

Packet Tracer Lab 13 Solution Guide

Enterprise Wireless Login Failure

Incident ID: INC-1013

Objective

This lab focuses on identifying and restoring enterprise wireless authentication following scheduled wireless maintenance.

Although the wireless infrastructure remains operational and the corporate SSID is visible, enterprise users are unable to authenticate successfully.

The objective is to troubleshoot the issue using a structured methodology, identify the root cause, restore authentication, and validate successful wireless connectivity. The solution guide structure mirrors your previous labs while adapting the troubleshooting steps for this enterprise wireless scenario.

Root Cause

The Wireless LAN Controller was configured with an incorrect RADIUS server IP address.

Instead of using the correct AAA server:

192.168.100.10

the WLC was configured to use:

192.168.100.20

As a result:

- The WLC could not communicate with the AAA server.
- Enterprise authentication failed.
- Wireless clients could not successfully authenticate.

BridgeOpsOne

Symptoms Observed

- Corporate SSID visible.
- Access Points online.
- WLC operational.
- AAA server powered on.
- Wireless clients unable to authenticate.
- Enterprise wireless unavailable.

Troubleshooting Process

Step 1 — Verify WLAN Availability

Verify:

- Corporate SSID visible.
- Access Points online.

This confirms the wireless infrastructure is functioning.

Step 2 — Verify Access Point Registration

Access the WLC.

Review:

AP Groups

Verify:

- AP1 Online
- AP2 Online

This confirms both Access Points remain registered with the controller.

BridgeOpsOne

Step 3 — Verify Enterprise Authentication Configuration

Review the WLAN configuration.

Verify:

- WPA2 Enterprise enabled
 - RADIUS authentication configured
-

Step 4 — Verify AAA Server Configuration

Access:

AAA-SRV

Navigate to:

Desktop → IP Configuration

Navigate to **AAA-SRV → Desktop → IP Configuration** and verify the server's IPv4 address is **192.168.100.10**.

Verify:

AAA Server IP

192.168.100.10

Step 5 — Compare RADIUS Configuration

Review the Wireless LAN configuration on the WLC.

Users should identify:

Configured RADIUS Server

192.168.100.20

Compare this with the actual AAA server IP.

This identifies the incorrect RADIUS server configuration as the root cause.

BridgeOpsOne

Commands Used / Tools Used

- ipconfig
- ping
- WLC Wireless LAN Configuration
- WLC AP Groups
- AAA Server IP Configuration

Resolution

Access:

WLC

Navigate to:

Wireless LANs

Update:

RADIUS Server IP

192.168.100.20

↓

192.168.100.10

Save the configuration.

Validation

Successful resolution should include:

- Laptop successfully authenticates.

BridgeOpsOne

- Tablet successfully authenticates.
- Smartphone successfully authenticates.
- DHCP address assigned successfully.
- Successful ping to the default gateway.
- Successful ping to the DNS server.
- Successful ping to the AAA server.
- Enterprise wireless authentication restored.
- Wireless clients automatically reconnect after correcting the RADIUS server IP.

Key Takeaways

- Enterprise wireless relies on successful communication between the WLC and the AAA server.
- Access Points can remain fully operational while enterprise authentication fails.
- Always compare infrastructure configurations instead of assuming they are correct.
- Verify both sides of a client/server relationship during troubleshooting.
- Follow a structured troubleshooting methodology.
- Validate successful authentication after completing repairs.