Assignment 4

Prepare a detailed report demonstrating the following with proper illustrations and screen shots as applicable.

A) CAT-5/CAT-6 cable preparation with RJ-45 connector; both straight and cross cabling.

B) IP address configuration (both Static and DHCP) on Linux and Windows systems.

C) Introduction to the following important network related tools and commands with appropriate examples,

1. ipconfig (Windows)
2. ifconfig (Linux)
3. ip
4. hostname
5. ping
6. netstat
7. route
8. traceroute or tracert
9. tcpdump
***10. Wireshark* Answer:**

Ans A: Preparing CAT-5/CAT-6 cables with RJ-45 connectors involves a few standard steps.

Tools Required:

- CAT-5/CAT-6 cable
- RJ-45 connectors
- Crimping tool
- Cable cutter/stripper
- Optional: Cable tester (for verifying connections)

Steps:

For ***Straight-Through Cable****:*

- Strip the Cable: Use a cable cutter/stripper to carefully remove about 1.5 inches (38 mm) of the outer insulation from the end of the cable. Inside, you will find four twisted pairs of wires.
- Untwist the Pairs: Gently untwist the pairs and straighten each wire.
- Arrange the Wires: Arrange the wires according to the T568B wiring standard. The order from left to right should be:
  - Orange Stripe
    - Orange
  - Green Stripe
    - Blue

- Blue Stripe
    - Green
- Brown Stripe
- Brown

- Trim Excess: Trim the wires to a uniform length, leaving approximately 1/2 inch (12 mm) extending past the jacket.
- Insert Wires into RJ-45 Connector: Carefully insert the wires into the RJ-45 connector, ensuring they go all the way to the end and are in the correct order.
- Crimp the Connector: Use a crimping tool to crimp the connector onto the cable securely. Apply enough pressure to ensure a good connection without damaging the cable.
- Repeat for the Other End: Repeat the above steps for the other end of the cable.
- Test the Cable: Optional but recommended, use a cable tester to ensure the connections are correct and there are no faults.

For ***Crossover Cable***:

A crossover cable is used to connect two similar devices directly, such as two computers without a switch in between. The wiring pattern for a crossover cable is slightly different from a straight-through cable.

The only difference in the process is the wiring arrangement:

Instead of following T568B on both ends, follow this wiring pattern on one end and T568A on the other:

- End 1 (T568B):
    - Orange Stripe
        - Orange
    - Green Stripe
        - Blue
    - Blue Stripe
        - Green
    - Brown Stripe
    - Brown ➢ End 2 (T568A):
        - Green Stripe
        - Green
    - Orange Stripe
        - Blue
    - Blue Stripe
        - Orange
    - Brown Stripe
    - Brown

This arrangement effectively swaps the transmit and receive lines, creating a crossover connection.

Repeat all other steps as described for a straight-through cable. By following these steps, you should be able to prepare both straight-through and crossover CAT-5/CAT6 cables with RJ-45 connectors.

<u>Ans B:</u> Linux:
Static IP Configuration:

- ✓ Open the terminal.
- ✓ Edit the network configuration file using a text editor like nano or vi:

```
sudo nano /etc/network/interfaces
```

- ✓ Find the line for your network interface (e.g., eth0).
- ✓ Modify it to include the static IP address, netmask, gateway, and DNS servers:

```
iface eth0 inet static address
        192.168.1.100 netmask
        255.255.255.0 gateway
        192.168.1.1 dns-nameservers
        8.8.8.8 8.8.4.4
```

- ✓ Save the file and exit the text editor. Restart the network service:

```
sudo systemctl restart networking
```

DHCP IP Configuration:

- ✓ Open the terminal.
- ✓ Edit the DHCP configuration file:

```
sudo nano /etc/network/interfaces
```

- ✓ Find the line for your network interface (e.g., eth0).
- ✓ Modify it to use DHCP:

```
iface eth0 inet dhcp
```

- ✓ Save the file and exit the text editor.
- ✓ Restart the network service:

```
sudo systemctl restart networking
```

Windows:

Static IP Configuration:

- ✓ Right-click on the network icon in the system tray and select "Open Network & Internet settings."
- ✓ Click on "Change adapter options."
- ✓ Right-click on the network adapter you want to configure and select "Properties."
- ✓ Select "Internet Protocol Version 4 (TCP/IPv4)" and click "Properties."

- ✓ Choose "Use the following IP address" and enter the IP address, subnet mask, default gateway, and DNS server addresses. □ Click "OK" to save the settings.

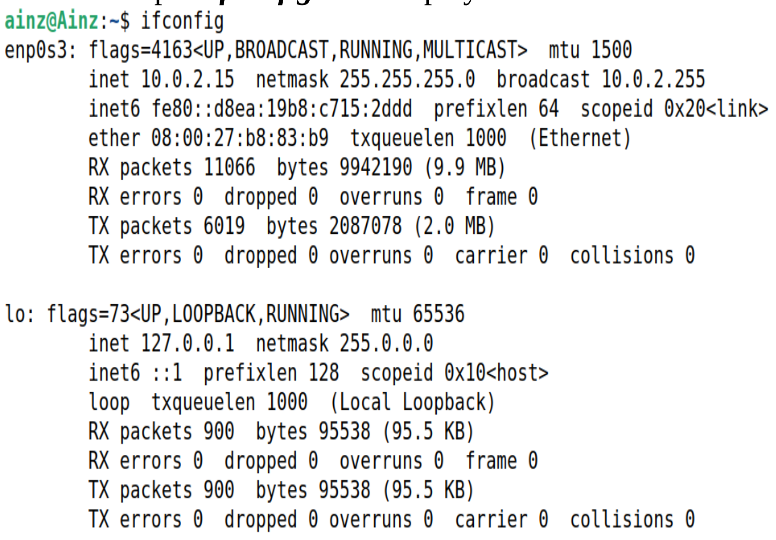
DHCP IP Configuration:

- ✓ Follow steps 1-3 from the Static IP Configuration section.
- ✓ Select "Obtain an IP address automatically" and "Obtain DNS server address automatically." Click "OK" to save the settings.

That's it! You've configured both cable connections with RJ-45 connectors and IP addresses on Linux and Windows systems.

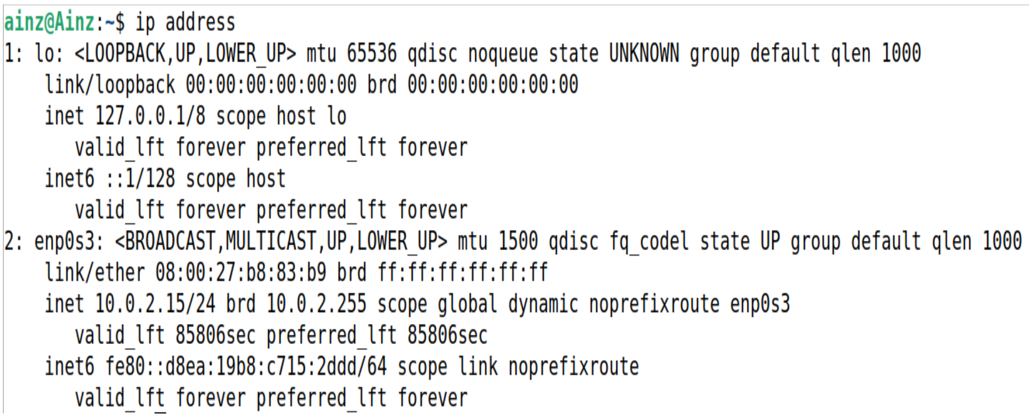
Ans C: Here's an introduction to each of the mentioned network-related tools and commands with appropriate examples:

1. ipconfig (Windows):
   - ipconfig is a command-line utility in Windows used to display and manage network configurations of the local system.
   - Example: ***ipconfig /all*** displays detailed information about all network interfaces.
2. ifconfig (Linux):
   - ifconfig is a command-line utility in Linux used to configure and display information about network interfaces.
   - Example: ***ifconfig eth0*** displays information about the Ethernet interface eth0.



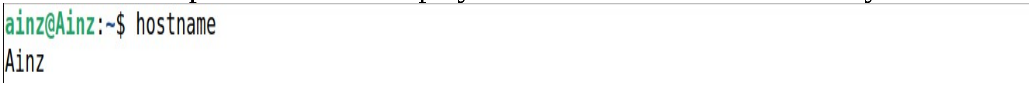
```
ainz@Ainz:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::d8ea:19b8:c715:2ddd  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:b8:83:b9  txqueuelen 1000  (Ethernet)
        RX packets 11066  bytes 9942190 (9.9 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6019  bytes 2087078 (2.0 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 900  bytes 95538 (95.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 900  bytes 95538 (95.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

3. ip:
   - The ip command is a powerful utility for network configuration in Linux. It is more versatile than ifconfig and route.
   - Example: ***ip*** address show displays IP addresses assigned to all network interfaces.



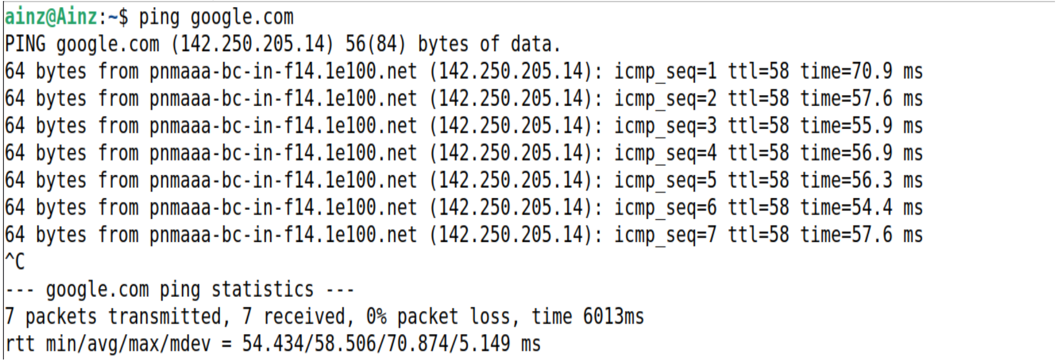
```
ainz@Ainz:~$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:b8:83:b9 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
       valid_lft 85806sec preferred_lft 85806sec
    inet6 fe80::d8ea:19b8:c715:2ddd/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

4. hostname:
   - hostname is a command that displays or sets the hostname of the system.
     - Example: ***hostname*** displays the current hostname of the system.



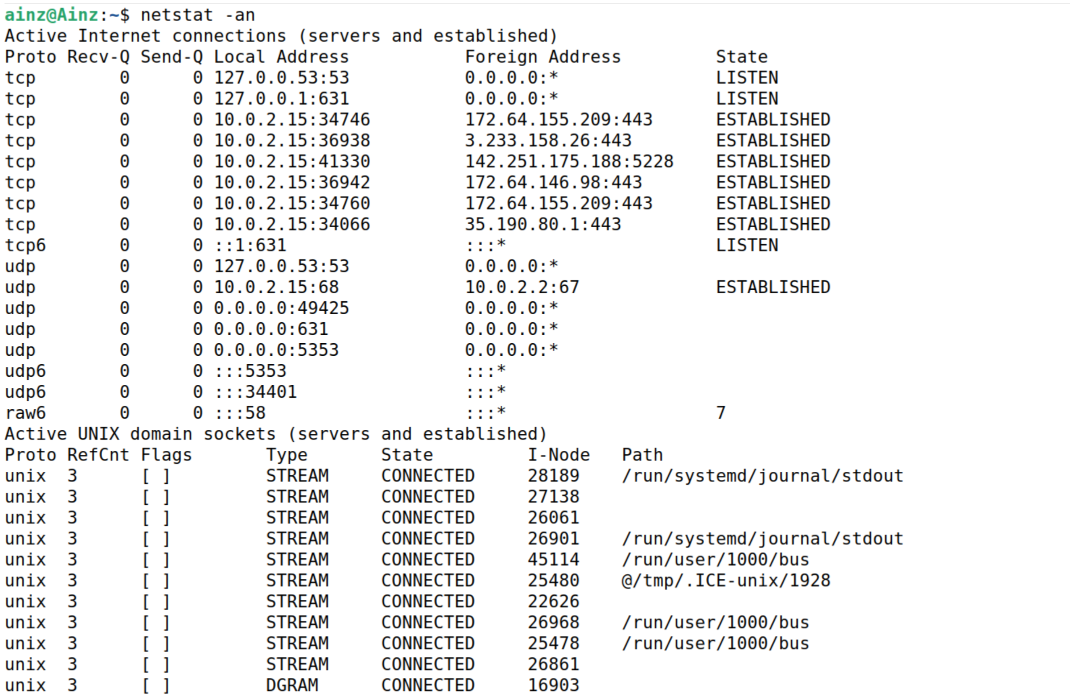
```
ainz@Ainz:~$ hostname
Ainz
```

5. ping:
   - ping is a utility used to test the reachability of a host on an Internet Protocol (IP) network.
   - Example: ***ping google.com*** sends ICMP echo requests to google.com to check connectivity.



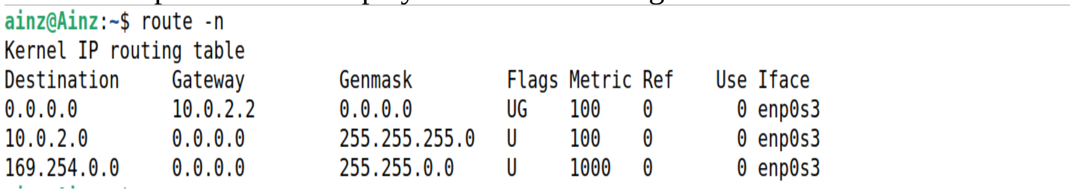
```
ainz@Ainz:~$ ping google.com
PING google.com (142.250.205.14) 56(84) bytes of data.
64 bytes from pnmaaa-bc-in-f14.1e100.net (142.250.205.14): icmp_seq=1 ttl=58 time=70.9 ms
64 bytes from pnmaaa-bc-in-f14.1e100.net (142.250.205.14): icmp_seq=2 ttl=58 time=57.6 ms
64 bytes from pnmaaa-bc-in-f14.1e100.net (142.250.205.14): icmp_seq=3 ttl=58 time=55.9 ms
64 bytes from pnmaaa-bc-in-f14.1e100.net (142.250.205.14): icmp_seq=4 ttl=58 time=56.9 ms
64 bytes from pnmaaa-bc-in-f14.1e100.net (142.250.205.14): icmp_seq=5 ttl=58 time=56.3 ms
64 bytes from pnmaaa-bc-in-f14.1e100.net (142.250.205.14): icmp_seq=6 ttl=58 time=54.4 ms
64 bytes from pnmaaa-bc-in-f14.1e100.net (142.250.205.14): icmp_seq=7 ttl=58 time=57.6 ms
^C
--- google.com ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6013ms
rtt min/avg/max/mdev = 54.434/58.506/70.874/5.149 ms
```

6. netstat:
   - netstat is a command-line tool used for displaying network connections, routing tables, interface statistics, masquerade connections, and multicast memberships.
   - Example: ***netstat -an*** displays all active network connections.



```
ainz@Ainz:~$ netstat -an
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp        0      0 10.0.2.15:34746         172.64.155.209:443      ESTABLISHED
tcp        0      0 10.0.2.15:36938         3.233.158.26:443        ESTABLISHED
tcp        0      0 10.0.2.15:41330         142.251.175.188:5228    ESTABLISHED
tcp        0      0 10.0.2.15:36942         172.64.146.98:443       ESTABLISHED
tcp        0      0 10.0.2.15:34760         172.64.155.209:443      ESTABLISHED
tcp        0      0 10.0.2.15:34066         35.190.80.1:443         ESTABLISHED
tcp6       0      0 ::1:631                 :::*                    LISTEN
udp        0      0 127.0.0.53:53           0.0.0.0:*
udp        0      0 10.0.2.15:68            10.0.2.2:67             ESTABLISHED
udp        0      0 0.0.0.0:49425           0.0.0.0:*
udp        0      0 0.0.0.0:631             0.0.0.0:*
udp        0      0 0.0.0.0:5353            0.0.0.0:*
udp6       0      0 :::5353                 :::*
udp6       0      0 :::34401                :::*
raw6       0      0 :::58                   :::*                    7
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  3      [ ]         STREAM     CONNECTED     28189    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     27138
unix  3      [ ]         STREAM     CONNECTED     26061
unix  3      [ ]         STREAM     CONNECTED     26901    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     45114    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     25480    @/tmp/.ICE-unix/1928
unix  3      [ ]         STREAM     CONNECTED     22626
unix  3      [ ]         STREAM     CONNECTED     26968    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     25478    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     26861
unix  3      [ ]         DGRAM      CONNECTED     16903
```

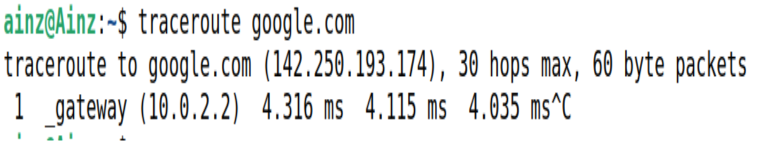
7. route:
    - route is a command-line utility in Linux used to view and manipulate the IP routing table.
    - Example: ***route -n*** displays the kernel routing table in numerical format.



```
ainz@Ainz:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.0.2.2        0.0.0.0         UG    100    0        0 enp0s3
10.0.2.0        0.0.0.0         255.255.255.0   U     100    0        0 enp0s3
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 enp0s3
```

8. traceroute or tracert:
    - traceroute (Linux) or tracert (Windows) is used to trace the route that packets take from the local host to a destination host.

- Example: ***traceroute google.com*** traces the route to google.com displaying the IP addresses of routers along the path.



```
ainz@Ainz:~$ traceroute google.com
traceroute to google.com (142.250.193.174), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.2)  4.316 ms  4.115 ms  4.035 ms^C
```

9. tcpdump:
   - tcpdump is a command-line packet analyzer. It allows the user to display TCP/IP and other packets being transmitted or received over a network. Example: ***tcpdump -i eth0*** captures packets on the eth0 interface.
10. Wireshark:
    - Wireshark is a GUI-based packet analyzer that allows the user to capture and interactively browse the traffic running on a computer network.
    - Example: Launch ***Wireshark***, select the network interface, and start capturing packets for analysis.

These tools and commands are essential for network troubleshooting, monitoring, and configuration in both Windows and Linux environments.