Computer Networks-Lab 03

Instructor: Hurmat Hidayat

CL30001 – Computer Networks-Lab

SEMESTER Fall 2023

Computer Networks Lab 03

Objective

The objective of this lab is to provide students with a comprehensive understanding of IPv4 addresses, IP addressing in network devices, and static routing. Through practical simulations using Packet Tracer, students will gain hands-on experience in configuring IP addresses, subnet masks, and static routing on network devices such as routers, switches, and laptops.

Learning Outcomes

By the end of this lab, students will be able to:

- Understand the structure and types of IPv4 addresses, including the concept of classes.
- Configure IPv4 addresses on network devices (routers, switches, and laptops) in Packet Tracer.
- Implement static routing on routers to establish network connectivity.
- Simulate various network topologies in Packet Tracer to enhance comprehension of IP addressing in network devices.
- Analyze and troubleshoot network connectivity issues using different network topologies and IP addressing configurations.

Table of Contents

IP Address

An IP (Internet Protocol) address is a numerical label assigned to the devices connected to a computer network that uses the IP for communication. IP address act as an identifier for a specific machine on a particular network. IP Version 4 (IPv4) was defined in 1981. It has not undergone much changes from that time. An IPv4 address consists of four numbers, each number contains one to three digits, with a single dot (.) separates each number or set of digits. IPv4 uses 32-bit IP address. So the maximum number of IP address is 2^{32} or 4,294,967,296. Unfortunately, there is a need of IP addresses more than IPv4 could supply.

IPv4 address: 216 . 27 . 61 . 137

Binary representation: 11011000 . 00011011 . 00111101 . 10001001

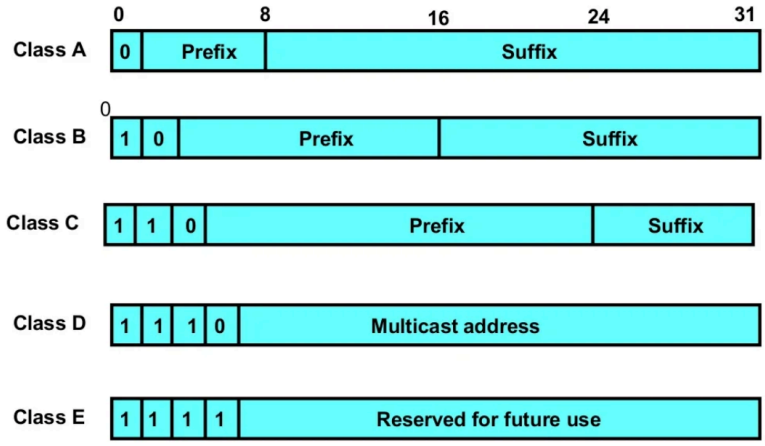
IPv4 Address is divided into two parts:

- **Prefix:** The prefix part of IP address identifies the physical network to which the computer is attached. . Prefix is also known as a **network address**.
- **Suffix:** The suffix part identifies the individual computer on the network. The suffix is also called the **host address.**

The classes of IPv4 addresses

The IP hierarchy contains many classes of the IP addresses. Broadly, the IPv4 addressing system is divided into five classes of IP address. All the five classes are identified by the first octet of the IP address. The different classes of the IPv4 address are the following:

1) Class A address
2) Class B address
3) Class C address
4) Class D address
5) Class E address



Each class has a specific range of IP addresses (and ultimately dictates the number of devices you can have on your network). Primarily, class A, B, and C are used by the majority of devices on the Internet. Class D and class E are for special uses.

Class A Address Range

Class A addresses are for networks with large number of total hosts. Class A allows for 126 i.e. (2^7 - 2) networks by using the first octet for the network ID. The first bit in this octet, is always zero. The remaining seven bits in this octet complete the network ID. The 24 bits in the remaining three octets represent the hosts ID and allows for approximately 17 million hosts per network (2^{24} -2 = 16777214). Class A network number values begin at 1 and end at 127.

Class A addresses 127.0.0.0 to 127.255.255.255 cannot be used and is reserved for loopback and diagnostic functions.

- Public IP Range: 1.0.0.0 to 127.0.0.0
    - First octet value range from 1 to 127
- Private IP Range: 10.0.0.0 to 10.255.255.255
- Subnet Mask: 255.0.0.0 (8 bits)
- Number of Networks: 126
- Number of Hosts per Network: 16,777,214

Class B Address Range

Class B addresses are for medium to large sized networks. Class B allows for 16,384 networks by using the first two octets for the network ID. The first two bits in the first octet are always 1 0. The remaining six bits, together with the second octet, complete the network ID. The 16 bits in the third and fourth octet represent host ID and allows for approximately 65,000 hosts per network. Class B network number values begin at 128 and end at 191.

- Public IP Range: 128.0.0.0 to 191.255.0.0
    - First octet value range from 128 to 191
- Private IP Range: 172.16.0.0 to 172.31.255.255
- Subnet Mask: 255.255.0.0 (16 bits)
- Number of Networks: 16,382
- Number of Hosts per Network: 65,534

Class C Address Range

Class C addresses are used in small local area networks (LANs). Class C allows for approximately 2 million networks by using the first three octets for the network ID. In a class C IP address, the first three bits of the first octet are always 1 1 0. And the remaining 21 bits of first three octets complete the network ID. The last octet (8 bits) represent the host ID and allows for 254 hosts per network. Class C network number values begins at 192 and end at 223.

- Public IP Range: 192.0.0.0 to 223.255.255.0
    - First octet value range from 192 to 223
- Private IP Range: 192.168.0.0 to 192.168.255.255
- Subnet Mask: 255.255.255.0 (24 bits)
- Number of Networks: 2,097,150
- Number of Hosts per Network: 254

Class	First octet value	Subnet mask
A	0-127	8
B	128-191	16
C	192-223	24
D	224-239	-
E	240-255	-

Network Address

A Network Address is a logical or physical address that uniquely identifies a host or a machine in a telecommunication network. A network may also not be unique and can contain some structural and hierarchical information of the node in the network.

Broadcast Address

A broadcast address is an IP address that is used to target all systems on a specific subnet network instead of single hosts. In other words broadcast address allows information to be sent to all machines on a given subnet rather than to a specific machine.

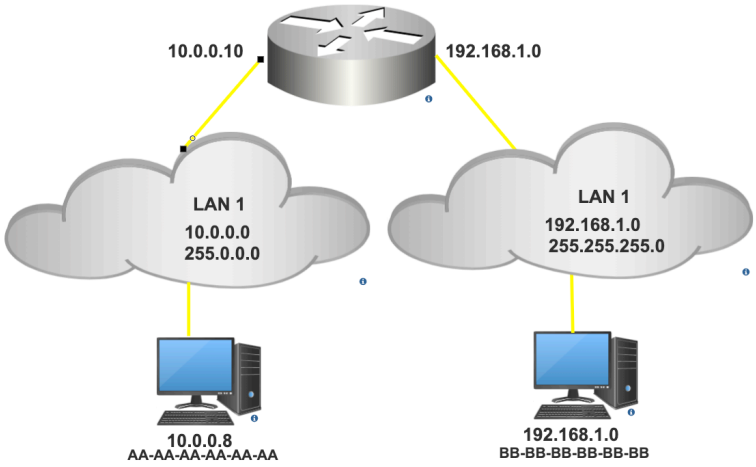
Router

A hardware device designed to take incoming packets, analyze the packets, moving the packets to another network, converting the packets to another network interface, dropping the packets, directing packets to the appropriate locations, and performing any other number of other actions. The picture shows the Linksys BEFSR11 router and is what most home routers resemble.

Figure 3.12. Linksys BEFSR11 Router

A router has a lot more capabilities than other network devices such as a hub or a switch that are only able to perform basic network functions. For example, a hub is often used to transfer data between computers or network devices, but does not analyze or do anything with the data it is transferring. Routers however can analyze the data being sent over a network, change how it is packaged and send it to another network or over a different network. For example, routers are commonly used in home networks to share a single Internet connection with multiple computers.

When two different local area network (LAN) wants to communicate with each other they needs a router. A router is connected to at least two Networks, commonly two LANs, WANs or a LAN and its ISP's Network.



Default Gateway

When a host wants to reach a destination that is **outside of its own network**, it has to use a default gateway. We use a router or multilayer switch (that's a switch that can do routing) as a default gateway.

A default gateway makes it possible for devices in one network to communicate with devices in another network. If a computer, for example, requests a web page, the request goes through the default gateway before exiting the local network (LAN) to reach the internet.

Think of a default gateway as an intermediate device between the local network and the internet. The default gateway transfers internal data to the internet and back again.

Routing

Routing is the process of selecting and defining paths for IP-packet traffic within or between networks as well as the process of managing network traffic overall.

Static Routing

Network administrators use static routing, or *nonadaptive routing*, to define a route when there is a single route or a preferred route for traffic to reach a destination. Static routing uses small routing tables with only one entry for each destination. It also requires less computation time than dynamic routing because each route is preconfigured.

Because static routes are preconfigured, administrators must manually reconfigure routes to adapt to changes in the network when they occur. Static routes are generally used in networks where administrators don't expect any changes.

Command

Router(config)#

ip route <Destination Network ID> <Destination Subnet Mask> <Next-hop IP address>

Lab Task 04

Inter LAN Communication in CPT

Design the following topologies and perform simulation in packet tracer.

- Assign IP Address of Class C
- Transfer packet between them.

1)

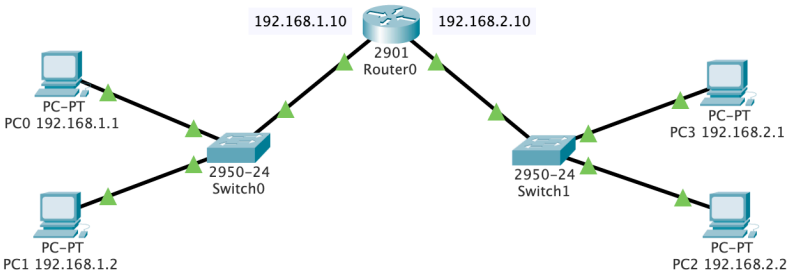


Figure 1 Communication using One Router

2)

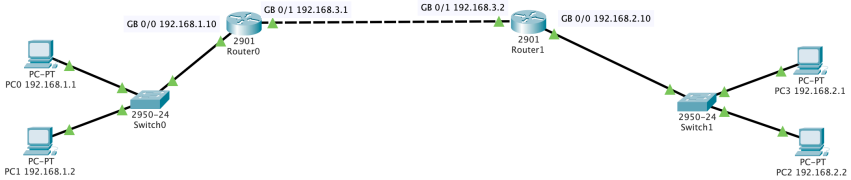


Figure 2 Communication using two Router

3)

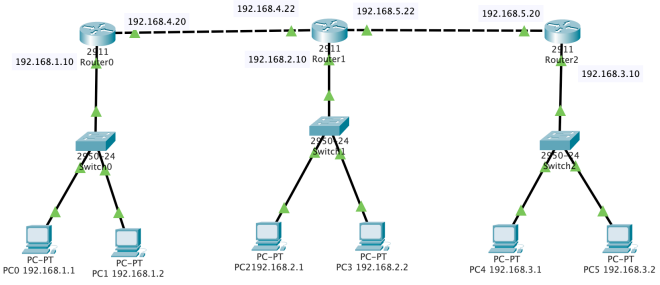


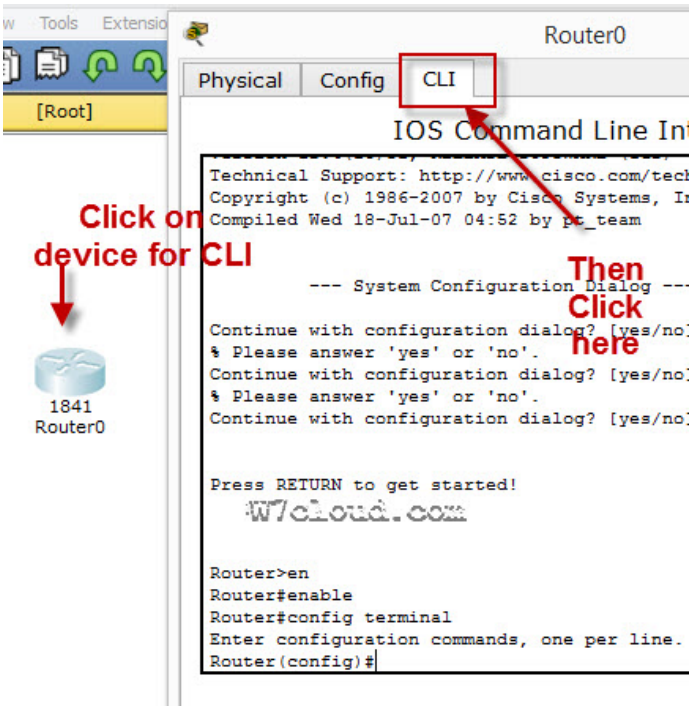
Figure 3 Communication using three routers

Assignment Manual

Cisco Router Configuration Step By Step

To configure any device in packet tracer you are required to open or access its CLI. You can do it by clicking any device and then navigating to CLI tab. Once you are at CLI you can perform all Cisco Commands here.

Mode	Symbol	How to access this mode	Command for leaving this mode
User EXEC Mode	Router >	Default mode after booting. Press enter for accessing this.	Use **exit** command
Privileged EXEC mode	Router #	Use **enable** command from user exec mode for entering into this mode	exit
Global Configuration mode	Router(config)#	Use **configure terminal** command from privileged exec mode	Exit or Ctrl+Z for user EXEC mode
Interface Configuration	Router(config-if)#	Use**Interface<interface+number>** command from global configuration mode	Use **exit** command to return in global mode



Cisco IOS supports numerous command modes which can be practice with packet tracer, followings are the main command modes of cisco CLI with specific commands to navigate from one mode to other.

IOS commands are not case sensitive it means that you can use them in uppercase, lowercase, or mixed case, but passwords are case sensitive. Therefore make sure you type it in correctly. In any mode, you can obtain a list of commands available on that mode by entering a question mark (?).

```
Braunch_office_router(config)#router ?
  bgp     Border Gateway Protocol (BGP)
  eigrp   Enhanced Interior Gateway Routing Protocol (EIGRP)
  ospf    Open Shortest Path First (OSPF)
  rip     Routing Information Protocol (RIP)
Braunch_office_router(config)#router
```

Router Modes

Router> enable

Note: This command allows you to enter into Privileged exec mode/enable mode, where you can have more options for show and other commands. The next prompt looks like this:

Router#

Router#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Note: This command allows you to enter into global configuration mode, where you can configure a range of commands. The prompt for this command looks like this:

Router(config)#

Router(config)# exit

Router#exit

Router>

Changing Hostname

To specify or modify the host name for the router, global configuration command HOSTNAME is used. HOSTNAME is case sensitive. The host name is used in prompts and default configuration filenames. The factory-assigned default host name is router.

Router> enable

Router#configure terminal

Router(config)#hostname NP

Router(config)# exit

NP#

Configuration of Date & Time

The system clock runs from the moment the system starts up and keeps track of the current date and the time based on coordinated Universal Time(UTC), also known as Greenwich Mean Time(GMT). The system clock can be set from a number of sources, and in turn can be used to distribute the current time through various mechanisms to other systems. To manually set the system clock, use one of the formats of the clock set Exec command.

NP#clock set ?

Hh:mm:ss current time

Note : Allow you to see the format of complete command.

NP#clock set 12:15:00 ?

<1-31> Day of the month

Month Month of the year

NP#clock set 12:15:00 17 ?

Month Month of the year

NP#clock set 12:15:00 17 March ?

<1993-2035> Year

NP#clock set 12:15:00 17 March 2021

Verification:

NP#show clock

12:16:56. 441 UTC Wed Mar 17 2021

Setting A Banner

When someone connects to the router, the MOTD (Message of the Day) banner appears before the login prompt.

NP>enable

NP#configure terminal

NP(config)#banner motd # welcome to Networks Professionals #

NP(config)#exit

NP#

Note: # is a delimiting character. It is used before the start and ending of a message. You can use any character.

Verification:

NP#exit

NP con0 is now available

Press return to get started

Welcome to Networks Professionals

NP>

Displaying Running-Configuration

NP#show running-config

Building configuration.

```
Current configuration : 599 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname NP
!


!
ip cef
no ipv6 cef
!
spanning-tree mode pvst
!
interface FastEthernet0/0
no ip address
```

```
duplex auto
speed auto
shutdown
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Vlan1
no ip address
shutdown
!
ip classless
!
ip flow-export version 9
!
```

```
!


banner motd ^C Welcome To Networks Professionals ^C

!

line con 0

!

line aux 0

!

line vty 0 4

login

!

!

end
```

Line Console Password

The router has a number of ports that allow access to the router, on each of these ports you can specify passwords to provide a layer of security to the router. There is also the option of disabling login password checking to any of the ports by entering the command to get to the Router (config-line)# section of the port and entering the no login command.

The console port is on the back of the router and is used to directly connect a console to the router for configuring the router. This port should allow logins with passwords if the router is physically

secured. The port should be disabled if it is not regularly used or the router is not secured. To specify a password on a line, use the password line configuration command. The first character cannot be a number. The string can contain any alphanumeric characters, including spaces, up to 80 characters. Console password is needed when logging into router at user EXEC mode from console.

NP>enable

NP#configure terminal

NP(config)#line console 0

NP(config-line)#password NP123

NP(config-line)#login

NP(config-line)#end

Verification:

NP#exit

NP con0 is now available

Press RETURN to get started

Welcome To Networks Professionals

User Access Verification

Password: NP123

NP>enable

LINE VTY / Telnet Password

Virtual terminal lines (vty) are used to allow remote access to the router (by telnet through its interfaces). The router has variable virtual terminal lines depending upon the model of router.

Telnet is a network protocol used **to virtually access a computer** and to provide a two-way, collaborative and text-based communication channel between two machines. It follows a user command Transmission Control Protocol/Internet Protocol (TCP/IP) networking protocol for creating remote sessions.

Telnet is a text-based program that lets you access the console on a router or other device and issue commands. You can Telnet into a router **using the Telnet client included with Windows**. ... Unlike other protocols, Telnet isn't secure and shouldn't be used over the Internet

For example, **typing telnet hostname would connect a user to a hostname named hostname**. Telnet enables a user to manage an account or device remotely. For example, a user may telnet into a computer that hosts their website to manage his or her files remotely. ... As shown, a telnet session is a command line interface.

The term “vty” stands for **Virtual teletype**. VTY is a virtual port and used to get Telnet or SSH access to the device. VTY is solely used for inbound connections to the device. ... The abstract “0 – 4” means that the device can allow 5 simultaneous virtual connections which may be Telnet or SSH.

router(config-line)#exit. The virtual terminal or “VTY” lines are virtual lines that **allow connecting to the device using telnet** or Secure Shell (SSH). Cisco devices can have up to 16 VTY lines.
The VTY lines are the Virtual Terminal lines of the router, used **solely to control inbound Telnet**

connections. They are virtual, in the sense that they are a function of software - there is no hardware associated with them.

The term “vty” stands for Virtual teletype. VTY is a virtual port and used to get Telnet or SSH access to the device. The abstract “0 – 4” means that **the device can allow 5 simultaneous virtual connections which may be Telnet or SSH**

The Line Configuration Mode is **used to manage the terminal line characteristics for output formatting**.

NP# configure terminal

NP(config)# line vty 0 4

NP(config-line) # password NP456

NP(config-line)# login

NP(config-line)# exit

NP(config)# exit

NP#

Auxiliary Line Password

The auxiliary port is on the back of the router and is commonly used to connect a modem to. It is used to allow a remote user access to the configuration of the router. If a modem is connected to the port, it should definitely have a password specified for it.

Modem is short for "**Modulator-Demodulator**." It is a hardware component that allows a computer or another device, such as a router or switch, to connect to the Internet. It converts or

"modulates" an analog signal from a telephone or cable wire to digital data (1s and 0s) that a computer can recognize.

A modem **modulates and demodulates electrical signals sent through phone lines, coaxial cables**, or other types of wiring; in other words, it transforms digital information from your computer into analog signals that can transmit over wires, and it can translate incoming analog signals back into digital data.

NP #configure terminal

NP(config)# line aux 0

NP(config-line)# password NP@786

NP(config-line)# exit

NP(config-line)#login

NP(config)# exit

NP#

Password For Privileged Mode

To set a local password to control access to various privilege levels, use the enable password global configuration command. An enable password is defined as follows:

It must contain uppercase and lowercase alphanumeric characters from 1 to 25. Must not have a number as the first character.

Can have leading spaces, but they are ignored. However, intermediate and trailing spaces are recognized.

NP# configure terminal

NP(config)# enable password NP222

NP(config)# exit

NP#

Verification:

NP con0 is now available

Press RETURN to get started.

Welcome To Networks Professionals

NP>

NP>enable

Password:NP222

NP#

```
NP#SHOW RUNNing-config
Building configuration...

Current configuration : 623 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname NP
!
!
!
enable password NP222
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
```

Secret (Encrypted) Password For Privileged Mode

The enable secret password is the password in encrypted form and is used to gain access to enable mode and to the global configuration mode on the router. The enable password is used when you do not specify an enable secret password. The enable password should be different from the enable secret password.

NP#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

NP(config)#enable ?

password Assign the privileged level password

secret Assign the privileged level secret

NP(config)#enable secret NP333

NP(config)#exit

NP#

Removing Line Console Password

NP>enable

NP#configure terminal

NP(config)#line console 0

NP(config-line)#no login

NP(config-line)#no password

NP(config-line)#end

NP#

Removing Line VTY / Telnet Password

NP>enable

NP#configure terminal

NP(config)#line vty 0 4

NP(config-line)#no login

NP(config-line)#no password

NP(config-line)#end

NP#

Removing Auxiliary Line Password

NP>enable

NP#configure terminal

NP(config)#line aux 0

NP(config-line)#no login

NP(config-line)#no password

NP(config-line)#exit

NP(config)#exit

NP#

Removing Password For Privileged Exec Mode

NP>enable

NP# configure terminal

NP(config)#no enable password

NP(config)# exit

NP#

Removing Secret Password

NP>enable

NP# configure terminal

NP(config)#no enable secret

NP(config)# exit

NP#

How to set the IP address to Cisco interface:

You can set the IP address to any Cisco device interface by using the following commands:

Router(config)#interface <interface name&number>

Router(config-if)#ip address <IP address> <subnet mask>

How to enable a port or interface

Router(config-if)#no shut

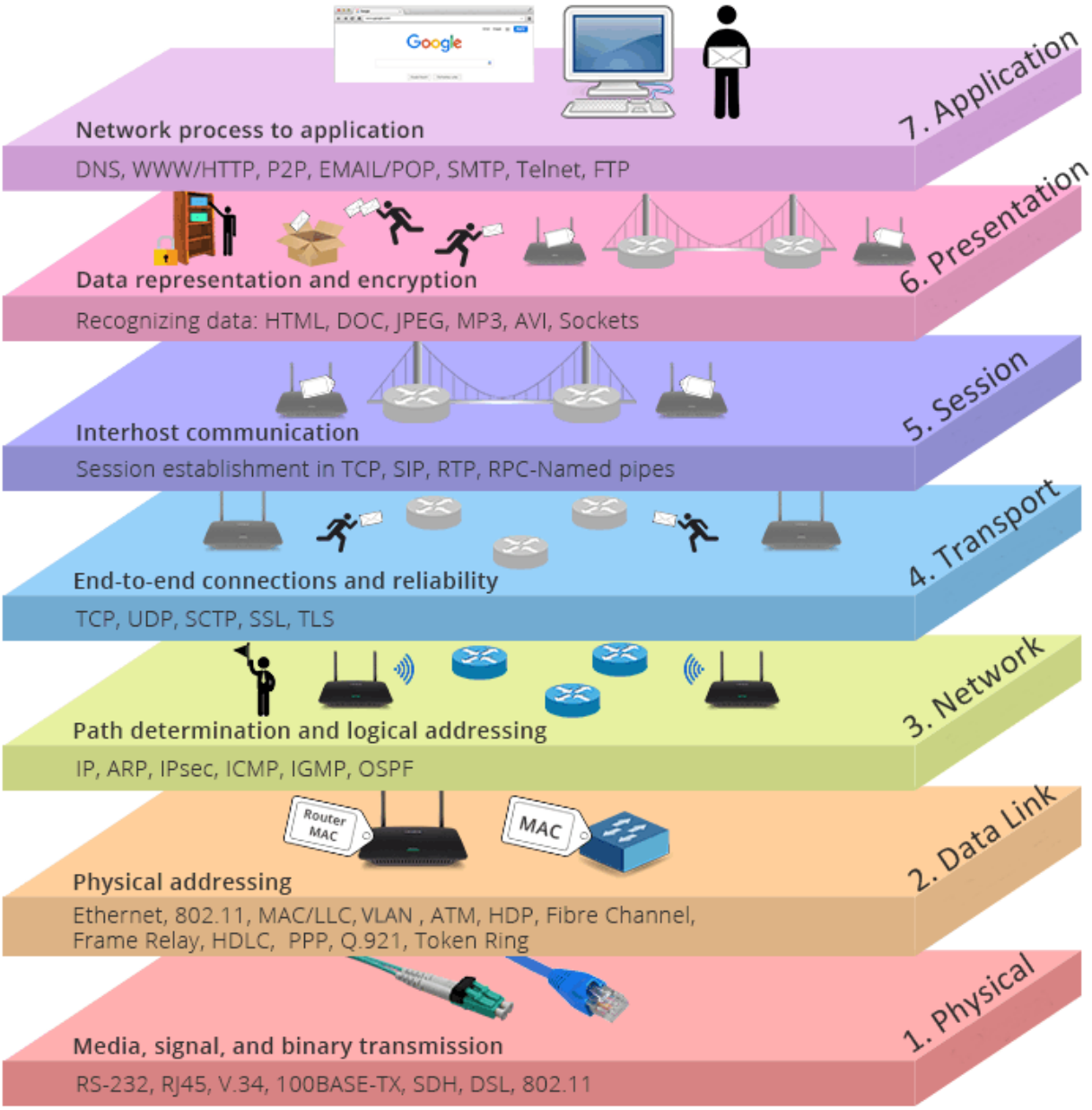
Example:

```
Router(config)#interface fastEthernet 4/0
Router(config-if)#ip address 192.168.77.88 255.255.255.0
Router(config-if)#no shut
```

How to check the IP address of all interfaces:

You can use the "**show ip interface brief**" command in Privileged EXEC mode for checking the IP address of all interface of Cisco device.

```
Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol

FastEthernet0/0        unassigned      YES NVRAM  administratively down down

FastEthernet1/0        unassigned      YES NVRAM  administratively down down

Serial2/0              unassigned      YES NVRAM  administratively down down

Serial3/0              unassigned      YES NVRAM  administratively down down

FastEthernet4/0        192.168.77.88   YES manual down                  down
```


Google
Network process to application
DNS, WWW/HTTP, P2P, EMAIL/POP, SMTP, Telnet, FTP
7. Application
Data representation and encryption
Recognizing data: HTML, DOC, JPEG, MP3, AVI, Sockets
6. Presentation
Interhost communication
Session establishment in TCP, SIP, RTP, RPC-Named pipes
5. Session
End-to-end connections and reliability
TCP, UDP, SCTP, SSL, TLS
4. Transport
Path determination and logical addressing
IP, ARP, IPsec, ICMP, IGMP, OSPF
3. Network
Router MAC
MAC
Physical addressing
Ethernet, 802.11, MAC/LLC, VLAN , ATM, HDP, Fibre Channel,
Frame Relay, HDLC, PPP, Q.921, Token Ring
2. Data Link
Media, signal, and binary transmission
RS-232, RJ45, V.34, 100BASE-TX, SDH, DSL, 802.11
1. Physical

References:

1) https://www.meridianoutpost.com/resources/articles/IP-classes.php#special
2) https://www.slideshare.net/vikasjagtap3/ip-addressing-routing
3) https://www.guru99.com/ip-address-classes.html#5
4) https://www.interserver.net/tips/kb/types-features-classes-ip-address/
5) https://www.techtarget.com/searchnetworking/answer/Static-and-dynamic-routing
6) https://www.cisco.com/c/en/us/products/routers/what-is-routing.html