Lab 2 – Ethernet Cable Wiring & TCP Packet Tracing

CS3263 Embedded Computer Networks

Dept. of Computer Science and Engineering, University of Moratuwa

Learning Outcomes

After completing the lab, you will be able to

1. Create an ethernet cable from scratch and connect that between two PCs and communicate between them.
2. Run a tcp server and client between those pc and use wire shark to capture the packets
3. Describe the TCP Protocol using captured packets

1. Crimping Ethernet Cable

A. Follow the Technical Officer's demonstration to strip the CAT cable, arrange the internal wires according to the standard, insert them into the RJ45 connector, and crimp them securely.

B. Use the cable tester to verify continuity and correct pin alignment.

2. Networking Two PCs together

Scenario A: Using Ethernet Ports (Direct Connection)

A. Connect the newly crimped Ethernet cable directly between the Ethernet ports of PC A and PC B.

Understanding IPs (Why Manual Configuration?):

Normally, when you connect to a router, a service called DHCP automatically assigns your computer an IP address.

In this direct connection, there is no router to hand out addresses. Therefore, you must manually configure Static IP addresses so the computers can find each other.

B. Configuration Steps

Windows

- Go to ***Control Panel > Network and Sharing Center > Change adapter settings***.
- Right-click your **Ethernet adapter > Properties**.
- Select **Internet Protocol Version 4 (TCP/IPv4) > Properties**.
- Select **"Use the following IP address"**:

```
PC A: IP 192.168.1.1, Subnet 255.255.255.0
```

PC B: IP 192.168.1.2, Subnet 255.255.255.0

Ubuntu (Linux)

- Go to **Settings > Network**.
- Click the **Gear icon** next to "Wired".
- IPv4 Tab > Method: Manual.

  PC A: IP 192.168.1.1, Subnet 255.255.255.0
  PC B: IP 192.168.1.2, Subnet 255.255.255.0

WSL (Windows Subsystem for Linux)

- WSL shares the network connection of your Windows host. You do not configure a static IP inside WSL itself. Configure the Windows Host (see "Windows" steps above). WSL will automatically route traffic through that configured connection.

C. Connectivity Test (Ping):

On PC A: Open terminal/command prompt and type `ping 192.168.1.2`
On PC B: Type `ping 192.168.1.1`
See terminal output

Troubleshooting: If ping fails, disable the Firewall on both PCs.

Scenario B: Using Wi-Fi (No Ethernet Ports)

A. Connect both PCs to the same Wi-Fi network (Router or Mobile Hotspot).

In this scenario, the Router/Hotspot acts as the DHCP server, so IP addresses are assigned automatically. You do not need manual configuration.

B. Finding IP Addresses.

Windows
Open Command Prompt (cmd) and type *`ipconfig`*. Look for "*`IPv4 Address`*" under the Wireless adapter.

Ubuntu/WSL
Open terminal and type *`ip addr`*. Look for the *`inet`* address under eth0 or wlan0.

C. Connectivity Test (Ping).

Note the IP address of the other computer.
Run *`ping <Other_PC_IP_Address>`* in the terminal.

3. TCP Client-Server Implementation

Ubuntu (Linux)

A. Run Server (PC A)

   Compile: `gcc server.c -o server`
   Run: `./server`

   Note: The server uses `INADDR_ANY`, so it automatically listens on all available interfaces (Ethernet or Wi-Fi).

B. Configure Client (PC B):

   Edit IP Address: Find the line `server.sin_addr.s_addr = inet_addr("...");`.

   Change the IP inside the quotes to PC A's IP address (the one you pinged successfully in Activity 2).

C. Run Client (PC B):

   Compile: `gcc client.c -o client`
   Run: `./client`

   Type a message and press Enter. Ensure the server receives it and sends a reply.

Note:
If PC A (Server) and PC B (Client) are both using WSL, the Client (PC B) cannot "see" the Server (PC A) directly. Because WSL 2 runs inside a virtual machine. This means your "WSL Linux" has its own IP address that is hidden behind your main Windows IP address (this is called Network Address Translation). So we must set up a Port Forwarding Rule on the Server PC to pass the message through.

Follow the below guideline to do so
https://gist.github.com/NimethM/5ccf675860d8f98799788ad52cf7de79

4. TCP Packet Analysis

Use Wireshark to inspect the protocol mechanics.

A. Capture Setup
   - Open Wireshark on the Client PC.
   - Select the active Interface (Ethernet if wired, Wi-Fi if wireless).
   - Apply Display Filter: tcp.port == 8888.
   - Start Capture before running the client program.

B. Analyze the 3 Key Stages:

- **Connection Establishment:** (3-Way Handshake Look for packets with the [SYN, ACK] flag)
- **Data Transfer:** Look for packets with the [PSH, ACK] flag.
- **Termination:** Look for packets with the [FIN, ACK] flag.

Exercise

Prepare a report including the following:

A. Clear screenshots highlighting the following three stages.
   - The 3-Way Handshake (Connection Establishment)
   - Data Transfer (The "Push" packets containing your message)
   - Connection Termination (The process of closing the socket)

B. For each screenshot, provide a brief but technical explanation of what is happening. Description must cover the following

   - Identify the specific flags set in each packet and explain what they signal to other computer
   - Briefly explain the flow of the session

C. Please adhere to the following standards when preparing your final report,

   - **Formatting**
     Use a professional font and clear headings. Ensure the text is justified for readability.

   - **Page Numbering**
     All pages must be numbered at the bottom right or center.

   - **Figures & Diagrams**
     All screenshots and diagrams must be numbered and Provide a caption below each figure explaining what it shows.

   - **References**
     List all resources (links, books, papers) used during the lab in a dedicated "References" section at the end of the document.

   - **AI Usage Disclosure**
     At the very end of your report, Briefly describe how Artificial Intelligence was used in the preparation of the report or code.

     Example:
     "AI was used to debug syntax errors in the C code and to summarize the differences between TCP and UDP sockets."