

Packet Tracer Lab 12 Solution Guide

Wireless Authentication Failure

Incident ID: INC-1012

Objective

This lab focuses on identifying and restoring wireless connectivity following scheduled wireless infrastructure maintenance.

Although the wireless network remains visible and Access Points continue operating normally, wireless clients are unable to successfully authenticate and obtain network connectivity.

The objective is to troubleshoot the issue using a structured methodology, identify the root cause, restore wireless authentication, and validate successful client connectivity.

Root Cause

The WPA2-PSK passphrase configured on the Wireless LAN Controller did not match the documented corporate wireless password.

As a result:

- Wireless clients failed WPA2 authentication.
- Clients were unable to complete association.
- DHCP leases were never obtained.
- Users were unable to access internal network resources.

Symptoms Observed

- Corporate SSID visible.
- Access Points online.
- Wireless clients unable to connect.
- Clients receive APIPA (169.254.x.x) addresses.

BridgeOpsOne

- No default gateway assigned.
- No DNS server assigned.
- Internal network resources inaccessible.

Troubleshooting Process

Step 1 — Verify Wireless Network Availability

From the wireless laptop:

Confirm that BridgeOps-Corp is visible.

This confirms:

- **Wireless infrastructure is operational.**
 - **Access Points are broadcasting the SSID.**
-

Step 2 — Verify Client IP Configuration

Run:

ipconfig

Users should observe:

- **APIPA (169.254.x.x) address**
- **No default gateway**
- **No DNS server**

This indicates the client never successfully authenticated to the wireless network, preventing DHCP from assigning an IP address.

Step 3 — Verify Wireless Infrastructure

Access the Wireless LAN Controller.

Verify:

BridgeOpsOne

- **AP1 Online**
- **AP2 Online**
- **BridgeOps-Corp WLAN enabled**

This confirms the issue is not caused by offline access points or a failed Wireless LAN Controller.

Step 4 — Review WLAN Configuration

Open the BridgeOps-Corp WLAN configuration.

Review the configured WPA2-PSK passphrase.

Users should identify that the configured passphrase does not match the documented corporate password.

This is the primary indicator of the issue.

Commands Used

ipconfig

ping

Resolution

Access the Wireless LAN Controller.

Navigate to:

Wireless LANs → BridgeOps-Corp

Correct the WPA2-PSK passphrase:

Incorrect

BridgeOps2026

Correct

BridgeOpsOne

BridgeOps2026!

Save the configuration.

The wireless client should automatically reauthenticate and obtain a valid DHCP lease.

Validation

Successful resolution should include:

- Wireless client successfully connects to BridgeOps-Corp.
- Valid DHCP address assigned.
- Default gateway assigned.
- DNS server assigned.
- Successful ping to the default gateway.
- Successful ping to the DNS server.
- Successful ping to the AAA server.
- Wireless client successfully associates with AP1 or AP2.

Key Takeaways

- Wireless authentication occurs before DHCP.
- A visible SSID does not guarantee successful client authentication.
- APIPA addresses often indicate a failure earlier in the connection process.
- Validate wireless infrastructure before assuming a DHCP issue.
- Compare documented configuration values with actual device configurations.
- Follow a structured troubleshooting methodology and validate successful service restoration.
- Authentication must succeed before a wireless client can obtain a DHCP lease.

BridgeOpsOne