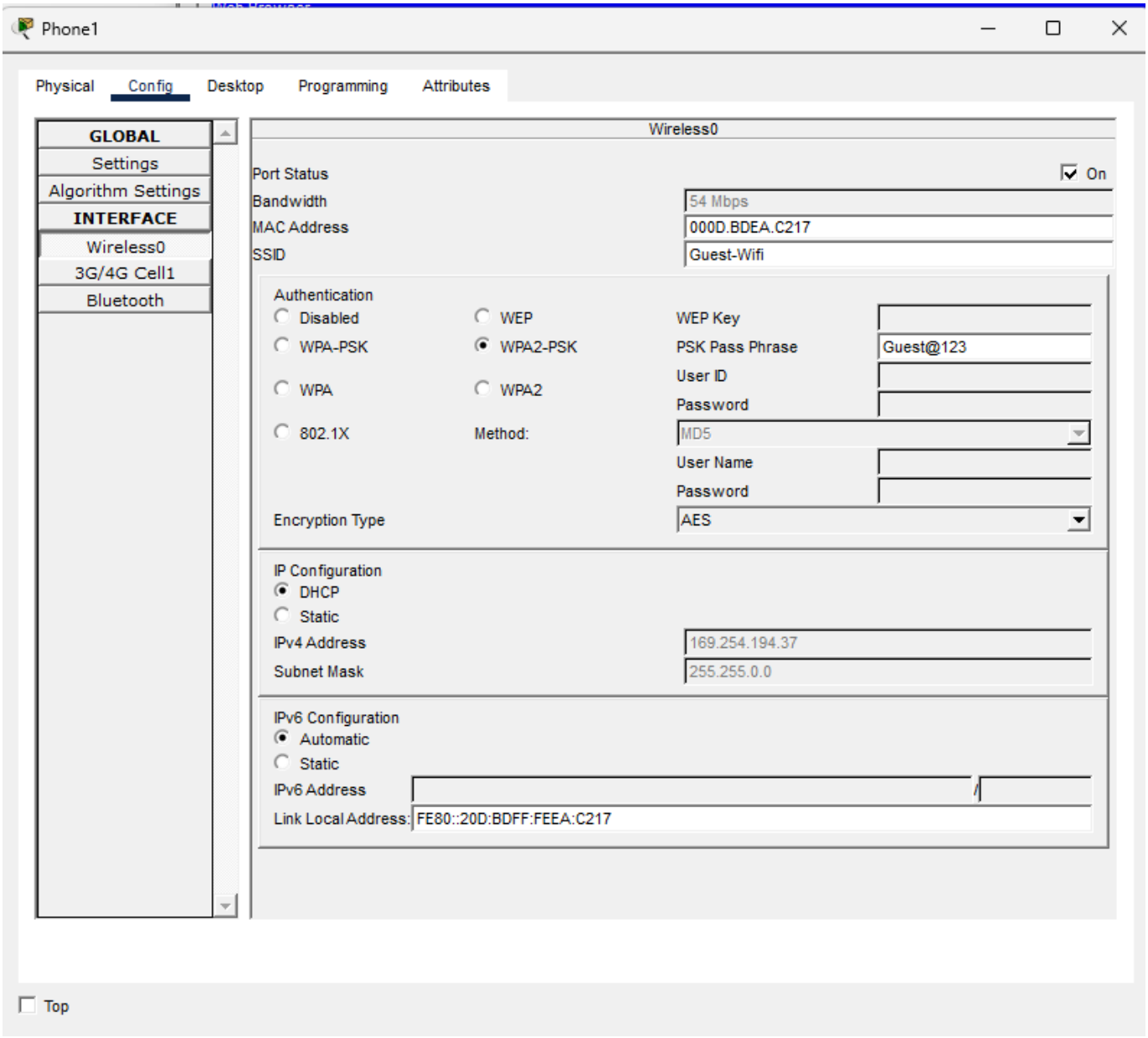






6. Connect a wireless client (Phone) to Guest-Wifi SSID. Follow the configuration shown in the screenshot below:

Note: Due to Packet Tracer's limitations, wireless clients won't be able to lease an IP address from the Wi-Fi DHCP pool.



7. Save all configurations.

- a. In WLC GUI, click **Save Configuration**
- b. Save configurations on all network devices: `write memory`

Part 6 - Access Control Lists (ACLs)

Tasks:

1. Create a Standard ACL to control SSH access to network devices.

- a. On R1, CSW1, ASW1, and ASW2, create ACL named **SSH_ACCESS**
- b. Permit source network 10.1.10.0/24 (Employees)
- c. Permit source network 10.1.99.0/24 (Management)
- d. Apply to VTY lines with `access-class SSH_ACCESS in`

2. Create an Extended ACL to isolate Guest network from internal resources.

- a. On CSW1, create ACL named **GUEST_ISOLATION**

- b. Deny IP from any source to 10.1.10.0/24 (block access to Employee VLAN)
- c. Deny IP from any source to 10.1.99.0/24 (block access to Management VLAN)
- d. Permit IP to any (allow Internet access)
- e. Apply inbound on VLAN 20 interface: `ip access-group GUEST_ISOLATION in`

Part 7 - SSH (Secure Shell)

Tasks:

1. Configure SSH on all network devices (R1, CSW1, ASW1, ASW2).

- a. Set domain name: **lab.local**
- b. Generate RSA crypto keys with 2048 bits
- c. Set SSH version 2
- d. Configure VTY lines to use SSH only (no Telnet)
- e. Set VTY timeout to 10 minutes

2. Test SSH connectivity.

- a. From a PC in VLAN 10, SSH to CSW1: `ssh -l Admin 10.1.99.1`
- b. From a PC in VLAN 10, SSH to R1: `ssh -l Admin 10.255.0.1`
- c. Verify you can login with username **Admin** and password **Admin@123**

3. Persist all configurations to NVRAM on all network devices.

More Labs on : https://github.com/dineproject/network-mega-labs