Network Troubleshooting Report

Task done by Kimberly Chigarira | Task provided by Teltonika

S2 and S3 Problems

Problem

S3 and S2 network devices cannot reach HTTP server and S2 network devices cannot reach S3 network devices. The devices could not reach the HTTP server because of misconfigurations in the routing table and DHCP settings, leading to packet loss.

Where was this problem located in the topology?

The issue was caused by routing misconfigurations on R2, and incorrect or missing configurations on the end devices in both S2 and S3.

Steps Taken to Troubleshoot and Resolve the Issue

1. Approach

I approached the problem by first troubleshooting each network separately, ensuring that the devices could communicate within their respective networks before addressing the inter-network connectivity and HTTP access issues.

2. S2 Network Troubleshooting

- On R2, I checked the routing table and discovered a misconfigured static route:
- Incorrect: 192.168.55.0/24 via 10.0.0.60
- Correct: 192.168.55.0/24 via 10.0.0.61 (WR1) •   Also, there was no static route from R2 to R1 at all.
- I corrected the static route entries accordingly.
- On end devices:
- PC0 had a wrong IP, incorrect subnet mask, and no default gateway.
- PC1 had an APIPA address due to a failed DHCP request. The issue was that the DHCP server had no default gateway set.
- I manually corrected PC0's settings.

- For PC1, I enabled DHCP again after fixing the DHCP server, and the correct IP was assigned.
- I verified connectivity between devices on S2 using ping, which was successful.

3. S3 Network Troubleshooting

- Similar issues were present:
- Devices were not getting IPs due to missing DHCP server configuration.
- R2 had no static route to WR1.
- I added the necessary static route on R2.
- I then configured the DHCP server to assign correct settings to S3 devices.
- After doing this, devices in S3 successfully communicated within the network.

4. Restoring S2 to S3 Communication and HTTP Access

- The final issue was that S2 didn't have a static route to S3, preventing inter-network communication.
- I added a static route from S2's router to S3's network via R2.
- I re-verified connectivity from both networks to each other.

5. HTTP Server Access

- The misconfiguration in the routing table and DHCP settings seemed to have been causing lost packets, preventing the devices from reaching the HTTP server.
- After all configurations were corrected, the devices could successfully communicate with the HTTP server.
- I verified HTTP access by pinging the server and then testing the web browser to access the server's HTML files. I successfully navigated through the pages, confirming the issue was resolved.

Why this solution?

The misconfigured static routes and DHCP settings prevented the devices from discovering correct paths and obtaining valid IP configurations. Once these were corrected, the devices were able to reach the HTTP server, and packet loss was eliminated. Ensuring that all routers had the correct static routes and all DHCP servers were properly configured allowed for proper inter-network communication and access to the HTTP server.

Cell Tower

Problem

Not all smartphones connected to cell tower can reach HTTP server and its HTML files/websites.

Where was this problem located in the topology?

The issue was traced to the iPhone 14's routing configuration settings.

Steps Taken to Troubleshoot the Problem

1. Initial Connectivity Test

I tested HTTP server connectivity by pinging from all phones. Every smartphone responded successfully except the iPhone 14.

2. Configuration Comparison

I compared the iPhone 14's configuration with other functioning smartphones and discovered that:

- iPhone 14 was set to static IP and routing configuration
- Other smartphones were using dynamic configuration (DHCP)

3. Adjusting Configuration

I switched the iPhone 14 from static to dynamic by:

- Disabling the static IP settings
- Enabling dynamic (DHCP) settings
- Performing a DHCP refresh to allow the phone to automatically obtain the correct network settings

4. Verification of Connectivity

I pinged the HTTP server from the iPhone 14 again, which now responded successfully. However, I didn't stop there.

5. HTTP Functionality Test (Beyond Ping)

To ensure full web access:

- I opened each smartphone's browser
- Typed http://169.15.80.160 (IP of server) in the URL bar
- Confirmed access to the Cisco default web page
- Navigated through various hyperlinks, confirming that images and content loaded correctly **Why this solution?**

Switching to DHCP ensures compatibility and centralized management of IP addressing and routing via the cell tower. Additionally, testing HTTP access using a browser ensured that application-layer services (not just network-layer pings) were functioning.

WR1 Router

Problem

Not all end devices can connect to router through wireless connection.

Where was this problem located in the topology?

The issue was traced to Router WR1's Wireless MAC Filter settings.

Steps Taken to Solve the Problem

1. Initial Investigation

I reviewed the wireless configuration of all four WR1 network devices. I compared the configurations of those that could connect (e.g., LAP1) with those that could not (e.g., PC5) to identify any inconsistencies.

2. Device-Specific Observation

LAP1's settings were correct, but it could not connect. Meanwhile, PC5 had a failed DHCP request, indicating it was not receiving an IP address.

3. Router Configuration Review

I checked Router WR1's wireless settings and discovered that MAC address filtering was enabled. LAP1's MAC address was not on the allowed list.

4. Solution Implementation

I added LAP1's MAC address to the filter list and saved the changes.

5. Verification

LAP1 successfully connected to the Wi-Fi. I verified connectivity by pinging both the router and other LAN devices — all responses were successful.

6. Next Device (PC5)

I moved on to PC5, which was still unable to connect to the network.

Why this solution?

MAC address filtering is a common security feature that restricts Wi-Fi access to approved devices. Adding the correct MAC address restored connectivity while maintaining network policy.

Conclusion

This task provided a valuable opportunity to engage in hands-on troubleshooting across multiple network segments. It enhanced my understanding of IP addressing, DHCP functionality, and static routing. It introduced me to a topology with a cell network and wireless connections. The exercise emphasized the importance of attention to detail, as a minor misconfiguration such as an incorrect IP address or missing default gateway can result in significant network issues.