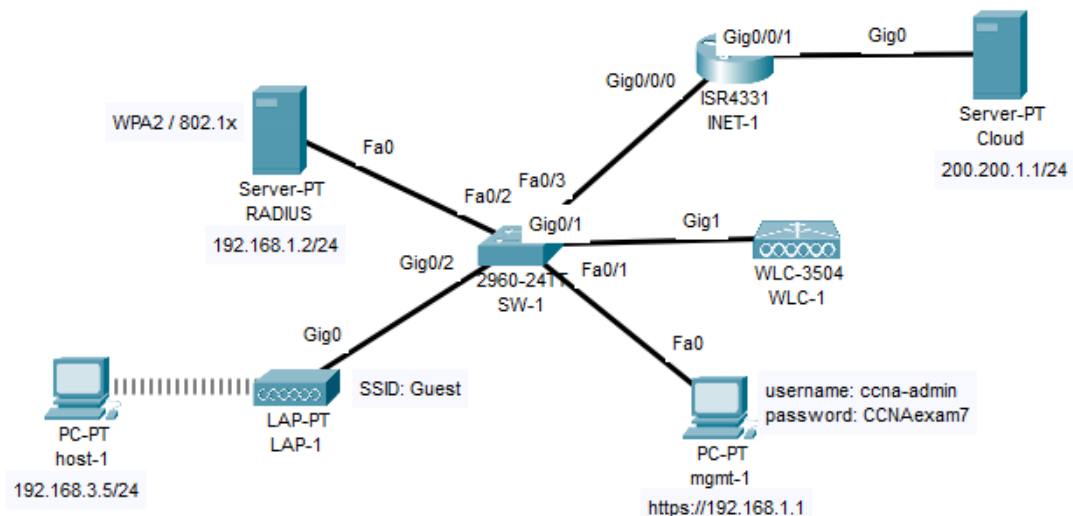


# Wireless LAN Controller

## Lab Summary

Configure wireless LAN controller via GUI to enable internet access for wireless clients. All network devices and hosts are configured except for the controller..

**Figure 1** Lab Topology



## Lab Configuration

Start Packet Tracer File: **wireless lan controller.pkt**

Click on *mgmt-1* icon and start web browser session to configure WLC-1 controller.

Step 1: **http://192.168.1.1** (15-20 seconds delay)

Create an admin account

Step 2. Username: **ccna-admin**

Step 3. Password: **CCNAexam7**

Step 4: Click Start

Initial Controller Setup

- System name: **WLC-1**
- Date and Time: update
- Timezone: local
- Management IP address: **192.168.1.1**

- Subnet mask: **255.255.255.0**
- Default gateway: **192.168.1.254** (INET-1)
- Management VLAN ID: **0** (untagged)
- Select Next

#### Create Wireless Network

- Network Name: **Guest**
- Security: **WPA2 Enterprise**
- Authentication Server IP Address: **192.168.1.2**
- Auth Server Shared Secret: **cisco**
- Select Next

#### Advanced Settings

- Default settings
- Select Next

#### Review and Click Apply

OK to reboot controller and close window manually instead of waiting.

Click on mgmt-1 icon to start web browser session and login to controller.

**https://192.168.1.1**

Username: **ccna-admin**

Password: **CCNAexam7**

\*Maximize MONITOR summary window

Click on CONTROLLER main tab .

- Click on Interfaces
- Select New
- Interface Name: **Guest**
- VLAN Id: **10**
- Select Apply

### Interfaces Edit Window

- port number **1**
- VLAN identifier: **10**
- IP address: **192.168.3.1**
- Netmask: **255.255.255.0**
- Gateway: **192.168.3.254**
- Select Apply
- Save Configuration

### Interfaces Window (no changes)

- Select management (default)
- Select back arrow
- Select virtual (default)

### Click on WLANs main tab

- Click on WLAN ID 1 and select remove
- Select Create New
- Profile Name: **Guest**
- SSID: **Guest**
- ID: 10
- Select Apply

### Click on General tab

- Select status enabled
- Select interface group: **Guest**
- Profile Name: **Guest**
- Select Apply

### Click on Security tab

- Select Layer 2 Security: **WPA + WPA2**
- Select WPA2 Policy
- Select WPA2 Encryption: **AES**
- Select Authentication Key Management: **802.1X**
- Select Apply

Click on Security tab

- Select AAA Servers tab
- Select Server 1: **192.168.1.2, Port: 1812**
- Select Apply

Click on QoS tab

- Silver best effort (default)

Click on CONTROLLER main tab .

- Click on Internal DHCP server
- Select DHCP Scope (LAP)
- Select day0-dhcp-mgmt
- Pool Start Address: **192.168.1.3**
- Pool End Address: **192.168.1.5**
- Netmask: **255.255.255.0**
- Default router: **192.168.1.1**
- Select Apply
- Save Configuration
- Select Ports
- Verify Port Number 1: 1000 Mbps / Full Duplex

Click on WIRELESS main tab .

- Verify automatic detection of LAP-1
- DHCP assigned address 192.168.1.3

Click on SECURITY main tab .

- Verify RADIUS server IP address and UDP 1812
- Verify status is enabled

Click on MANAGEMENT main tab .

- Verify HTTPS default mode is enabled for security
- Select SNMP General tab
- Verify SNMP default settings

- Add location / contact email and apply (optional)
- Select Local Management Users tab
- Create a backup account for troubleshooting and apply (optional)
- Select Logs tab and verify system messages

Click on COMMANDS main tab .

- Verify date, time, and timezone settings
- Review other management commands available
- Save Configuration

Click on MONITOR main tab .

- Review the current controller operational status
- **ping 192.168.1.254** (INET-1) from controller GUI (top corner)
- Logout

#### Verify Lab

Ping host-1 from INET-1 router to populate ARP table.

**ping 192.168.3.5**

Start a web browser session from host-1 to the cloud server.

**https://200.200.1.1**