CDP, LLDP, and NTP Configuration Lab Report

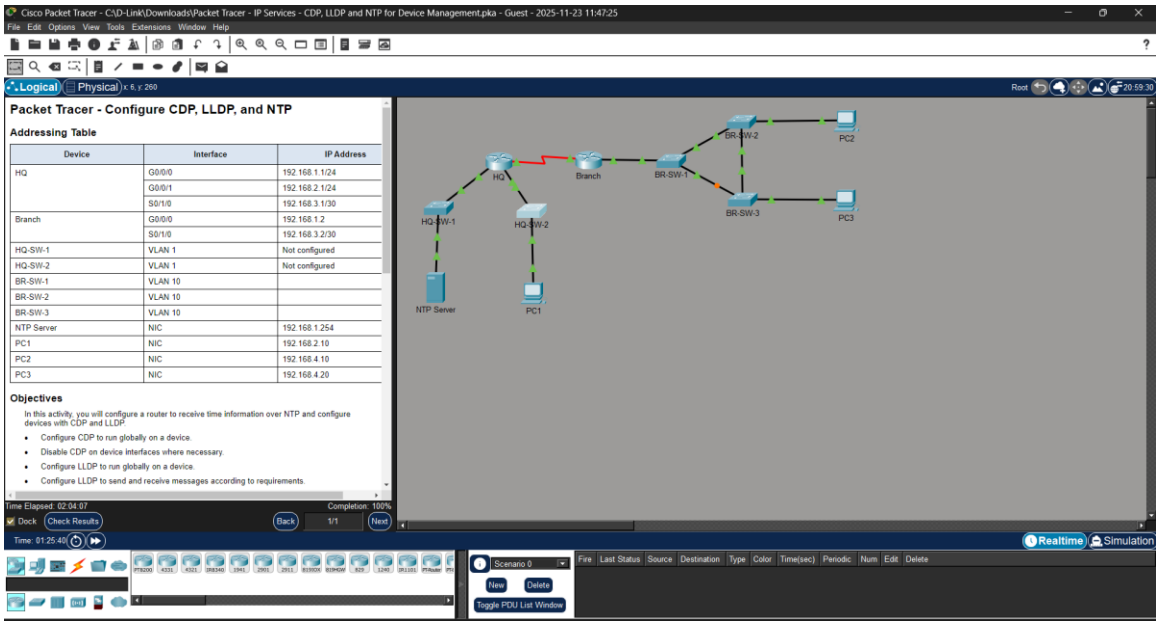
1. Introduction

This report documents the configuration and verification of CDP (Cisco Discovery Protocol), LLDP (Link Layer Discovery Protocol), and NTP (Network Time Protocol) across the HQ and Branch network infrastructure. The objective is to enable secure discovery protocols, disable unwanted protocol traffic on access ports, configure LLDP according to network design, and synchronize the HQ router to an NTP server for accurate timekeeping.

2. Network Topology Overview

The completed network topology, as shown in the screenshot below, consists of HQ and Branch routers connected through a WAN serial link. HQ is connected to two distribution switches (HQ-SW1 and HQ-SW2), while the Branch router connects to BR-SW1, BR-SW2, and BR-SW3. An NTP server is located at the HQ side.

Figure 1: Completed Network Topology



3. CDP and LLDP Configuration

This section provides labeled screenshots validating CDP enablement on Branch devices and LLDP configuration across HQ routers and switches. CDP was activated on Branch, and disabled on HQ side to improve security. LLDP was enabled on HQ and configured for controlled direction on uplinks and disabled on access ports.

Figure 2: HQ Router - LLDP Interface Configuration and Status

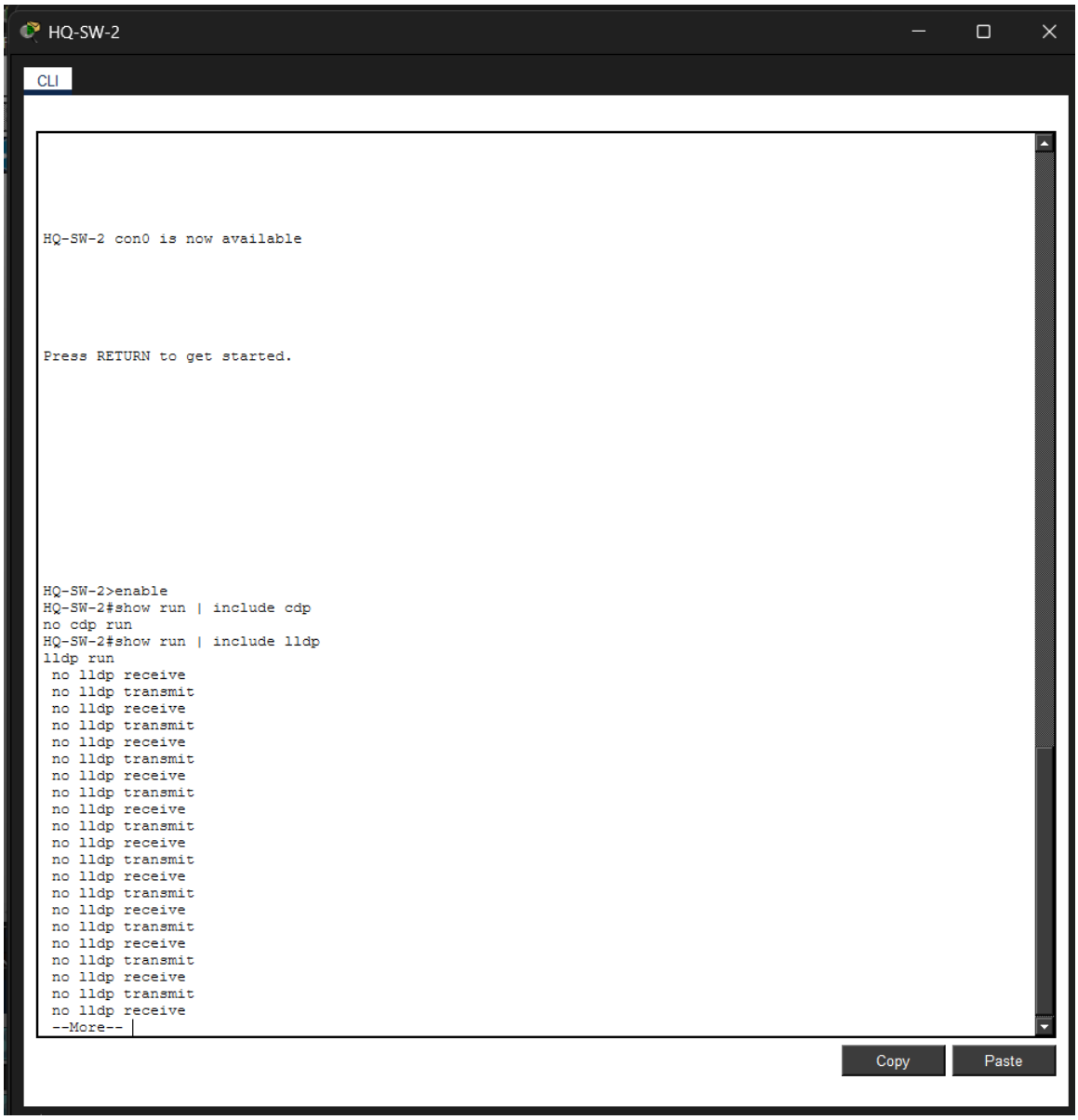


Figure 3: HQ Router - LLDP Global Status and Interface Direction Control

4. NTP Configuration and Verification

The HQ router was configured to use the NTP server at 192.168.1.254. Verification confirms NTP associations and synchronization. This ensures accurate logging, consistent timestamps, and cross-device event correlation.

Figure 4: HQ Router - NTP Configuration and Sync Verification

5. Conclusion

The lab objectives were successfully completed. CDP was selectively enabled on Branch and disabled on HQ in alignment with network security standards. LLDP was deployed on HQ routers and switches with controlled sending and receiving directions to prevent unnecessary discovery traffic. NTP synchronization was properly configured, validated, and fully operational. The network is now prepared with secure discovery mechanisms and accurate time services as required for network monitoring, troubleshooting, and log correlation.