ESCUELA COLOMBIANA DE INGENIERÍA JULIO GARAVITO

UNIVERSIDAD

Computer Networks Laboratory

Laboratory No. 4
Application Layer and Physical Layer Protocols

Network Protocol Analysis and Structured Cabling Implementation

Students:

Cristian Santiago Pedraza Rodríguez

Andersson David Sánchez Méndez

Instructor: Professor Fabian Eduardo Sierra Sánchez
Course: Computer Networks

Institution: Escuela Colombiana de Ingeniería Julio Garavito

September 28, 2025

Contents

1 Objectives

- Monitor the application layer protocols
- Review the structured cabling standard and its application
- Perform cable punching with RJ-45 connectors and patch panels

2 Tools and Equipment

2.1 University-Provided Items

- Computers with network access
- Internet connectivity
- Patch panels and faceplates
- Professional punch tools (patch cords and impact punches)
- Cable strippers and wire cutters
- Network cable testers

2.2 Student-Provided Materials

- 4-6 meters of UTP/FTP CAT5 or CAT6 cable
- 8 RJ-45 connectors
- **Optional (if available):**
  - Personal cable stripper or utility knife
  - Personal wire cutters
  - Personal punch tool for patch cords
  - Personal cable tester

3 Introduction

Modern enterprise IT infrastructure encompasses a complex ecosystem of interconnected components. This infrastructure typically includes both wired and wireless user stations, physical and virtualized servers, all interconnected through sophisticated networking equipment including Layer 2 and Layer 3 switches, wireless access points, and routers providing internet connectivity.

Contemporary networks often integrate cloud infrastructure where resources are dynamically provisioned based on organizational requirements. Server infrastructure commonly hosts essential services including web servers, DNS, email systems, databases, storage solutions, and various business applications.

This laboratory focuses on two critical aspects of network infrastructure:

1. **Application Layer Protocol Analysis** - Understanding how data flows through network protocols
2. **Physical Layer Implementation** - Hands-on structured cabling and connector installation

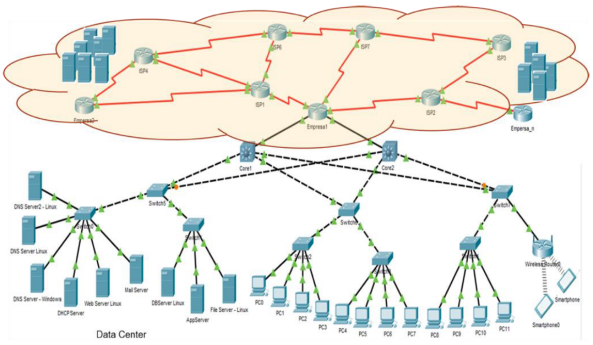

Figure 1: Network Infrastructure Overview

4 Laboratory Experiments

Network message analysis and content examination are fundamental skills for network optimization and troubleshooting. This section covers application layer protocols and transport layer port analysis as covered in our coursework.

Exercise 1: Cisco Packet Tracer Configuration

Target Group: Teams of 1-3 students
Using Cisco Packet Tracer, configure the network topology as specified and document the complete implementation process. Required services to be configured on designated servers:

- DNS service configuration
- HTTP web server setup
- FTP file transfer service
- Email server implementation (SMTP/POP3)

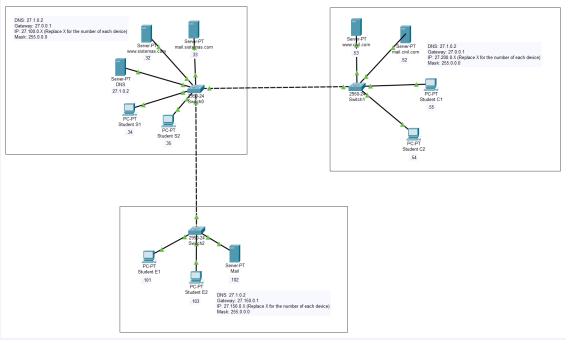

Figure 2: Cisco Packet Tracer Network Configuration

Exercise 2: Network Infrastructure Setup

Target Group: Teams of 1-3 students
Complete network implementation tasks:

1. Deploy all required servers and client devices
2. Establish physical and logical connections
3. Configure network parameters for each device:
   - DNS server addresses
   - Default gateway configuration
   - IP address assignment
   - Subnet mask configuration

4. Verify end-to-end connectivity between all network devices

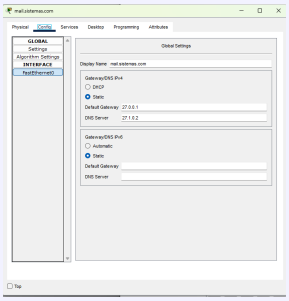

Figure 3: Deployed Servers and Services Overview

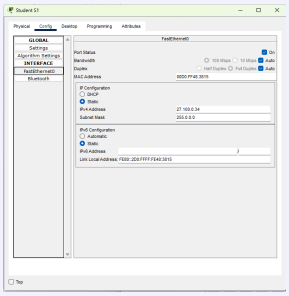

Figure 4: End-to-End Device Connectivity Diagram

Exercise 3: Service Configuration and Testing

Target Group: Teams of 1-3 students
Configure and test essential network services as detailed below.

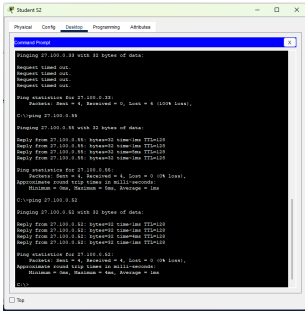

Figure 5: End-to-End Test 1: Device Connectivity Verification

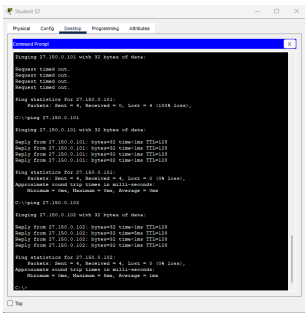

Figure 6: End-to-End Test 2: Service Response Verification

4.0.1 3.1 DNS Service Configuration

Primary DNS Server (IP: 27.1.0.2)

Configure the following DNS entries:

sistemas.com domain:

```
# Mail server record
sistemas.com      A     [mail_server_ip]
# Service aliases
pop3.sistemas.com CNAME sistemas.com
smtp.sistemas.com CNAME sistemas.com
# Web server records
http.sistemas.com A     [web_server_ip]
www.sistemas.com  CNAME http.sistemas.com
```

civil.com domain:

```
# Mail server record
civil.com         A     [mail_server_ip]
# Service aliases
pop3.civil.com    CNAME civil.com
smtp.civil.com    CNAME civil.com
# Web server records
http.civil.com    A     [web_server_ip]
www.civil.com     CNAME http.civil.com
```

electrica.com domain:

```
# Mail server record
electrica.com     A     [mail_server_ip]
# Service aliases
pop3.crear.com    CNAME electrica.com
smtp.crear.com    CNAME electrica.com
```

Verification Process:

1. Start the DNS service
2. From client machines in each faculty, execute ping commands using domain names
3. Verify successful name resolution

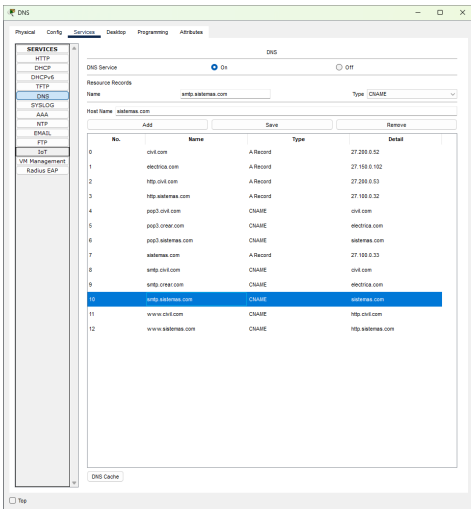

Figure 7: DNS service configuration on the primary DNS server (27.1.0.2)

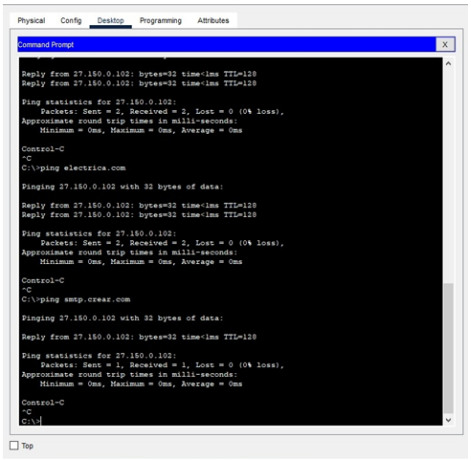

Figure 8: DNS resolution test (ping by domain name) from a client host

4.0.2 3.2 HTTP Web Service Configuration

Web Server Setup:

1. Configure HTTP service on designated web servers
2. Customize web pages for each faculty with distinctive content
3. Ensure proper service startup and availability

Client Testing Procedures:

1. Access web servers using IP addresses directly
2. Access web servers using configured domain names (URLs)
3. **Packet Analysis:** Use simulation mode to examine PDU contents at the application layer

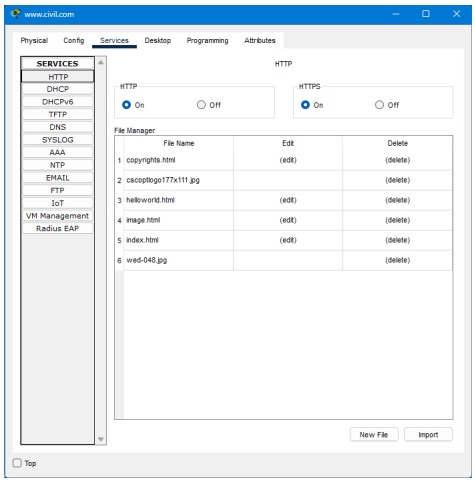

Figure 9: HTTP service configuration on the web server

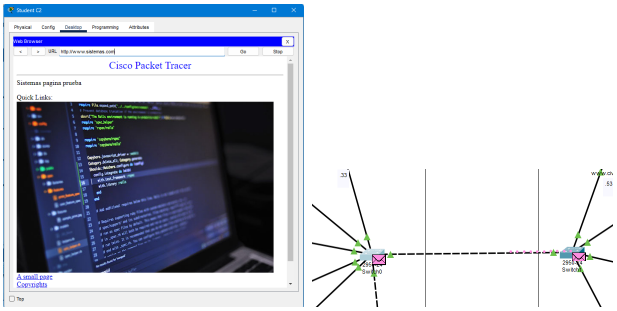

Figure 10: Left: Web page accessed by domain name. Right: Application-layer PDU inspection for HTTP traffic

4.0.3 3.3 Email Service Implementation

Mail Server Configuration:

1. Create user accounts for each faculty using client computer names as usernames
2. Configure SMTP and POP3 services
3. Start email services on all mail servers

Client Testing Protocol:

1. Configure email clients for respective domains
2. Test intra-domain email communication
3. Verify email reception and reply functionality
4. Test inter-domain email communication
5. Verify cross-domain email delivery and responses
6. **Protocol Analysis:** Use simulation tools to examine PDU content during:
   - Client-to-SMTP server communication
   - Client-to-POP3 server communication

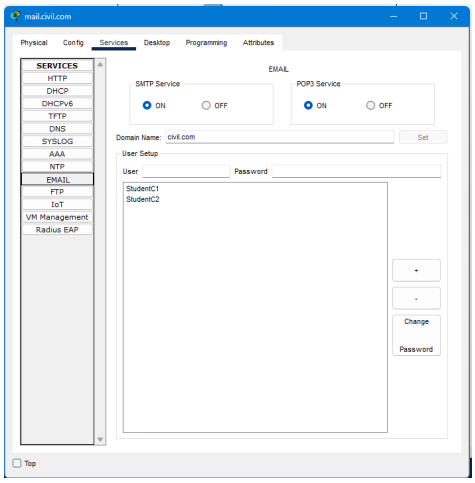

Figure 11: Mail server configuration and running services

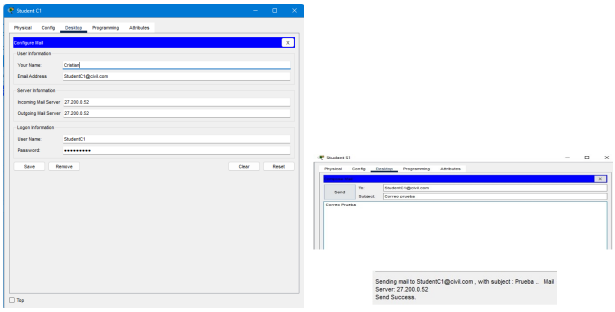

Figure 12: Left: Email client configuration for domain accounts. Right: Sending an email (client-to-SMTP)

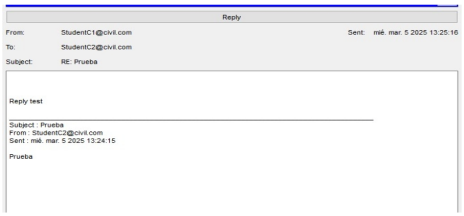

Figure 13: Received email confirmation on the recipient client

4.0.4 3.4 FTP Service Configuration

Server Setup (sistemas web server):

1. Configure FTP service
2. Create user account: Username = [your first name], Password = [your last name]
3. Start FTP service

Client Access Testing:

1. Command-line FTP access:

```
telnet [server_name_or_ip] 21
# Login with created credentials
# Download available files
# Exit and verify file transfer
# Document command sequence
```

2. **Simulation Mode Analysis:**
   - Re-access FTP server in simulation mode
   - Upload .TXT file from client
   - Examine application layer headers for:
     - Connection establishment
     - Authentication (username/password)
     - Transfer confirmation messages
     - File upload process
     - Session termination

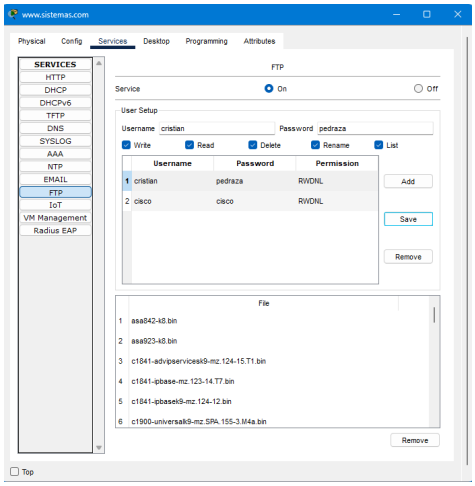

Figure 14: FTP service configuration on the sistemas web server

Figure 15: Left: FTP client connecting to the server. Right: Downloading files via FTP

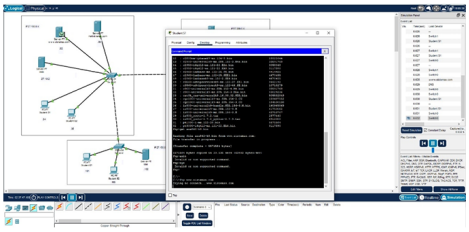

Figure 16: FTP transfer and application-layer PDU analysis (simulation mode)

5 Real Network Analysis

Exercise 4: Wireshark Protocol Analysis

Target Group: Teams of 1-3 students
Utilize Wireshark for comprehensive network traffic analysis and documentation.

5.0.1 4.1 Web Traffic Analysis

1. Access the Computer Lab website
2. Identify active application layer protocols
3. Analyze captured packets for:
   - Application layer information
   - Transport layer port assignments

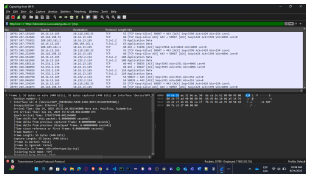

Figure 17: Web Traffic Capture (Computer Lab Website)

Wireshark filter used: `http.host =="http://laboratorio.is.escuelaing.edu.co" || tcp`

5.0.2 4.2 DHCP Traffic Capture

Procedure:

1. Initiate Wireshark capture
2. Release current IP address:

```
ipconfig /release
```

3. Request new IP address:

```
ipconfig /renew
```

4. Analyze DHCP packets for:
   - Client-server communication patterns
   - Application layer content
   - Transport layer port usage

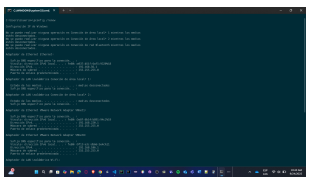

Figure 18: DHCP Client Commands (ipconfig /release and /renew)

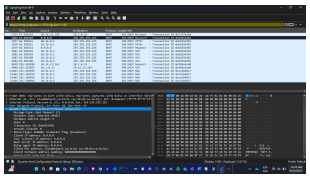

Figure 19: Wireshark Capture of DHCP/BOOTP Traffic

Wireshark filter used: `dhcp || bootp || udp.port == 67 || udp.port == 68`

5.0.3 4.3 HTTP vs TELNET Protocol Comparison

Prerequisites:

1. Enable TELNET protocol on your system
2. Prepare Wireshark for packet capture

Target URL: http://profesores.is.escuelaing.edu.co/~csantiago/RECO/index.html

TELNET Protocol Testing:

```
# Connect to web server
telnet profesores.is.escuelaing.edu.co 80

# HTTP GET requests
GET /~csantiago/RECO/index.html HTTP/1.1
Host: profesores.is.escuelaing.edu.co

# Download specific files
GET /~csantiago/RECO/prueba.pdf HTTP/1.1
Host: profesores.is.escuelaing.edu.co

GET /~csantiago/RECO/network.png HTTP/1.1
Host: profesores.is.escuelaing.edu.co
```

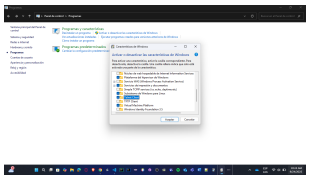

Figure 20: Enabling Telnet Client on Windows

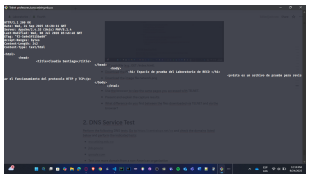

Figure 21: TELNET: HTTP GET Request Result (index.html)

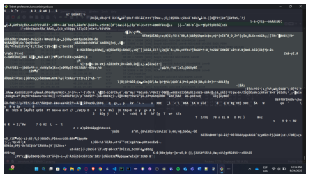

Figure 22: TELNET: HTTP GET Request for network.png

HTTP Browser Testing:

1. Access identical pages using web browser
2. Compare capture results between protocols
3. Document differences in file handling between TELNET and browser methods

Wireshark filter used for browser capture: `http.host == "profesores.is.escuelaing.edu.co"`

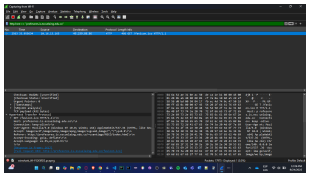

Figure 23: HTTP Browser Capture Comparison

Differences observed between TELNET and Browser-based HTTP requests

- **Headers HTTP:**
  - **Telnet:** Solo los headers básicos que se escribieron anteriormente
  - **Browser:** Headers adicionales automáticos (User-Agent, Accept, cookies, etc.)
- **Gestión de conexiones:**
  - **Telnet:** Una conexión por archivo, se cierra después de cada descarga
  - **Browser:** Se puede reutilizar conexiones (keep-alive), conexiones paralelas
- **Archivos descargados:**
  - **Telnet:** Archivos con headers HTTP mezclados
  - **Browser:** Archivos procesados y guardados correctamente
- **Comportamiento de red:**
  - **Telnet:** Comunicación HTTP manual, una solicitud simple
  - **Browser:** Puede hacer solicitudes adicionales (CSS, JS, imágenes automáticas)

Exercise 5: DNS Service Analysis

Target Group: Teams of 1-3 students
Conduct comprehensive DNS analysis using https://centralops.net/co

Target Domains for Analysis:

- escuelaing.edu.co
- jbb.gov.co
- google.com
- One additional non-American organization domain - samsung.com

Required Analysis Parameters:

1. Number of domain servers
2. Domain assignment date
3. Registration authority
4. Registration entity ID
5. Last record update timestamp
6. Record validity period
7. Assigned IP address ranges
8. IP assignment authority
9. Assigned organization details

5.1 escuelaing.edu.co

- **Number of domain servers:** only 2 servers: ns1.escuelaing.edu.co and ns2.escuelaing.edu.co.
- **Domain assignment date:** since 02/05/1998 (+26 years).
- **Registration authority:** cointernet.
- **Registration entity ID:** 111111.
- **Last record update timestamp:** 06/10/2022 (+2 years).
- **Record validity period:** until 31/12/2025 (10 months remaining).
- **Assigned IP address ranges:** 45.239.88.0/22.
- **IP assignment authority:** LACNIC.
- **Assigned organization details:** Escuela Colombiana de Ingeniería Julio Garavito.

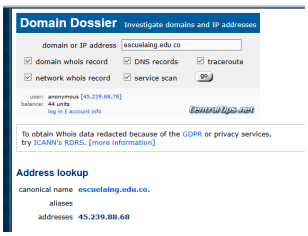

Figure 24: DNS analysis - escuelaing.edu.co

5.2 jbb.gov.co

- **Number of domain servers:** 2 servers: ns31.domaincontrol.com and ns32.domaincontrol.com.
- **Domain assignment date:** since 20/01/2000 (+25 years).
- **Registration authority:** cointernet.
- **Registration entity ID:** Private for privacy.
- **Last record update timestamp:** 06/10/2022 (+2 years).
- **Record validity period:** until 20/01/2026 (10 months remaining).
- **Assigned IP address ranges:** 20.33.0.0 – 20.128.255.255.
- **IP assignment authority:** ARIN.
- **Assigned organization details:** Microsoft Corporation.

Figure 25: DNS analysis - jbb.gov.co

5.3 google.com

- **Number of domain servers:** 6 IPv4 and 4 IPv6, total of 10 servers.
- **Domain assignment date:** since 15/09/1997 (+27 years).
- **Registration authority:** MarkMonitor.
- **Registration entity ID:** 292.
- **Last record update timestamp:** 10/08/2024 (+0.5 year).
- **Record validity period:** until 13/09/2028 (+3 years remaining).
- **Assigned IP address ranges:** 142.250.0.0 – 142.251.255.255.
- **IP assignment authority:** ARIN.
- **Assigned organization details:** Google LLC.

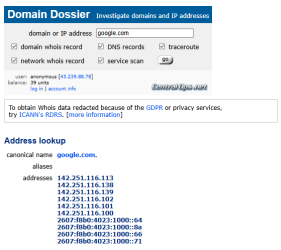

Figure 26: DNS analysis - google.com

5.4 samsung.com

- **Number of domain servers:** 1 IPv4.
- **Domain assignment date:** since 29/11/1994 (+31 years).
- **Registration authority:** Whois Corp.
- **Registration entity ID:** 100.
- **Last record update timestamp:** 23/09/2025.
- **Record validity period:** until 28/11/2025.
- **Assigned IP address ranges:** 211.45.27.231.
- **IP assignment authority:** APNIC.
- **Assigned organization details:** Samsung Electronics CO., Ltd.

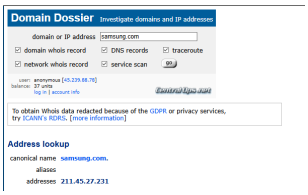

Figure 27: DNS analysis - samsung.com

Exercise 6: Network Time Protocol (NTP) Implementation

This exercise demonstrates a concise NTP deployment: one Slackware host acts as the NTP server (10.2.77.176) while other hosts act as clients (Solaris, Windows Server with GUI, Windows Server Core, and Android). The section lists the implementation requirements, team assignment, essential commands, troubleshooting notes and evidence screenshots.

Implementation requirements

1. Install and configure an NTP server on the designated machine.
2. Configure the remaining systems to synchronize to the server as NTP clients.
3. Verify synchronization and document troubleshooting steps and evidence.

Team configuration

- Slackware – NTP Server (10.2.77.176)
- Solaris – NTP Client
- Windows Server (GUI) – NTP Client
- Windows Server (Core) – NTP Client
- Android – NTP Client

Brief summary

Slackware is configured as the authoritative local NTP server and synchronizes with public pool servers. Clients are configured to use 10.2.77.176 as their time source. Typical issues encountered: missing ntp system user/group on some distributions and large initial clock offsets that require a manual one-time correction.

Slackware (server) — essential commands

```
# Stop the NTP daemon
/etc/rc.d/rc.ntpd stop
# Create a minimal /etc/ntp.conf
cat > /etc/ntp.conf << 'EOF'
server 0.pool.ntp.org iburst
server 1.pool.ntp.org iburst
server 2.pool.ntp.org iburst
driftfile /var/lib/ntp/drift
restrict 127.0.0.1
restrict ::1
restrict 10.2.77.0 mask 255.255.255.0 nomodify notrap
EOF
# Start the NTP daemon
/etc/rc.d/rc.ntpd start
# Verify
ntpq -p
ntpstat
```

Solaris client — notes

- Disable service to edit configuration: `svcadm disable ntp`
- Edit `/etc/inet/ntp.conf` to point to `10.2.77.176`
- If the `ntp` user/group is missing: create and adjust permissions for `/var/ntp`
- If the clock offset is large: use `ntpdate -s 10.2.77.176` or `sntp -sS 10.2.77.176` for initial sync
- Re-enable service and verify: `svcadm enable ntp` and `ntpq -p`

Windows Server (GUI and Core) — essential commands

```
# Stop Windows Time service (PowerShell)
Stop-Service w32time -Force
# Configure the NTP peer
w32tm /config /manualpeerlist:"10.2.77.176"
     /syncfromflags:manual /reliable:yes /update
# Start and force resync
Start-Service w32time
w32tm /resync /force
# Check status
w32tm /query /status
```

Use the GUI on Windows Server with Desktop Experience to verify the time source and service status; use the Core command sequence above on Server Core installations.

Android client — notes

- Android devices typically use "Automatic date & time" (network-provided). If enabled, time sync is automatic.
- To point a device to a specific NTP server requires elevated privileges or a device-specific configuration app. Example commands (root required): `settings put global ntp_server 10.2.77.176` or `setprop net.ntp.server1 10.2.77.176`

Troubleshooting summary

- Missing `ntp` user/group: create it (e.g. `groupadd ntp; useradd -g ntp -s /bin/false -d /var/ntp ntp`) and adjust ownership of NTP-related directories.
- Large initial offset: perform a one-time manual sync with `ntpdate -s <server>` or `sntp -sS <server>` before starting the NTP daemon.
- Verify with: `ntpq -p` (small offset, increasing reach, and a "*" marking the selected server).

Evidence (screenshots)

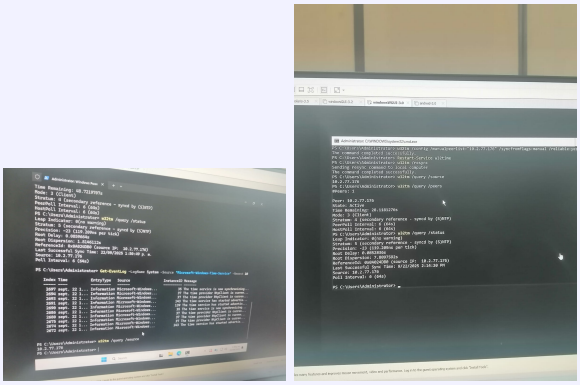

Figure 28: Windows Server (GUI and CLI) – configuration and service status

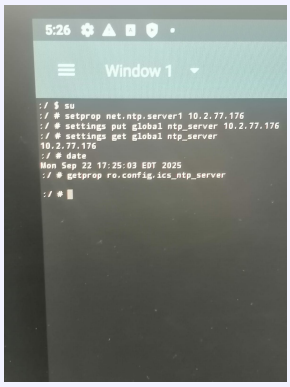

Figure 29: Android – Automatic date & time and network synchronization

6 Physical Layer Implementation

Exercise 7: Structured Cabling and Cable Construction

Target Group: Teams of 1-3 students
Proper technological infrastructure requires standardized physical connectivity components. Structured cabling standards ensure organized connections, facilitate network growth, and promote efficient management of physical network elements.

6.1 7.1 Patch Cord Construction (Individual Task)

Construction Requirements:

1. Following instructor guidance and classroom presentation materials
2. Crimp two RJ45-RJ45 cables:
   - One straight-through cable
   - One crossover cable

Analysis Questions:

- **What is the specific purpose of each cable type?**
  Straight-through cables connect devices operating at different OSI layers (host to switch, switch to router). The wire arrangement follows the same standard (T568A or T568B) on both ends. Crossover cables connect devices operating at the same OSI layer (host to host, switch to switch) by crossing the transmit and receive pairs between connectors.
  The cable configuration is determined by the color arrangement: a cable is straight-through when both ends use the same standard (T568A to T568A or T568B to T568B), and it is crossover when one end uses T568A and the other uses T568B.

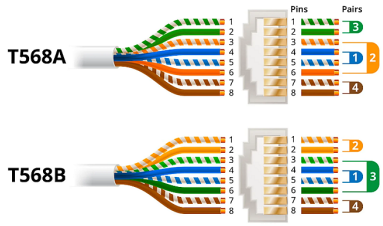

Figure 30: T568A and T568B wiring standards comparison

- **When would you use straight-through vs crossover cables?**
  Use straight-through cables for: computer to switch, switch to router, computer to hub connections. Use crossover cables for: computer to computer direct connection, switch to switch, hub to hub, router to router connections. Modern devices with Auto-MDIX can automatically detect and adapt to either cable type.

Quality Assurance:

The cable construction process was systematically executed following professional standards. Initially, cables were cut to an estimated length of 2.5 meters each to ensure adequate working distance. The cable jacket was carefully stripped to the appropriate length matching the RJ45 connector specifications.

Wire organization followed strict color-coding standards to differentiate between straight-through and crossover configurations. For straight-through cables, both ends follow the same wiring standard (T568B: white-orange, orange, white-green, blue, white-blue, green, white-brown, brown). For crossover cables, one end uses T568A while the other uses T568B standard, effectively crossing the transmit and receive pairs.

After proper wire arrangement, each connector was inserted ensuring all wires reached the connector's far end completely. Visual verification confirmed proper seating before crimping. The crimping process applied consistent pressure to establish reliable electrical contact between wires and connector pins.

Each cable end underwent identical construction procedures, resulting in two straight-through cables and two crossover cables. Quality verification was performed using professional cable testing equipment to ensure proper continuity and wiring configuration.

(a) Crossover cable test results

(b) Straight-through cable test results

Figure 31: Cable tester verification for both cable types

6.1.1 7.2 Patch Panel Implementation (Team Task)

Objective: Perform horizontal cabling crimping to connect two computers using professional patch panel infrastructure with faceplates.

Setup Requirements:

- Patch panel with multiple ports
- Two faceplates (minimum one information outlet each)
- Appropriate cable lengths
- Professional crimping tools

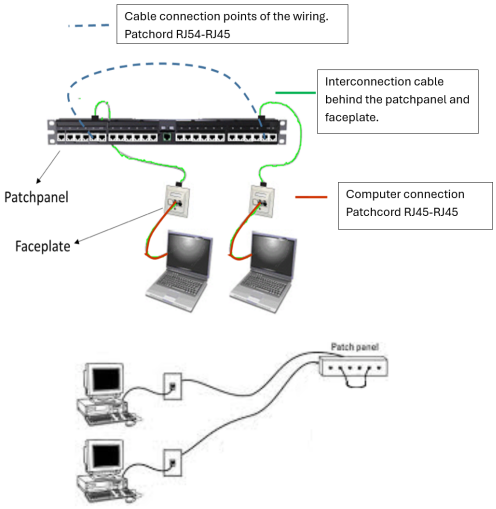

Figure 32: Horizontal Cabling Setup with Patch Panel

Testing Methodologies:

Network configuration was established by assigning IPv4 addresses to each computer within the designated IP range (10.2.77.176 to 10.2.77.181) with subnet mask 255.255.0.0, gateway 10.2.65.1, and DNS server 10.2.65.1. This configuration enabled connectivity testing through the patch panel infrastructure without relying on external network access.

The following test scenarios were systematically evaluated:

Test Case 1: Triple Crossover Configuration Three crossover connections were established between computers, with an additional crossover connection to the university's network server. This configuration tested crossover cable functionality in a multi-hop environment.

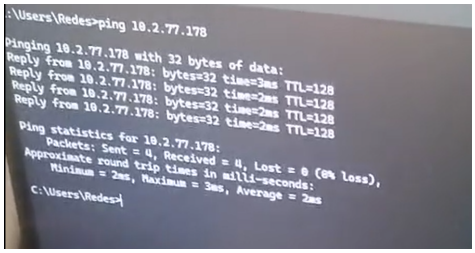

Figure 33: Triple crossover configuration test results

Test Case 2: Mixed Crossover-Straight Configuration Two crossover connections followed by one straight-through connection tested hybrid cabling scenarios commonly found in professional network installations.

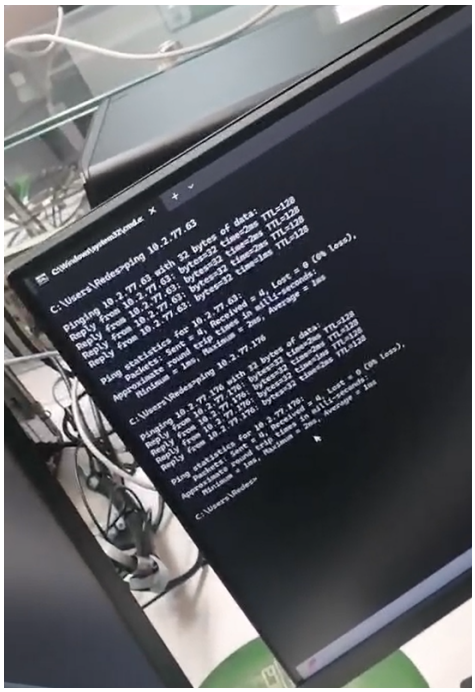

Figure 34: Mixed crossover-straight configuration test results

Test Case 3: Double Straight-Through Configuration Two straight-through connections tested standard computer-to-switch-to-computer communication paths typical in structured cabling environments.

Figure 35: Double straight-through configuration test results

Test Case 4: Mixed Straight-Crossover Configuration Two straight-through connections followed by one crossover connection evaluated transitional network topologies.

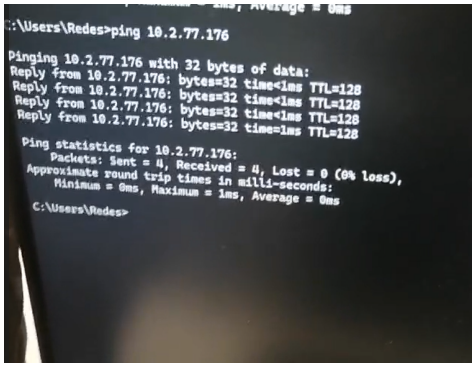

Figure 36: Mixed straight-crossover configuration test results

Test Case 5: Triple Straight-Through Configuration Three straight-through connections tested optimal structured cabling implementation with proper device layer separation.

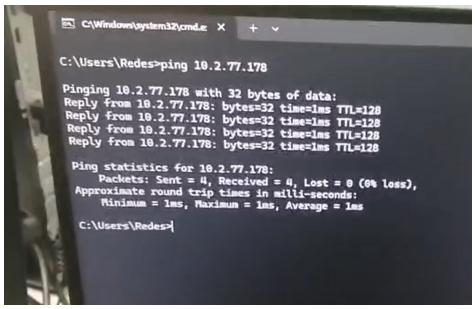

Figure 37: Triple straight-through configuration test results

Test Case 6: Double Crossover Configuration Two crossover connections were implemented to test direct device-to-device communication scenarios. This configuration evaluated the performance of crossover cables in peer-to-peer network connections without intermediate switching devices.

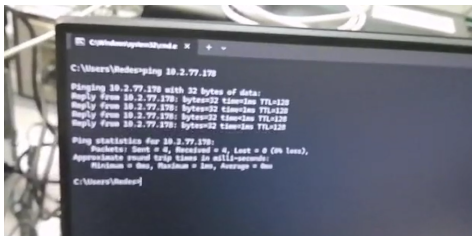

Figure 38: Double crossover configuration test results

University Network Server Connection Connection testing with the university's network server verified external connectivity through the structured cabling system.

Figure 39: University network server connection test

6.1.2 7.3 University Infrastructure Analysis

Field Study Objective: Analyze structured cabling implementation in Building I at the School.

Investigation Requirements:

1. Identify structured cabling components throughout the building
2. Document cable management systems
3. Photograph infrastructure elements (with proof of personal documentation)
4. Analyze compliance with structured cabling standards

Field Study Results:

In this final phase, we conducted a comprehensive site visit to Building I to observe and analyze the distribution and structuring of network components throughout the facility. The primary objective was to understand and document the implementation of structured cabling systems in a real-world academic environment.

The investigation focused on analyzing two fundamental types of structural cabling. Vertical cabling refers to network infrastructure that runs within the building structure and is typically not easily visible to casual observation. This includes backbone cabling that connects different floors and major network distribution points. In contrast, horizontal cabling is more visible and represents the connections between various network devices that interact directly with end users.

Building I provides an excellent case study for infrastructure analysis due to its open architectural design. Unlike many conventional buildings where cabling is completely concealed within walls and ceiling spaces, this facility features exposed structural elements that allow for direct observation of the cable organization and management systems throughout the building.

During our analysis, we observed the systematic implementation of cable management techniques, including proper cable routing, labeling systems, and adherence to industry standards for cable separation and protection. The vertical cabling infrastructure demonstrated professional installation practices with appropriate cable trays, conduits, and fire-stopping measures where cables traverse floor boundaries.

The horizontal cabling distribution showed effective use of patch panels, telecommunications rooms, and structured pathways that facilitate both current operations and future expansion requirements. Cable management hardware, including cable trays, J-hooks, and cable ties, was properly implemented to maintain organization and prevent cable stress.

Figure 40: Building I structured cabling infrastructure overview

7 Conclusions

Based on the laboratory implementation and analysis, provide comprehensive conclusions addressing:

1. **Application Layer Protocol Understanding:** Insights gained from protocol analysis and simulation
2. **Physical Infrastructure Importance:** Role of structured cabling in network reliability

3. **Integration Challenges:** Relationship between logical and physical network layers
4. **Professional Best Practices:** Industry-standard implementation techniques learned
5. **Troubleshooting Skills:** Problem-solving methodologies developed

8 References

1. Cisco Systems, Inc. *Cisco Packet Tracer User Guide*. Version 8.2, 2023.
2. Wireshark Foundation. *Wireshark User's Guide*. Available: https://www.wireshark.org/docs/wsug_html_chunked/
3. TIA/EIA-568 Commercial Building Telecommunications Cabling Standard. Telecommunications Industry Association, 2020.
4. RFC 5905 - Network Time Protocol Version 4: Protocol and Algorithms Specification. IETF, 2010.
5. RFC 1035 - Domain Names - Implementation and Specification. IETF, 1987.
6. RFC 2616 - Hypertext Transfer Protocol – HTTP/1.1. IETF, 1999.
7. RFC 959 - File Transfer Protocol (FTP). IETF, 1985.
8. RFC 5321 - Simple Mail Transfer Protocol. IETF, 2008.