Name & ID: Basil khowaja (bk08432) **Date: 20-08-2024**_____ **Section: T1**_____

EE-424L Data Communication and Networking Lab

Fall 2024

Habib University

Dhanani School of Science & Engineering

LAB 1: Networking Fundamentals: Exploring Basic Networking Commands and making UTP Cable

Objectives	**After the lab student should be able to trouble shoot the basic networking connectivity issue using Command prompt and make UTP straight through & cross-over cable for data transmission.**

Lab #1 Marks distribution:

		LR4=35	LR5=40	LR9=5	AR4=20
In-Lab Tasks	**Task 1**	20	10	5	20
	Task 2	15	20		
	Task 3		10		
Total Marks	**100**				

Lab #1 Marks Obtained:

		LR4=35	LR5=40	LR9=5	AR4=20
In-Lab Tasks	**Task 1**				
	Task 2				
	Task 3				
Marks Obt.					

In Lab Tasks

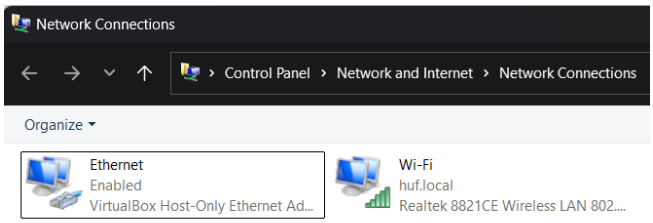
Task 1

Check your computer network connections settings.

When you set up or troubleshoot a network connection in a Windows PC, you have to access Network Connection screen to view and manage all your wired / wireless adapters. This exercise focuses on quickest way to open Network Connections in Windows PC, and discuss some of the feature of network connection setting

1. In the search box on the taskbar, type **ncpa.cpl**, and then hit **Enter** and it will instantly open Network Connection screen.

2. Observe how many connections are available. What are their different type, and why some have cross on them? Write down connections available and status in box below:



Ethernet:

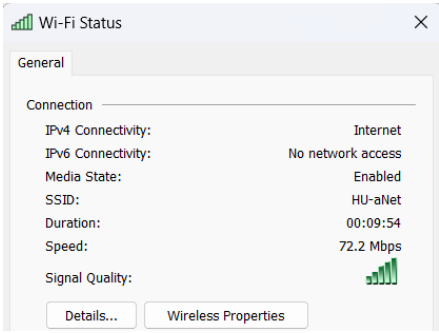
- Type: Wired (Ethernet)
- Status: Enabled
- Adapter: VirtualBox Host-Only Ethernet Adapter

Wi-Fi:

- Type: Wireless (Wi-Fi)
- Status: Connected to the network "huf.local"
- Adapter: Realtek 8821CE Wireless LAN 802.

None of the connections have a cross on them.

3. Double click on one of the enabled Connection. Note that the connection has two type of connectivity: IPV4 and IPV6. What are their status and what do they stand for?



IPV4 status: internet (enabled)

IPV6 status: No network access (disabled)

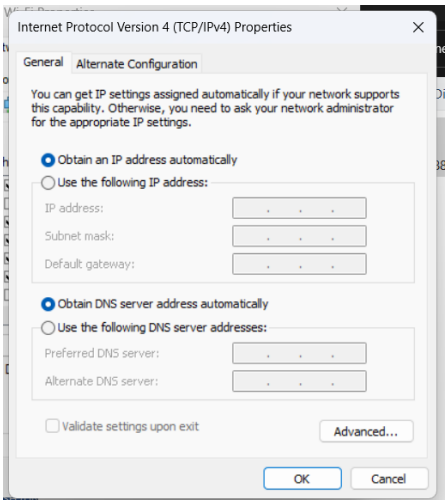
IPV4 stands for internet protocol version 4 and IPV6 stands for internet protocol version 6.

4. Click on details button and fill the following parameters in table for wired & wireless connection.

Description	Wired	Wireless
Physical Address	0A-00-27-00-00-0B	F8-89-D2-33-44-15
DHCP Enabled	NO	YES
IPV4 Address	192.168.56.1	10.15.2.221
IPV4 Subnet Mask	255.255.255.0	255.255.248.0
IPV4 Default Gateway	none	10.15.0.1
IPV4 DHCP Server	none	10.10.0.5
IPV4 DNS Server	none	10.10.0.1

Table 1

5. Click on properties of network connection window and double click, internet protocol 4. Observe and note down, how does your PC is allocated IP (Automatic or manually). What are pros and cons of allocating IP manually & automatically? Mention at least 2 Pros & 2 Cons.



The IPv4 settings indicate that the IP address and DNS server address are both set to be obtained automatically. This means that my laptop is using Automatic (DHCP) configuration for IP allocation.

Automatic IP Allocation (DHCP):

Pros:
Ease of Use: Users may connect to several networks without altering settings as there is no need for hand configuration.
IP addresses are assigned dynamically, therefore lowering the possibility of IP conflicts when devices link to the network.

Cons:

Less Control: The user has less control over which IP address is issued, which can be problematic in networks where particular IPs are required for particular uses.
Dependency on DHCP Server: Should the DHCP server fail, devices might not be able to find an IP address, therefore causing connection problems.

Manual IP Allocation:

Pros:
1) Consistent IP addresses let servers or devices needing a fixed IP access consistent IP.
2) Offers gateways and bespoke DNS servers among other network settings control over.
drawbacks include:

Cons:
1) Manual setup might cause mistakes like IP conflicts should the same IP be provided to several devices.
2) Particularly in big networks, manually configuring IP addresses might take time, hence is time consuming.

Command Prompt Network configuration information.

1. Use the Start menu to open the Command Prompt or write cmd in start menu.

2. Type ipconfig in command prompt window. Observe if the command is case sensitive or not? **No its not case sensitive**

3. Record the following internet connectivity information:

Connection Type: Ethernet (vEthernet WSL)

- IP Address: 172.31.96.1
- Subnet Mask: 255.255.240.0
- Default Gateway: (None Listed)

Connection Type: Wi-Fi

- IP Address: 10.15.2.221
- Subnet Mask: 255.255.248.0
- Default Gateway: 10.15.0.15

4. Are the values same, as the values obtained in task 1. _____

Task 2

Basic Networking Commands:

1. Ping

The ping is a network command used to test the ability of the source computer to reach a specified destination computer. It is a simple way to verify that a computer can communicate with another computer or network device.
The ping command operates by sending **Internet Control Message Protocol** (ICMP) **Echo Request messages** to the destination computer and waiting for a response. The receipt of corresponding Echo Reply messages are displayed, along with **round-trip times.**

The syntax of ping command is as follow

1. Ping ip address (you can mention domain name for e.g. www.google.com instead of IP address)
   Ping www.google.com and note down how many packets are sent & received?

```
C:\Users\Dell>ping www.google.com

Pinging www.google.com [192.178.24.196] with 32 bytes of data:
Reply from 192.178.24.196: bytes=32 time=17ms TTL=116
Reply from 192.178.24.196: bytes=32 time=17ms TTL=116
Reply from 192.178.24.196: bytes=32 time=16ms TTL=116
Reply from 192.178.24.196: bytes=32 time=18ms TTL=116

Ping statistics for 192.178.24.196:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 16ms, Maximum = 18ms, Average = 17ms
```

   Packets sent: 4

   Packets received: 4

2. Ping ip address or Domain name –n count (where count is the number of packets you want to send). This option sets the number of ICMP Echo Requests to send, from 1 to 4294967295.

   Ping the class fellow sitting next to you & send 2 ICMP packets. Check this to RA.

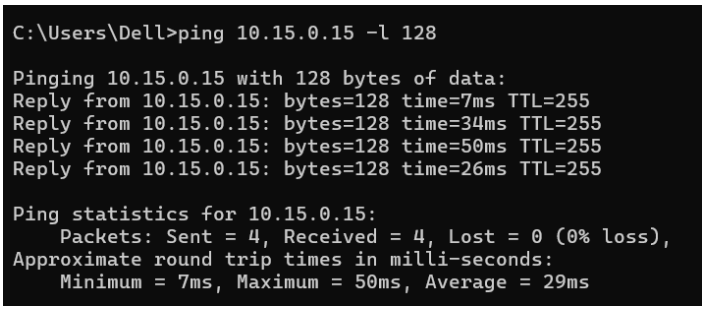
```
C:\Users\Dell>ping 10.30.1.108 -n 2

Pinging 10.30.1.108 with 32 bytes of data:
Reply from 10.30.1.108: bytes=32 time=21ms TTL=127
Reply from 10.30.1.108: bytes=32 time=4ms TTL=127

Ping statistics for 10.30.1.108:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 21ms, Average = 12ms
```

3. Ping ip address or Domain name –l (Use this option to set the size, in bytes, of the echo request packet from 32 to 65,527)

   - Ping the IP address of default gateway by sending 128-byte echo packets. Check this to RA.



What do the words marked in bold in the above statement mean?

Internet Control Message Protocol (ICMP), **Echo Request messages** and **round-trip times.**

Internet Control Message Protocol (ICMP):

Network protocols like Internet Control Message Protocol (ICMP) let devices in a network send problem messages and information about how the network works. Devices in a network include routers, computers, and servers. Its main purpose is to diagnose or control things, or to send error messages when a network device can't reach another device to let others know there's a problem. "Ping" is the most well-known way to use ICMP. It sends an ICMP Echo Request to a target address and waits for an ICMP Echo Reply.

Echo Request messages:

Echo Request messages are a type of ICMP message that the ping tool uses. Computers send an Echo Request message to other computers when you "ping" them. An Echo Reply message is sent back if the target device can be reached and is working. This process lets you see if a device is online and how long it takes for the request to get to the device and back. This can help you figure out why a device isn't connecting.

Round-trip times:

A signal's round-trip time (RTT) is the amount of time it takes to go from its source to its target and back again. It is the amount of time it takes for an ICMP Echo Request to be sent to a device and for that device to receive the matching Echo Reply. RTT measures the latency, or delay, between two networked devices and is an important measure of network speed. Connections that are faster and more sensitive have lower RTT numbers.

4. Write down the response of following:
    - Ping the IP address of local host (your system or PC) and record your observation (how many packets are sent/received and what other parameters in response telling us?

```
C:\Users\Dell>ping localhost

Pinging DESKTOP-BRH2KGB [::1] with 32 bytes of data:
Reply from ::1: time<1ms
Reply from ::1: time<1ms
Reply from ::1: time<1ms
Reply from ::1: time<1ms

Ping statistics for ::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Observations:

- Packets Sent/Received:
    - Packets Sent: 4
    - Packets Received: 4
    - Packet Loss: 0% (No packet loss)
- Round-Trip Time:
    - Minimum RTT: 0 ms
    - Maximum RTT: 0 ms
    - Average RTT: 0 ms

What the Results Tell Us:

- IPv6 Localhost: The `::1` address indicates that the ping was performed using the IPv6 loopback address (equivalent to `127.0.0.1` in IPv4). This confirms that my system's IPv6 stack is functioning correctly.
- Network Stack Health: The fact that all packets were sent and received without any loss confirms that the network stack on your computer is functioning properly.
- Latency: The round-trip time being 0 ms is expected when pinging the localhost, as the packets do not travel over an external network and are handled internally by your system.

5. Use ping command to find the IP address of Habib University website and note down it in space below. Also, discuss the response why are you getting this response?

```
C:\Users\Dell>ping www.habib.edu.pk

Pinging www.habib.edu.pk [52.30.165.170] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 52.30.165.170:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Details: Setting up the server:

As a safety step, a lot of public servers, like those that run websites, are set up to avoid ICMP Echo Requests, which are what the ping command uses. Denial-of-Service (DoS) attacks, which can be made easier by ping requests, can't happen. This is done to stop those kinds of attacks.
This is likely because the server at 52.30.165.170 is set up to drop or ignore ping requests, which is why we see "Request timed out."
Rules for the firewall:
There is a chance that an ICMP firewall on the server or network is stopping ICMP data, which includes ping requests. Many companies do this to stop network activity that isn't needed and to avoid possible security risks.

2. Tracert

The Tracert diagnostic utility determines the route taken to a destination by sending Internet Control Message Protocol (ICMP) echo packets with varying IP Time-to-Live (TTL) values to the destination. Each router along the path is required to decrement the TTL on a packet by at least 1 before forwarding it. When the TTL on a packet reaches 0, the router should send an "ICMP Time Exceeded" message back to the source computer.

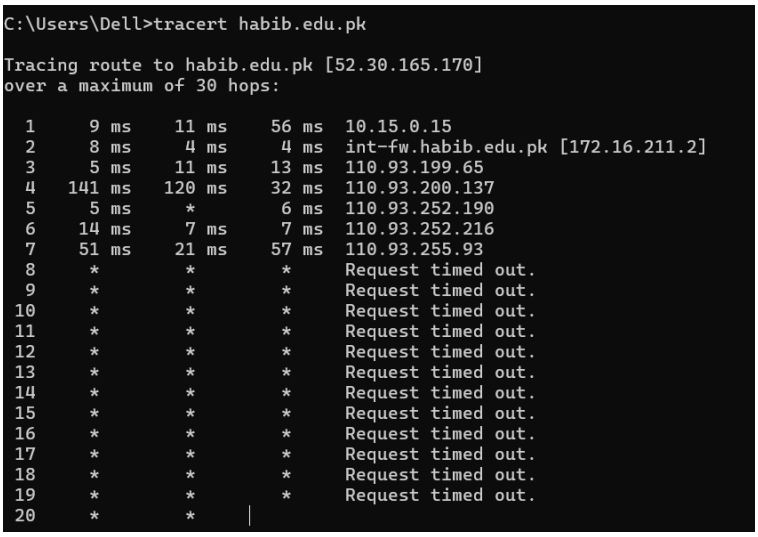
1. Trace the route to Yahoo and Habib Site and write down the response and your observations in box below:

```
Tracing route to yahoo.com [74.6.143.26]
over a maximum of 30 hops:

  1    28 ms     3 ms    28 ms  10.15.0.15
  2     4 ms    19 ms     4 ms  int-fw.habib.edu.pk [172.16.211.2]
  3     8 ms     4 ms     5 ms  110.93.199.65
  4    16 ms     5 ms     5 ms  110.93.200.137
  5     *        *        *     Request timed out.
  6    15 ms     5 ms     5 ms  110.93.252.222
  7   122 ms   122 ms   122 ms  110.93.255.175
  8   127 ms   129 ms   129 ms  ge-1-3-0.pat1.dee.yahoo.com [80.81.192.115]
  9   128 ms   131 ms   136 ms  ae-3.pat1.frz.yahoo.com [209.191.112.17]
 10   214 ms   237 ms   214 ms  ae3.pat2.dcz.yahoo.com [209.191.65.144]
 11   219 ms   213 ms   221 ms  ae-21.pat2.nyc.yahoo.com [209.191.68.27]
 12   216 ms   230 ms   223 ms  ae-1.pat1.bfw.yahoo.com [209.191.64.163]
 13   225 ms   230 ms   284 ms  ae-34.msr1.bf1.yahoo.com [74.6.227.55]
 14   221 ms   275 ms   221 ms  et-9-0-0.clr2-a-gdc.bf2.yahoo.com [74.6.122.25]
 15   219 ms   217 ms   216 ms  lo0.fab2-1-gdc.bf2.yahoo.com [74.6.123.243]
 16   215 ms   215 ms   215 ms  usw2-1-lbb.bf2.yahoo.com [74.6.98.139]
 17   227 ms   224 ms   224 ms  media-router-fp74.prod.media.vip.bf1.yahoo.com [74.6.143.26]
```

The traceroute to `yahoo.com` (IP: `74.6.143.26`) shows the packet's journey through both local and public networks:

1. Local Network: The first few hops are within the internal network with low latency.
2. Timeout: Hop 6 shows a request timeout, likely due to a network device blocking ICMP packets.
3. Public Internet: From Hop 7 onwards, the packet transitions to the public internet, passing through several Yahoo data centers.
4. Latency: Latency increases as the packet moves further, reaching over 200 ms by the final hop.



The traceroute to `habib.edu.pk` (IP: `52.30.165.170`) shows the following key observations:

1. Initial Hops (1-6):
    - The first few hops are within the local and internal network, showing low latency and successful communication with IP addresses like `10.15.0.15`, `172.16.211.2`, and several public IPs (`110.93.199.65`, `110.93.200.137`, etc.).
2. Request Timeouts (Hops 7-20):
    - Starting from Hop 7, all subsequent hops result in "Request timed out." This indicates that the packets are not being acknowledged beyond the 6th hop. This could be due to the destination network being configured to block ICMP packets or a firewall/security measure on the network preventing further trace responses.

TASK 3:

Make Straight-through and Cross-over UTP cable and verify its connection.

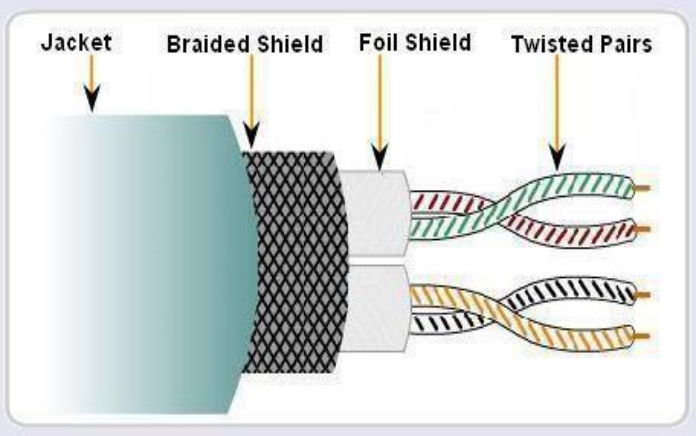
Introduction

Physical media refers to the physical materials that are used to transmit information in data communications. It is referred to as physical media because the media is generally a physical object such as copper or glass.

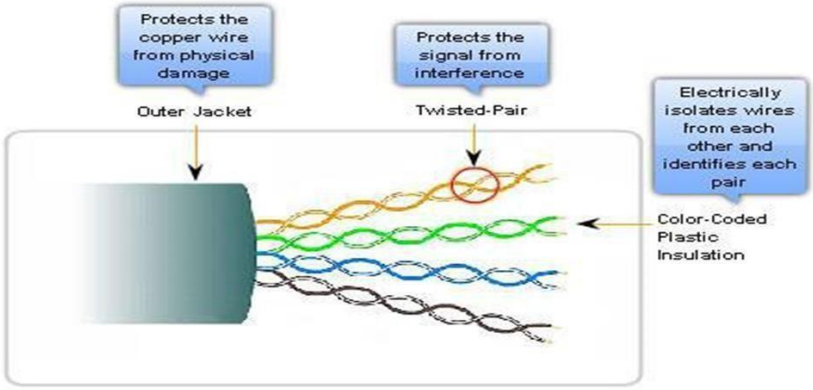
Although it is possible to use several forms of wireless networking, such as radio frequency and Infrared, the majority of installed LANs today communicate via some sort of cable. All data cables fall into three main types, namely, twisted pair, coaxial cable, and optic fiber cable. These cable types carry signals at different frequencies, and they have unique applications.

Twisted Pair Cables

Twisted-pair cable consists of multiple, individually insulated wires that are twisted together in pairs. Sometimes a metallic shield is placed around the twisted pairs. Hence, the name *shielded twisted-pair (STP)*.



Also you will see cable without outer shielding; it's called *unshielded twisted-pair (UTP)*.



UTP is commonly used in twisted-pair Ethernet (10Base-T, 100Base-TX, etc.), star-wired networks. Let's take a look at why the wires in this cable type are twisted. When

electromagnetic conducted on copper wires that are in close proximity (such as inside a cable), some electromagnetic interference occurs. In this scenario, this interference is called *crosstalk*. Twisting two wires together as a pair minimizes such interference and also provides some protection against interference from outside sources.

Connecting UTP

Most telephones connect with an RJ-11 ((RJ means "Registered Jack") connector. The connector used with UTP cable is called RJ-45. The RJ-11 has four wires, or two pairs, and the network connector RJ-45 has four pairs, or eight wires.

Types of Interfaces

In an Ethernet LAN, devices use one of two types of UTP interfaces - MDI or MDIX.

The MDI (media-dependent interface) uses the normal Ethernet pinouts. Pins 1 and 2 are used for transmitting and pins 3 and 6 are used for receiving. Devices such as computers, servers, or routers will have MDI connections. The devices that provide LAN connectivity - usually hubs or switches - typically use MDIX (media-dependent interface, crossover) connections. The MDIX connection swaps the transmit pairs internally. This swapping allows the end devices to be connected to the hub or switch using a straight-through cable.

Typically, when connecting different types of devices, use a straight-through cable and when connecting the same type of device, use a crossover cable.

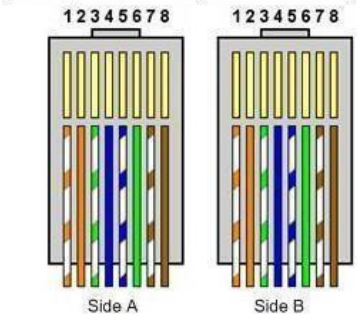
UTP Cables Connections types

1. **Straight-through UTP Cables**

A straight-through cable has connectors on each end that are terminated the same in accordance with either the T568A or T568B standards. Identifying the cable standard used allows you to determine if you have the right cable for the job. More importantly, it is a common practice to use the same colour codes throughout the LAN for consistency in documentation. Straight-through cables are used for the following connections:

- Switch to a router
- Computer to switch
- Computer to Hub

Pin ID	Side A	Side B
1	Orange-white	Orange-white
2	Orange	Orange
3	Green-white	Green-white
4	Blue	Blue
5	Blue-white	Blue-white
6	Green	Green
7	Brown-white	Brown-white
8	Brown	Brown



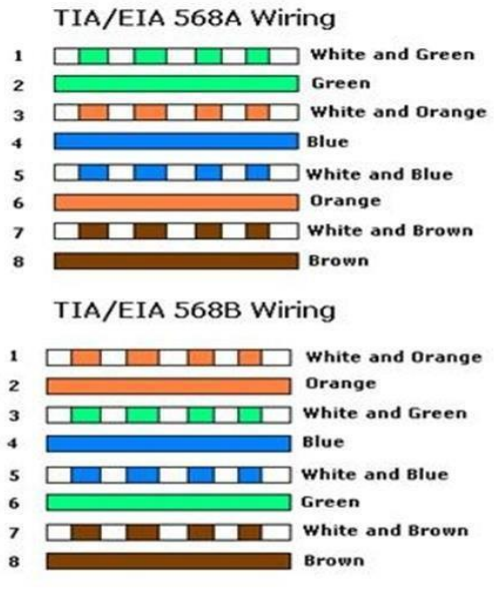


Figure A

Shows the Pin Out of Straight through Cables

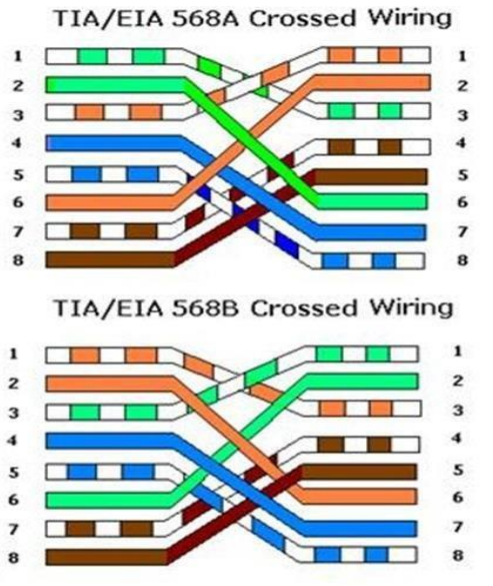


Figure B

Shows the Pin Out of Crossover Cables

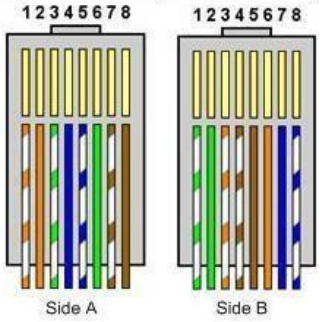
2. Cross-Over UTP cables

For two devices to communicate through a cable that is directly connected between the two, the transmit terminal of one device needs to be connected to the receive terminal of the other device. The cable must be terminated so the transmit pin, Tx, taking the signal from device A at one end, is wired to the receive pin, Rx, on device B. Similarly, device B's Tx pin must be connected to device A's Rx pin. If the Tx pin on a device is numbered 1, and the Rx pin is numbered 2, the cable connects pin 1 at one end with pin 2 at the other end. These "crossed over" pin connections give this type of cable its name, crossover.

To summarize, crossover cables directly connect the following devices on a LAN:

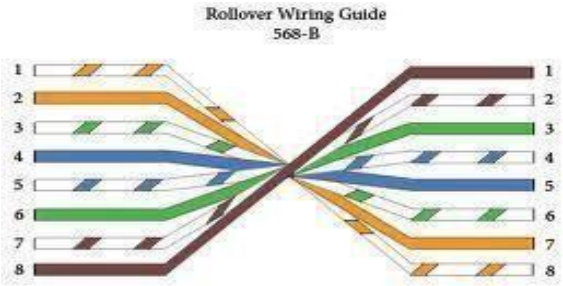
a. Switch to switch
b. Computer to computer
c. Hub to hub
d. Router to router

Pin ID	side A	side B
1	Orange-white	green-white
2	Orange	green
3	green-white	orange-white
4	blue	brown-white
5	blue-white	Brown
6	green	orange
7	brown-white	Blue
8	brown	blue-white



3. Roller Over UTP cables

In a rolled cable, the coloured wires at one end of the cable are in the reverse sequence of the coloured wires at the other end of the cable.



Network Cable Tools

1. Modular Plug Crimp Tool

2. Stripping Tool

How to prepare a UTP cable

The components needed for this include:

a. Category 5e cable
b. RJ-45 connectors
c. Crimpers
d. A stripper
e. Cable testers

Step 1: Take the roll of UTP cable and cut the cable to 1 metre length using the cutting blade on the crimp tool.

Step 2: Use the wire stripper to strip the insulation jacket off the cable to expose the wires (inside wire pairs). You will need to rotate the wire about 1-2 turns to strip away all the jacket. If you turn it too far, it will damage the wires inside the cable.

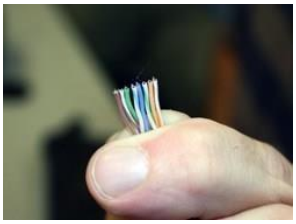
Carefully strip the cable jacket away to expose the four wire pairs

Step 3: Take each twisted pair and make four wire strands, each going out from the centre of the wire.

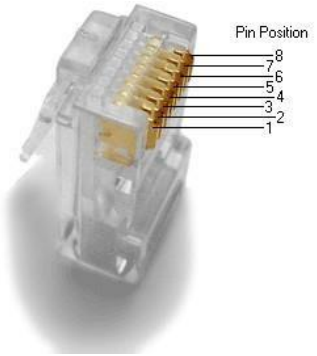
Step 4: Now take the individual twisted wire pairs and untwist them down to individual wires according to the TIA/EIA 568B (Figure A) wire colour sequence

Step 5: Next, grasp the wires with your thumb and index finger of your non-dominant hand. Take each wire and snug them securely side by side.

Step 6: Using the cutting blade of the crimp tool, cut the ends of the wires to make each wire the same height.



Step 7: Still grasping the wires, insert the RJ-45 jack on the wires with the clip facing away from you. Pin positions of RJ-45 connector is as follows:



Step 8: Insert the jack into the crimper and press down tightly on the tool to seal the wires in place.

Step 9: Once the first head is made, repeat steps two through eight for second head. When untwisting the wires down to sing strands, use the same order of pairs as above for Straight through cable. For crossover cable, Figure b (TIA/EIA 568B) will be followed for second head.

Step 10: Plug in the cable to test connectivity and show this to RA.

Application of Ethernet crossover cable is to copy/share files between two PCs.

CABLING RULES

- Do not bend cables to less than four times the diameter of the cable.
- If you bundle a group of cables together with cable ties (zip ties), do not over-cinch them. It is okay to snug them together firmly; but don't tighten them so much that you deform the cables.
- Keep cables away from devices which can introduce noise into them. Here's a short list: copy machines, electric heaters, speakers, printers, TV sets, fluorescent lights, copiers, welding machines, microwave ovens, telephones, fans, elevators motors, electric ovens, dryers, washing machines, and shop equipment.
- Avoid stretching UTP cables (the force should not exceed 25 LBS).
- Do not run UTP cable outside of a building. It presents a very dangerous lightning hazard!
- Do not use a stapler to secure UTP cables. Use telephone wire hangers which are available at most hardware stores.

Acronym

IP: Internet Protocol

DHCP: Dynamic Host Configuration protocol

DNS: Domain Name Server

LAN: Local Area Network

UTP: Unshielded Twisted Pair

Lab Evaluation Assessment Rubric
EE-424 Lab 1

#	Assessment Elements	Level 1: Unsatisfactory Points 0-1	Level 2: Developing Points 2	Level 3: Good Points 3	Level 4: Exemplary Points 4
LR2	**Program/Code/ Simulation Model/ Network Model**	Program/code/simulation model/network model does not implement the required functionality and has several errors. The student is not able to utilize even the basic tools of the software.	Program/code/simulation model/network model has some errors and does not produce completely accurate results. Student has limited command on the basic tools of the software.	Program/code/simulation model/network model gives correct output but not efficiently implemented or implemented by computationally complex routine.	Program/code/simulation /network model is efficiently implemented and gives correct output. Student has full command on the basic tools of the software.
LR4	**Data Collection**	Measurements are incomplete, inaccurate and imprecise. Observations are incomplete or not included. Symbols, units and significant figures are not included.	Measurements are somewhat inaccurate and imprecise. Observations are incomplete or vague. Major errors are there in using symbols, units and significant digits.	Measurements are mostly accurate. Observations are generally complete. Minor errors are present in using symbols, units and significant digits.	Measurements are both accurate and precise. Data collection is systematic. Observations are very thorough and include appropriate symbols, units and significant digits and task completed in due time.
LR5	**Results & Plots**	Figures/ graphs / tables are not developed or are poorly constructed with erroneous results. Titles, captions, units are not mentioned. Data is presented in an obscure manner.	Figures, graphs and tables are drawn but contain errors. Titles, captions, units are not accurate. Data presentation is not too clear.	All figures, graphs, tables are correctly drawn but contain minor errors or some of the details are missing.	Figures / graphs / tables are correctly drawn and appropriate titles/captions and proper units are mentioned. Data presentation is systematic.
LR9	**Report**	All the in-lab tasks are not included in report.	Most of the tasks are included in report but are not well explained. All the necessary figures / plots are not included.	Good summary of most of the in-lab tasks is included in report. The work is supported by figures and plots with explanations.	Detailed summary of the in-lab tasks is provided. All tasks are included and explained well. Data is presented clearly including all the necessary figures, plots and tables.
AR2	***[1]Attendance**	Marked attendance and did not attend the lab or left very early.	Present but very late (31-60 minutes) or left early (31-60 minutes) without completing the tasks.	*Present but late (15-30 minutes), or left early (30 minutes) without completing the tasks.	Present and entered the lab on time and left on time.
AR4	***Report Submission**	Late submission after 1 week and in between 2 weeks.	Late submission after 2 days and within a week.	Late submission after the lab timing and within 2 days of the due date.	Timely submission of the report and in the lab time.

***[3]Report:** Report will not be accepted after 1 week of due date