GURU GOBIND SINGH INDRAPRASTHA UNIVERSITY

East Delhi Campus , Surjamal Vihar
Delhi – 110092

COMPUTER NETWORK LAB

File

COURSE CODE: ARM258

SUBMITTED TO:
DR.Ashok Kumar

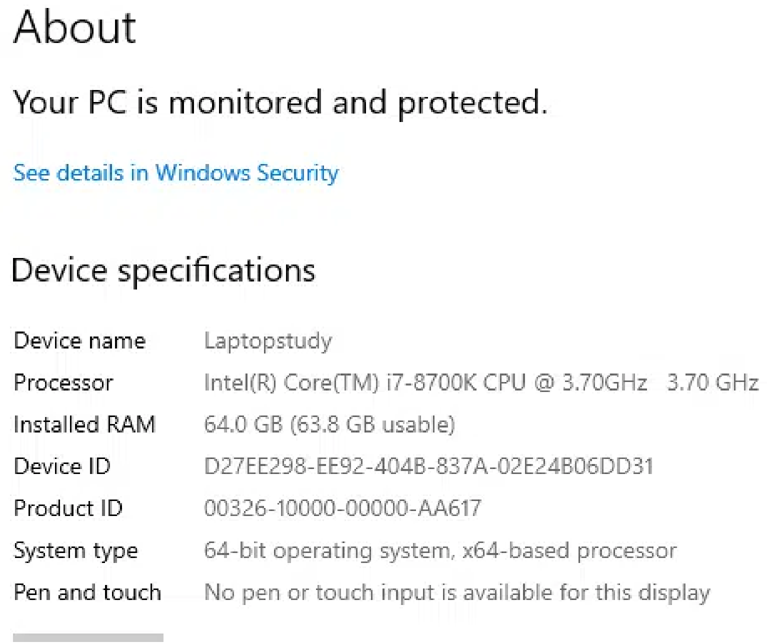
SUBMITTED BY:
Ankit Sharma
AI-ML B2
20319051622

S. No	Program	Date	Signature

Experiment No 1

Aim: To study about the components and specifications of Computer and Laptop

- **Computer :**
  A computer is a machine or device that performs processes, calculations and operations based on instructions provided by a software or hardware program. It is designed to execute applications and provides a variety of solutions by combining integrated hardware and software components.
- **Computer Specification :**



About

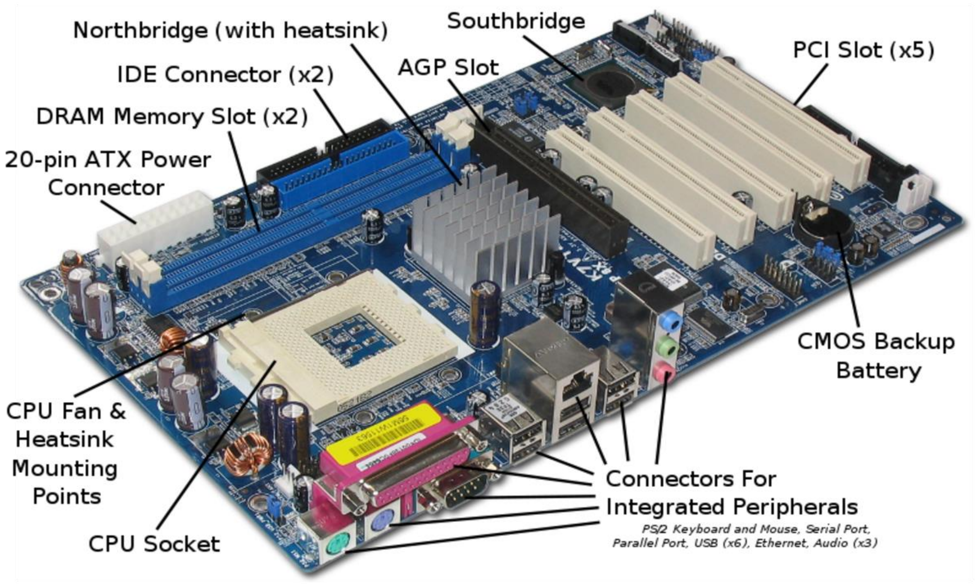
Your PC is monitored and protected.

See details in Windows Security

Device specifications

Device name	Laptopstudy
Processor	Intel(R) Core(TM) i7-8700K CPU @ 3.70GHz 3.70 GHz
Installed RAM	64.0 GB (63.8 GB usable)
Device ID	D27EE298-EE92-404B-837A-02E24B06DD31
Product ID	00326-10000-00000-AA617
System type	64-bit operating system, x64-based processor
Pen and touch	No pen or touch input is available for this display

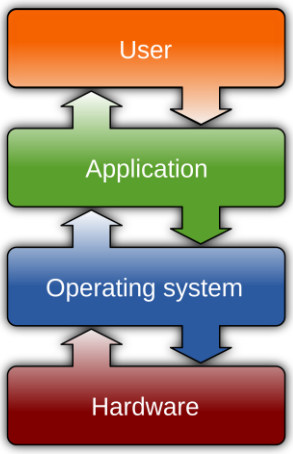
1. **Motherboard:**
   The motherboard is the backbone of your PC and it provides the electrical connections between every component so that they are able to communicate with each other.


Northbridge (with heatsink)
Southbridge
IDE Connector (x2)
AGP Slot
PCI Slot (x5)
DRAM Memory Slot (x2)
20-pin ATX Power Connector
CMOS Backup Battery
CPU Fan & Heatsink Mounting Points
CPU Socket
Connectors For Integrated Peripherals
PS/2 Keyboard and Mouse, Serial Port, Parallel Port, USB (x6), Ethernet, Audio (x3)

2. Processors:

A processor (CPU) is the logic circuitry that responds to and processes the basic instructions that drive a computer. The CPU is seen as the main and most crucial integrated circuitry (IC) chip in a computer, as it is responsible for interpreting most of computers commands. Mentioned computer's processor has a **speed of 3.70 GHz.**

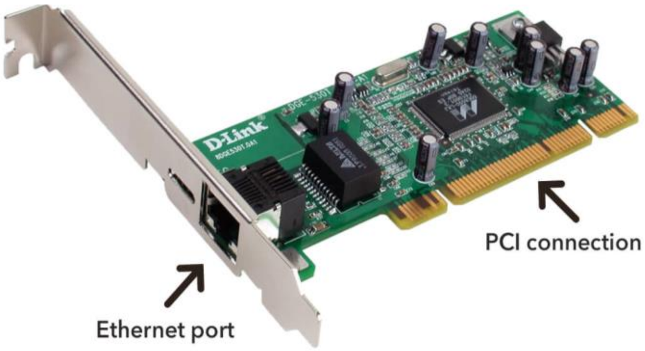
3. Operating System:



An Operating System (OS) is an interface between a computer user and computer hardware. An operating system is a software which performs all the basic tasks like file management, memory management, process management, handling input and output, and controlling peripheral devices such as disk drives and printers. The Computer has **Window 10 & 64-bit** operating system.

4. Network Interface Card:

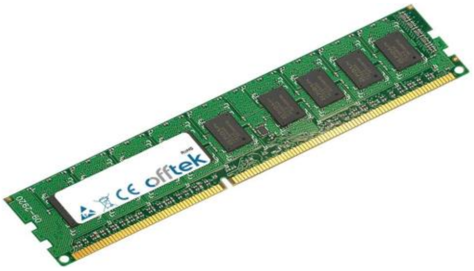
A network interface card (NIC) is a hardware component without which a computer cannot be connected over a network. It is a circuit board installed in a computer that provides a dedicated network connection to the computer. It is also called network interface controller, network adapter or LAN adapter.



5. Memory:

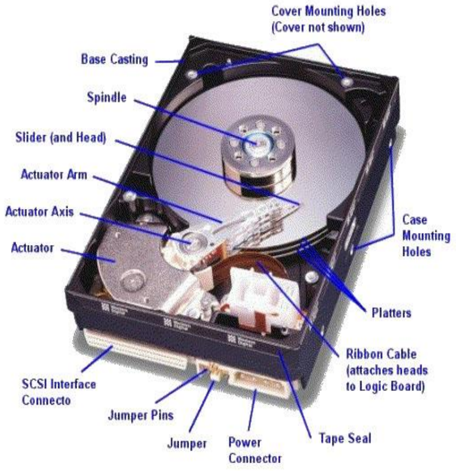
It is used to store data and instructions. Computer memory is the storage space in the computer, where data is to be processed and instructions required for processing are stored. The memory is divided into large number of small parts called cells. Each location or cell has a unique address, which varies from zero to memory size minus one.

a. RAM:



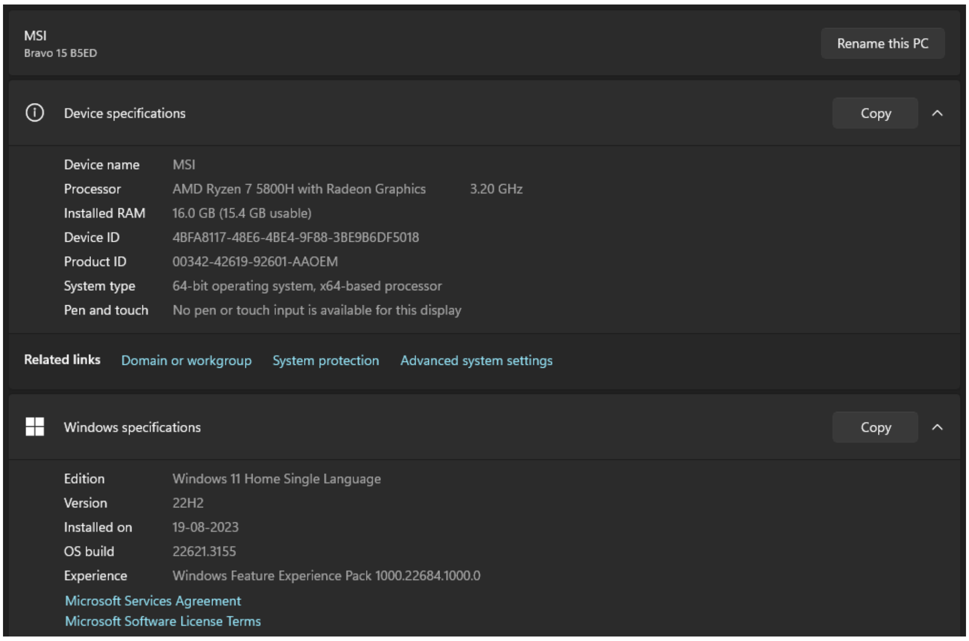
RAM is the working memory of your computer. The higher the RAM, the more multi-tasking the computer can do. Mentioned computer have **64 GB ram.**

b. Hard Disk Drive:



HDD is an electro-mechanical storage device, which is an abbreviation of Hard Disk Drive. It uses magnetic storage for storing and retrieving the digital data. It is a non-volatile storage device. Mentioned computer have HDD of **1TB.**

- **Laptop:**
  Laptop is a small, portable personal computer(pc) with a screen and alphanumeric keyboard. It is also known as laptop computer, notebook computer.
- **Laptop Specifications:**



MSI
Bravo 15 B5ED

Device specifications

Device name	MSI
Processor	AMD Ryzen 7 5800H with Radeon Graphics 3.20 GHz
Installed RAM	16.0 GB (15.4 GB usable)
Device ID	4BFA8117-48E6-4BE4-9F88-3BE9B6DF5018
Product ID	00342-42619-92601-AAOEM
System type	64-bit operating system, x64-based processor
Pen and touch	No pen or touch input is available for this display

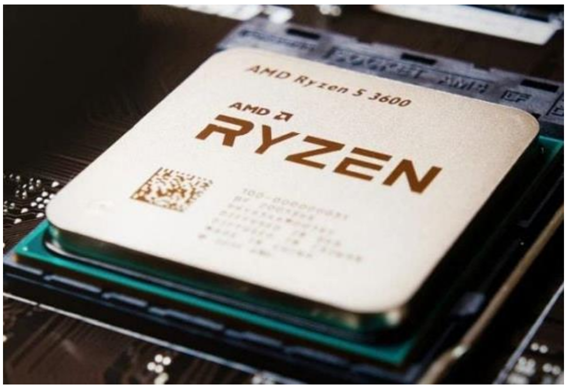
Related links Domain or workgroup System protection Advanced system settings

Windows specifications

Edition	Windows 11 Home Single Language
Version	22H2
Installed on	19-08-2023
OS build	22621.3155
Experience	Windows Feature Experience Pack 1000.22684.1000.0

Microsoft Services Agreement
Microsoft Software License Terms

1. **Processor:**



A processor is an integrated electronic circuit that performs the calculations that run a Laptop. A processor performs arithmetical, logical, input/output (1/0) and other basic instructions that are passed from an operating system (OS). Mentioned Laptop have **Ryzen 7 5800H.**

2. **Operating System:**
   An operating system is a program that acts as an interface between the user and the computer hardware and controls the execution of all kinds of programs. Mentioned Laptop have **Window 11 & 64-bit** operating system.

3. **Types of Memory used:**
   - **Cache Memory:**
     It is an extremely fast memory type that acts as a buffer between RAM and the CPU. It holds frequently requested data and instructions so that they are immediately available to the CPU when needed. Cache memory is used to reduce the average time to access data from the Main memory.

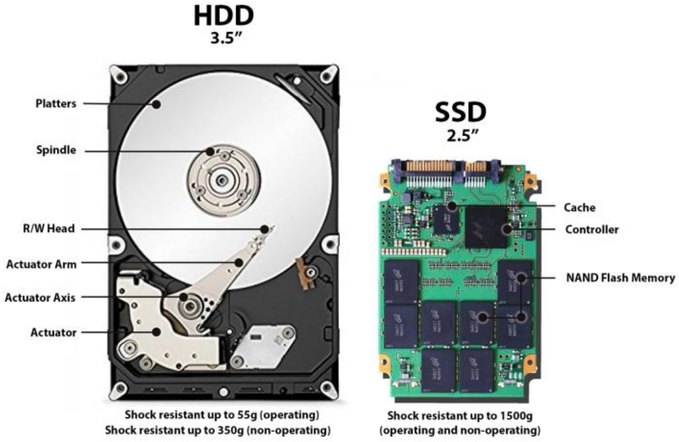
- **RAM:**

RAM (Random Access Memory) is the internal memory of the CPU for storing data, program, and program result. It is a read/write memory which stores data until the machine is working. Mentioned LAptop has **16GB** RAM.

- **Hard Disk drive:**

HDD is used in computer to facilitate the user to store data permanently as it is non volatile.

- **Solid State Drive:**


HDD
3.5″
Platters
Spindle
R/W Head
Actuator Arm
Actuator Axis
Actuator
Shock resistant up to 55g (operating)
Shock resistant up to 350g (non-operating)
SSD
2.5″
Cache
Controller
NAND Flash Memory
Shock resistant up to 1500g
(operating and non-operating)

It is a new generation of storage device. It is faster but expensive than HDD. Mentioned Laptop have **512GB** SSD.

4. Ports in Laptop:

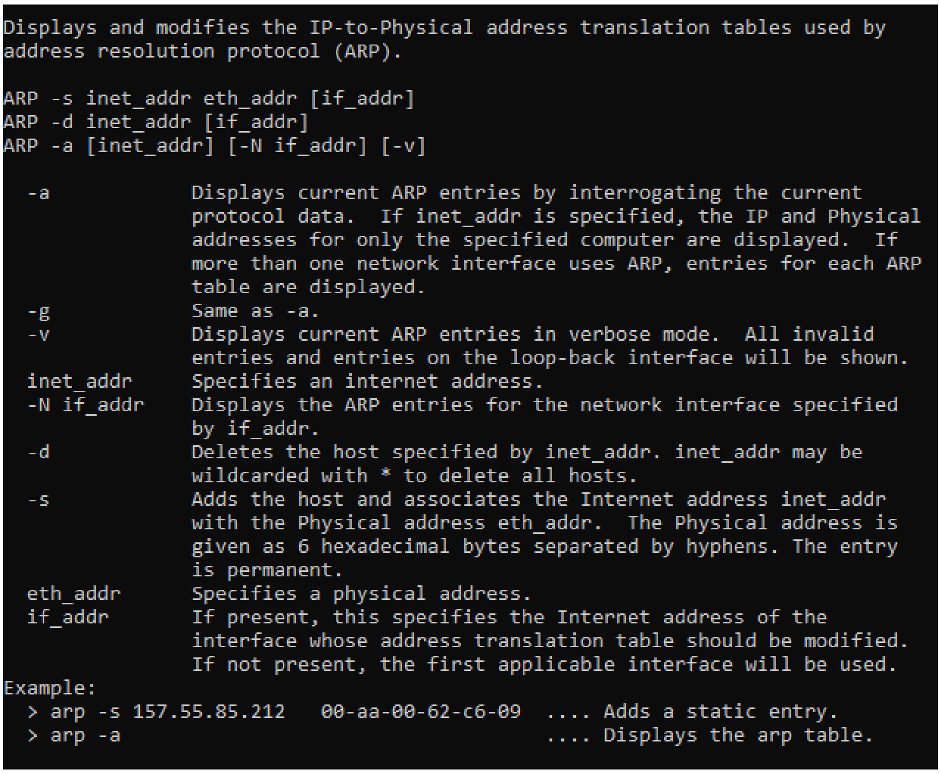
Laptops generally have 5 types of ports.

- Charging port (used to charge laptop).
- USB type C port (used for Bidirectional data transfer, taking power supply).
- RJ-45 port for Ethernet connection.
- HDMI port
- Headphone 2.0 port

Experiment No 2

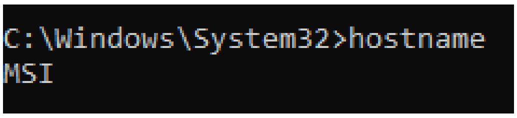
Aim: To Study basic Networking Commands

- **ARP:** Used to display and modify the ARP cache, which translates IP addresses to MAC addresses and vice versa.



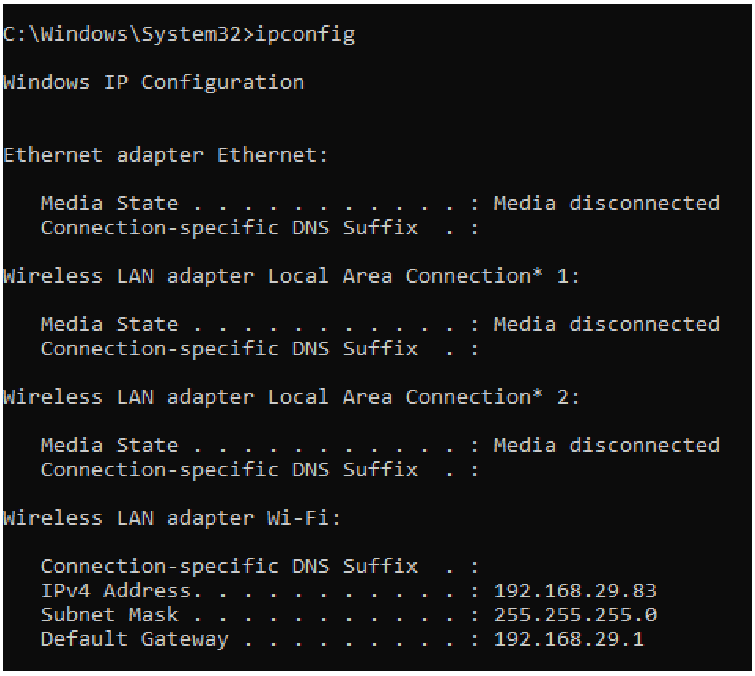
```
Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

  -a            Displays current ARP entries by interrogating the current
                protocol data.  If inet_addr is specified, the IP and Physical
                addresses for only the specified computer are displayed.  If
                more than one network interface uses ARP, entries for each ARP
                table are displayed.
  -g            Same as -a.
  -v            Displays current ARP entries in verbose mode.  All invalid
                entries and entries on the loop-back interface will be shown.
  inet_addr     Specifies an internet address.
  -N if_addr    Displays the ARP entries for the network interface specified
                by if_addr.
  -d            Deletes the host specified by inet_addr. inet_addr may be
                wildcarded with * to delete all hosts.
  -s            Adds the host and associates the Internet address inet_addr
                with the Physical address eth_addr.  The Physical address is
                given as 6 hexadecimal bytes separated by hyphens. The entry
                is permanent.
  eth_addr      Specifies a physical address.
  if_addr       If present, this specifies the Internet address of the
                interface whose address translation table should be modified.
                If not present, the first applicable interface will be used.
Example:
  > arp -s 157.55.85.212   00-aa-00-62-c6-09  .... Adds a static entry.
  > arp -a                                    .... Displays the arp table.
```

- **Hostname:** Displays the name of the current host or sets the hostname for the computer.



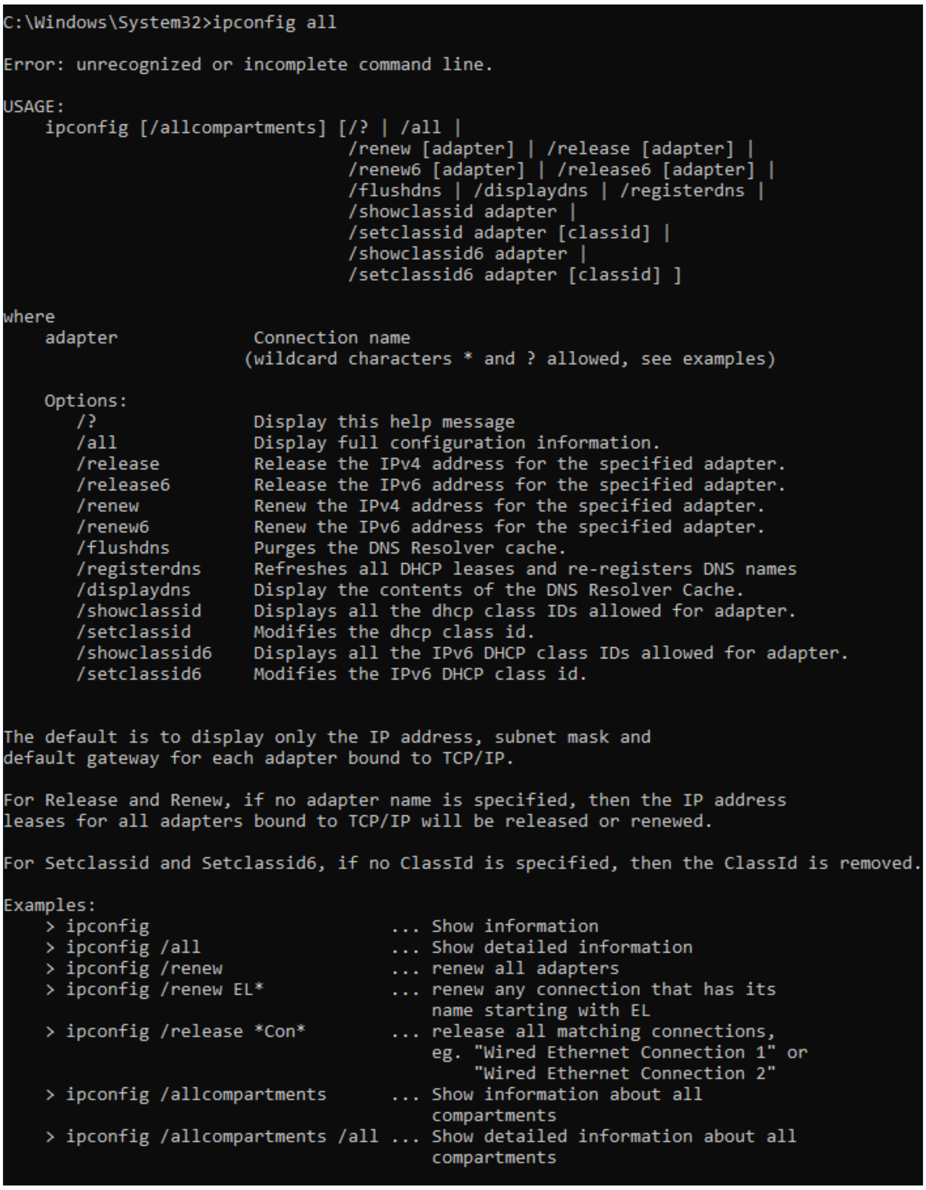
```
C:\Windows\System32>hostname
MSI
```

- **Ipconfig:** Displays all current TCP/IP network configuration values, including IP address.



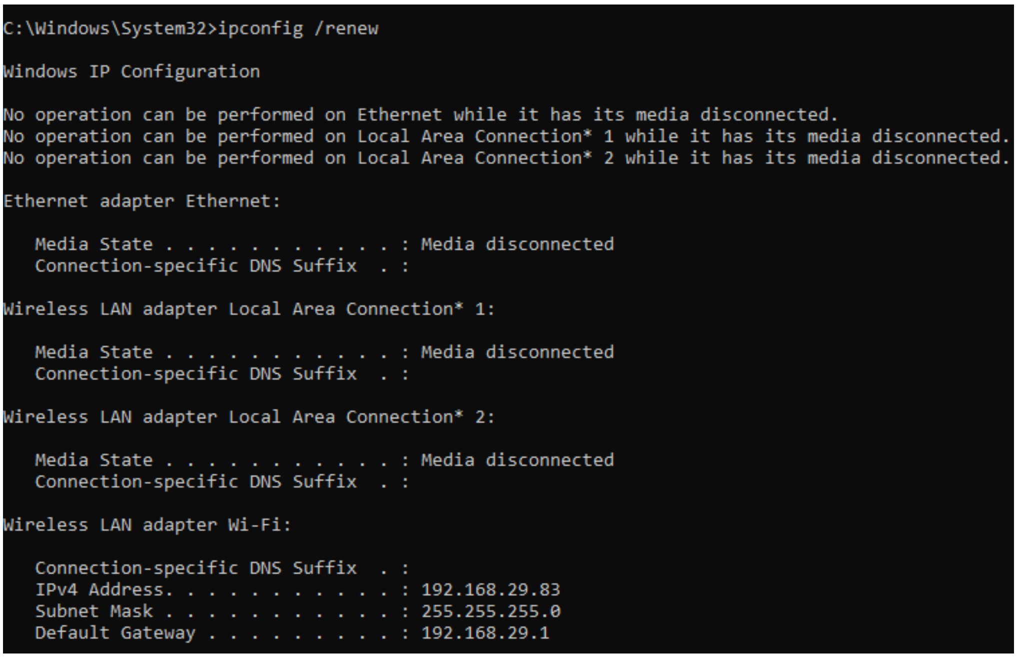
```
C:\Windows\System32>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.29.83
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.29.1
```

- **Ipconfig /all:** Displays detailed information about all network interfaces, including physical and virtual adapters, along with DNS and DHCP settings.



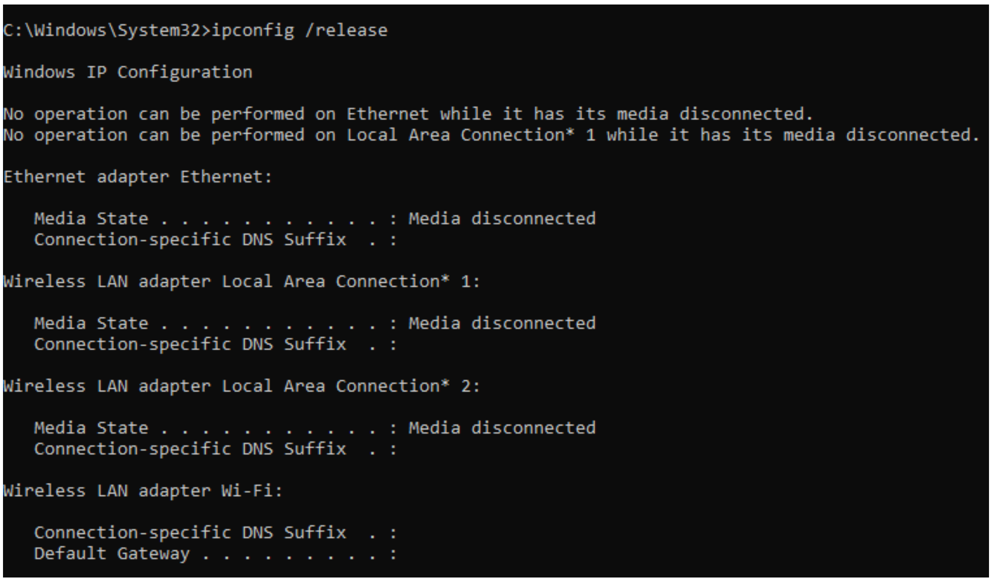
```
C:\Windows\System32>ipconfig all

Error: unrecognized or incomplete command line.

USAGE:
    ipconfig [/allcompartments] [/? | /all |
                                 /renew [adapter] | /release [adapter] |
                                 /renew6 [adapter] | /release6 [adapter] |
                                 /flushdns | /displaydns | /registerdns |
                                 /showclassid adapter |
                                 /setclassid adapter [classid] |
                                 /showclassid6 adapter |
                                 /setclassid6 adapter [classid] ]

where
    adapter             Connection name
                       (wildcard characters * and ? allowed, see examples)

    Options:
       /?               Display this help message
       /all             Display full configuration information.
       /release         Release the IPv4 address for the specified adapter.
       /release6        Release the IPv6 address for the specified adapter.
       /renew           Renew the IPv4 address for the specified adapter.
       /renew6          Renew the IPv6 address for the specified adapter.
       /flushdns        Purges the DNS Resolver cache.
       /registerdns     Refreshes all DHCP leases and re-registers DNS names
       /displaydns      Display the contents of the DNS Resolver Cache.
       /showclassid     Displays all the dhcp class IDs allowed for adapter.
       /setclassid      Modifies the dhcp class id.
       /showclassid6    Displays all the IPv6 DHCP class IDs allowed for adapter.
       /setclassid6     Modifies the IPv6 DHCP class id.


The default is to display only the IP address, subnet mask and
default gateway for each adapter bound to TCP/IP.

For Release and Renew, if no adapter name is specified, then the IP address
leases for all adapters bound to TCP/IP will be released or renewed.

For Setclassid and Setclassid6, if no ClassId is specified, then the ClassId is removed.

Examples:
    > ipconfig                       ... Show information
    > ipconfig /all                  ... Show detailed information
    > ipconfig /renew                ... renew all adapters
    > ipconfig /renew EL*            ... renew any connection that has its
                                         name starting with EL
    > ipconfig /release *Con*        ... release all matching connections,
                                         eg. "Wired Ethernet Connection 1" or
                                             "Wired Ethernet Connection 2"
    > ipconfig /allcompartments      ... Show information about all
                                         compartments
    > ipconfig /allcompartments /all ... Show detailed information about all
                                         compartments
```

- **Ipconfig /renew:** Renews the IP address configuration for all network adapters, typically used to request a new IP address from a DHCP server.



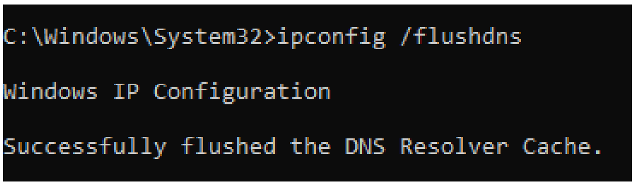
```
C:\Windows\System32>ipconfig /renew

Windows IP Configuration

No operation can be performed on Ethernet while it has its media disconnected.
No operation can be performed on Local Area Connection* 1 while it has its media disconnected.
No operation can be performed on Local Area Connection* 2 while it has its media disconnected.

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.29.83
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.29.1
```

- **Ipconfig /release:** Releases the IP address configuration for all network adapters, effectively disconnecting the computer from the network.



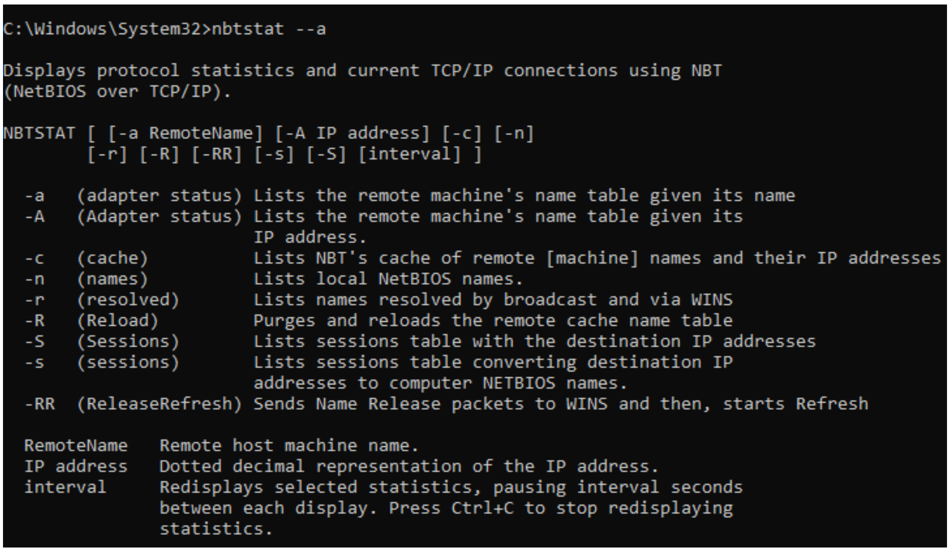
```
C:\Windows\System32>ipconfig /release

Windows IP Configuration

No operation can be performed on Ethernet while it has its media disconnected.
No operation can be performed on Local Area Connection* 1 while it has its media disconnected.

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Default Gateway . . . . . . . . . :
```

- **Ipconfig /flushdns:** Clears and resets the DNS resolver cache, which stores DNS query results for faster access.



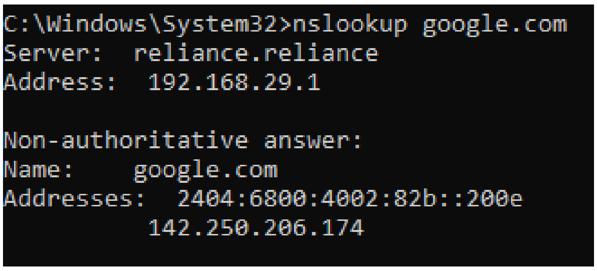
```
C:\Windows\System32>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
```

- **Nbtstat –a:** Displays the NetBIOS name table of a remote computer and the associated IP addresses.



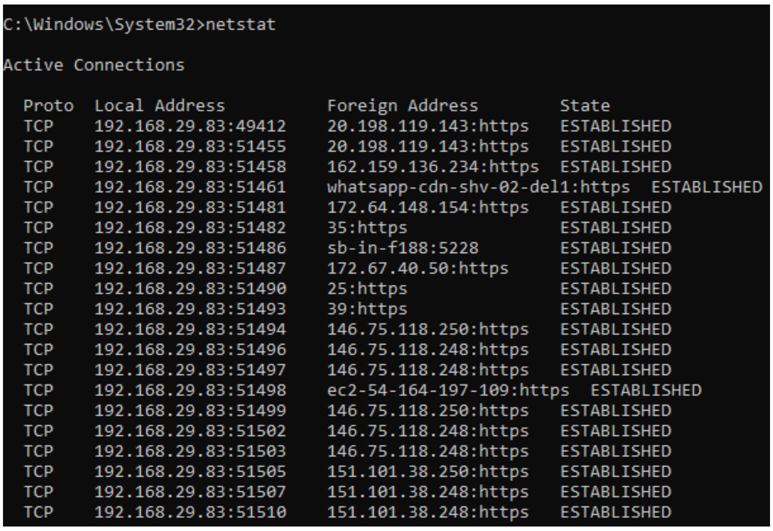
```
C:\Windows\System32>nbtstat --a

Displays protocol statistics and current TCP/IP connections using NBT
(NetBIOS over TCP/IP).

NBTSTAT [ [-a RemoteName] [-A IP address] [-c] [-n]
        [-r] [-R] [-RR] [-s] [-S] [interval] ]

  -a   (adapter status) Lists the remote machine's name table given its name
  -A   (Adapter status) Lists the remote machine's name table given its
                        IP address.
  -c   (cache)          Lists NBT's cache of remote [machine] names and their IP addresses
  -n   (names)          Lists local NetBIOS names.
  -r   (resolved)       Lists names resolved by broadcast and via WINS
  -R   (Reload)         Purges and reloads the remote cache name table
  -S   (Sessions)       Lists sessions table with the destination IP addresses
  -s   (sessions)       Lists sessions table converting destination IP
                        addresses to computer NETBIOS names.
  -RR  (ReleaseRefresh) Sends Name Release packets to WINS and then, starts Refresh

  RemoteName   Remote host machine name.
  IP address   Dotted decimal representation of the IP address.
  interval     Redisplays selected statistics, pausing interval seconds
               between each display. Press Ctrl+C to stop redisplaying
               statistics.
```

- **Nslookup:** A command-line tool used to query DNS servers to obtain domain name or IP address mapping, as well as other DNS information.



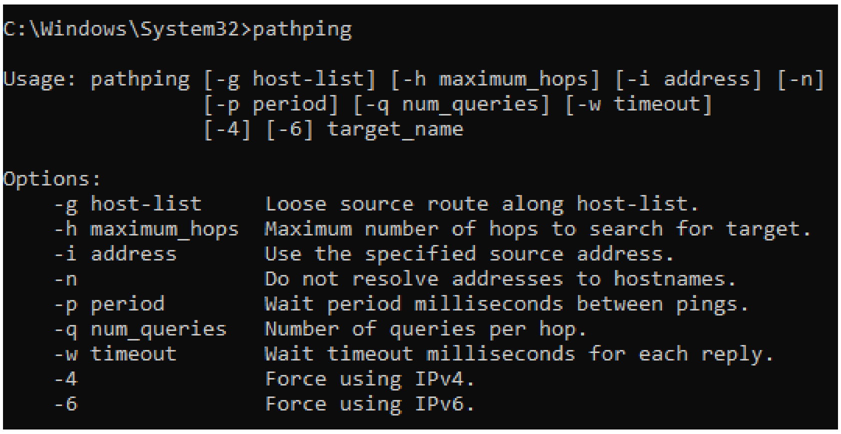
```
C:\Windows\System32>nslookup google.com
Server:  reliance.reliance
Address:  192.168.29.1

Non-authoritative answer:
Name:    google.com
Addresses:  2404:6800:4002:82b::200e
          142.250.206.174
```

- **Netdiag:** A command-line tool used to diagnose network problems by performing a series of tests on the network configuration and components.
- **Netstat:** Displays network statistics and active connections, including ports and routing tables.



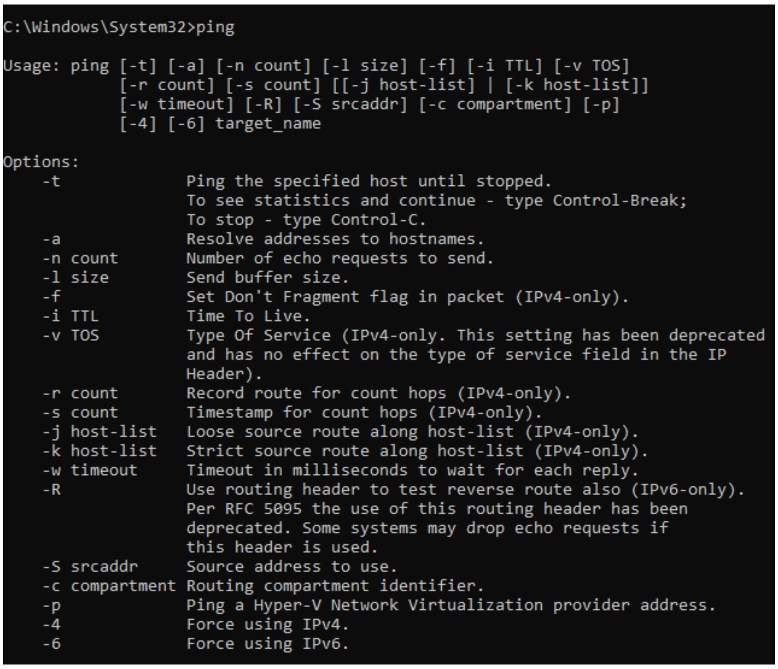
```
C:\Windows\System32>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.29.83:49412    20.198.119.143:https   ESTABLISHED
  TCP    192.168.29.83:51455    20.198.119.143:https   ESTABLISHED
  TCP    192.168.29.83:51458    162.159.136.234:https  ESTABLISHED
  TCP    192.168.29.83:51461    whatsapp-cdn-shv-02-del1:https  ESTABLISHED
  TCP    192.168.29.83:51481    172.64.148.154:https   ESTABLISHED
  TCP    192.168.29.83:51482    35:https               ESTABLISHED
  TCP    192.168.29.83:51486    sb-in-f188:5228        ESTABLISHED
  TCP    192.168.29.83:51487    172.67.40.50:https     ESTABLISHED
  TCP    192.168.29.83:51490    25:https               ESTABLISHED
  TCP    192.168.29.83:51493    39:https               ESTABLISHED
  TCP    192.168.29.83:51494    146.75.118.250:https   ESTABLISHED
  TCP    192.168.29.83:51496    146.75.118.248:https   ESTABLISHED
  TCP    192.168.29.83:51497    146.75.118.248:https   ESTABLISHED
  TCP    192.168.29.83:51498    ec2-54-164-197-109:https  ESTABLISHED
  TCP    192.168.29.83:51499    146.75.118.250:https   ESTABLISHED
  TCP    192.168.29.83:51502    146.75.118.248:https   ESTABLISHED
  TCP    192.168.29.83:51503    146.75.118.248:https   ESTABLISHED
  TCP    192.168.29.83:51505    151.101.38.250:https   ESTABLISHED
  TCP    192.168.29.83:51507    151.101.38.248:https   ESTABLISHED
  TCP    192.168.29.83:51510    151.101.38.248:https   ESTABLISHED
```

- **Pathping:** Combines the functionality of traceroute and ping, providing detailed information about the path packets take to a destination and any packet loss or latency along the way.



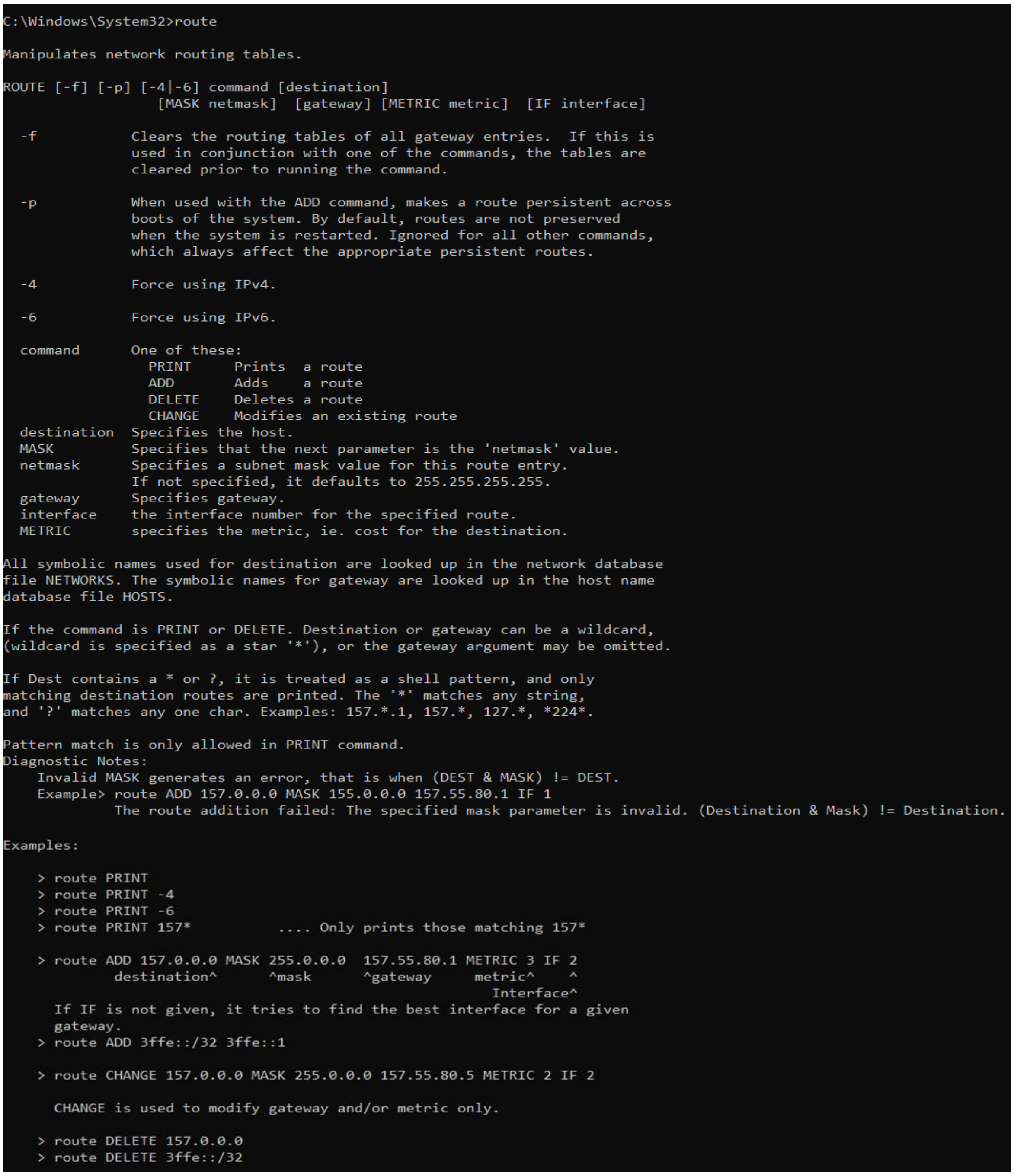
```
C:\Windows\System32>pathping

Usage: pathping [-g host-list] [-h maximum_hops] [-i address] [-n]
                [-p period] [-q num_queries] [-w timeout]
                [-4] [-6] target_name

Options:
    -g host-list     Loose source route along host-list.
    -h maximum_hops  Maximum number of hops to search for target.
    -i address       Use the specified source address.
    -n               Do not resolve addresses to hostnames.
    -p period        Wait period milliseconds between pings.
    -q num_queries   Number of queries per hop.
    -w timeout       Wait timeout milliseconds for each reply.
    -4               Force using IPv4.
    -6               Force using IPv6.
```

- **Ping:** Sends ICMP echo requests to a specified network host to test connectivity and measure round-trip time.



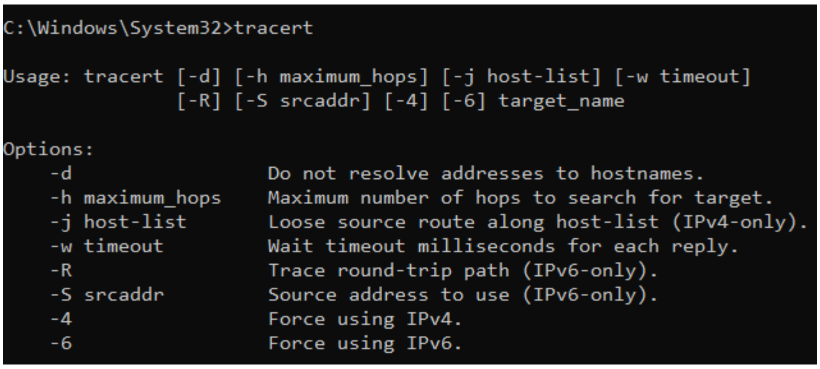
```
C:\Windows\System32>ping

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
            [-4] [-6] target_name

Options:
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break;
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        Send buffer size.
    -f             Set Don't Fragment flag in packet (IPv4-only).
    -i TTL         Time To Live.
    -v TOS         Type Of Service (IPv4-only. This setting has been deprecated
                   and has no effect on the type of service field in the IP
                   Header).
    -r count       Record route for count hops (IPv4-only).
    -s count       Timestamp for count hops (IPv4-only).
    -j host-list   Loose source route along host-list (IPv4-only).
    -k host-list   Strict source route along host-list (IPv4-only).
    -w timeout     Timeout in milliseconds to wait for each reply.
    -R             Use routing header to test reverse route also (IPv6-only).
                   Per RFC 5095 the use of this routing header has been
                   deprecated. Some systems may drop echo requests if
                   this header is used.
    -S srcaddr     Source address to use.
    -c compartment Routing compartment identifier.
    -p             Ping a Hyper-V Network Virtualization provider address.
    -4             Force using IPv4.
    -6             Force using IPv6.
```

- **Route:** Displays and modifies the IP routing table, which determines the path packets take to reach their destination.



```
C:\Windows\System32>route

Manipulates network routing tables.

ROUTE [-f] [-p] [-4|-6] command [destination]
                  [MASK netmask]  [gateway] [METRIC metric]  [IF interface]

  -f           Clears the routing tables of all gateway entries.  If this is
               used in conjunction with one of the commands, the tables are
               cleared prior to running the command.

  -p           When used with the ADD command, makes a route persistent across
               boots of the system. By default, routes are not preserved
               when the system is restarted. Ignored for all other commands,
               which always affect the appropriate persistent routes.

  -4           Force using IPv4.

  -6           Force using IPv6.

  command      One of these:
                 PRINT     Prints  a route
                 ADD       Adds    a route
                 DELETE    Deletes a route
                 CHANGE    Modifies an existing route
  destination  Specifies the host.
  MASK         Specifies that the next parameter is the 'netmask' value.
  netmask      Specifies a subnet mask value for this route entry.
               If not specified, it defaults to 255.255.255.255.
  gateway      Specifies gateway.
  interface    the interface number for the specified route.
  METRIC       specifies the metric, ie. cost for the destination.

All symbolic names used for destination are looked up in the network database
file NETWORKS. The symbolic names for gateway are looked up in the host name
database file HOSTS.

If the command is PRINT or DELETE. Destination or gateway can be a wildcard,
(wildcard is specified as a star '*'), or the gateway argument may be omitted.

If Dest contains a * or ?, it is treated as a shell pattern, and only
matching destination routes are printed. The '*' matches any string,
and '?' matches any one char. Examples: 157.*.1, 157.*, 127.*, *224*.

Pattern match is only allowed in PRINT command.
Diagnostic Notes:
    Invalid MASK generates an error, that is when (DEST & MASK) != DEST.
    Example> route ADD 157.0.0.0 MASK 155.0.0.0 157.55.80.1 IF 1
             The route addition failed: The specified mask parameter is invalid. (Destination & Mask) != Destination.

Examples:

    > route PRINT
    > route PRINT -4
    > route PRINT -6
    > route PRINT 157*          .... Only prints those matching 157*

    > route ADD 157.0.0.0 MASK 255.0.0.0  157.55.80.1 METRIC 3 IF 2
             destination^      ^mask      ^gateway     metric^    ^
                                                         Interface^
      If IF is not given, it tries to find the best interface for a given
      gateway.
    > route ADD 3ffe::/32 3ffe::1

    > route CHANGE 157.0.0.0 MASK 255.0.0.0 157.55.80.5 METRIC 2 IF 2

      CHANGE is used to modify gateway and/or metric only.

    > route DELETE 157.0.0.0
    > route DELETE 3ffe::/32
```

- **Tracert:** Traces the route packets take to a specified destination by sending ICMP echo requests with increasing TTL (Time to Live) values and displaying the IP addresses of the routers along the path.



```
C:\Windows\System32>tracert

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
               [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -d                 Do not resolve addresses to hostnames.
    -h maximum_hops    Maximum number of hops to search for target.
    -j host-list       Loose source route along host-list (IPv4-only).
    -w timeout         Wait timeout milliseconds for each reply.
    -R                 Trace round-trip path (IPv6-only).
    -S srcaddr         Source address to use (IPv6-only).
    -4                 Force using IPv4.
    -6                 Force using IPv6.
```

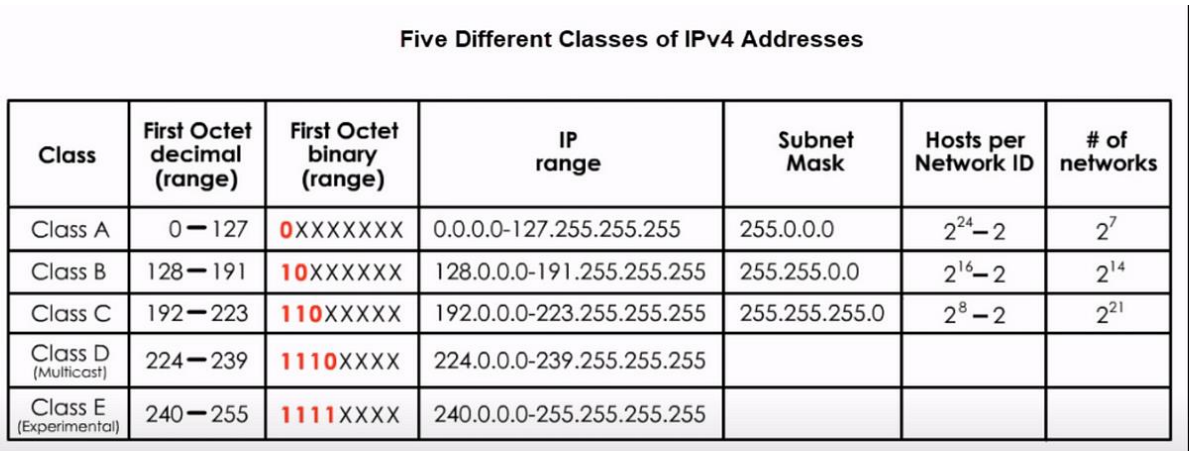
Experiment No 3

Aim:

- **Study of network IP**
- **Classification of IP address**
- **Sub netting**
- **Super netting**

Procedure:

- **Classification of IP Address**



Five Different Classes of IPv4 Addresses

Class	First Octet decimal (range)	First Octet binary (range)	IP range	Subnet Mask	Hosts per Network ID	# of networks
Class A	0 – 127	0XXXXXXX	0.0.0.0-127.255.255.255	255.0.0.0	$2^{24}-2$	2^{7}
Class B	128 – 191	10XXXXXX	128.0.0.0-191.255.255.255	255.255.0.0	$2^{16}-2$	2^{14}
Class C	192 – 223	110XXXXX	192.0.0.0-223.255.255.255	255.255.255.0	$2^{8}-2$	2^{21}
Class D (Multicast)	224 – 239	1110XXXX	224.0.0.0-239.255.255.255			
Class E (Experimental)	240 – 255	1111XXXX	240.0.0.0-255.255.255.255			

- **Subnetting**

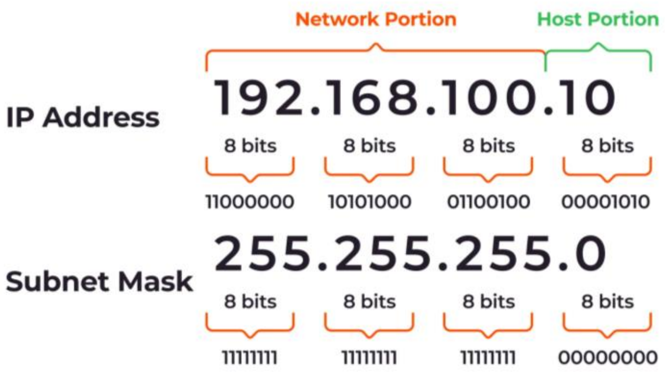
Why we Develop sub netting and How to calculate subnet mask and how to identify subnet address.

When a bigger network is divided into smaller networks, to maintain security, then that is known as Subnetting. So, maintenance is easier for smaller networks. For example, if we consider a class A address, the possible number of hosts is 224 for each network, it is obvious that it is difficult to maintain such a huge number of hosts, but it would be quite easier to maintain if we divide the network into small parts.

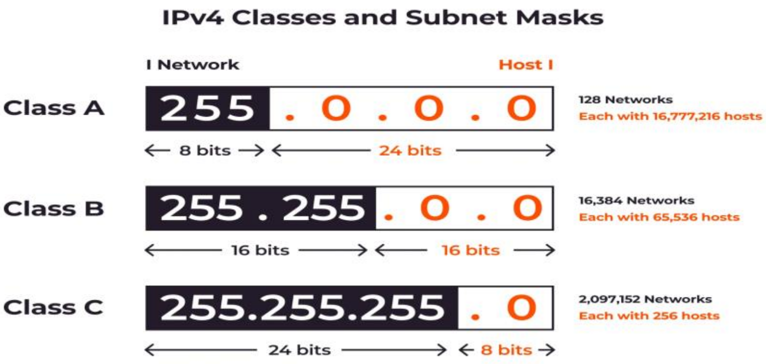
Uses of Subnetting

- Subnetting helps in organizing the network in an efficient way which helps in expanding the technology for large firms and companies.
- Subnetting is used for specific staffing structures to reduce traffic and maintain order and efficiency.
- Subnetting divides domains of the broadcast so that traffic is routed efficiently, which helps in improving network performance.

- Subnetting is used in increasing network security.



The network can be divided into two parts: To divide a network into two parts, you need to choose one bit for each Subnet from the host ID part.
In class C the first 3 octets are network bits so it remains as it is.
For Subnet-1: The first bit which is chosen from the host id part is zero and the range will be
from (193.1.2.00000000 till you get all 1's in the host ID part i.e, 193.1.2.01111111) except for the first bit which is chosen zero for subnet id part.
Thus, the range of subnet 1 is: 193.1.2.0 to 193.1.2.127
Subnet id of Subnet-1 is: 193.1.2.0
The direct Broadcast id of Subnet-1 is: 193.1.2.127
The total number of hosts possible is: 126 (Out of 128, 2 id's are used for Subnet id & Direct Broadcast id)
The subnet mask of Subnet- 1 is: 255.255.255.128
For Subnet-2: The first bit chosen from the host id part is one and the range will be from (193.1.2.100000000 till you get all I's in the host ID part i.e, 193.1.2.11111111).
Thus, the range of subnet-2 is: 193.1.2.128 to 193.1.2.255
Subnet id of Subnet-2 is: 193.1.2.128
The direct Broadcast id of Subnet-2 is: 193.1.2.255
The total number of hosts possible is: 126 (Out of 128, 2 id's are used for Subnet id & Direct Broadcast id)
The subnet mask of Subnet- 2 is: 255.255.255.128
The best way to find out the subnet mask of a subnet is to set the fixed bit of host-id to 1 and the rest to 0.
Finally, after using the subnetting the total number of usable hosts is reduced from 254 to 252.



- ## Supernetting

Why we develop super netting and How to calculate supernet mask and how to identify supernet address.

Supernetting is the opposite of Subnetting. In subnetting, a single big network is divided into multiple smaller subnetworks. In Supernetting, multiple networks are combined into a bigger network termed a Supernetwork or Supernet. In this article, we'll explore the purpose and advantages of supernetting, along with essential considerations for its implementation.

What is Supernetting?

Supernetting is the process of aggregating routes to multiple smaller networks. Thus saving storage space in the routing table, simplifying routing decisions, and reducing route advertisements to neighboring gateways. Supernetting has helped address the increasing size of routing tables as the Internet has expanded. Supernetting is mainly used in Route summarization, where routes to multiple networks with similar network prefixes are combined into a single routing entry with the routing entry pointing to a super network, encompassing all the networks.

Supernetting is mainly used in Route Summarization, where routes to multiple networks with similar network prefixes are combined into a single routing entry, with the routing entry pointing to a Super network, encompassing all the networks. This in turn significantly reduces the size of routing tables and also the size of routing updates exchanged by routing protocols.

More specifically, When multiple networks are combined to form a bigger network, it is termed super-netting Super netting is used in route aggregation to reduce the size of routing tables and routing table updates

Important Points for Supernetting

All the Networks should be contiguous.

The block size of every network should be equal and must be in form of 2n.

First Network id should be exactly divisible by whole size of supernet.

Example: Suppose 4 small networks of class C:

200.1.0.0,
200.1.1.0,
200.1.2.0,
200.1.3.0

Build a bigger network that has a single Network Id

First, let's check whether **three conditions** are satisfied or not:

Contiguous: You can easily see that all networks are contiguous all having size 256 IP Addresses(or 254 Hosts)..

Range of first Network from 200.1.0.0 to 200.1.0.255. If you add 1 in last IP address of first network that is 200.1.0.255+0.0.0.1, you will get the next network id which is 200.1.1.0.

Similarly, check that all network are contiguous.

Equal size of all networks: As all networks are of class C, so all of them have a size of 256 which is in turn equal to 28.

First IP address exactly divisible by total size: When a binary number is divided by 2n then last n bits are the remainder. Hence in order to prove that first IP address is exactly divisible by while size of Supernet Network. You can check that if last n (n here refers to the number of bits required to represent the Total Size of the Supernet) bits are 0 or not.In the given example first IP is 200.1.0.0 and whole size of supernet is 4*28=210. If last 10 bits of first IP address are zero then IP will be divisible.

110010000	00000001	000000**00**	**00000000**
200	1	0	0

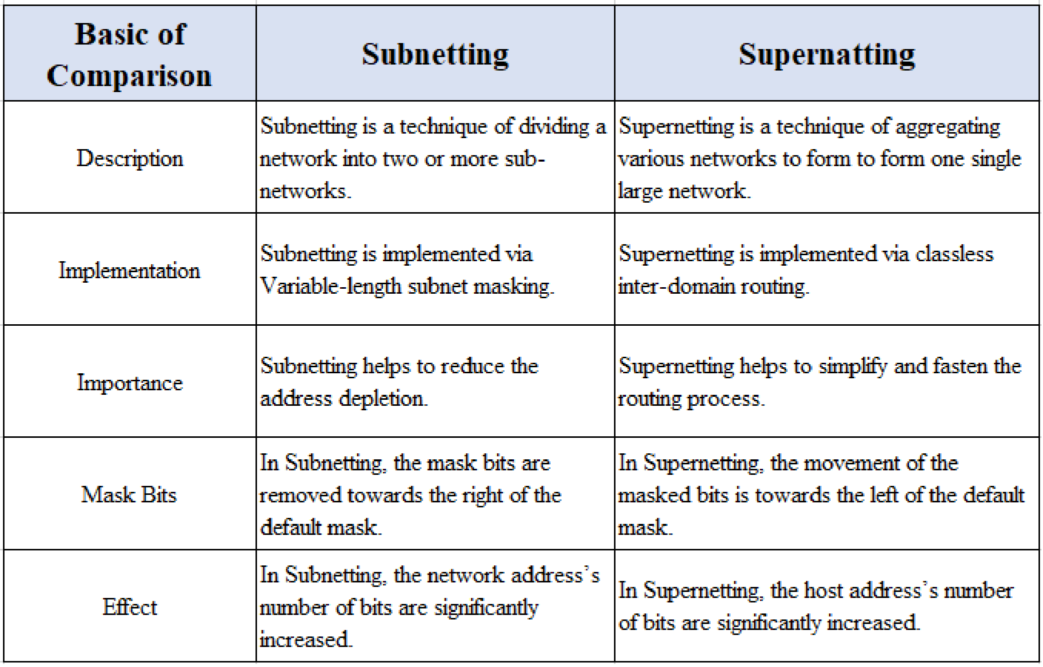
Last 10 bits of first IP address are zero (highlighted by green color). So 3rd condition is also satisfied.

Advantages of Supernetting:

- Control and reduce network traffic
- Helpful to solve the problem of lacking IP addresses
- Minimizes the routing table i.e, it cannot cover a different area of the network when combined and all the networks should be in the same class and all IP should be contiguous

Conclusion:

In conclusion, **supernetting** is a networking technique that consolidates multiple smaller networks into a larger one, simplifying routing and reducing the size of routing tables. It's a valuable tool in managing the growth of internet routing tables and optimizing network performance. However, it requires careful consideration of network characteristics and adherence to specific conditions for effective implementation.



Basic of Comparison	Subnetting	Supernatting
Description	Subnetting is a technique of dividing a network into two or more sub-networks.	Supernetting is a technique of aggregating various networks to form to form one single large network.
Implementation	Subnetting is implemented via Variable-length subnet masking.	Supernetting is implemented via classless inter-domain routing.
Importance	Subnetting helps to reduce the address depletion.	Supernetting helps to simplify and fasten the routing process.
Mask Bits	In Subnetting, the mask bits are removed towards the right of the default mask.	In Supernetting, the movement of the masked bits is towards the left of the default mask.
Effect	In Subnetting, the network address's number of bits are significantly increased.	In Supernetting, the host address's number of bits are significantly increased.

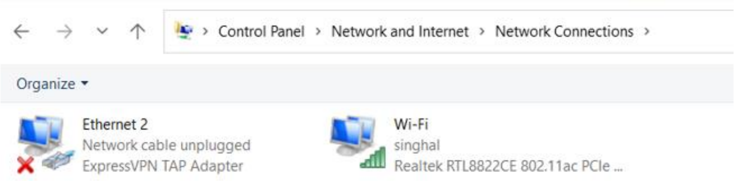
Experiment No 4

Aim: Connect the computers in Local Area Network

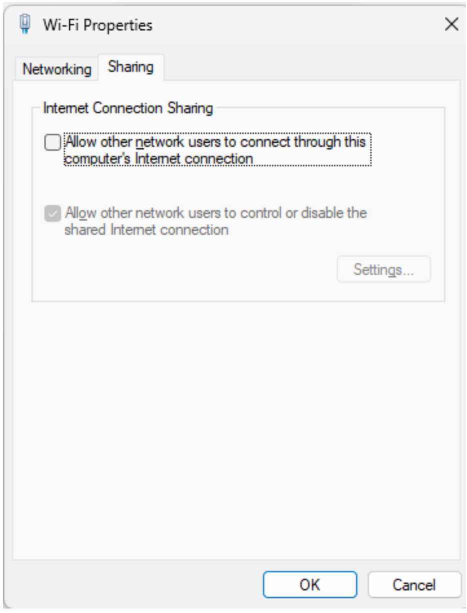
Procedure: On the host computer

On the host computer, follow these steps to share the Internet connection:

1. Log on to the host computer as Administrator or as Owner.
2. Click **Start**, and then click **Control Panel**.
3. Click **Network and Internet Connections**.
4. Click **Network Connections**.
5. Right-click the connection that you use to connect to the Internet. For example, if you connect to the Internet by using a modem, right-click the connection that you want under Dial-up / other network available.


Control Panel › Network and Internet › Network Connections ›
Organize ▾
Ethernet 2
Network cable unplugged
ExpressVPN TAP Adapter
Wi-Fi
singhal
Realtek RTL8822CE 802.11ac PCIe ...

6. Click **Properties**.
7. Click the **Sharing** tab.
8. Under **Internet Connection** Sharing, select the **Allow other network users to connect through this computer's Internet connection** check box.



□ Allow other network users to connect through this computer's Internet connection

☑ Allow other network users to control or disable the shared Internet connection

9. If you are sharing a dial-up Internet connection, select **Establish a dial-up connection whenever a computer on my network attempts to access the Internet** check box if you want to permit your computer to automatically connect to the Internet.

10. Click **OK**. You receive the following message:
When Internet Connection Sharing is enabled, your LAN adapter will be set to use IP address 192.168.0. 1. Your computer may lose connectivity with other

computers on your network. If these other computers have static IP addresses, it is a good idea to set them to obtain their IP addresses automatically. Are you sure you want to enable Internet Connection Sharing?

11. Click Yes.

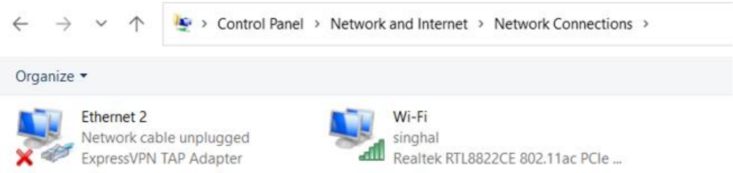
The connection to the Internet is shared to other computers on the local area network (LAN).

The network adapter that is connected to the LAN is configured with a static IP address of 192.168.0. 1 and a subnet mask of 255.255.255.0

On the client computer

To connect to the Internet by using the shared connection, you must confirm the LAN adapter IP configuration, and then configure the client computer. To confirm the LAN adapter IP configuration, follow these steps:

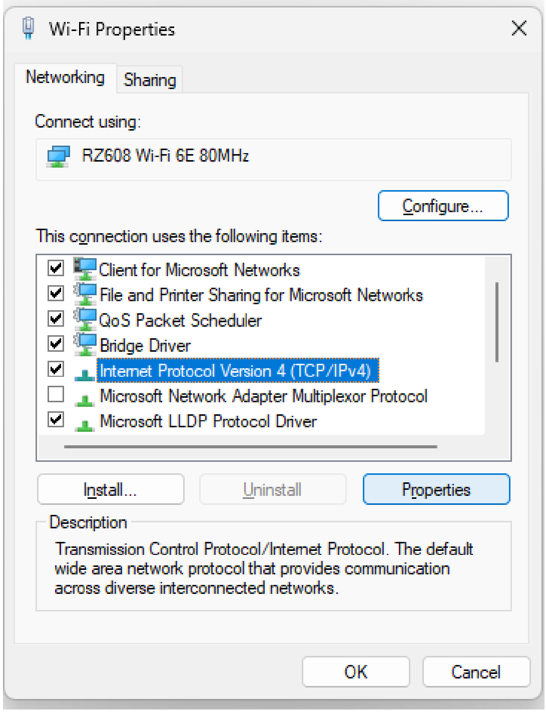
1. Log on to the client computer as Administrator or as Owner.
2. Click **Start**, and then click **Control Panel.**
3. Click **Network** and **Internet Connections**.
4. Click **Network Connections**.


Control Panel › Network and Internet › Network Connections ›
Organize ▾

Ethernet 2
Network cable unplugged
ExpressVPN TAP Adapter

Wi-Fi
singhal
Realtek RTL8822CE 802.11ac PCIe ...

5. Right-click **Local Area Connection** and then click **Properties**.



Connect using:

RZ608 Wi-Fi 6E 80MHz

This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Bridge Driver
☑ Internet Protocol Version 4 (TCP/IPv4)
□ Microsoft Network Adapter Multiplexor Protocol
☑ Microsoft LLDP Protocol Driver

Description

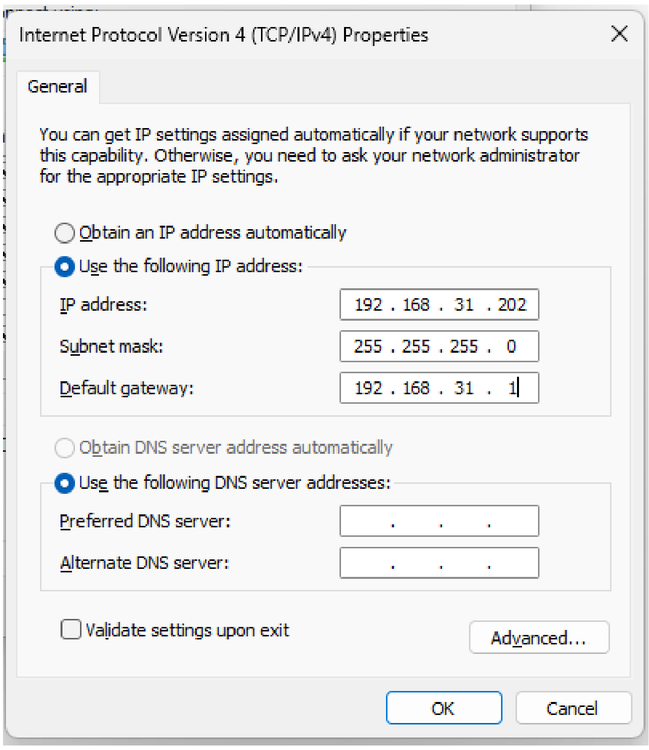
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

6. Click the **General** tab, click **Internet Protocol (TCP/IP)** in the **connection uses the following items list**, and then click **Properties**.

7. In the **Internet Protocol (TCP/IP)** Properties dialog box, click **Obtain an IP address automatically** (if it is not already selected), and then click **OK**.

   Note: You can also assign a unique static IP address in the range of 192.168.0.2 to 254. For example, you can assign the following static IP address, subnet mask, and default gateway:

8. IP Address 192.168.31.202
9. Subnet mask 255.255.255.0
10. Default gateway 192.168.31.1
11. In the **Local Area Connection Properties** dialog box, click **OK**.
12. Quit Control Panel.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address:	192 . 168 . 31 . 202
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	192 . 168 . 31 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server:	. . .
Alternate DNS server:	. . .

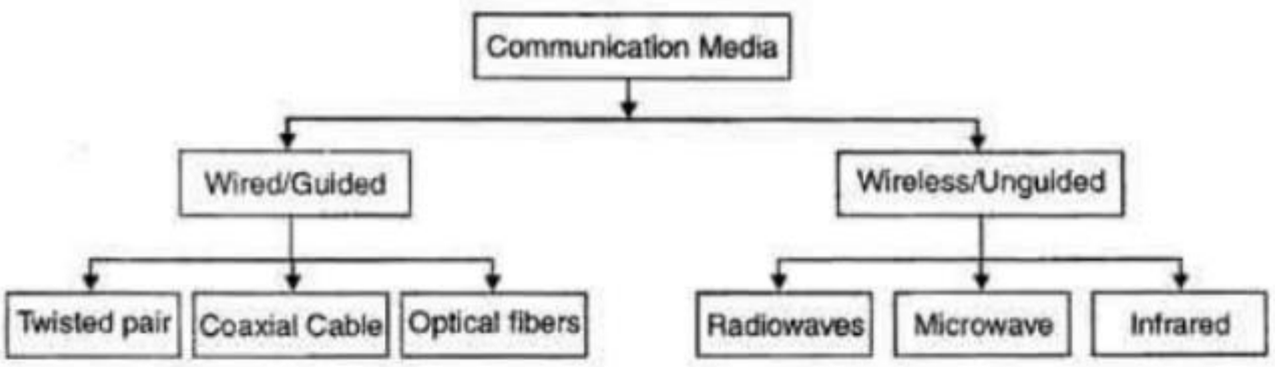
□ Validate settings upon exit

Experiment No 5

Aim : Familiarization with Transmission media and Tools Coaxial cable, UTP Cable, Crimping Tools, Connectors etc.

Transmission Media

A communication channel that is used to carry the data from one transmitter to the receiver through the clectromagnctic signals .The main function of this is to carry the data in the bits form through the Local Area Network(LAN). In data communication, it works like a physical path between the sender & receiver .For instance in a copper cable network the bits in the form of electrical signals whereas in a fiber network ,the bits are available in the form of light pulses. The quality as well as characteristics of data transmission ,can be determined from the characteristics of medium &signal. The properties of diferent transmission media are delay, bandwidth, maintenance, cost and casy installation.

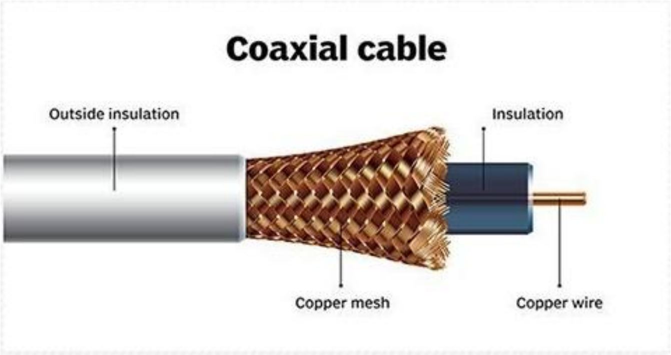


Bounded/Guided Transmission Media:

This kind of transmission media is also known as wired otherwise bounded media. In this type ,the signals can be transmitted directly & restricted in a thin path through physical links. The types of Bounded /Guided transmission are discussed below:

- **Coaxial Cable:**

  Coaxial cable (or coax) carries signals of higher frequency ranges than those in twisted pair cable. It has a central core conductor of solid or stranded wire (usually copper) enclosed in an insulating sheath, which is, in turn, encased in an outer conductor of metal foil, braid, or a combination of the two. The outer conductor is also enclosed in an insulating sheath, and the whole cable is protected by a plastic cover.



Applications:

Coaxial cable was widely used for both analog and digital data transmission.

It has higher bandwidth.

Inexpensive when compared to fiber optical cables.

It uses for longer distances at higher data rates.

Excellent noise immunity.

Used in LAN and Television distribution.

Disadvantage:

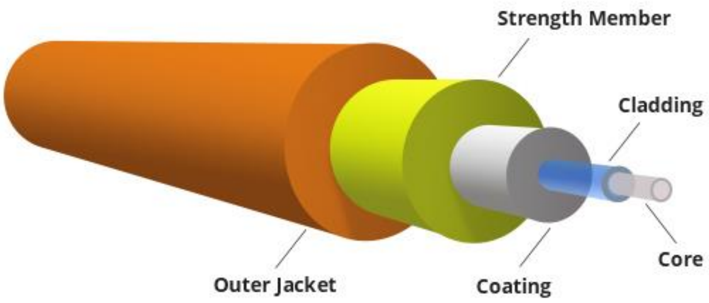
Single cable failure can fail the entire network.

Difficult to install and expensive when compared with twisted pairs.

If the shield is imperfect,it can lead to grounded loop.

- **Fiber Optic Cable:**

A fiber optic cable is a network cable that contains strands of glass fibers inside an insulated casing. They're designed for long-distance, high-performance data networking, and telecommunications. Compared to wired cables, fiber optic cables provide higher bandwidth and transmit data over longer distances. Fiber optic cables support much of the world's internet, cable television, and telephone systems.



Advantages:

1. The loss of signal in optical fiber is less than that in copper wire.
2. Opticalfibers usually have a longer life cycle for over 100 years.

Disadvantage:

1. It is expensive.
2. Difficult to install.

- ## Twisted Pair Cable:

  A twisted pair cable is a type of cable made by putting two separate insulated wires together in a twisted pattern and running them parallel to each other. This type of cable is widely used in different kinds of data and voice infrastructures.

  Twisted pair is of two types:

  1. Shielded Twisted Pair(STP)
  2. Unshielded Twisted Pair(UTP)

Shielded Twisted Pair:

Shielded Twisted Pair (STP) cables additionally have an overall conducting metallic shields covering four twisted pair wires. There may be another conducting metallic shields covering individual twisted pairs also. These metallic shields blocks out electromagnetic interference to prevent unwanted noise from the communication circuit.

Advantage of Shielded Twisted Pair:

1. The cost of the shielded twisted pair cable is not very high and not very low.
2. An installation of STP is easy.
3. It has higher capacity as compared to unshielded twisted pair cable.
4. It has a higher attenuation.
5. It is shielded that provides the higher data transmission rate.

Disadvantages:

1. It is more expensive as compared to UTP and coaxial cable.
2. It has a higher attenuation rate.

Unshielded Twisted Pair:

An unshielded twisted pair is widely used in telecommunication. It is most common type when compared with shielded twisted pair cable which consists of two conductors usually copper, each with its own colour plastic insulator.

Categories:

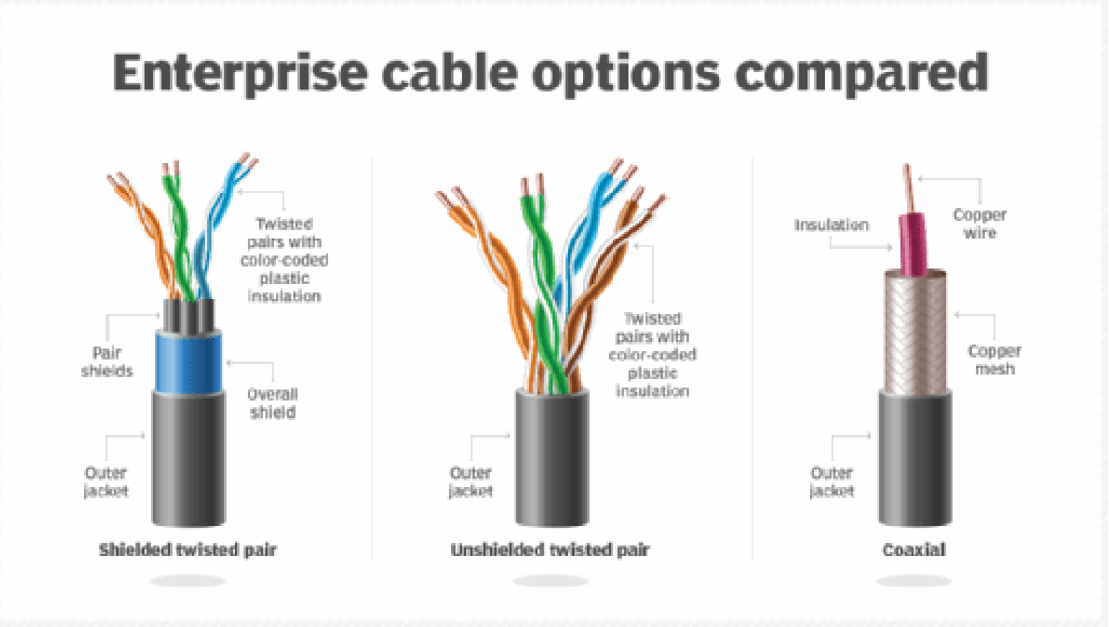
Category 1: Category 1 is used for telephone lines that have low-speed data.
Category 2: It can support up to 4Mbps.
Category 3: It can support up to 16Mbps.
Category 4: It can support up to 20Mbps. Therefore, it can be used for long-distance communication.
Category 5: It can support up to 200Mbps.
Category 6: It can support up to 1000Mbps.

Advantages Of Unshielded Twisted Pair:

1. It is cheap.
2. Installation of the unshielded twisted pair is easy.
3. It can be used for high-speed LAN.

Disadvantage:

1. This cable can only be used for shorter distances because of attenuation.



Unbounded/Unguided Transmission Media:

Unguided medium transport electromagnetic waves without using a physical conductor. This type of communication is often referred to as wireless communication. Signals are normally broadcast through free space and thus are available to anyone who has a device capable of receiving them.

Types of unguided Transmission media:

- **Radio Transmission:**

  Its frequency is between 10Khz to 1Ghz. It is simple to install and has high attenuation. These waves are used for multicast communication.

  Types of propagation:

  1. Troposphere
  2. Ionosphere

- **Microwaves:**

  It is a line of sight transmission i.e. the sending and receiving antennas need to be properly aligned with each other. The distance covered by the signal is directly proportional to the height of the antenna. Frequency Range: 1GHz - 300GHz. These are majorly used for mobile phone communication and television distribution.

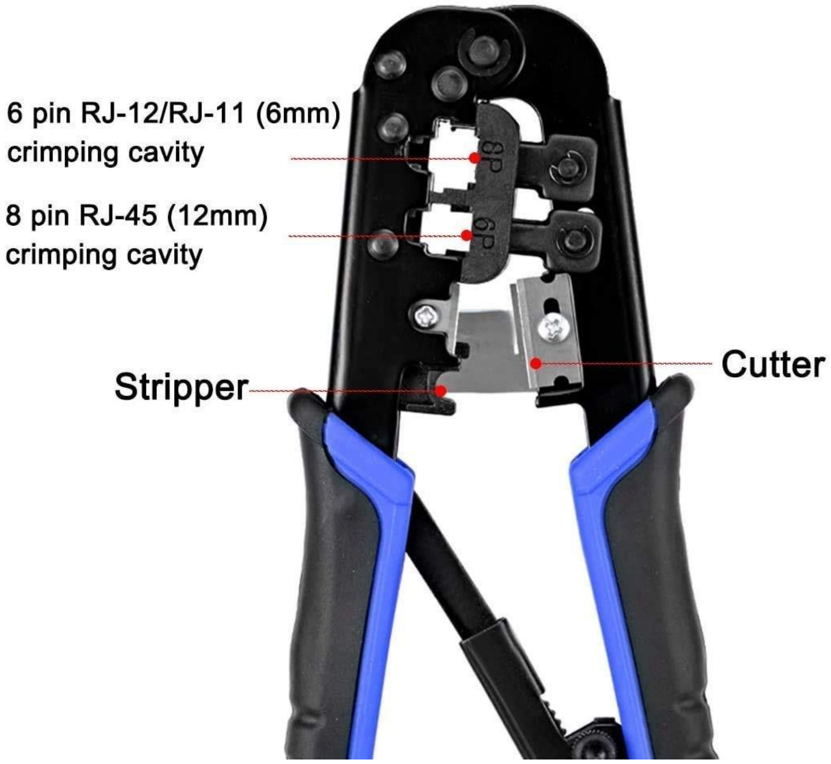
- **Infrared:**

  Infrared waves are used for very short distance communication. They cannot penetrate through obstacles. This prevents interference between systems. Frequency Range:300GHz - 400THz. It is used in TV remotes, wireless mouse, keyboard, printer, etc.

- **Crimping tool:**

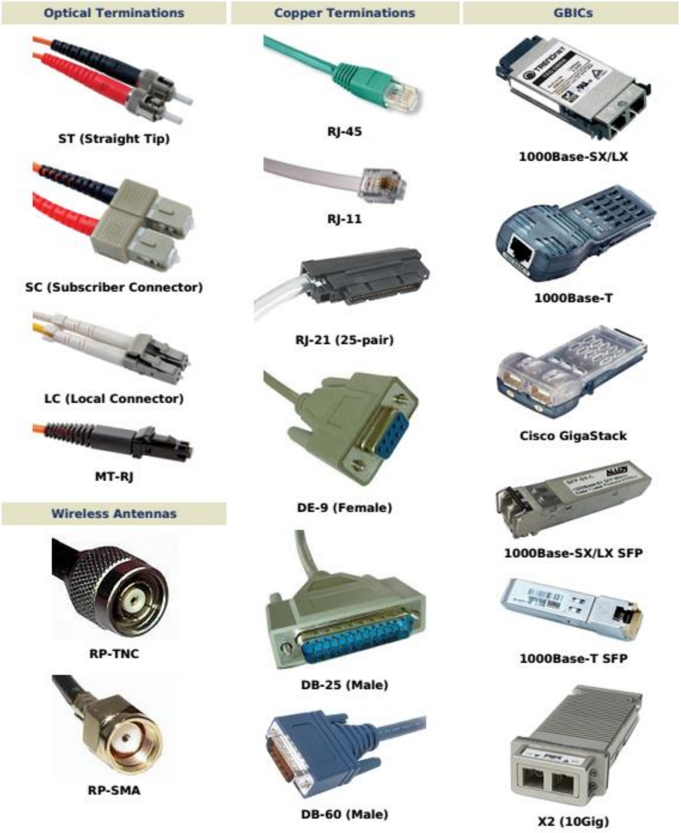
  A crimping tool is a device used to conjoin two pieces of metal by deforming one or both of them to hold each other. The result of the tool's work is called a crimp. An example of crimping is affixing a connector to the end of a cable. For instance, network cables and phone cables are created using a crimping tool (shown below) to join RJ-45 and RJ-11 connectors to both ends of phone or Cat 5 cable.

RJ-11 (6-Pin) and RJ-45 (8-Pin) Crimping Tool



- **Connector:**

  A device that terminates a segment of cabling or provides a point of entry for networking devices such as computers, hubs, and routers. Connectors can be distinguished according to their physical appearance and mating properties, such as jacks and plugs (male connectors) or sockets and ports (female connectors).



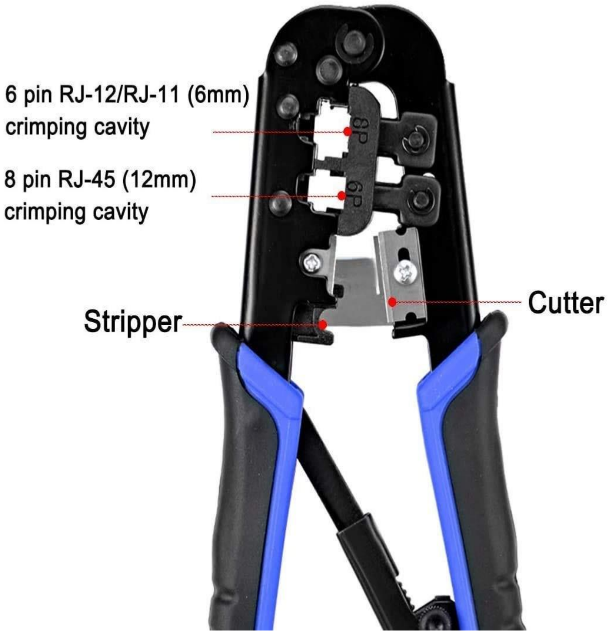
Experiment No 6

Aim : Preparing the UTP cable for cross and direct connection using Crimping Tools.

Procedure:

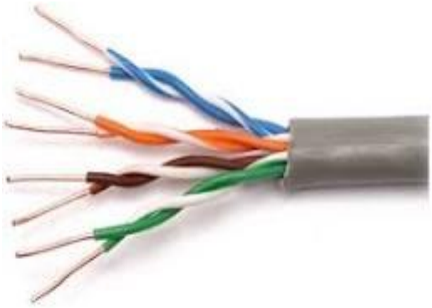
- **Crimping Tools:**

  A crimping tool is a device used to conjoin two pieccs of metal by deforming one or both of them to hold each other. The result of the tool's work is called a crimp. An example of crimping is affixing a connector to the end of a cable. For instance, network cables and phone cables are created using a crimping tool to join RJ-45 and RJ-11 connectors to both ends of phone or Cat 5 cable.



- **UTP Cable:**

  UTP stands for Unshielded Twisted Pair cable. UTP cable is a 100 ohm copper cable that consists of 2 to 1800 unshielded twisted pairs surrounded by an outer jacket. They have no metallic shield. This makes the cable small in diameter but unprotected against electrical interference. The twist helps to improve its immunity to electrical noise and EMI.



- **RJ-45 Connector:**

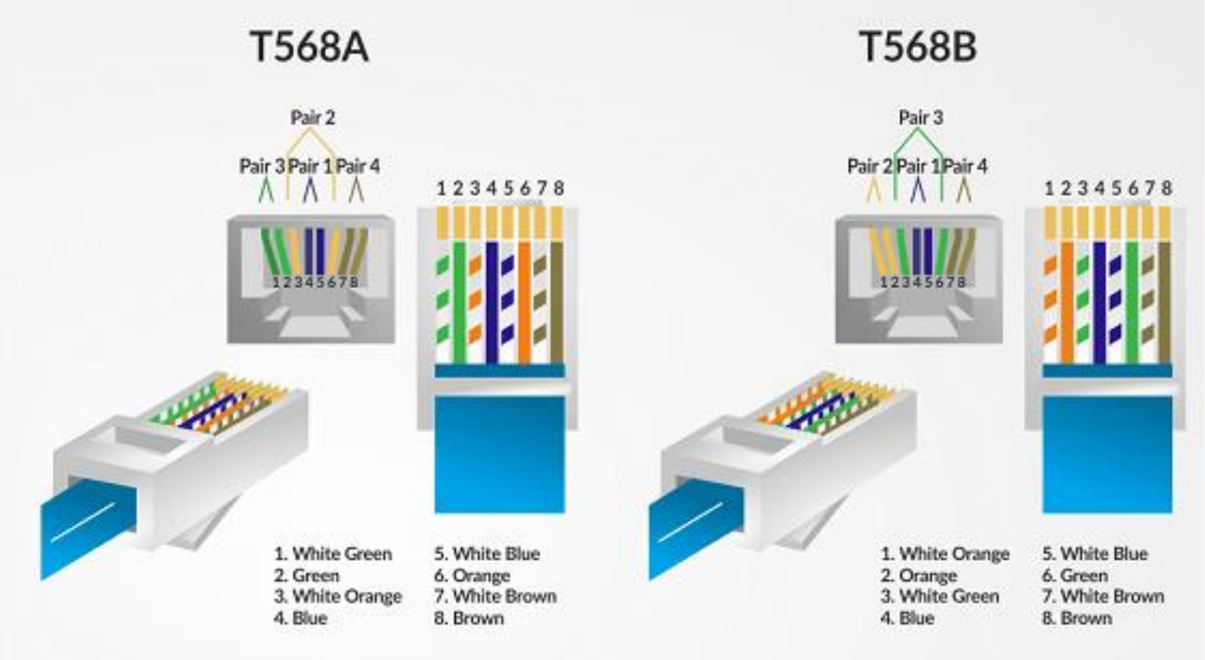
RJ-45 connector is a tool that we put on the end of the UTP cable. With this we can plug the cable in the LAN port.

- **Cable test:**

  A cable tester is a electronic device used to verify the electrical connections in a signal cable or other wired assembly. Basic cable testers are continuity tester that verify the existence of a conductive path between ends of the cable, and verify the corect wiring of connectors on the cable.

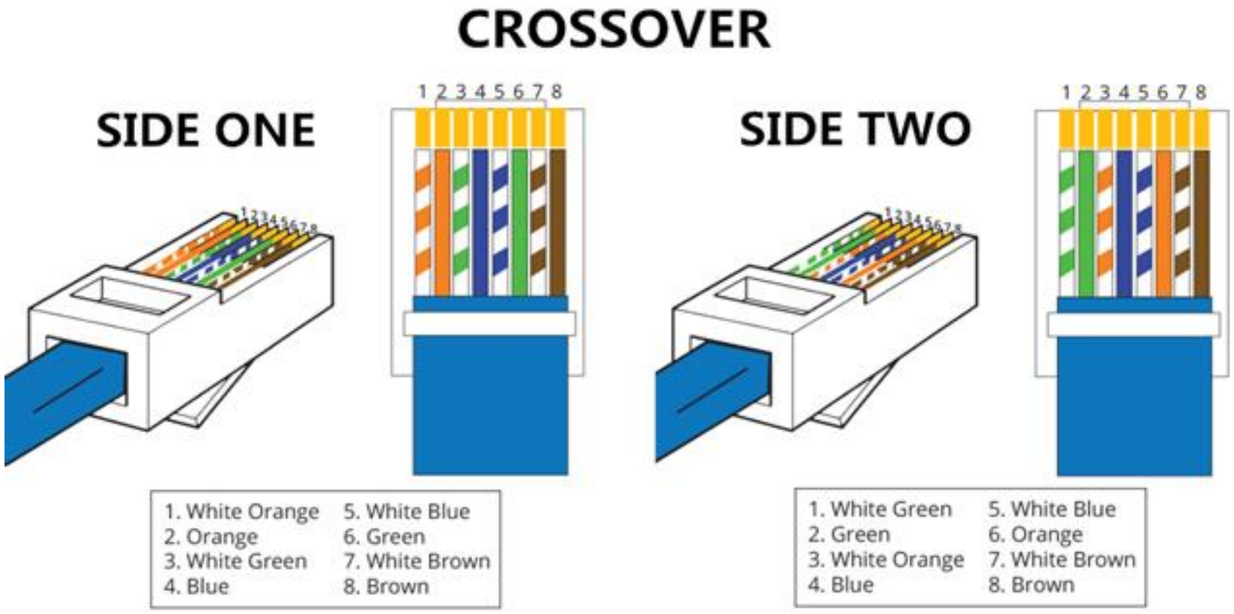
- **Straight cable:**

  A straight-through cable is a type of twisted pair cable that is used in local area networks to connect a computer to a network hub such as a router. This type of cable is also sometimes called a patch cable and is an alternative to wireless connections where one or more computers access a router through a wireless signal. On a straight-through cable, the wired pins match. Straight- through cable use one wiring standard: **both ends use T568A wiring standard or both ends use T568B wiring standard**.

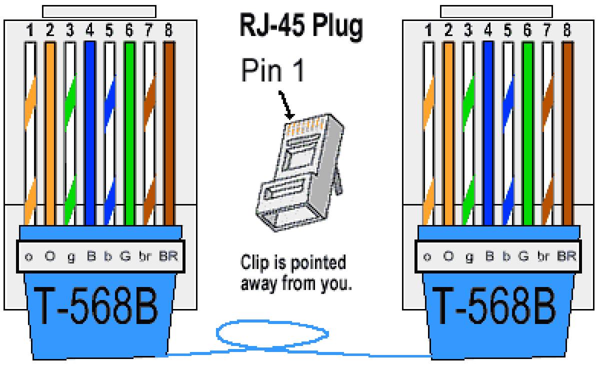


- **Cross cable:**

  An Ethernet crossover cable is a type of Ethernet cable used to connect computing devices together directly. Unlike straight-through cable, crossover cables use two different wiring standards: **one end uses the T568A** wiring standard, and **the other end uses the T568B** wiring standard. The internal wiring of Ethernet crossover cables reverses the transmit and receive signals. It is most often used to connect two devices of the same type: eg. two computers (via network interface controller) or two switches to each other.



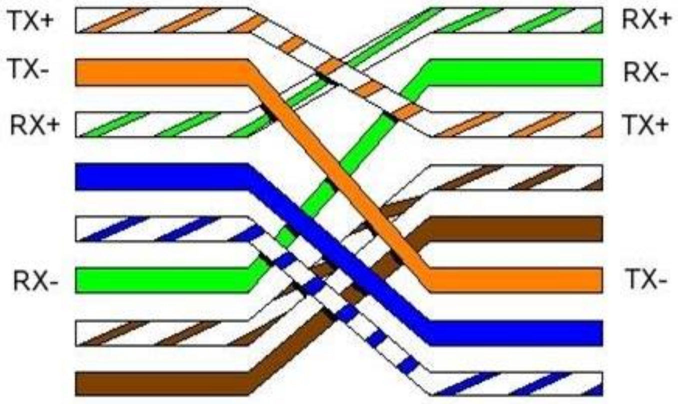
- **Making Straight UTP Cable:**
  1. Peel the end of the UTP cable, approximately 2 cm.
  2. Open the cable strands, align and follow the arrangement as standard cable image shown below.
  3. Once the order is according to the standard, cut and flatten the ends of the cable.
  4. Put the cable is straight and aligned into the RJ45 connector, and make sure all cables are in correct position as follows:
     a. Orange White
     b. Orange
     c. Green White
     d. Blue
     e. Blue White
     f. Green
     g. White Brown
     h. Brown



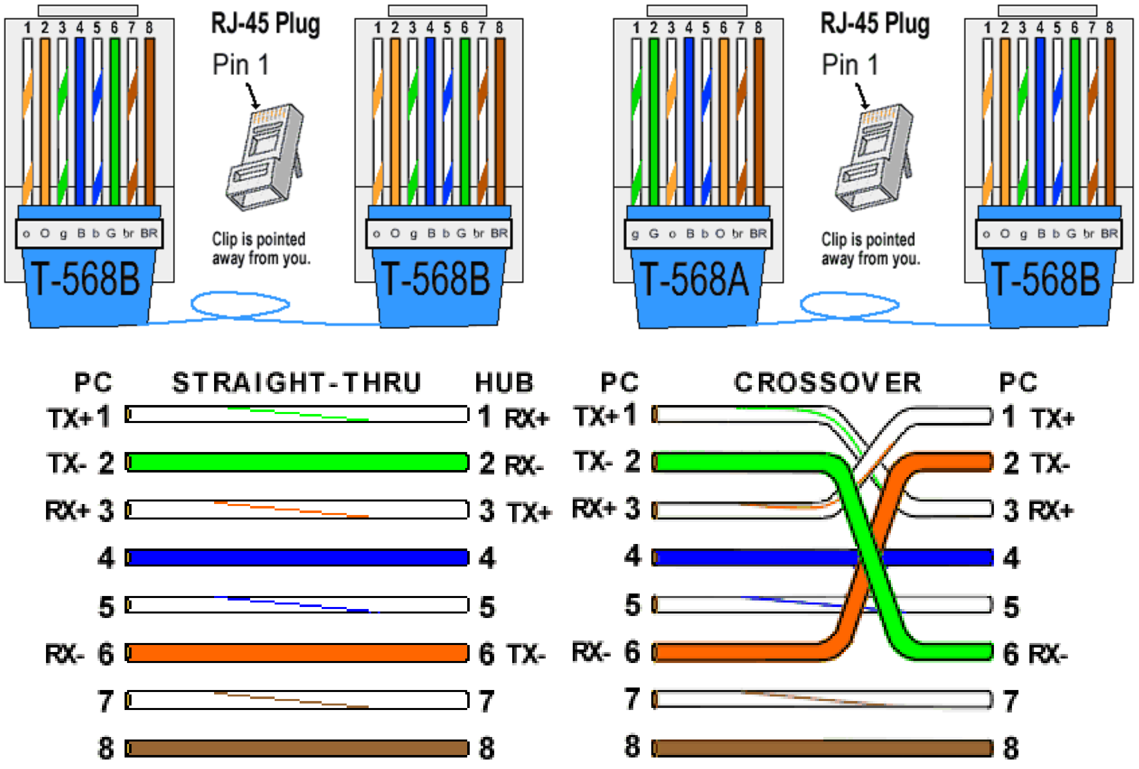
     i. Make crimping using crimp tools, press crimping tool and make sure all the pins (brass on the RJ-45 connector has " bite " of each cable. usually when done will sound "click". Once finished at the end of this one, do it again at the other end cable.
  5. The final step is to check the cable that you created earlier using the LAN tester, enter each end of the cable (RJ-45) to each LAN port available on the tester, turn and make sure all of the LEDs light up according to the order of the wires we created.
- **Making Cross UTP Cable:**
  1. Creating a cross cable has almost the same steps with straight cable, the difference lies only in the colour sequence from both ends of the cable. Unlike

the straight cable that has the same colour sequence at both ends of the cable, the cross cable has a different colour sequences at both ends of the cable.

2. The first ends is same with straight cable:
    a. Orange White
    b. Orange
    c. Green White
    d. Blue
    e. Blue White
    f. Green.
    g. White Brown
    h. Brown
    i.

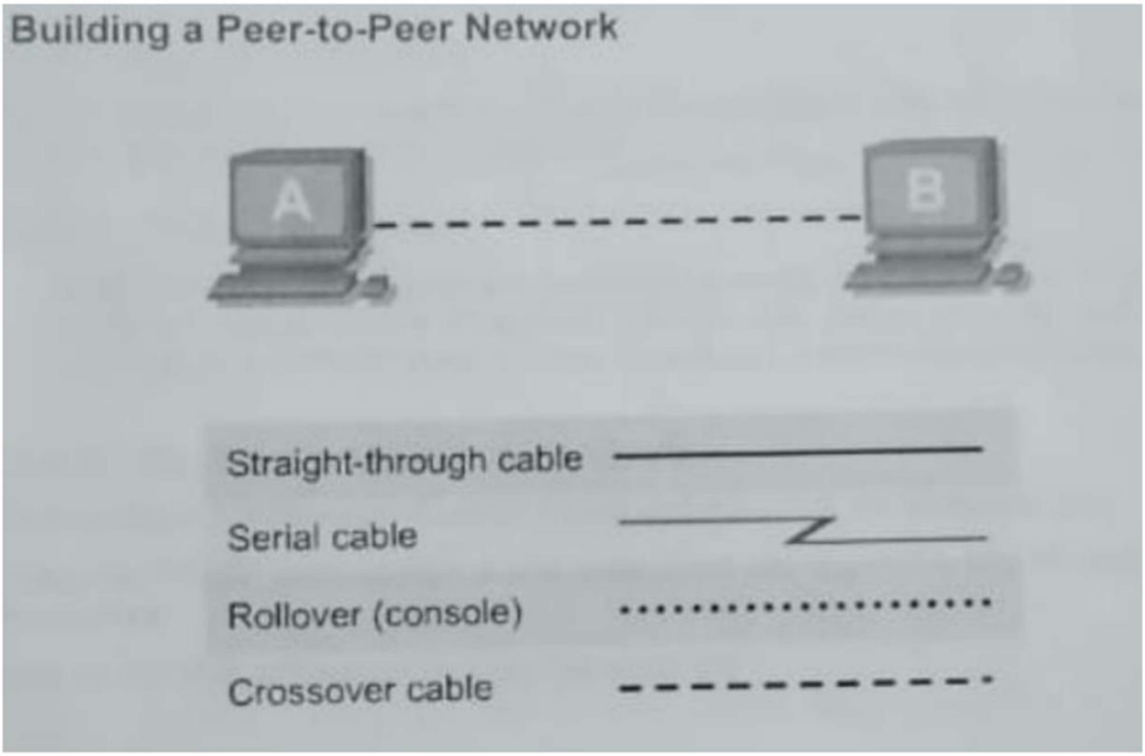


3. For the second end of the cable, the colour composition is different from the first. The colour arrangement is as follows:
    a. Green White
    b. Green
    c. Orange White
    d. Blue
    e. Blue White
    f. Orange
    g. White Brown
    h. Brown



Program 7

Aim: Create a LAN using Hubs, Switches and crossover cable



Objective:

- Create a simple peer-to-peer network between two PCs
- Identify the proper cable to connect the two PCs
- Configure workstation IP address information
- Test connectivity using the ping command

Background/Preparation:

This lab focuses on the ability to connect two PCs to create a simple peer-to-peer Ethernet LAN between two workstations. The workstations will be directly connected to each other without using a hub or switch in addition to the Layer 1 physical and Layer 2 data link connections, the computers must also be configured with the correct IP network settings, which is Layer 3, so that they can communicate. A basic Category 5/5e UTP crossover cable is all that is needed. A crossover cable is the same type that would be used as backbone or vertical cabling to connect switches together Connecting the

PCs in this manner can be very useful for transferring files at high speed and for troubleshooting interconnecting devices between PCs. If the two PCs can relate to a single cable and are able to communicate, then any networking problems are not with the PCs themselves Start this lab with the equipment turned off and with cabling disconnected Work in teams of two with one person per PC. The following resources will be required.

- Two workstations with an Ethernet 10/100 NIC installed
- Several Ethernet cables, which are both straight-through and crossover, to choose from for connecting the two workstations

Step 1:- Identify the proper Ethernet cable and connect the two PCS

- The connection between the two PCs will be accomplished using a Category 5 or 5e crossover cable Locate a cable that is long enough to reach from one PC to the other and attach one end to the NIC in each of the PCs. Be sure to examine the cable ends carefully and select only a crossover cable

Step 2:- Verify the physical connection

- Plug in and turn on the computers. To verify the computer connections, ensure that the link lights on both NICs are lit. Are both link lights lit?

Step 3:- Access the IP settings window

Note: Be sure to write down the existing IP settings, so that they can be restored at the end of the lab. These include IP address, subnet mask, default gateway, and DNS servers If the workstation is a DHCP client, it is not necessary to record this information.

Windows 95/98/Me/ users should do the following

- Click on Start Settings Control Panel and then click the Network icon
- Select the TCP/IP protocol icon that is associated with the NIC in this PC and click on Properties
- Click on the IP Address tab and the Gateway tab

Windows NT/2000 users should do the following

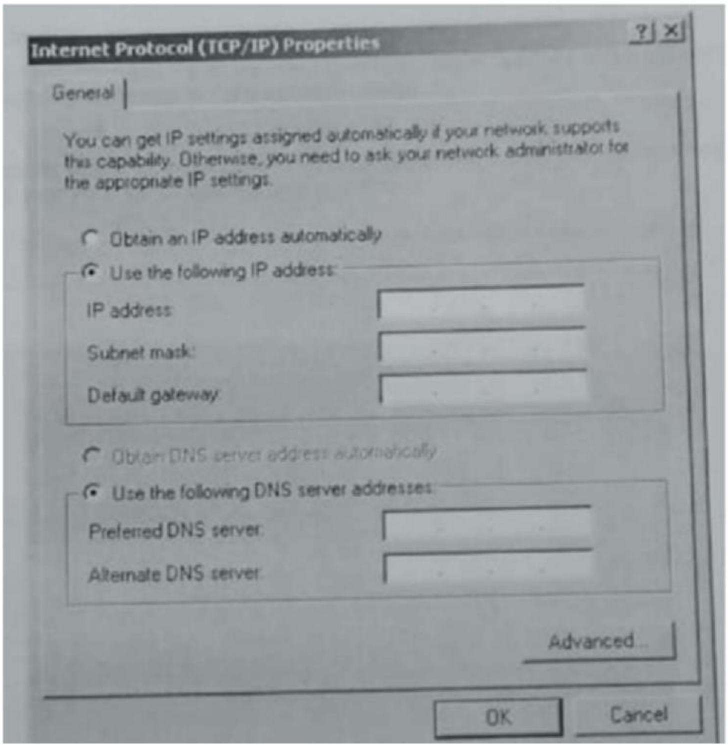
- Click on Start Settings > Control Panel and then open the Network and Dial-up Connections folder.

- Click ad open the Local Area Connection icon
- Select the TCP/IP protocol icon that is associated with the NIC in this PC
- Click on Properties and click on Use the following IP address

Windows XP users should do the following

- Click on Start Settings > Control Panel and then click the Network Connection icon.
- Select the Local Area Network Connection and click on Change settings of this connection
- Select the TCP/IP protocol icon that is associated with the NIC in this PC.
- Click on Properties and click on Use the following IP address

See the example below:



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address:

Subnet mask:

Default gateway:

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

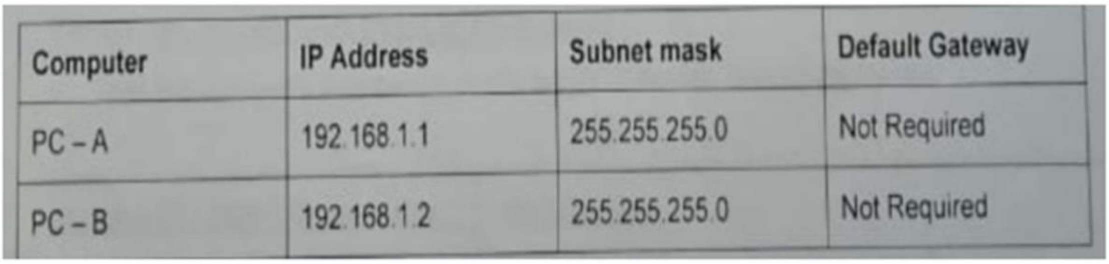
Preferred DNS server:

Alternate DNS server:

Step 4:- Configure TCP/IP settings for the two PCS

- Set the IP address information for each PC according to the information in the table:

- Note that the default gateway IP address is not required, since these computers are directly connected. The default gateway is only required on local area networks that are connected to a router



Computer	IP Address	Subnet mask	Default Gateway
PC – A	192.168.1.1	255.255.255.0	Not Required
PC – B	192.168.1.2	255.255.255.0	Not Required

Step 5:- Access the Command or MS-DOS prompt

- Use the Start menu to open the Command Prompt (MS-DOS- like) window :
  Windows 95/98/Me users should do the following
  Start > Programs > MS-DOS Prompt
  Windows NT/2000 users should do the following

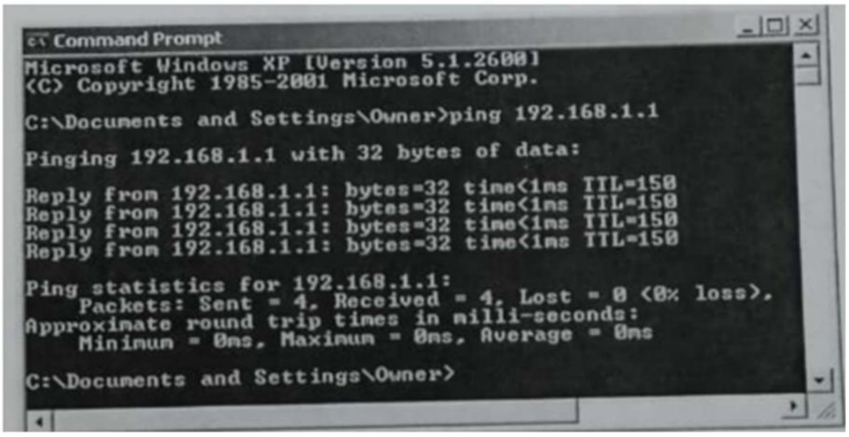
  Start > Programs > Accessories > Command Prompt

  Windows XP users should do the following

  Start > Programs > Accessories Command Prompt

Step 6:- Verify that the PCs can communicate

- Test connectivity from one PC to the other by pinging the IP address of the opposite computer
- Use the following command at the command prompt C :> ping 192.168.1.1 (or 192.168.1.2)
  - Look for results like those shown below. If not, check the PC connections and TCP/IP settings for both PCs. What was the ping result?



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Owner>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=150
Reply from 192.168.1.1: bytes=32 time<1ms TTL=150
Reply from 192.168.1.1: bytes=32 time<1ms TTL=150
Reply from 192.168.1.1: bytes=32 time<1ms TTL=150

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Owner>
```

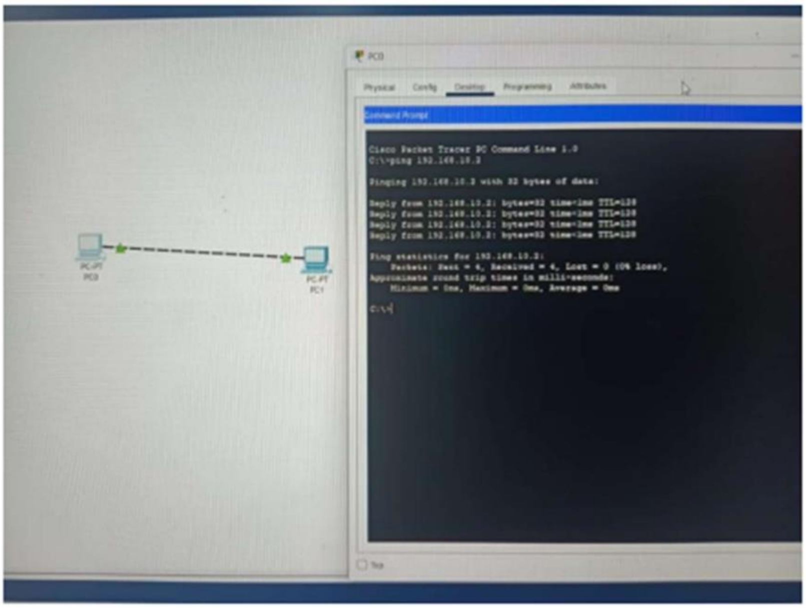
Step 7:- Confirm the TCP/IP network settings

Windows 95/98/Me users should do the following

- Type the winipcfg command from the MS-DOS Prompt. Record the results

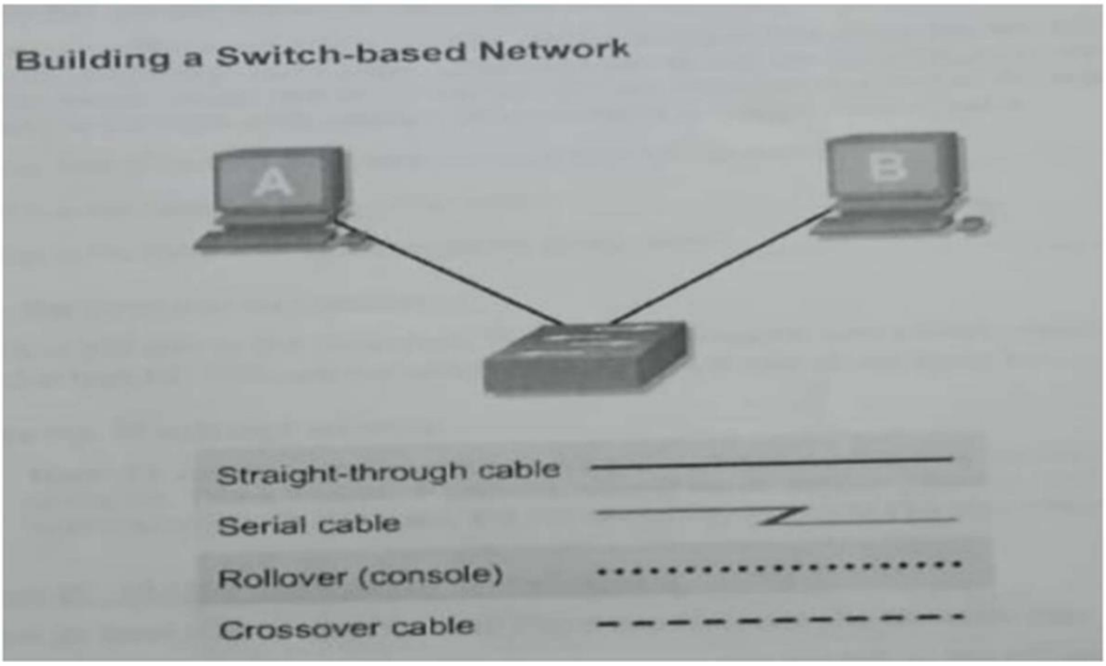
Windows NT/2000/XP users should do the following

- Type the ipconfig command from the Command Prompt. Record the results

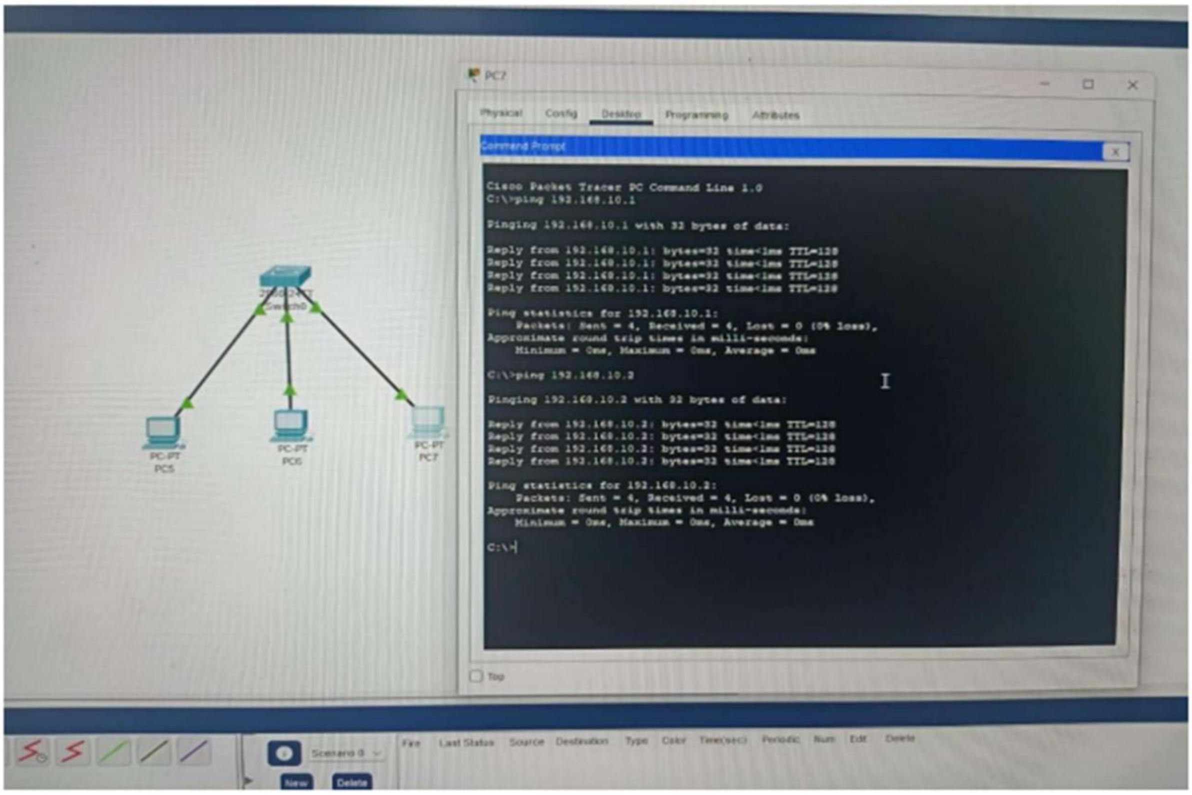


```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Reply from 192.168.10.2: bytes=32 time<1ms TTL=128
Reply from 192.168.10.2: bytes=32 time<1ms TTL=128
Reply from 192.168.10.2: bytes=32 time<1ms TTL=128
Reply from 192.168.10.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Step 8:- Restore the PCs to their original IP settings, disconnect the equipment, and store the cables

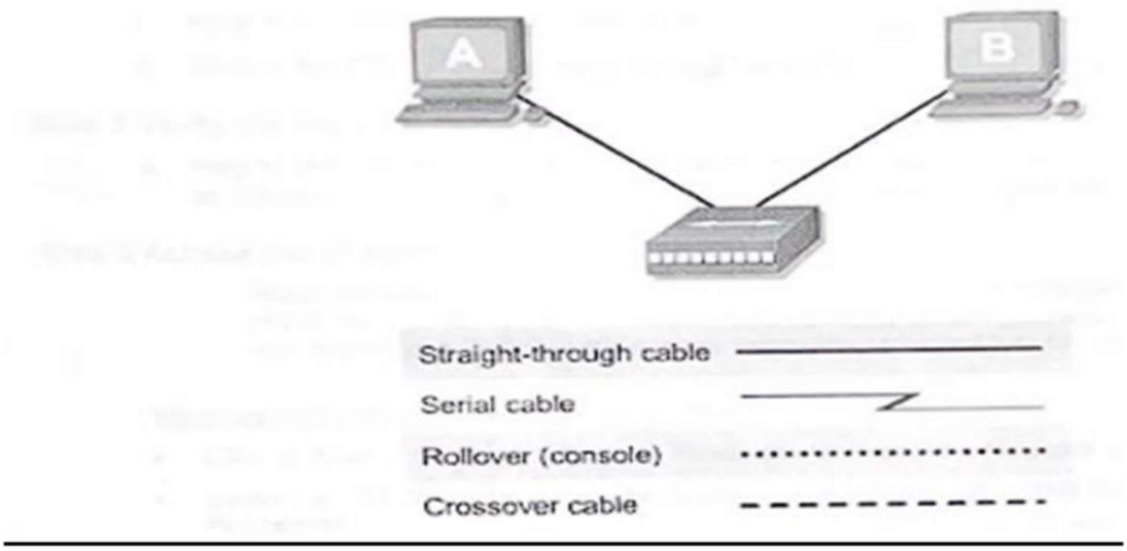


All steps same as Peer-to-Peer Network

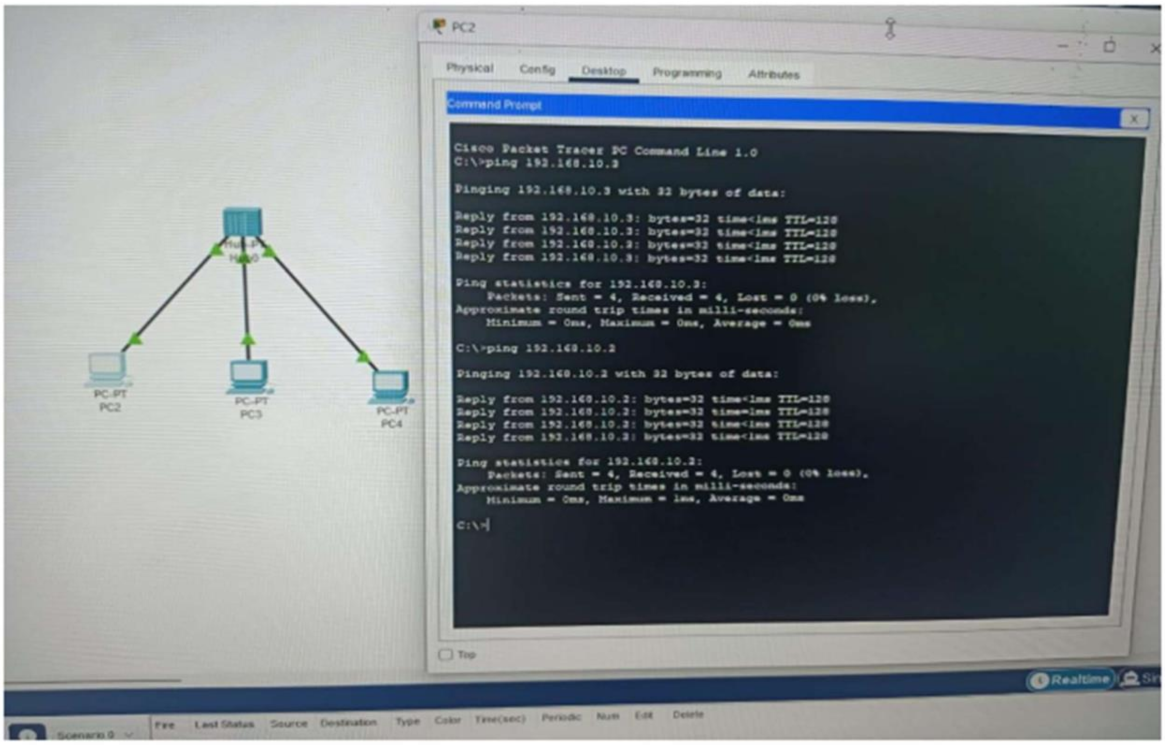


```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.10.1: bytes=32 time<1ms TTL=128
Reply from 192.168.10.1: bytes=32 time<1ms TTL=128
Reply from 192.168.10.1: bytes=32 time<1ms TTL=128
Reply from 192.168.10.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Reply from 192.168.10.2: bytes=32 time<1ms TTL=128
Reply from 192.168.10.2: bytes=32 time<1ms TTL=128
Reply from 192.168.10.2: bytes=32 time<1ms TTL=128
Reply from 192.168.10.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Lab 5.1.13a Building a Hub-based Network



All steps same as Peer-to-Peer Network

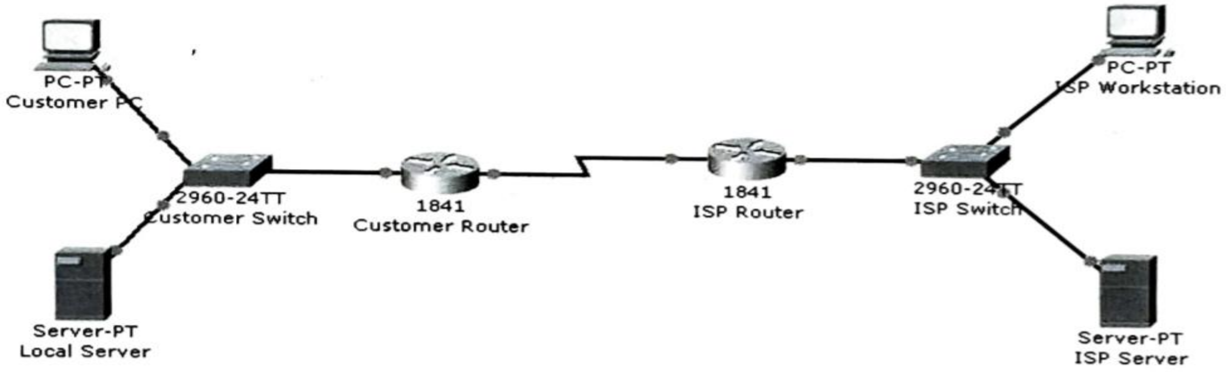


```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.3

Pinging 192.168.10.3 with 32 bytes of data:

Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Reply from 192.168.10.2: bytes=32 time<1ms TTL=128
Reply from 192.168.10.2: bytes=32 time=1ms TTL=128
Reply from 192.168.10.2: bytes=32 time<1ms TTL=128
Reply from 192.168.10.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Program 8

Aim: Performing an Initial Switch Configuration.

Topology Diagram



Objectives:

Perform an initial configuration of a Cisco Catalyst 2960 switch.

Background / Preparation:

Configure settings on the Cisco Catalyst 2960 switch:

- Host name
- Console password
- vty password
- Privileged EXEC mode password
- Privileged EXEC mode secret
- IP address on VLAN1 interface
- Default gateway

Note: Not all commands are graded by Packet Tracer.

Step 1: Configure the switch host name.

- From the Customer PC, use a console cable and terminal emulation software to connect to the console of the customer Cisco Catalyst 2960 switch.

- Set the host name on the switch to Customer Switch using these commands

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname CustomerSwitch
```

Step 2: Configure the privileged mode password and secret.

- From global configuration mode, configure the password as cisco

```
CustomerSwitch(config)#enable password cisco
```

- From global configuration mode, configure the secret as cisco123.

```
CustomerSwitch(config)#enable secret cisco123
```

Step 3: Configure the console password.

- From global configuration mode, switch to configuration mode to configure the console line.

```
CustomerSwitch(config)#line console 0
```

- From line configuration mode, set the password to cisco and require the password to be entered at login.

```
CustomerSwitch(config-line)#password cisco
CustomerSwitch(config-line)#login
CustomerSwitch(config-line)#exit
```

Step 4: Configure the vty password.

- From global configuration mode, switch to the configuration mode for the vty lines 0 through 15.

```
CustomerSwitch(config)#line vty 0 15
```

- From line configuration mode, set the password to cisco and require the password to be entered at login.

```
CustotherSwitch(config-line)#password cisco
CustomerSwitch(config-line)#login
CustomerSwitch(config-line)#exit
```

Step 5: Configure an IP address on interface VLAN1.

- From global configuration mode, switch to interface configuration mode for VLANI, and assign the IP address 192.168.1.5 with the subnet mask of 255.255.255.0.

```
CustomerSwitch(config)#interface vlan 1
CustomerSwitch(config-if)#ip address 192.168.1.5 255.255.255.0
CustomerSwitch(config-if)#no shutdown
CustomerSwitch(config-if)#exit
```

Step 6: Configure the default gateway.

- From global configuration mode, assign the default gateway to 192.168.1.1.

```
CustomerSwitch(config)#ip default-gateway 192.168.1.1
```

Click the Check Results button at the bottom of this instruction window to check your work.

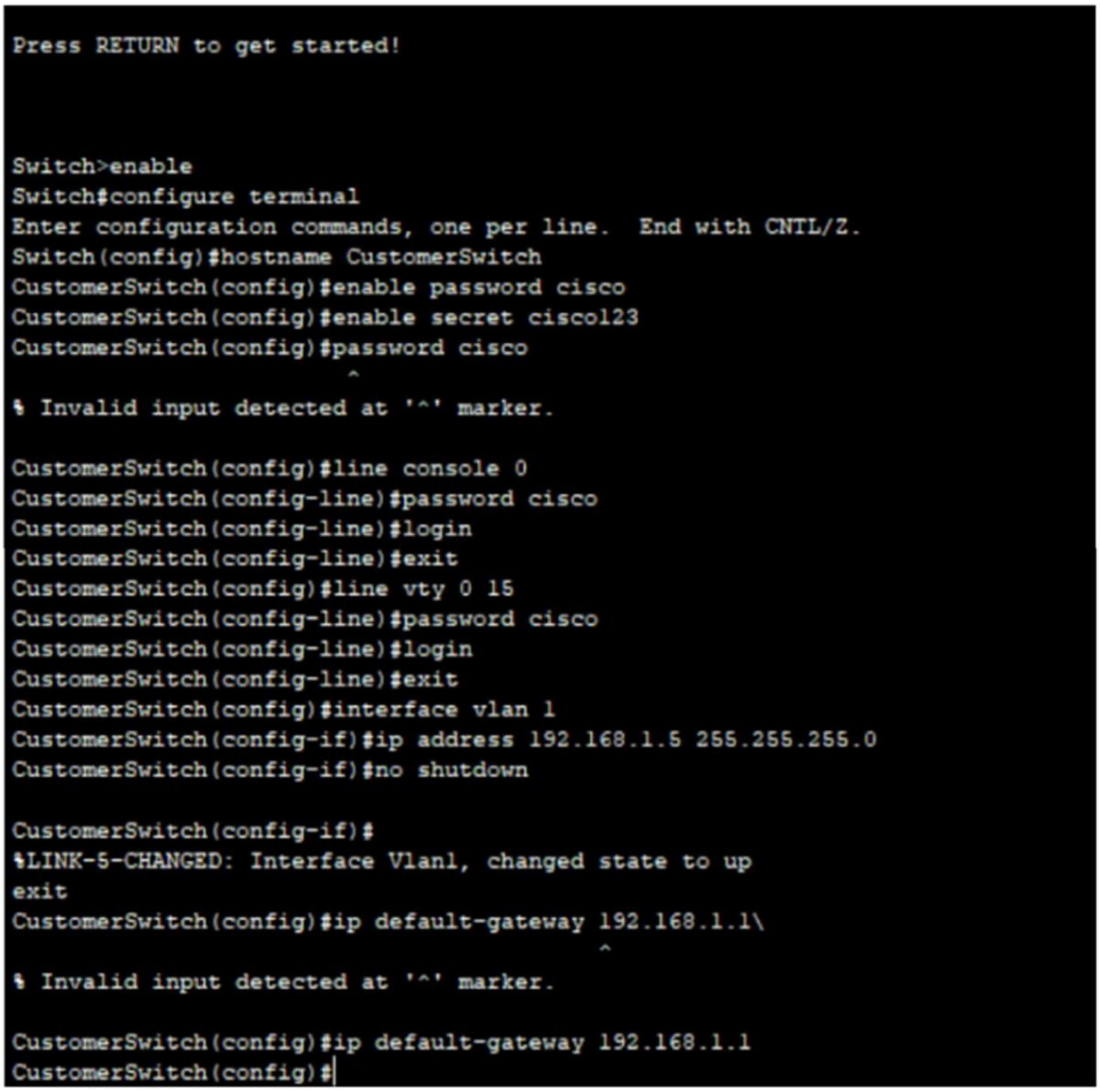
Step 7: Verify the configuration.

- The Customer Switch should now be able to ping the ISP Server as 209.165.201.10. The first one or two pings may fail while ARP converges

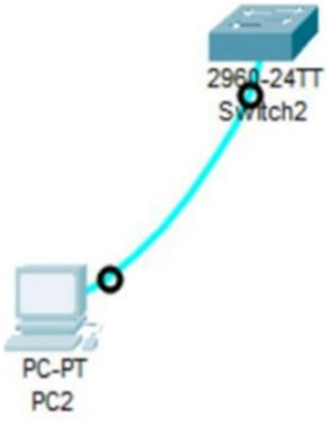
```
Customer Switch(config)#end
CustomerSwitch#ping  209.165.201.10
```

- Type escape sequence to abort

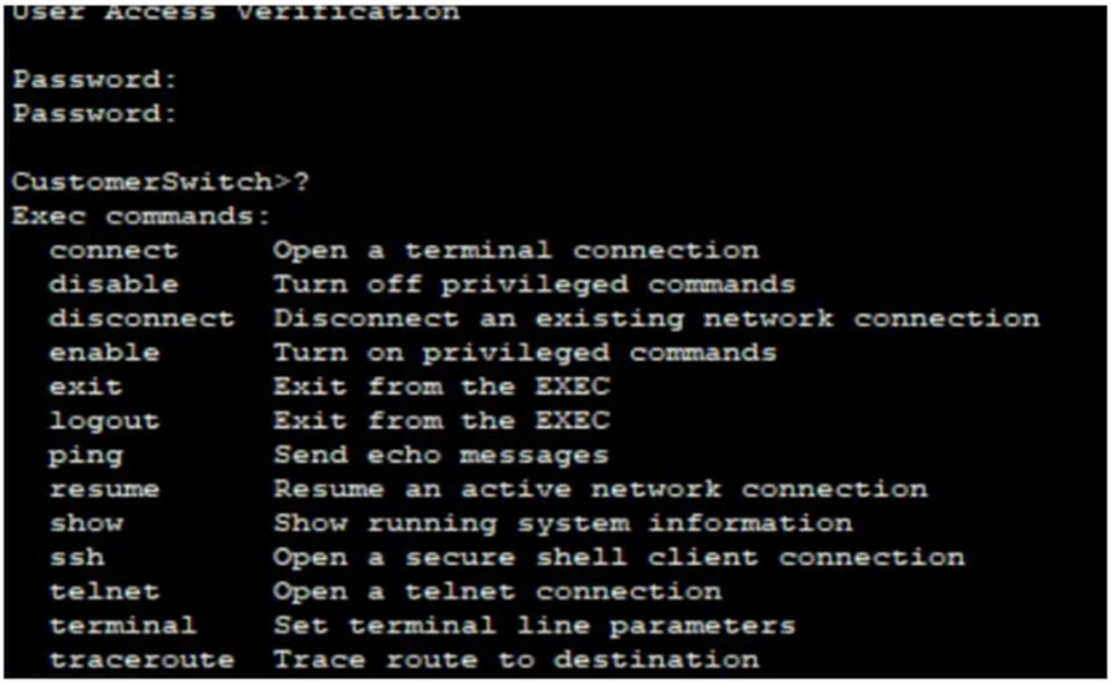
```
Sending 5, 100-byte ICMP Echos to 209. 165.201.10, timeout is 2 seconds:
.....!!!!
Success rate is 60 percent (3/5), round-trip min/avg/max 181/189/197 ms
Customer Switch#
```



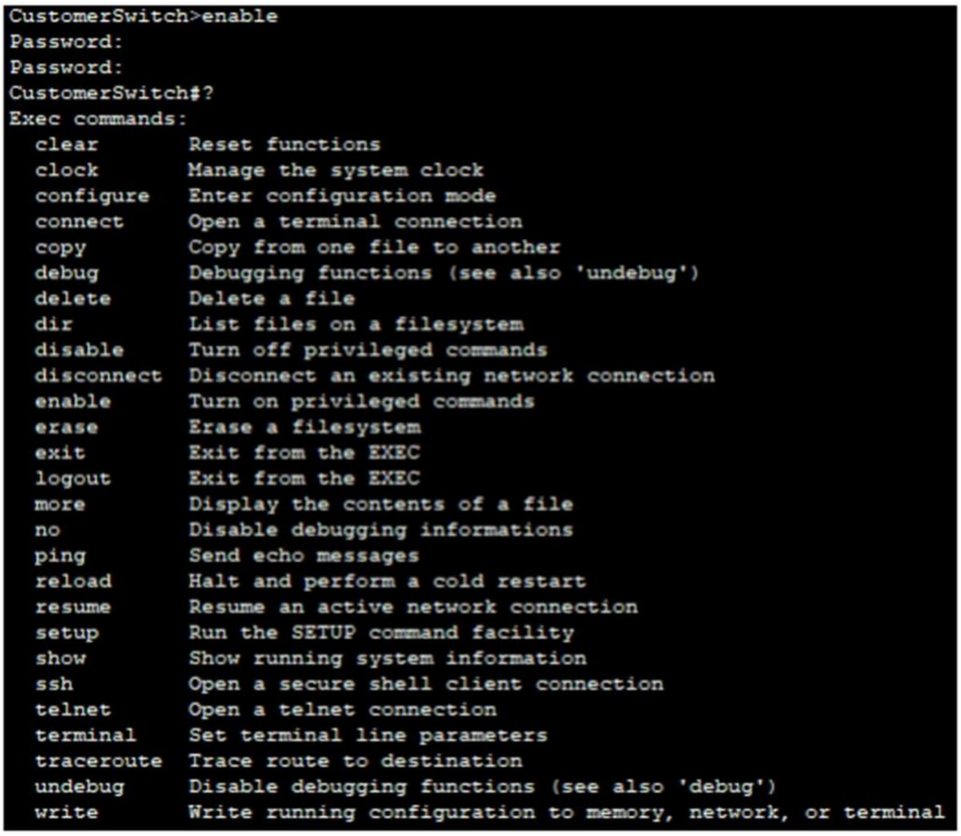
```
Press RETURN to get started!



Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname CustomerSwitch
CustomerSwitch(config)#enable password cisco
CustomerSwitch(config)#enable secret cisco123
CustomerSwitch(config)#password cisco
                        ^
% Invalid input detected at '^' marker.

CustomerSwitch(config)#line console 0
CustomerSwitch(config-line)#password cisco
CustomerSwitch(config-line)#login
CustomerSwitch(config-line)#exit
CustomerSwitch(config)#line vty 0 15
CustomerSwitch(config-line)#password cisco
CustomerSwitch(config-line)#login
CustomerSwitch(config-line)#exit
CustomerSwitch(config)#interface vlan 1
CustomerSwitch(config-if)#ip address 192.168.1.5 255.255.255.0
CustomerSwitch(config-if)#no shutdown

CustomerSwitch(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up
exit
CustomerSwitch(config)#ip default-gateway 192.168.1.1\
                                          ^
% Invalid input detected at '^' marker.

CustomerSwitch(config)#ip default-gateway 192.168.1.1
CustomerSwitch(config)#
```



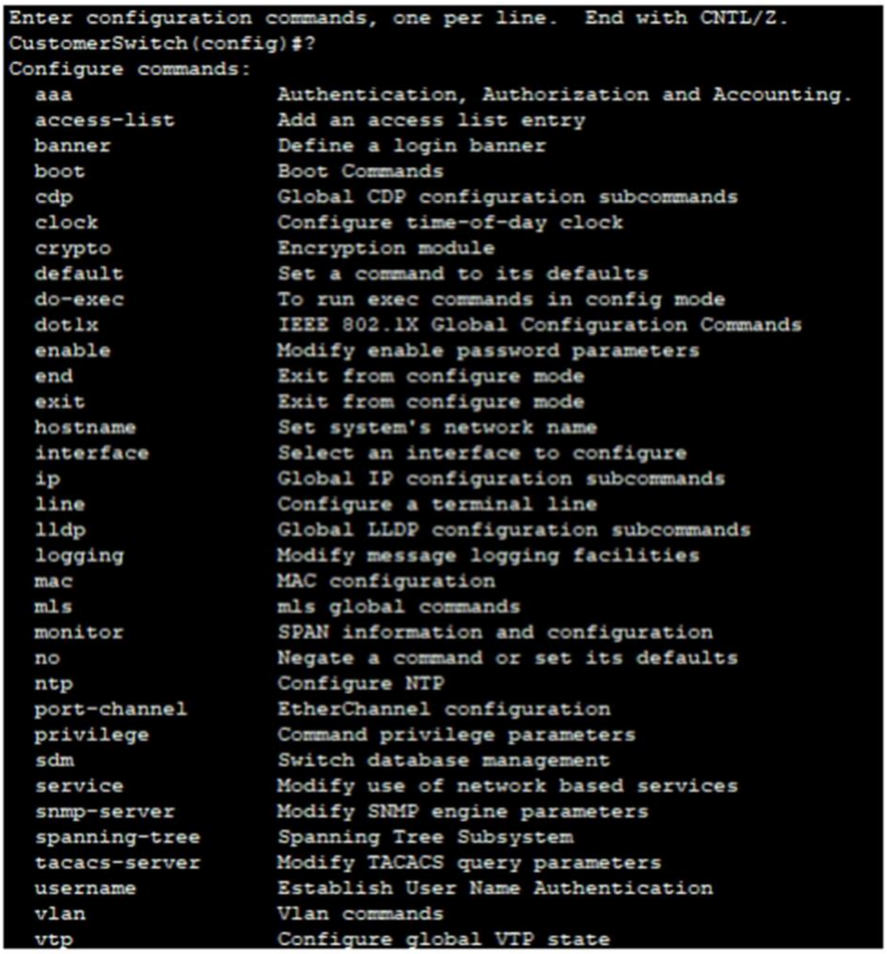
Some Extra Executable Commands:



```
User Access Verification

Password:
Password:

CustomerSwitch>?
Exec commands:
  connect      Open a terminal connection
  disable      Turn off privileged commands
  disconnect   Disconnect an existing network connection
  enable       Turn on privileged commands
  exit         Exit from the EXEC
  logout       Exit from the EXEC
  ping         Send echo messages
  resume       Resume an active network connection
  show         Show running system information
  ssh          Open a secure shell client connection
  telnet       Open a telnet connection
  terminal     Set terminal line parameters
  traceroute   Trace route to destination
```



```
CustomerSwitch>enable
Password:
Password:
CustomerSwitch#?
Exec commands:
  clear        Reset functions
  clock        Manage the system clock
  configure    Enter configuration mode
  connect      Open a terminal connection
  copy         Copy from one file to another
  debug        Debugging functions (see also 'undebug')
  delete       Delete a file
  dir          List files on a filesystem
  disable      Turn off privileged commands
  disconnect   Disconnect an existing network connection
  enable       Turn on privileged commands
  erase        Erase a filesystem
  exit         Exit from the EXEC
  logout       Exit from the EXEC
  more         Display the contents of a file
  no           Disable debugging informations
  ping         Send echo messages
  reload       Halt and perform a cold restart
  resume       Resume an active network connection
  setup        Run the SETUP command facility
  show         Show running system information
  ssh          Open a secure shell client connection
  telnet       Open a telnet connection
  terminal     Set terminal line parameters
  traceroute   Trace route to destination
  undebug      Disable debugging functions (see also 'debug')
  write        Write running configuration to memory, network, or terminal
```

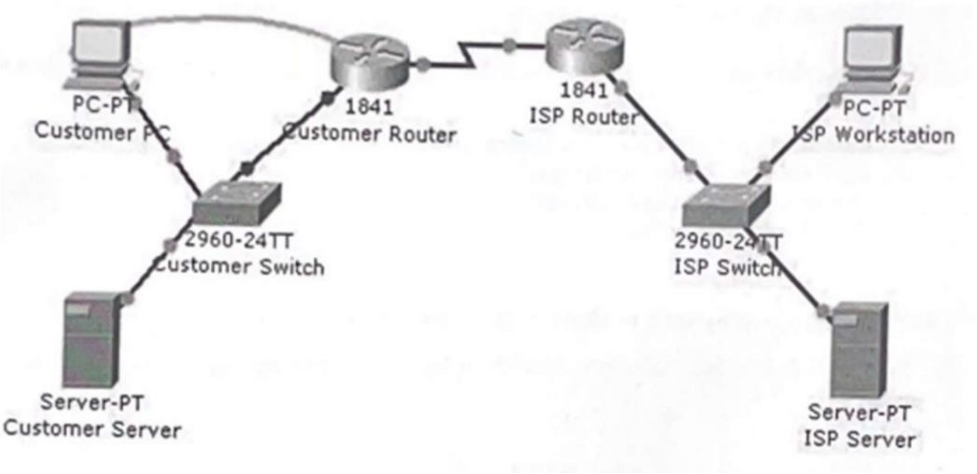


```
Enter configuration commands, one per line.  End with CNTL/Z.
CustomerSwitch(config)#?
Configure commands:
  aaa                 Authentication, Authorization and Accounting.
  access-list         Add an access list entry
  banner              Define a login banner
  boot                Boot Commands
  cdp                 Global CDP configuration subcommands
  clock               Configure time-of-day clock
  crypto              Encryption module
  default             Set a command to its defaults
  do-exec             To run exec commands in config mode
  dot1x               IEEE 802.1X Global Configuration Commands
  enable              Modify enable password parameters
  end                 Exit from configure mode
  exit                Exit from configure mode
  hostname            Set system's network name
  interface           Select an interface to configure
  ip                  Global IP configuration subcommands
  line                Configure a terminal line
  lldp                Global LLDP configuration subcommands
  logging             Modify message logging facilities
  mac                 MAC configuration
  mls                 mls global commands
  monitor             SPAN information and configuration
  no                  Negate a command or set its defaults
  ntp                 Configure NTP
  port-channel        EtherChannel configuration
  privilege           Command privilege parameters
  sdm                 Switch database management
  service             Modify use of network based services
  snmp-server         Modify SNMP engine parameters
  spanning-tree       Spanning Tree Subsystem
  tacacs-server       Modify TACACS query parameters
  username            Establish User Name Authentication
  vlan                Vlan commands
  vtp                 Configure global VTP state
```

Program 9

Aim: Performing an Router Configuration.

Topology Diagram Initial



Objectives

- Configure the router host name.
- Configure passwords.
- Configure banner messages.
- Verify the router configuration.

Background / Preparation

- In this activity, you will use the Cisco IOS CLI to apply an initial configuration to a router, including host name, passwords, a message-of-the-day (MOTD) banner, and other basic settings.

Note: Some of the steps are not graded by Packet Tracer.

Step I: Configure the router host name.

- On Customer PC, use the terminal emulation software to connect to the console of the customer Cisco 1841 ISR
- Set the host name on the router to **CustomerRouter** by using these commands.

```
Router>enable
Router#configure terminal
Router(config)#hostname CustomerRouter
```

Step 2: Configure the privileged mode and secret passwords.

- In global configuration mode, set the password to Cisco.

```
CustomerRouter(config)#enable password cisco
```

- Set an encrypted privileged password to cisco123 using the secret command.

```
CustomerRouter(config)#enable secret cisco123
```

Step 3: Configure the console password

- In global configuration mode, switch to line configuration mode to specify the console line.

```
CustomerRouter(config)#line console 0
```

- Set the password to cisc0123, require that the password be entered at login, and then exit line configuration mode.

```
CustomerRouter(config-line)#password cisc0123
CustomerRouter(config-line)#login
CustomerRouter(config-line)#exit
CustomerRouter(config)#
```

Step 4: Configure the vty password to allow Telnet access to the router.

- In global configuration mode, switch to line configuration mode to specify the vty lines.

```
CustomerRouter(config)#line vty 0 4
```

- Set the password to cisc0123, require that the password be entered at login, exit line configuration mode, and then exit the configuration session.

```
CustomerRouter(config-line)#password cisco123
CustomerRouter(config-line)#login
CustomerRouter(config-line)#exit
CustomerRouter(config)#
```

Step 5: Configure password encryption, a MOTD banner, and turn off domain server lookup.

- Currently, the line passwords and the enable password are shown in clear text when you show the running configuration. Verify this now by entering the show running- config command.
- To avoid the security risk of someone looking over your shoulder and reading the passwords, encrypt all clear text passwords.

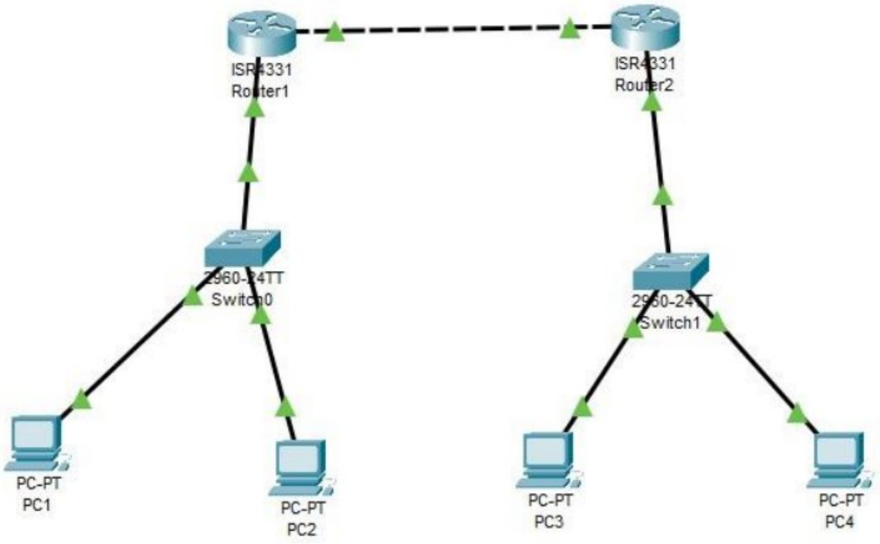
```
CustomerRouter(config)#service password-encryption
```

- Use the show running-config command again to verify that the passwords are encrypted.
- To provide a warning when someone attempts to log in to the router, configure a MOTD banner.

```
CustomerRouter(config)#banner motd SAuthorized Access Only!$
```

Experiment 10

Aim: Connecting two networks and sending data across them

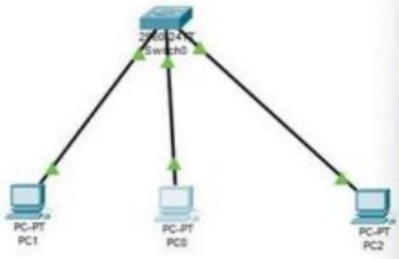


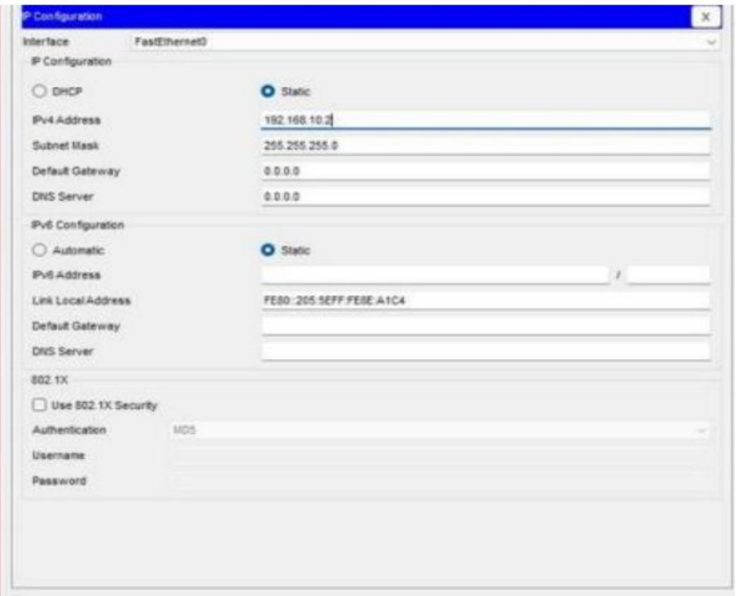
Procedure:

- Let's configure three routers (Router0, Router1, and Router2) with IP addresses and static routes:
  - Router0:
    - FastEthernet0/0: IP 192.168.1.1, Subnet mask 255.255.255.0
    - Serial2/0: IP 11.0.0.1, Subnet mask 255.0.0.0
  - Router1:
    - Serial2/0: IP 11.0.0.2, Subnet mask 255.0.0.0
    - Serial3/0: IP 12.0.0.1, Subnet mask 255.0.0.0
  - Router2:
    - FastEthernet0/0: IP 192.168.3.1, Subnet mask 255.255.255.0
    - Serial2/0: IP 12.0.0.2, Subnet mask 255.0.0.0
  - Then, ping all router using command ping and ip address where you need to send data

Building hub-based Network:

1. Identify the proper ethernet cable and connect the two PCs to the switch.
2. Verify the physical connection.
3. Access the IP settings window.
4. Configure TCP/IP settings for two PCs.
5. Access the command or MS-DOS prompt.
6. Verify that the PCs can communicate.
7. Confirm the TCP/IP network settings.





Interface FastEthernet0

P Configuration

○ DHCP ● Static

IPv4 Address 192.168.10.2

Subnet Mask 255.255.255.0

Default Gateway 0.0.0.0

DNS Server 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address /

Link Local Address FE80::205:5EFF:FE8E:A1C4

Default Gateway

DNS Server

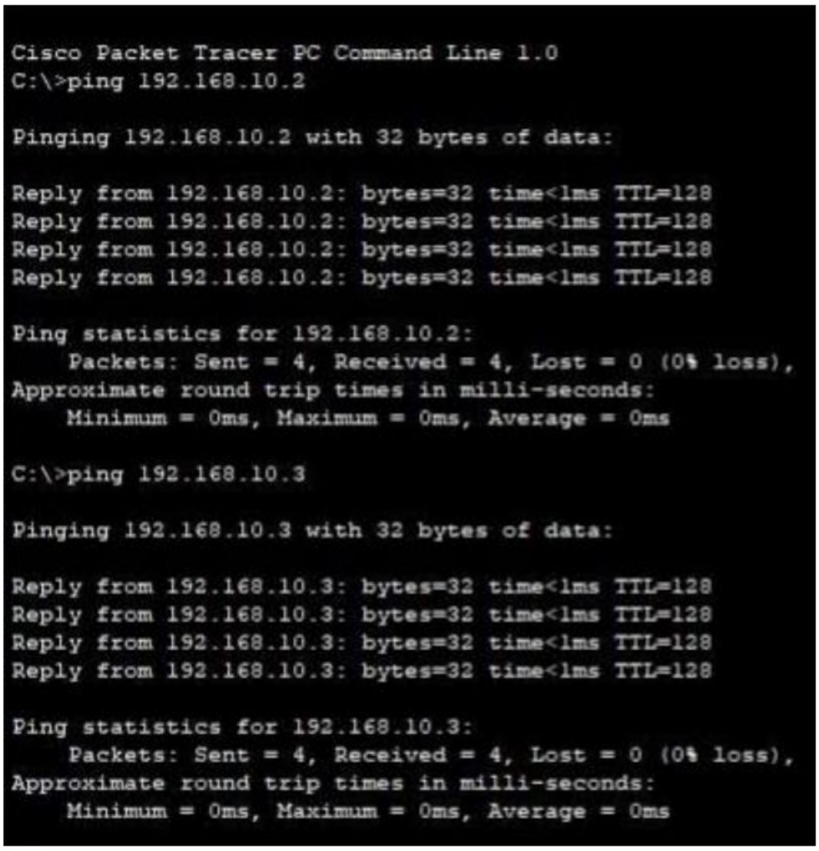
802.1X

□ Use 802.1X Security

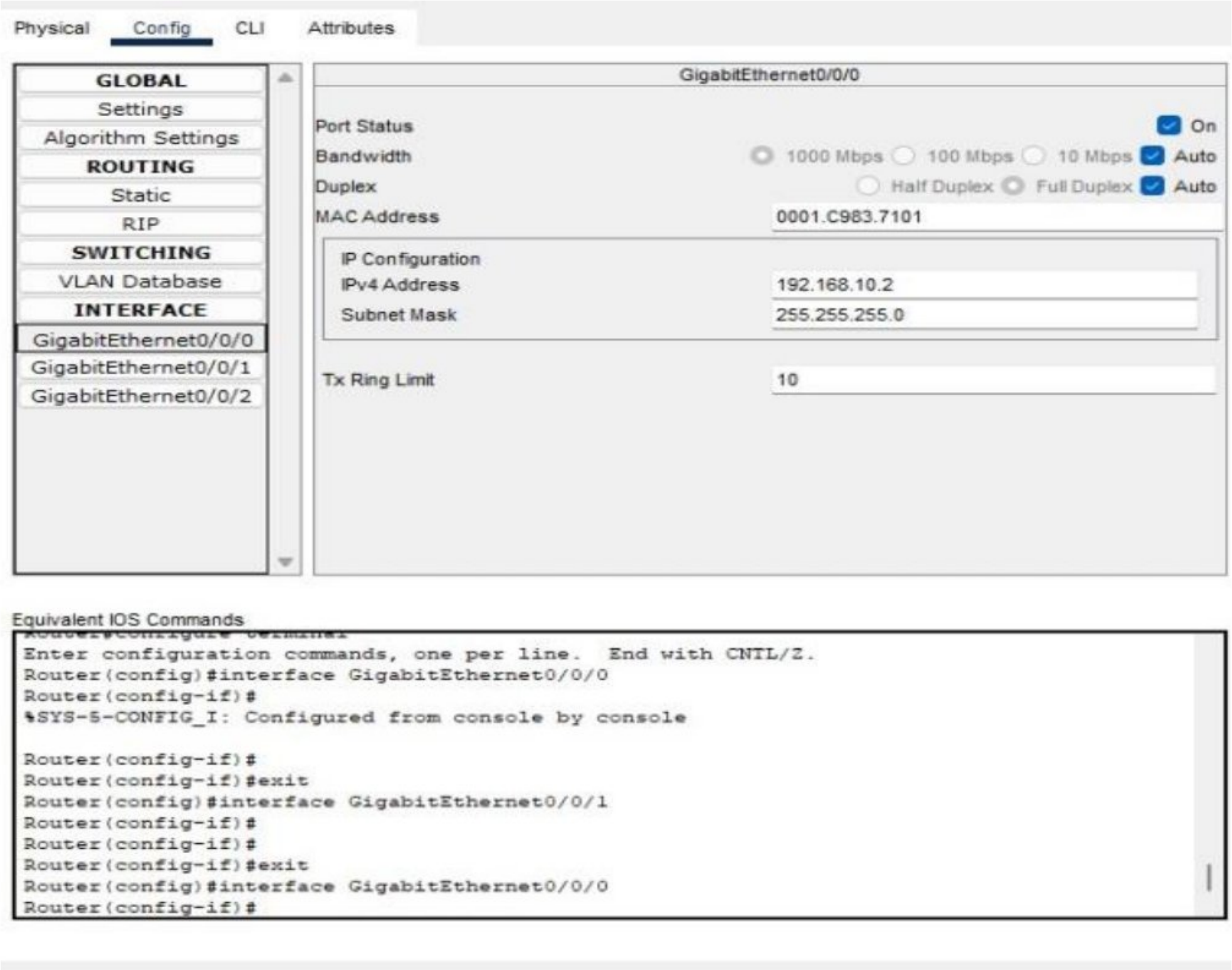
Authentication MD5

Username

Password



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Reply from 192.168.10.2: bytes=32 time<1ms TTL=128
Reply from 192.168.10.2: bytes=32 time<1ms TTL=128
Reply from 192.168.10.2: bytes=32 time<1ms TTL=128
Reply from 192.168.10.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.10.3

Pinging 192.168.10.3 with 32 bytes of data:

Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```



GigabitEthernet0/0/0

Port Status ☑ On

Bandwidth ○ 1000 Mbps ○ 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ○ Full Duplex ☑ Auto

MAC Address 0001.C983.7101

IP Configuration

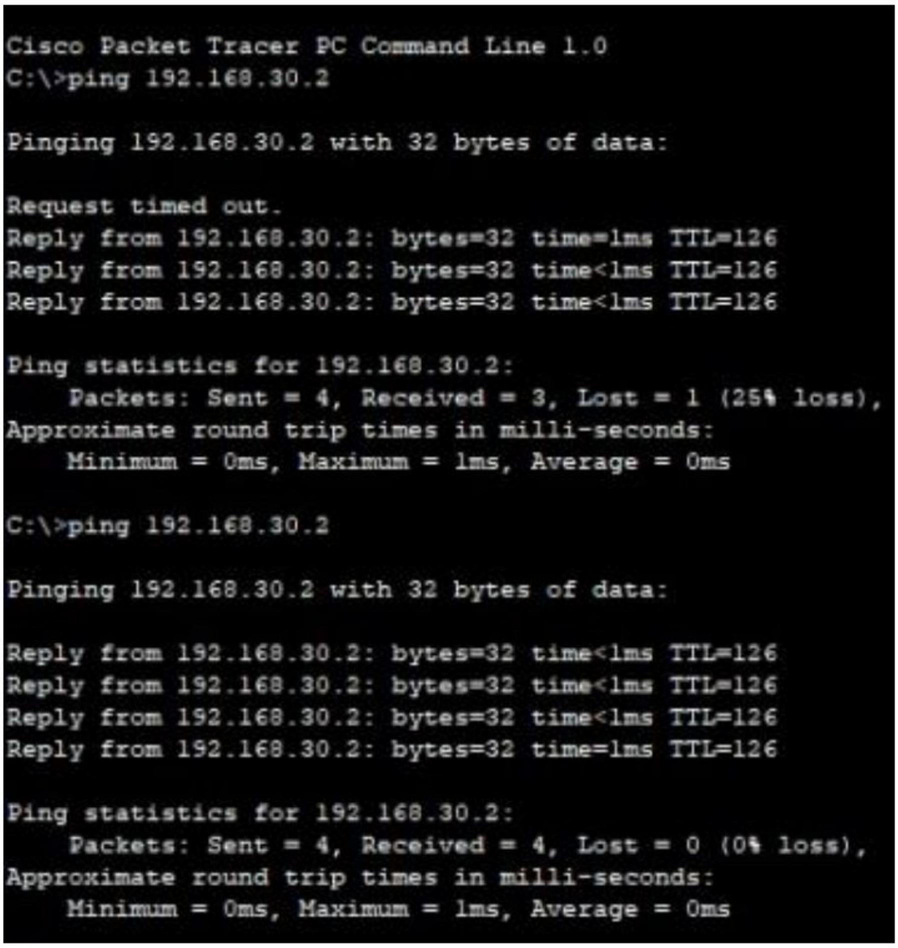
IPv4 Address 192.168.10.2

Subnet Mask 255.255.255.0

Tx Ring Limit 10

Equivalent IOS Commands

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0/0
Router(config-if)#
%SYS-5-CONFIG_I: Configured from console by console

Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0/1
Router(config-if)#
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0/0
Router(config-if)#
```



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.30.2

Pinging 192.168.30.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.30.2: bytes=32 time=1ms TTL=126
Reply from 192.168.30.2: bytes=32 time<1ms TTL=126
Reply from 192.168.30.2: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.30.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.30.2

Pinging 192.168.30.2 with 32 bytes of data:

Reply from 192.168.30.2: bytes=32 time<1ms TTL=126
Reply from 192.168.30.2: bytes=32 time<1ms TTL=126
Reply from 192.168.30.2: bytes=32 time<1ms TTL=126
Reply from 192.168.30.2: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.30.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```