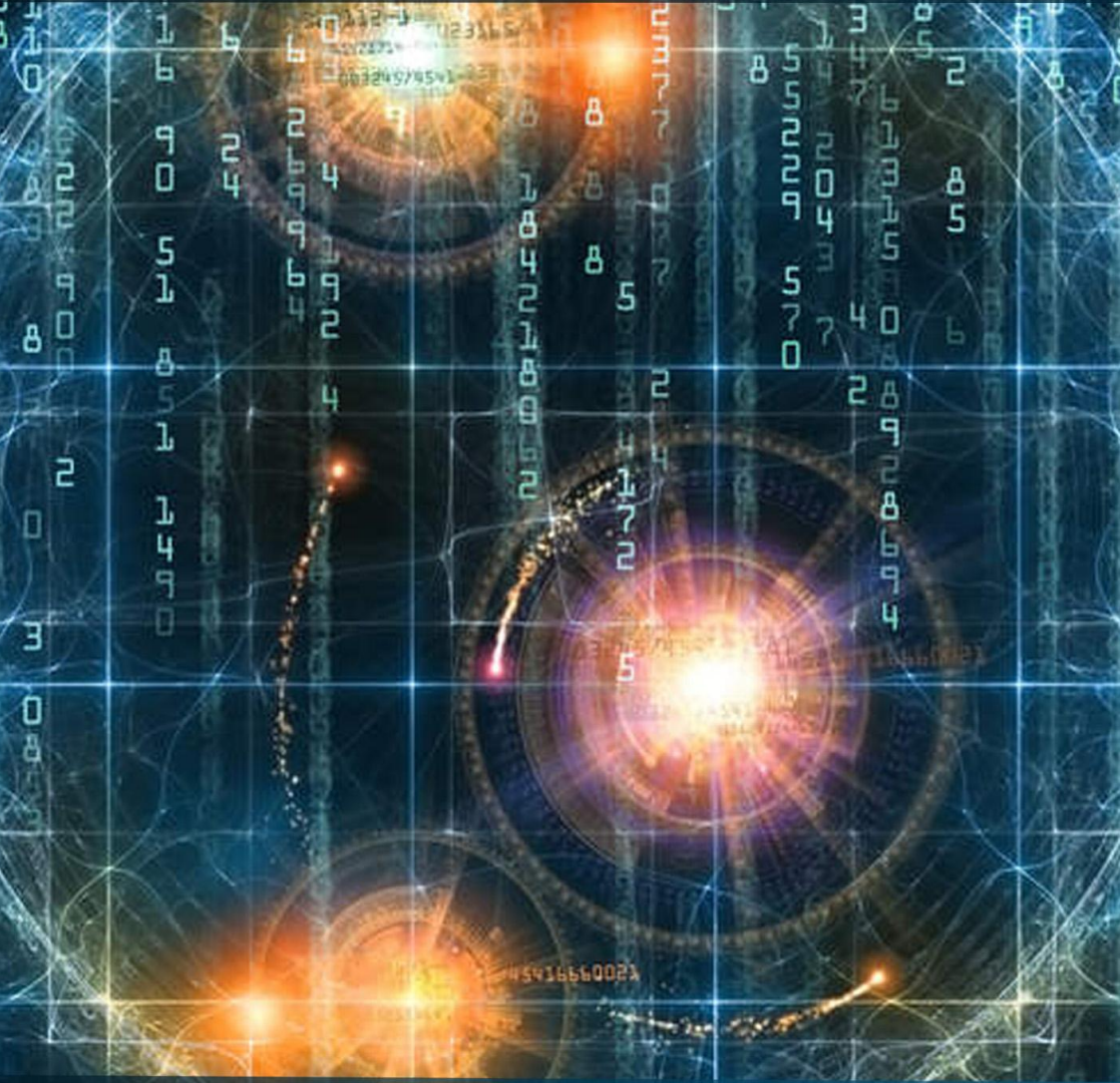


Internet Protocol (IP) Addressing



Mahdi Saleh

Internet Protocol (IP) Addressing Mahdi Saleh

2017

To my Family

Writer: Mahdi Saleh

Email: Khfajim@Gmail.com

First Version: 2017

All copyrights reserved

About the Writer

(Mahdi Saleh)

- Iraqi
- Computer Techniques Engineer
- Lecturer of Communication and
Computer Networks.
- Work in Photosynthesis
Department / Communication
Directorate.
- Work in The Internet Company.

Abstract

An Internet Protocol address (IP address) is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication. An IP address serves two principal functions: host or network interface identification and location addressing.

The information in this book highlights on the types of the **Internet Protocol** and the ways that are used to search about it, moreover the ways that are used to subnet the **IP** with many examples.

The Book Contains Five Chapters, the **First Chapter** will define the Internet protocol and its versions, the **Second Chapter** discusses the ways that are used to search about IP and other information about its work, the **Third Chapter** will discuss the Subnet ways of the IP, **Fourth Chapter** will contains many examples about Sub netting, finally the **Fifth Chapter** will discuss the suitable way to use a virtual program to design full virtual networks, this program called Cisco Packet Tracer.

Contains

1	Chapter One: Introduction	7
1.1	OSI references model.....	10
1.2	TCP/IP references model.....	10
1.3	IP address.....	12
2	Chapter Two: IP address	15
2.1	IP Lookup.....	16
2.2	IPv4 Package.....	17
2.3	Addressing.....	20
2.3.1	Unicast.....	20
2.3.2	Multicast.....	20
2.3.3	Broadcast.....	21
2.4	Subnet Mask.....	22
3	Chapter Three: Sub netting	23
3.1	Host addressing.....	25
3.2	CIDR notation.....	26
3.3	Methods of sub netting.....	27
3.3.1	Classful Method.....	27
3.3.1.1	Class A.....	29
3.3.1.2	Class B.....	30
3.3.1.3	Class C.....	30
3.3.2	Procedure of Sub netting.....	31
3.3.3	Classless Method.....	35
3.3.3.1	Fixed Length Subnet Mask.....	35
3.3.3.2	Variable Length Subnet Mask.....	37
3.4	Dynamic Host Configuration Protocol.....	40
3.5	Routing.....	42
3.5.1	Routing steps in any Router in the network.....	42
3.5.2	Static Routing.....	43
4	Chapter 4: Processes and examples	45
4.1	Processes.....	46
4.1.1	ANDing.....	46
4.1.2	ORing.....	47
4.2	Example.....	48
5	Chapter5: Configuration of Switches & Routers	56
5.1	Cisco Packet Tracer.....	57
5.2	Designing of Networks.....	60
5.2.1	Procedure of work.....	60
5.2.2	Cables.....	61
5.3	Examples.....	62
5.4	Configuration of Router and Switch.....	81

5.4.1	The Mode of Configuration.....	82
5.4.2	Configuration Steps.....	83
5.4.3	Basic Commands.....	84
5.5	Active IP on the Switch.....	86
5.6	Configuration of Router.....	88
5.6.1	Set IP-address.....	88
5.6.2	Static Routing.....	89
	References	92

About This Book

This book is for Beginner level, those who don't know anything about "The Internet Protocol" and the IP-address, with simple explanation and photos.

The Writer`s Letter

When you finish this book, don't stop, keep searching and practicing by using all programs that you found, because of the Network world doesn't stop. With my best wishes.

Mahdi Saleh

1

CHAPTER ONE



Chapter One: Introduction

A Network in the world of computers is said to be a collection of interconnected hosts, via some shared media which can be wired or wireless. A computer network enables its hosts to share and exchange data and information over the media. Network can be a Local Area Network spanned across an office or Metro Area Network spanned across a city or Wide Area Network which can be spanned across cities and provinces.

To reduce their design complexity, most networks are organized as a stack of **layers** or **levels**, each one built upon the one below it. The number of layers, the name of each layer, the contents of each layer, and the function of each layer differ from network to network.

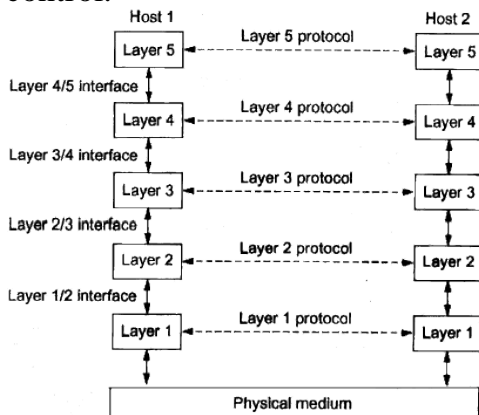
When Layer n on one machine carries on a conversation with layer n on another machine, the rules and conventions used in this conversation are collectively known as the layer n protocol.

A **Protocol** is an agreement between the communication parties on how communication is to proceed. In fact, the protocol itself can change in some layers without the layers above and below it even noticing. A list of protocols used by a certain system, one protocol per layer, is called a **protocol**

stack, and a set of layers and protocols is called **Network architecture**.

The glue that holds the whole Internet together is the network layer protocol **IP (Internet Protocol)**. Unlike older layer protocols, IP was designed from the beginning with internetworking in mind. A good way to think of the network layer is this: its job is to provide a best- effort (i.e., not guaranteed) way to transport packets from source to destination, without regard to whether these machines are on the same network or whether there are other networks in between them.

The internet protocol does not provide a reliable communication facility. There are no acknowledgments either end-to-end or hop-by-hop. There is no error control for data, only a header checksum. There are no retransmissions. There is no flow control.



As we mentioned before, the networks are organized as a stack of layers or levels, the number of layers depending on its references model, there are two references models (OSI References model and TCP/IP references model). In this book we will list the layers only to show where IP address works.

1.1 OSI References Model

This model was revised in 1995, it is called the ISO **OSI (Open System Interconnection)** References model because it deals with connecting open systems – that is, systems that are open for communication with other systems. It has Seven layers, these layers are:

- 1- Physical Layer.
- 2- Data link Layer.
- 3- Network Layer.
- 4- Transport Layer.
- 5- Session Layer.
- 6- Presentation Layer.
- 7- Application Layer.

1.2 TCP/ IP References Model

It was first described by Cerf and Kahn (1974), and later refined and defined as a standard in the Internet community (Braden, 1989). From nearly the beginning, the ability to connect multiple networks

in a seamless way was one of the major design goals. This model has four layers, these layers are:

- 1- Link Layer.
- 2- Internet Layer.
- 3- Transport Layer.
- 4- Application Layer.

The network layer (TCP/IP) or Internet layer (OSI) is responsible for carrying data from one host to another. It provides means to allocate logical addresses to hosts, and identify them uniquely using the same. Network layer takes data units from Transport Layer and cuts them into smaller unit called Data Packet. Network layer defines the data path; the packets should follow to reach the destination. Routers work on this layer and provide mechanism to route data to its destination.

The main two functions in these layers are:

- 1- Connection model:
Connectionless communication, For example, IP is connectionless, in that a datagram can travel from a sender to a recipient without the recipient having to send an acknowledgement. Connection-oriented protocols exist at other, higher layers of the OSI model.

2- Host addressing:

Every host in the network must have a unique address that determines where it is. This address is normally assigned from a hierarchical system.

The internet protocol implements two basic functions: addressing and fragmentation. This book will explain **the addressing function** only.

1.3 IP address

It is a numerical label assigned to each device (e.g., Computers, Printers...), it is like an Identification card of the device in the network.

There are two main versions of IP address, IP version4 and version6. In this part will know what the differences between them are.

1. IP address version Four (IPv4)

Its 32- bit addresses. Every host and router on the internet has an IP address that can be used in the source address and destination address fields of IP packets. It is important to note that an IP address does not actually refer to a host. It really refers to a network interface, so if a host is on two networks, it must have two IP addresses. However, in practice, most

hosts are on one network and thus have one IP address. In contrast, router has multiple interfaces and thus multiple IP addresses. IPv4 is described in IETF publication RFC 791 (September 1981), replacing an earlier definition (RFC 760, January 1980).

Example: 192.168.1.1

As an aside on numbering, IPv5 was an experimental real-time stream protocol that was never widely used.

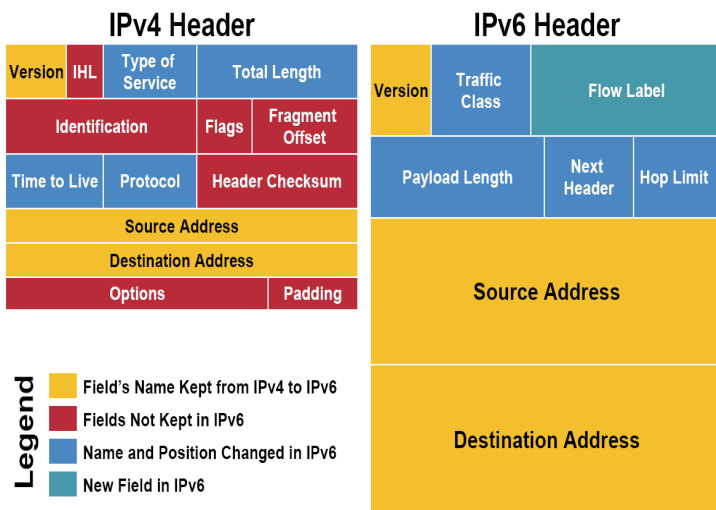
2. IP address version Six (IPv6)

It is a replacement design that does just that. It uses 128-bit addresses. It is a different network layer protocol that does not really interwork with IPv4, despite many similarities. Also, companies and users are not really sure why they should want IPv6 in any case. The result is that IPv6 is deployed and used on only a tiny fraction of the Internet (estimates are 1%) despite having been an internet standard since 1998. The next several years will be an interesting time, as the few remaining IPv4 addresses are allocated.

Example:

8000:0000:0000:0000:0123:4567:89AB:CDEF

The next Picture shows the Internet Header Format in Version 4 and Version 6



This book will explain IPv4 (classes and Sub netting and Routing) because it is the main version that used by organizations today.

2

CHAPTER TWO



Chapter Two: IP Address

In this chapter will discuss the algorithms that used to look up for IP address and the Package of IPv4.

2.1 IP Lookup

The primary role of routers is to forward packets toward their final destinations. To this purpose, a router must decide for each incoming packet where to send it next, that is, finding the address of the next-hop router as well as the exiting port through which the packet should be sent. This forwarding information is stored in a forwarding table that the router computes based on the information gathered by routing protocols. To consult the forwarding table, the router uses the packet's destination address as a key – this operation is called address lookup.

The algorithms that used in this operation (IP Lookup) are:

❖ Trie-Based Algorithms

1. Binary Trie
 2. Path-Compressed Trie
 3. Multi-Bit Trie
 4. Level Compression Trie
 5. Lulea Algorithm
 6. Tree Bitmap Algorithm
 7. Tree-Based Pipelined Search
 8. Binary Search on Prefix Lengths
 9. Binary Search on Prefix Range
- #### ❖ Hardware-Based Schemes

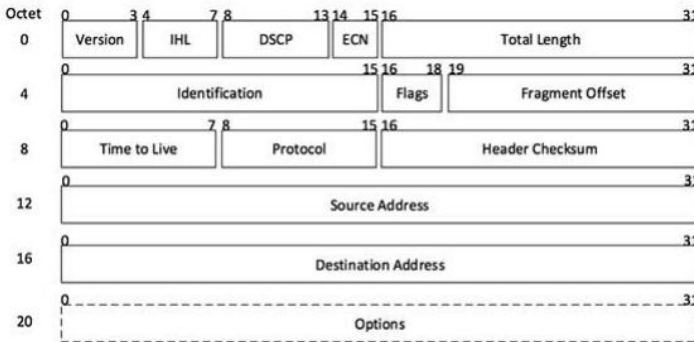
1. DIR-24-8-BASIC Scheme
2. DIR-Based Scheme with Bitmap Compression (BC-16-16)
3. Ternary CAM for Route Lookup
4. Two Algorithms for Reducing TCAM Entries
5. Reducing TCAM Power – CoolCAMs
6. TCAM-Based Distributed Parallel Lookup

2.2 IPv4 Package

Internet Protocol being a layer-3 protocol (OSI) takes data Segments from layer-4 (Transport) and divides it into packets. IP packet encapsulates data unit received from above layer and add to its own header information.



The encapsulated data is referred to as IP Payload. IP header contains all the necessary information to deliver the packet at the other end.



IP header includes much relevant information including Version Number, which, in this context, is 4. Other details are as follows:

- Version: Version no. of Internet Protocol used (e.g. IPv4)
- IHL: Internet Header Length; Length of entire IP header.
- DSCP: Differentiated Services Code Point; this is Type of Service.
- ECN: Explicit Congestion Notification; It carries information about the congestion seen in the route.
- Total Length: Length of entire IP Packet (including IP header and IP Payload).
- Identification: If IP packet is fragmented during the transmission, all the fragments contain same identification number to identify original IP packet they belong to.

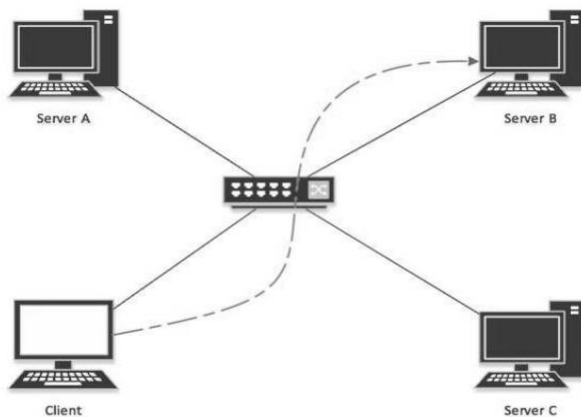
- Flags: As required by the network resources, if IP Packet is too large to handle, these ‘flags’ tell if they can be fragmented or not. In this 3-bit flag, the MSB is always set to ‘0’.
- Fragment Offset: This offset tells the exact position of the fragment in the original IP Packet.
- Time to Live: To avoid looping in the network, every packet is sent with some TTL value set, which tells the network how many routers (hops) this packet can cross. At each hop, its value is decremented by one and when the value reaches zero, the packet is discarded.
- Protocol: Tells the Network layer at the destination host, to which Protocol this packet belongs to, i.e. the next level Protocol. For example protocol number of ICMP is 1, TCP is 6 and UDP is 17.
- Header Checksum: This field is used to keep checksum value of entire header which is then used to check if the packet is received error-free.
- Source Address: 32-bit address of the Sender (or source) of the packet.
- Destination Address: 32-bit address of the Receiver (or destination) of the packet.

- Options: This is optional field, which is used if the value of IHL is greater than 5. These options may contain values for options such as Security, Record Route, Time Stamp, etc.

2.3 Addressing

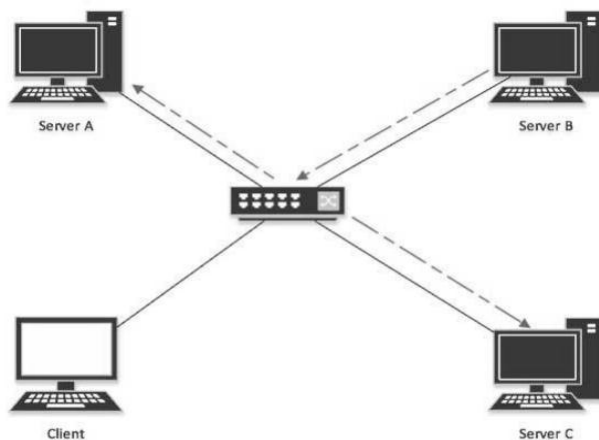
IPv4 supports three different types of addressing modes (Unicast, Multicast and Broadcast).

2.3.1 Unicast: In this mode, data is sent only to one destined host. The Destination Address field contains 32-bit IP address of the destination host. Here the client sends data to the targeted server:



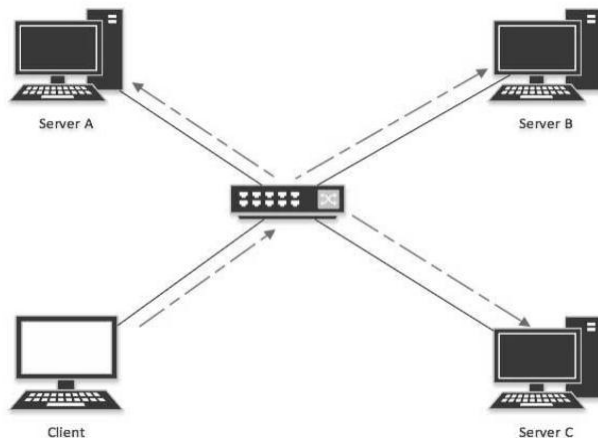
2.3.2 Multicast: This mode is a mix of (unicast and broadcast), i.e. the packet sent is neither destined to a single host nor all the hosts on the segment. In this

packet, the Destination Address contains a special address which starts with 224.x.x.x and can be entertained by more than one host.



Here a server sends packets which are entertained by more than one servers. Every network has one IP address reserved for the Network Number which represents the network and one IP address reserved for the Broadcast Address, which represents all the hosts in that network.

2.3.3 Broadcast: In this mode, the packet is addressed to all the hosts in a network segment. The Destination Address field contains a special broadcast address, i.e. 255.255.255.255. When a host sees this packet on the network, it is bound to process it. Here the client sends a packet, which is entertained by all the Servers:



2.4 Subnet Mask

The 32-bit IP address contains information about the host and its network. It is very necessary to distinguish both. For this, routers use Subnet Mask, which is as long as the size of the network address in the IP address. Subnet Mask is also 32 bits long.

Example:

IP address 192.168.1.0 with **subnet mask 255.255.255.0**

3

CHAPTER THREE



Chapter Three: Sub netting

A computer network can be as simple as two PCs connected together via a single copper cable or it can be grown up to the complexity where every computer in this world is connected to every other, called the Internet. A network then includes more and more components to reach its ultimate goal of data exchange. Below is a brief description of the components involved in computer network:

- **Hosts:** Hosts are said to be situated at ultimate end of the network, i.e. a host is a source of information and another host will be the destination. Information flows end to end between hosts. A host can be a user's PC, an internet Server, a database server etc.
- **Media:** If wired, then it can be copper cable, fiber optic cable, and coaxial cable. If wireless, it can be free-to-air radio frequency or some special wireless band. Wireless frequencies can be used to interconnect remote sites too.
- **Hub:** A hub is a multiport repeater and it is used to connect hosts in a LAN segment. Because of low throughputs hubs are now rarely used. Hub works on Layer-1 (Physical Layer) of OSI Model.
- **Switch:** A Switch is a multiport bridge and is used to connect hosts in a LAN segment.

Switches are much faster than Hubs and operate on wire speed. Switch works on Layer-2 (Data Link Layer), but Layer-3 (Network Layer) switches are also available.

- **Router:** A router is Layer-3 (Network Layer) device which makes routing decisions for the data/information sent for some remote destination. Routers make the core of any interconnected network and the Internet.
- **Gateways:** A software or combination of software and hardware put together, works for exchanging data among networks which are using different protocols for sharing data.
- **Firewall:** Software or combination of software and hardware, used to protect users' data from unintended recipients on the network/ internet.

All components in a network ultimately serve the hosts.

3.1 Host Addressing

Communication between hosts can happen only if they can identify each other on the network. In a single collision domain (where every packet sent on the segment by one host is heard by every other host) hosts can communicate directly via MAC address.

MAC address is a factory coded 48-bits hardware address which can also uniquely identify a host. But if a host wants to communicate with a remote host, i.e. not in the same segment or logically not connected, then some means of addressing is required to identify the remote host uniquely. A logical address is given to all hosts connected to Internet and this logical address is called **Internet Protocol Address**.

3.2 CIDR notation

Classless inter-domain routing (CIDR) is a set of Internet protocol (IP) standards that is used to create unique identifiers for networks and individual devices.

The ability to group blocks of addresses into a single routing network is the hallmark of CIDR, and the prefix standard used for interpreting IP addresses makes this possible. CIDR blocks share the first part of the bit sequence that comprises the binary representation of the IP address, and blocks are identified using the same decimal-dot CIDR notation system that is used for IPv4 addresses. For example, 10.10.1.16/32 is an address prefix with 32 bits, which is the highest number of bits allowed in IPv4. Addresses with identical prefixes and the same number of bits always belong to the same block. In

addition, larger blocks can be easily distinguished from smaller blocks by the length of the prefix. Short prefixes allow for more addresses while large prefixes identify small blocks.

- **The CIDR is equal to the number of 1's in Subnet mask.**

3.3 Methods of Sub netting

Network administrators can group devices and services into subnets that are determined by: Location, Organizational unit and Device type. There are two major methods of subnetting, these methods are:

- **Classful**
- **Classless**
 - **Fixed Length Subnet Mask**
 - **Variable Length Subnet Mask**

3.3.1 Classful Method

A Classful network is a network addressing architecture used in the Internet from 1981 until the introduction of Classless Inter-Domain Routing in 1993. The method divides the address space for Internet Protocol Version 4 (IPv4) into five address classes by address range. Classes A, B, C are networks of three different network sizes, i.e.

number of hosts for unicast addresses. Class D is for multicast. The class E address range is reserved for future or experimental purposes. Under classful networking, the subnet mask was implied by which address range (class) the address occupied and did not need to be specified separately.

Originally, a 32-bit IPv4 address was logically subdivided into the network number field, the most significant 8 bits of an address, which specified the particular network a host was attached to, and the local address, also called rest field (the rest of the address), which uniquely identifies a host connected to that network.

Table 1: Range of Classes

Class A
N: 0 – 127.0.0.0
Class B
N: 128 – 191.0.0.0
Class C
N: 192 – 223.0.0.0
Class D
N: 224 – 239.0.0.0
Class E
N: 240 – 255.0.0.0

N= Network ID

The IP address has four octets; each octet has 8 bits (1 byte), as shown:

First Byte	Second Byte	Third Byte	Fourth Byte
bbbbbbbbb	bbbbbbbbb	bbbbbbbbb	bbbbbbbbb

Each IP address can be written on either decimal or binary way by using this role for each octet:

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

3.3.1.1 Class A

In Class A only first Octet (Byte) is for Network ID, and the other 3 octets are for Hosts. So the number of network bits is (8).

First Byte	Second Byte	Third Byte	Fourth Byte
nnnnnnnn	hhhhhhhh	hhhhhhhh	hhhhhhhh

The number of networks will be $2^7 - 2 = 126$, and the number of hosts will be $2^{24} = 16,777,214$.

This example illustrates an IP address from Class A

First Byte	Second Byte	Third Byte	Fourth Byte
12.	0.	0.	0

3.3.1.2 Class B

In class **B** first octet and second octet are for network ID and the other 2 octets are for Hosts. So the number of network bits is (16)

First Byte	Second Byte	Third Byte	Fourth Byte
nnnnnnnn	nnnnnnnn	hhhhhhh	hhhhhhh

The number of networks will be $2^{14} = 16,382$ and the number of hosts will be $2^{16} - 2 = 65,534$

This example illustrates an IP address from Class **B**

First Byte	Second Byte	Third Byte	Fourth Byte
130.	10.	0.	0

3.3.1.3 Class C

In class **C** first, second and third octet for network ID and the last octet for hosts. So the number of network bits is (24).

First Byte	Second Byte	Third Byte	Fourth Byte
nnnnnnnn	nnnnnnnn	nnnnnnnn	hhhhhhh

The number of networks will be $2^{21} - 2 = 2,097,150$, and the number of hosts will be $2^8 - 2 = 254$

This example illustrates an IP address from class C

First Byte	Second Byte	Third Byte	Fourth Byte
192.	168.	10.	0

3.3.2 Procedure of Classful Subnetting

When we want to subnetting any network in Class A, we will follow these steps:

- 1- We will deal with the (**Subnet mask and CIDR notation**) to know how many bits we need to the Network, and the other bits will be for the hosts.
- 2- Convert the Subnet mask to the binary.
- 3- Number of (1s) for the Networks and Number of (0s) for the Hosts in subnet mask
 - No. Networks = 2^{1s}
 - No. Hosts = $2^{0s} - 2$
- 4- Block size = $2^{0s} \rightarrow = 256 - \text{last byte of subnet mask (not zero)}$

5- In Classful method we have 2 lost sub networks, so when we need two networks the result will be 4 networks (2 required + 2 lost)

Example: Subnet this IP address 192.168.10.0 255.255.255.0 to two subnets N1 and N2

Solution:

At the beginning, let`s write the IP address with subnet mask:

IP address = 192.168.10.0

Subnet mask = 255.255.255.0

Last byte of subnet mask = 0

The Class is : C because the first octet = 192

Because we have 2 networks with two lost network the result will be (4 Sub networks), so we will need 2 bits to get 4 sub networks.

- *We deal with the fourth octet (byte) in class C.*
- *Number of (1s) in the fourth octet used to determine the number of subnets.*
- *Number of remaining (0s) used to determine the number of available hosts at each subnet.*

1. $2^n \geq \text{no. of required networks}$
 $2^n \geq 3 \rightarrow n = 2$

$$\text{Number of subnet} = 2^2 = 4$$

255	255	255	192
bbbbbbbb	bbbbbbbb	bbbbbbbb	bbbbbbbb
11111111	11111111	11111111	11000000

New Subnet mask : 255.255.255.192

2. Number of **Hosts** = $2^h - 2$ where h = number of (0s) In our example $h=6$ so,

$$\text{Number of hosts} = 2^6 - 2 = 62$$

3. **Block size** = $2^{0s} = 2^6 = 64$

$$\text{Or : } 256 - 192 = 64$$

So, the range of each sub network will be:

Network ID	Broadcast ID	Use
1- 192.168.10.0/26	192.168.10.63 /26	No
2- 192.168.10.64/26	192.168.10.127/26	Yes
3- 192.168.10.128/26	192.168.10.191/26	Yes
4- 192.168.10.192/26	192.168.10.255/26	No

- The first sub network is not usable and the last one also.
- The usable sub networks are :
 - ✓ 192.168.10.64
 - ✓ 192.168.10.128

Check Point

Q1: Subnet this network address 172.16.0.0/17

to three sub networks (X1, X2, X3).

Q.2: Subnet this network address 172.16.0.0 / 20

to four sub network (X1, X2, Y1, Y2)

Q.3: Subnet this network address 172.16.0.0 / 24

to 2 sub networks (Z1, Z2)

Q.4: Subnet this network address 172.20.0.0 / 26

to 2 sub networks (X1, Y1)

Q.5: Subnet this network address 10.0.0.0 / 12

to 5 sub networks (X1, X2, X3, X4, X5)

Hints: You can use the CIDR to get the subnet mask

Hints: You have 2 lost sub networks don't forget

3.3.3 Classless Method

Classless addressing system is also known as CIDR (Classless Inter-Domain Routing). Classless Inter-Domain Routing: is a method for allocating IP addresses and IP routing. The Internet Engineering Task Force introduced CIDR in 1993 to replace the previous addressing architecture of Classful network design in the Internet. Its goal was to slow the growth of routing tables on routers across the Internet, and to help slow the rapid exhaustion of IPv4 addresses. In this method there is two methods to subnet the network, these two methods are: FLSM & VLSM

3.3.3.1 Fixed Length Subnet Mask

This method depends on the **number of required sub networks**, so each sub network will have the same range. The use of an FLSM saves a router the task of having to handle an entire IP address because the router deals only with the digits selected by the mask. Nevertheless, this method of subnet masking can result in inefficient use of IP address space because subnets are rarely filled to capacity. The procedure of this method will be clear in the next example

Example: by using *FLSM* method Subnet this Network 192.168.30.0/26 in three subnets as shown:

- 14 hosts
- 5 hosts
- 2 hosts

Solution:

At the beginning we will use the **number of required networks**

$$2^n \geq \text{no. of required networks}$$

$$2^n \geq 3 \rightarrow n = 2$$

The new CIDR notation is: **$n + \text{old CIDR notation}$**

$$\text{New CIDR} = 2 + 26 = 28$$

$$\text{Subnet mask} = 255.255.255.240$$

$$h = \text{total CIDR} - \text{New CIDR}$$

$$h = 32 - 28$$

$$h = 4$$

$$\text{Block size} = 2^h \rightarrow 2^4 = 16$$

Now let's show the range of each sub network in the next table:

Network ID	Broadcast ID
1- 192.168.30.00/28	192.168.30.15/28
2- 192.168.30.16/28	192.168.30.31/28
3- 192.168.30.32/28	192.168.30.47/28
4- 192.168.30.48/28	192.168.30.63/28

This procedure can use for any network that needs sub netting in this method.

3.3.3.2 Variable Length Subnet Mask

In Classless addressing subnets can be designed to fit your needs. Subnets can be of different sizes and this gives better usage of hosts IP addresses. In Variable lengths subnetting we start with the largest subnet(s) followed by the rest discerningly.

In order to use VLSM, a network administrator must use a routing protocol that supports it, such as Routing Information Protocol v2 (RIPv2), Open Shortest Path First (OSPF), Intermediate System-to-Intermediate System (IS-IS), Enhanced Interior Gateway Routing Protocol (EIGRP) and Border Gateway Protocol (BGP).

Example: by using VLSM Subnet this Network 192.168.30.0/26 in three subnets:

A- 14 Hosts

B- 5 Hosts

C- 2 Hosts

Solution:

At the beginning we will use the biggest network with biggest number of hosts. And in this example the network A with 14 hosts, so we will begin our subnet with it.

*Block size: $2^h - 2 \geq 14 \rightarrow h = 4$ 11**bb** 0000*

So the block size 16 hosts

New CIDR: $32 - 4 = 28$

*Because we have two bits **bb**, so we will have **four** networks*

No. Sub networks = $2^2 = 4$

In the table we will write only last 2 bytes of IP-address, the user can write all IP-address or only the last two bytes.

Always the first subnet will go to the first request (14 hosts).

192.168.30.00/28			
A	2	3	4
30.00/28	30.16/28	30.32/28	30.48/28
30.15 /28	30.31/28	30.47/28	30.63/28

❖ *B with 5 hosts*

Block size: $2^h - 2 \geq 5 \rightarrow h = 3$ 1111 b 000

So the block size = 8 hosts

New CIDR: $32 - 3 = 29$

192.168.30.00/28			
A	B	3	4
	30.16/29		
	30.23 /29		
30.00/28		30.32/28	30.48/28
	Remind		
30.15 /28	30.24/29	30.47/28	30.63/28
	30.31/29		

❖ *C with 2 hosts*

Block size: $2^h - 2 \geq 2 \rightarrow h = 2$ 11111 b 00

So the block size = 4 hosts

New CIDR: $32 - 2 = 30$

192.168.30.00/28			
A	B	3	4
	30.16/29 30.23 /29		
	C	30.32/28	30.48/28
30.00/28	30.24/30 30.27/30		
30.15 /28			
	Reminder		
	30.28/30		
	30.31/30		

Now we can find the remind IPs (available)

- ✓ 192.168.30.28/30 – 192.168.30.31/30
- ✓ 192.168.30.32/28 – 192.168.30.47/28
- ✓ 192.168.30.48/28 – 192.168.30.63/28

This sub networks can be used in the future

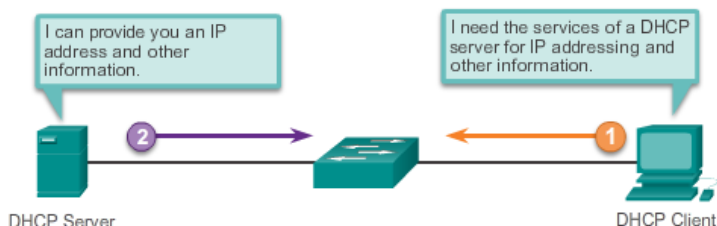
3.4 Dynamic Host Configuration Protocol

Every device that connects to a network needs a unique IP address. Network administrators assign static IP addresses to routers, servers, printers, and other network devices whose locations (physical and logical) are not likely to change. These are usually devices that provide services to users and devices on

the network; therefore, the addresses assigned to them should remain constant. Additionally, static addresses enable administrators to manage these devices remotely. It is easier for network administrators to access a device when they can easily determine its IP address.

However, computers and users in an organization often change locations, physically and logically. It can be difficult and time consuming for administrators to assign new IP addresses every time an employee moves. Additionally, for mobile employees working from remote locations, manually setting the correct network parameters can be challenging. Even for desktop clients, the manual assignment of IP addresses and other addressing information presents an administrative burden, especially as the network grows.

Introducing a Dynamic Host Configuration Protocol (DHCP) server to the local network simplifies IP address assignment to both desktop and mobile devices. Using a centralized DHCP server enables organizations to administer all dynamic IP address assignments from a single server. This practice makes IP address management more effective and ensures consistency across the organization, including branch offices.



- **The practise example will be in the Chapter 5**

3.5 Routing

It is the process of moving a packet of data from source to destination, routing is usually performed by a dedicated device called a router, Routing is a key feature of the Internet because it enables messages to pass from one computer to another and eventually reach the target machine. Each intermediary computer performs routing by passing along the message to the next computer. Part of this process involves analysing a routing tablet to determine the best path.

3.5.1 Routing steps in any Router in the network

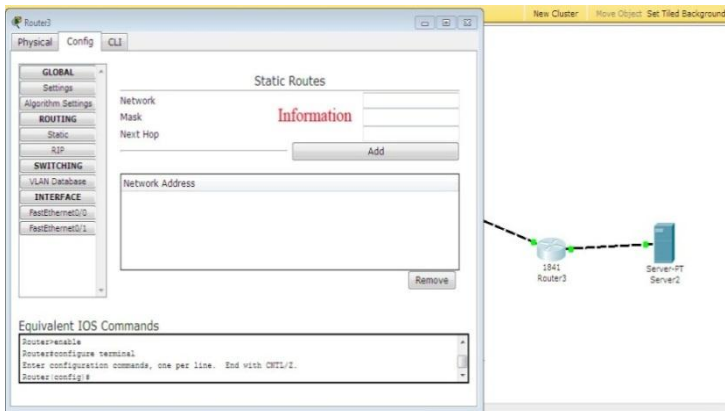
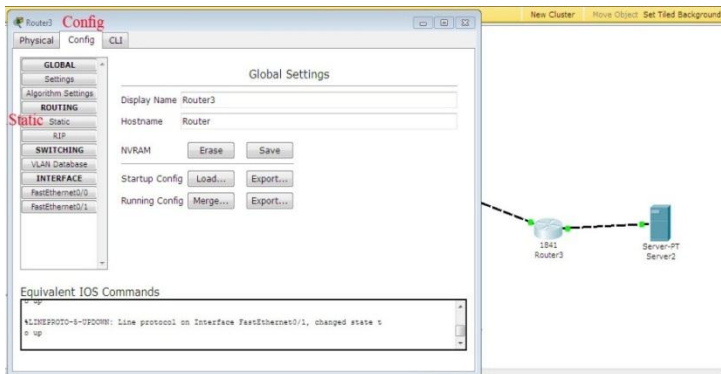
- Firstly, we should select the Network IP and it's Subnet mask.
- Secondly, we must select the next hop.

- Finally, write this information in the routing static in the router.

This process called **Dynamic Routing** and there is another way to do this process statically, called **Static Routing**, we will explain it in Chapter 5.

3.5.2 Static Routing

- 1- Double click on the Router >> select Configure.
- 2- Choose from **Routing >> Static**
- 3- Now we can write the Information (Network, Subnet mask and Next hop).
 - **Network:** The IP of the network that we want to connect to it.
 - **Subnet mask:** It is the subnet of the network that we want to connect to it.
 - **Next hop:** The IP of the port of the next router.
- 4 We will repeat these steps on all routers in the network.
- 5 More examples in **chapter 5**



4

CHAPTER FOUR



Chapter 4: Processes and examples

In this chapter, we will explain how to deal with any question in the sub netting of networks.

4.1 Processes

There are two main processes used to find the first and last IP-address in the block, these two processes are (ANDing, ORing)

4.1.1 ANDing

It's used to know the first IP-address in the network (network ID). To use this method follow these steps:

- Convert the given IP-address to the binary.
- Convert the subnet mask to the binary.
- ANDing between them.
- Convert the result to the decimal.

Example: What is the Network ID of this IP-address 192.168.10.13/24

IP: 11000000.10101000.10100000.11010000

SM: 11111111.11111111.11111111.00000000

N ID:11000000.10101000.10100000.00000000

N ID:192.168.10.0

4.1.2 ORing

It's used to know the last IP-address in the network (Broadcast ID). To use this method follow these steps:

- Convert the given IP-address to the binary.
- Convert the subnet mask to the binary.
- Replace any (0) to (1) and any (1) to (0) in the subnet mask.
- ORing between them.
- Convert the result to the decimal.

Example: What is the Broadcast ID of this address 192.168.35.8/25

SM: 11111111.11111111.11111111.10000000

IP: 11000000.10101000.00100011.00001000

SM: 00000000.00000000.00000000.01111111

N ID: 11000000.10101000.00100011.01111111

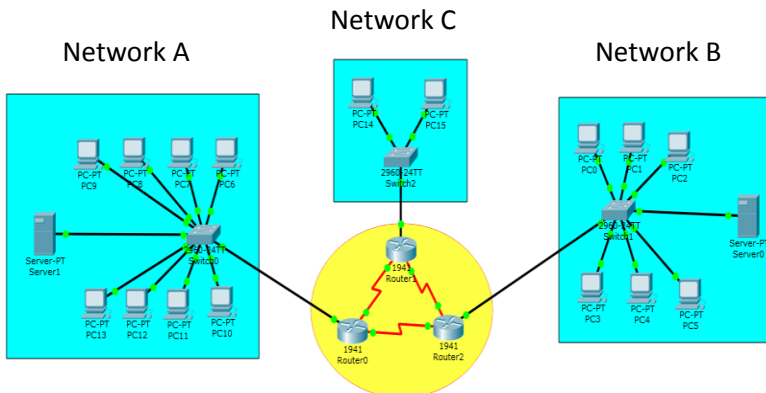
N ID: 192.168.35.127

4.2 Example

We will explain one example and the others will be solved in the same way with different IP-addresses.

Q)The Block 192.168.10.0/26 is sub netted as shown in the figure, considering the followings:

- The gateway takes the 1st usable address in each subnet.
- The DHCP servers takes the 2nd usable address in each subnet
- PCs will take the rest of IP-addresses in each subnet.



Solution:

Because of the number of hosts is different, we will use (VLSM) method.

Determine the largest sub network.

- ***Network A:*** (8 PCs + 1 Server = 9 hosts)
- ***Network B:*** (6 PCs + 1 Server = 7 hosts)
- ***Network C:*** (2 PCs = 2 hosts)

Now, we will begin with the Network A because it has the largest number of hosts (9).

Network A:

$9 \text{ hosts} + (1 \text{ default gateway}) + (1 \text{ Net ID}) + (1 \text{ B.C. ID}) = 12$

So the total IP-addresses on the Network A is 12 IPs

IP : 192.168.10.0/26

Block Size = $2^h - 2 \geq 12 \rightarrow h = 4$

So the block size will be (16 IP-addresses)

h = Number of zeros in the last byte in the Subnet mask:

/26 h=4

11111111.11111111.11111111.11 bb **0000**

No. Sub networks = $2^b \rightarrow 2^2 = 4$

New CIDR: $26 + b \rightarrow 26 + 2 = 28$

In this table we will write only last two bytes:

192.168.10.00/26			
A	2	3	4
10.00/28	10.16/28	10.32/28	10.48/28
10.15/28	10.31/28	10.47/28	10.63/28

Network B:

$7\text{hosts} + (1\text{default gateway}) + (1\text{Net ID}) + (1\text{B.C. ID}) = 10$

It will begin from the end of the network A.

IP: 192.168.10.16 /28

Block size: $2^h - 2 \geq 10 \rightarrow h = 4$

New CIDR: Still /28 because of the block size is still same as A, there is no change.

The Network B will take the second subnet block.

192.168.10.00/26			
A	B	3	4
10.00/28	10.16/28	10.32/28	10.48/28
10.15/28	10.31/28	10.47/28	10.63/28

Network C:

$2\text{hosts} + (1\text{default gateway}) + (1\text{Net ID}) + (1\text{B.C. ID}) = 5$

It will begin from the end of the Network B.

IP: 192.168.10.32/28

Block size: $2^h - 2 \geq 5 \rightarrow h = 3$

So the Block size will be (8 IP-addresses)

h = Number of zeros in the last byte in the Subnet mask:

/28 h=3

11111111.11111111.11111111.1111 b **000**

No. Sub Networks = $2^b \rightarrow 2^1 = 2$

New CIDR: $28 + b \rightarrow 28 + 1 = 29$

192.168.10.00/26			
		3	
		10.32/29	
A	B	10.39/29	4
10.00/28	10.16/28		10.48/28
10.15/28	10.31/28	Reminder	10.63/28
		10.40/29	
		10.47/29	

Now the main three networks completed, but there is three networks that connects the routers with each other.

- a) R0 to R1
- b) R1 to R2
- c) R2 to R0

The three networks are the same Block size (2 hosts), and the total hosts are:

$$2\text{hosts} + 1 \text{ Net ID} + 1 \text{ B.C. ID} = 4$$

IP: 192.168.10.40 / 29

Block size: $2^h - 2 \geq 4 \rightarrow h = 2$

So the Block size will be (4 IP-addresses)

h= Number of zeros in the last byte in the Subnet mask:

$$\frac{\text{11111111.11111111.11111111.11111111}}{29} \quad \text{h}=2 \quad \text{b} \text{00}$$

No. Sub Networks = $2^b \rightarrow 2^1 = 2$

New CIDR: $29 + b \rightarrow 29 + 1 = 30$

192.168.10.00/26			
A 10.00/28	B 10.16/28	C 10.32/29	c 10.48/30
10.15/28	10.31/28	10.39/29	10.51/30
		a 10.40/30	Reminder1 10.52/30
		10.43/30	10.55/30
		b 10.44/30	Reminder2 10.56/29
		10.47/30	10.63/29

The Result:

Network A: 192.168.10.00/28 – 192.168.10.15/28

Network B: 192.168.10.16/28 – 192.168.10.31/28

Network C: 192.168.10.32/29 – 192.168.10.39/29

Network a: 192.168.10.40/30 – 192.168.10.43/30

Network b: 192.168.10.44/30 – 192.168.10.47/30

Network c: 192.168.10.48/30 – 192.168.10.51/30

Reminder1: 192.168.10.52/30 – 192.168.10.55/30

Reminder2: 192.168.10.56/29 – 192.168.10.63/29

Other examples in the next page should be solved by the user himself. (Using same procedure in the previous example).

Check Point

- ❖ **Q1** If you know that this IP **177.10.30.0/20** sub netted to three sub networks, these networks have:
 - **20** hosts
 - **13** hosts
 - **4** hosts

- ❖ What is the range of each Network? Write it and **Design** these networks by using Cisco packet tracer.

- ❖ **Q2** An organization bought This IP **130.15.4.0/24** from ISP, The organization needs **9** hosts to the employees room and **2** hosts to the employer room. **Subnet** and **Design** this network by using Cisco packet tracer.

- ❖ **Q3** In your college, there are four classes need Internet in its computers. The first class has **40 PCs**, the second class has **29 PCs**, the third class is network laboratory needs **13 PCs** for its hosts and the last class needs **1 PC**. If you know that the IP address is **140.60.30.0/25** **Subnet** this network and **design** it by using Cisco packet tracer.

- ❖ **Q4** In the company of Communication need **56** hosts distributed on four rooms equally. If you know that the IP is **120.20.15.0/26** what is the range of each network that will appear after subnet. Design these networks by Cisco packet tracer.

- ❖ **Q5** If you know that the IP address is **192.168.15.0/27** and you need just **1** IP for your PC what will you do? Design this network by Cisco packet tracer.

- ❖ **Q6** If you know that this IP **192.168.10.3 /28** is one IP in range. What is the network IP and the Broadcast IP. Design this network by using Cisco packet tracer.

- ❖ **Q7** An Employer need **three** IPs in four rooms (each one has 3) in his company, He bought an IP from ISP, This IP **154.90.10.0/26**. Design this network by using Cisco packet tracer.

- ❖ **Q8** To get **256** networks each network has **254** usable IPs What will you do if you know that the IP address is **210.70.0.0/16**.

5

CHAPTER FIVE

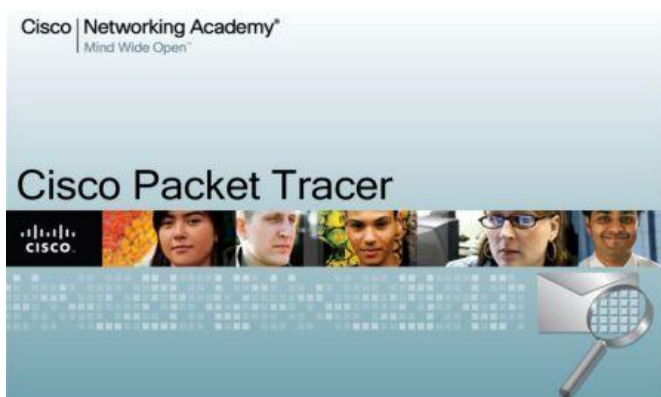


Chapter5: Configuration of Switches & Routers

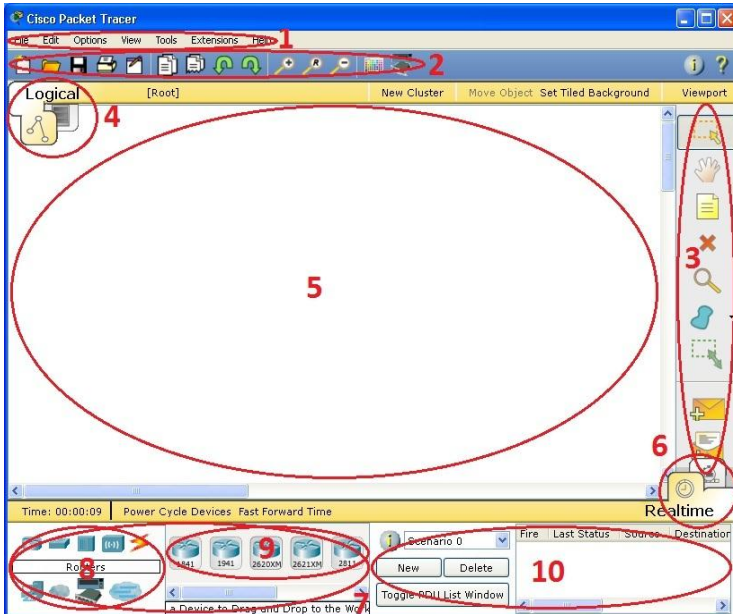
In this chapter we will explain how to configure Switches and Routers by using Cisco Packet Tracer.

5.1 Cisco Packet Tracer

Cisco Packet Tracer is a powerful network simulation, visualization, collaboration, and assessment tool that allows students to experiment with network designs and behavior. As an integral part of the Networking Academy learning experience, Packet Tracer provides simulation, visualization, authoring, assessment, and collaboration capabilities and facilitates the teaching and learning of complex technology concepts.



When you open Packet Tracer, by default you will be presented with the following interface:



1	Menu Bar	This bar provides the File, Edit, Options, View, Tools, Extensions, and Help menus. You will find basic commands such as Open, Save, Save as Pkz, Print, and Preferences in these menus. You will also be able to access the Activity Wizard from the Extensions menu.
2	Main Tool Bar	This bar provides shortcut icons to the File and Edit menu commands.
3	Common Tools Bar	This bar provides access to these commonly used workspace tools: Select, Move Layout, Place Note, Delete, Inspect, Resize Shape, Add Simple PDU, and Add Complex PDU. See "Workspace Basics" for more information.

4	Logical/Physical Workspace and Navigation Bar	You can toggle between the Physical Workspace and the Logical Workspace with the tabs on this bar. In Logical Workspace, this bar also allows you to go back to a previous level in a cluster, create a New Cluster, Move Object, Set Tiled Background, and Viewport. In Physical Workspace, this bar allows you to navigate through physical locations, create a New City, create a New Building, create a New Closet, Move Object, apply a Grid to the background, Set Background, and go to the Working Closet.
5	Workspace	This area is where you will create your network, watch simulations, and view many kinds of information and statistics.
6	Realtime/Simulation Bar	You can toggle between Realtime Mode and Simulation Mode with the tabs on this bar. This bar also provides buttons to Power Cycle Devices and Fast Forward Time as well as the Play Control buttons and the Event List toggle button in Simulation Mode. Also, it contains a clock that displays the relative Time in Realtime Mode and Simulation Mode.
7	Network Component Box	This box is where you choose devices and connections to put into the workspace. It contains the Device-Type Selection Box and the Device-Specific Selection Box.
8	Device-Type Selection Box	This box contains the type of devices and connections available in Packet Tracer. The Device-Specific Selection Box will change depending on which type of device you choose.
9	Device-Specific Selection Box	This box is where you choose specifically which devices you want to put in your network and which

		connections to make.
10	User Created Packet Window*	This window manages the packets you put in the network during simulation scenarios. See the "Simulation Mode" section for more details.

5.2 Designing of Networks

To be able to design your networks you will need a special laboratory (Networks Lab), it is difficult to get one because of the cost of devices such as (switches or Computers) so the user will need Cisco packet tracer. It is a virtual lab that contains all main devices of networks.

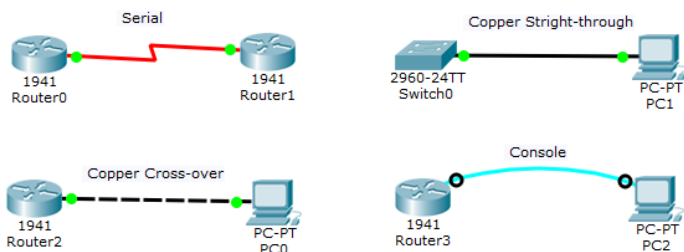
5.2.1 Procedure of work

1. Choose your devices from (**Device-Type Selection Box**) like (Pcs, Switches, Routers,,,,).
2. Connect your networks with suitable cables (straight, cross, console ,,,,).
3. Complete the information of devices like (IP, Subnet mask,,,,).
4. Check the connectivity of the networks.

5.2.2 Cables

To choose the right cable, the designer should know that there is more than one cable and each two devices has special cable to connect. The main three Cables that use in the networks are:

- a) **Console:** when the designer needs to make a configuration to the **Router/Switch**, he will use this type of connection.
- b) **Copper Straight – Through:** when the designer needs to connect two devices and these devices are different (e.g. **Pc – Switch**,,, etc.).
- c) **Copper Cross – Over:** when the designer needs to connect two devices and these devices are similar (e.g. **Pc – Router**,,,, etc.).
- d) **Serial:** When the designer needs to connect two routers. He also can use the cable in the point(c)



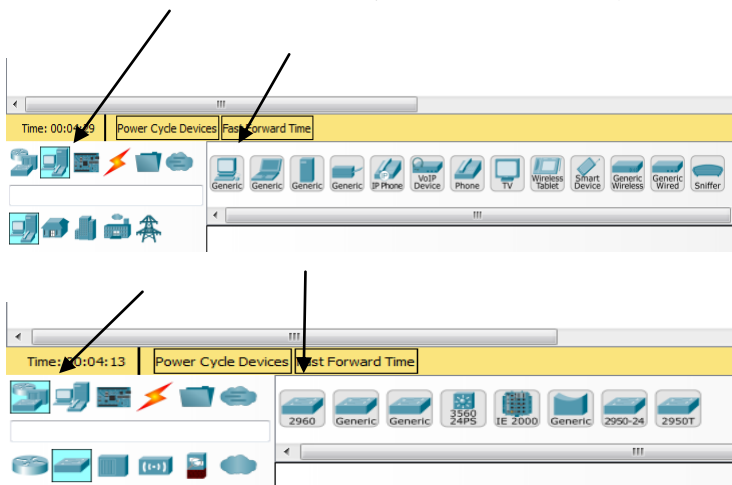
5.3 Examples

Example One: Design a network that has one switch with two PCs. Use these IP addresses:

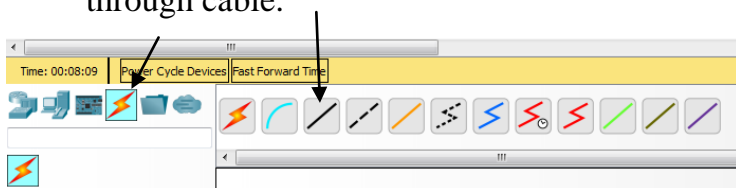
192.168.1.1 for PC0 192.168.1.2 for PC1

Solution:

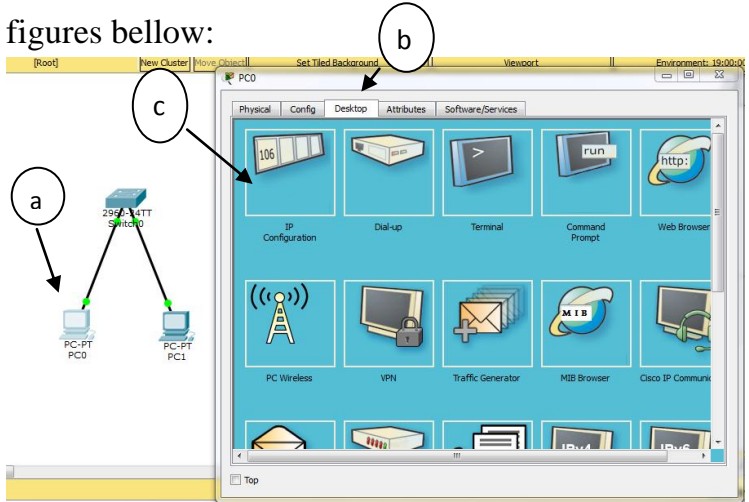
- 1. Choose the devices (1 switch & 2 PCs)*



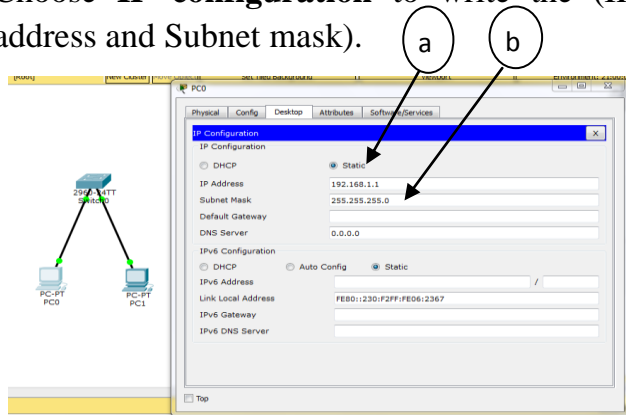
- 2. Connect the devices with each other, the designer will need only copper straight-through cable.*



3. Enter the information to the devices, like (IP, Subnet Mask) to be able to exchange the resources with each other, as shown in the figures below:



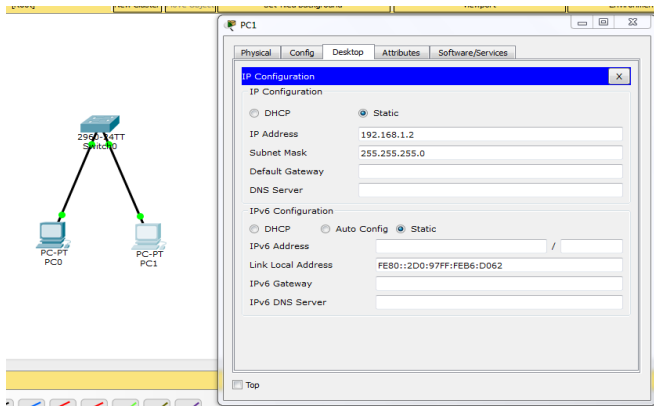
- a) Double click on **Pc0**.
- b) Choose **Desktop**.
- c) Choose **IP configuration** to write the (IP address and Subnet mask).



- a) Choose **Static** to be able to write your special Information

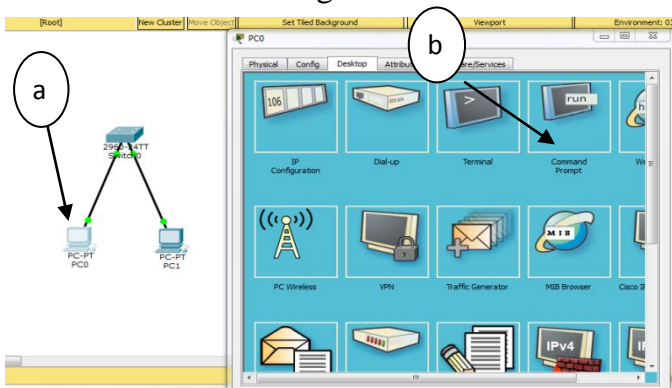
b) Write the IP address and subnet mask in these text boxes as shown in figure above.

Repeat these steps on the **PC1** with different information.

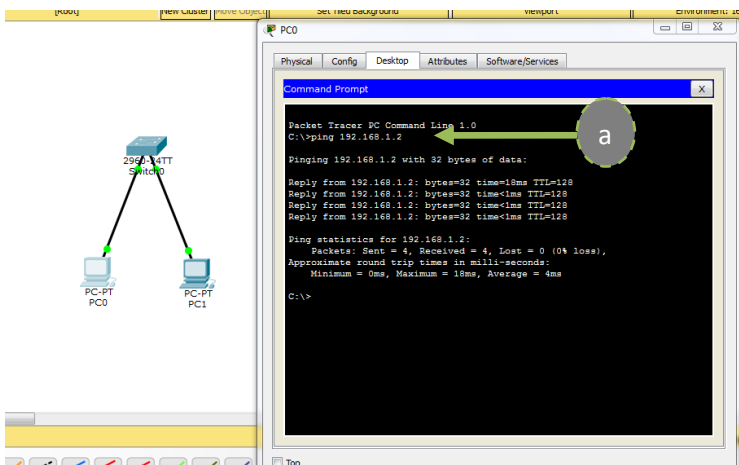


The switch doesn't have IP address because it depends on MAC address only (physical address).

4. Check the connectivity between these devices as shown in the figures below:



- a) Double Click on **Pc0**.
- b) Choose **Command Prompt** to write the commands.



- a) Here we will write the commands.
- b) The command that check the connectivity between the devices called "**Ping**". This command is written by this method
Ping IP-address of the other Pc
- c) In **Pc0** we will write the IP-address of **Pc1**:
C:\ Ping 192.168.1.2
- d) The result will be four Messages that sent successfully from Pc0 to Pc1with special TTL.
- e) If there is an error in the network, the result will be "**Request timed out**", it means that the designer did a mistake. So be careful when you design the network.

- In the "Ping" command there is a space between the word 'Ping' and the IP-address.
- Be careful when you write the command because any error in the command the device will reject it.

This procedure should be repeated in each network, because these are the basic steps of the LAN.

Example Two: Design a network that has one router with two Pcs. Use these IP-addresses

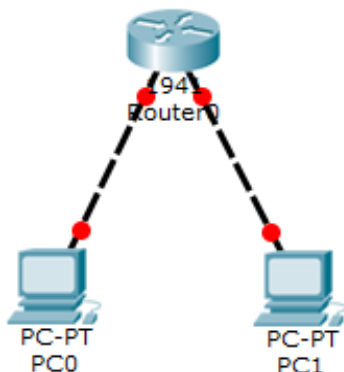
192.168.1.0 for N1

192.168.2.0 For N2

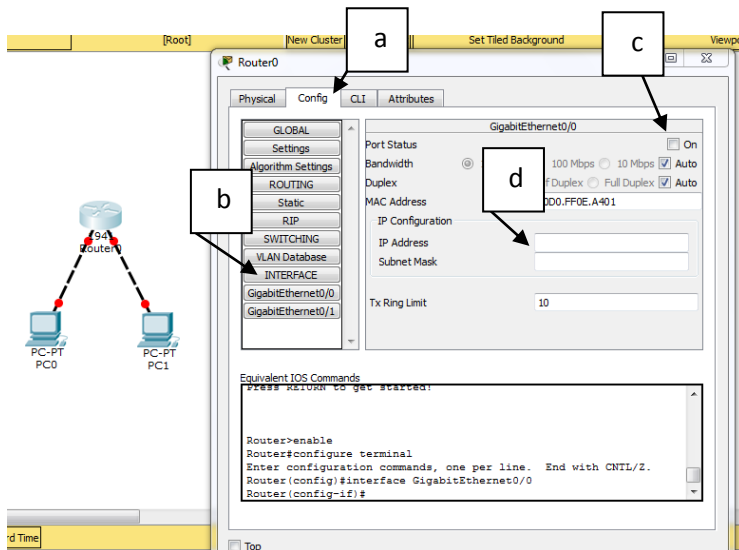
Solution:

Because there is a router here, the steps will begin from it. The router has ports and each port is considered as a separate Network. Each port has (IP-address and Subnet Mask). The IP-address of the port is called (Default Gateway) in each device connected to the router.

1. Connect the Network as shown:

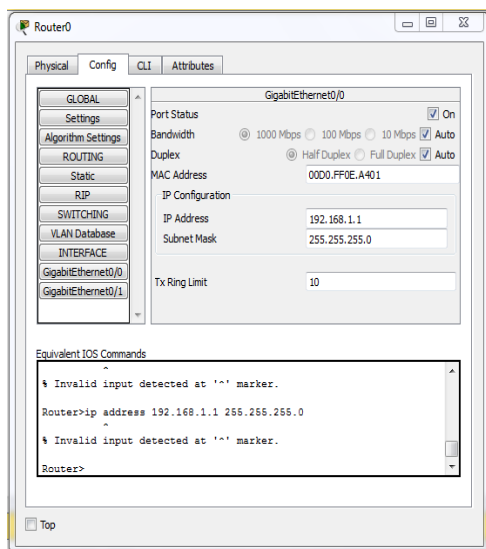
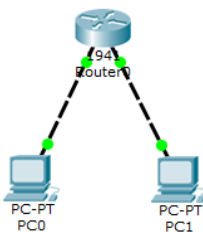


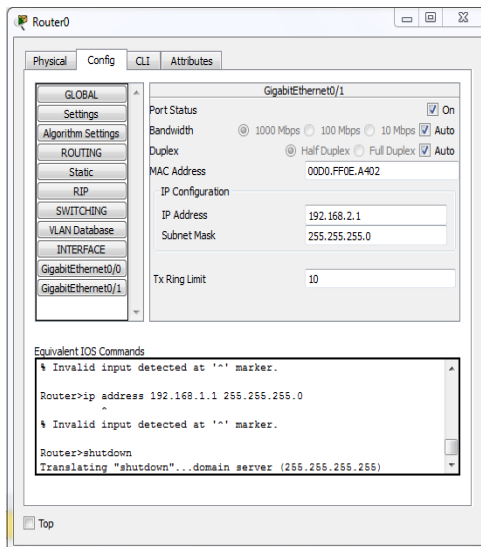
2. Double Click on the router,



- a) Choose "**Config**" to modify the information of the **ports**.
- b) Choose "**Interface**" then all Ports of the routers will show, here the route has two ports (Gigabit Ethernet0/0 and Gigabit Ethernet0/1)

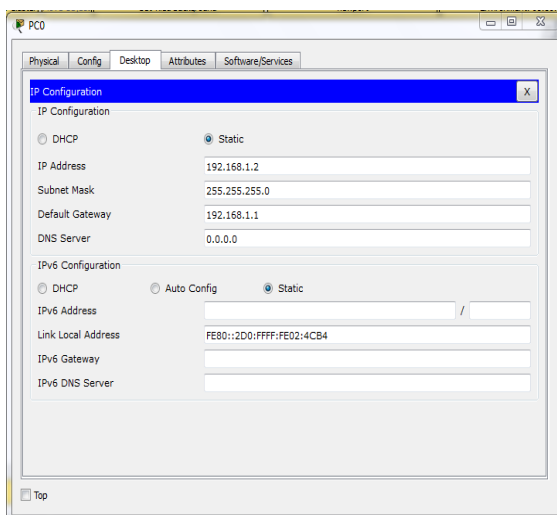
- c) Activate the port by clicking on the "On" check box.
- d) Enter (IP-address and Subnet Mask) for the first port. **Repeat this step on the other port.** Each port has different IP-address because each port represents different Network. So in the port1(Gigabit Ethernet0/0) the IP-address will be **192.168.1.1** and in the port2 (Gigabit Ethernet0/1) the IP-address will be **192.168.2.1**

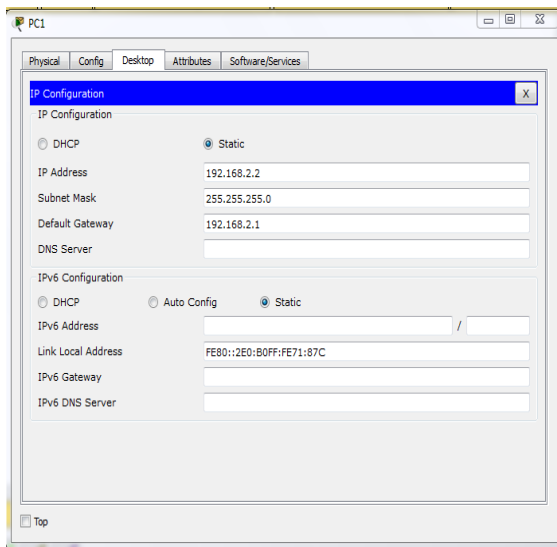




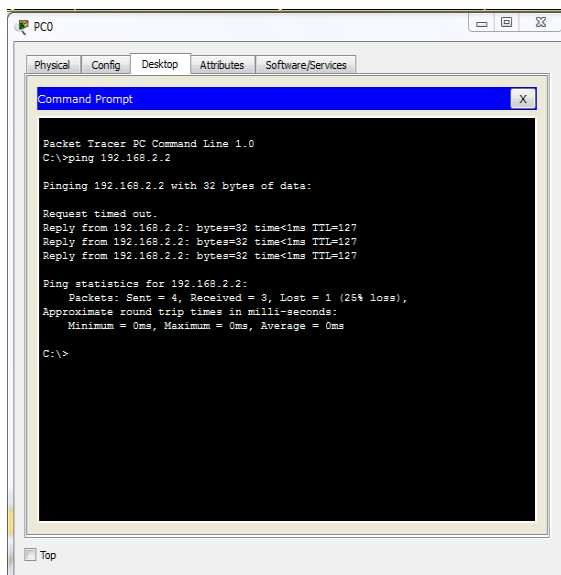
All Information of router completed.

3- Enter information on each Pc. As shown in the figure:

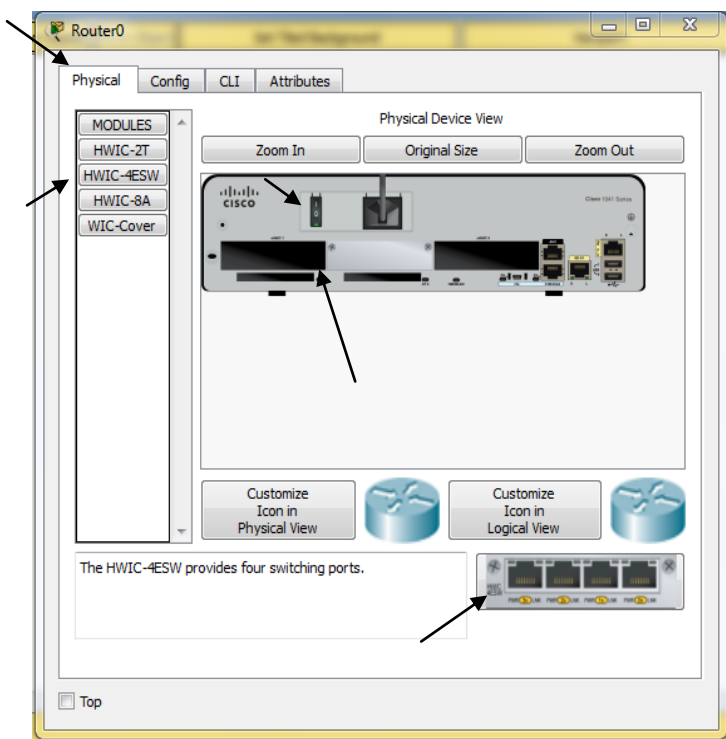




- 4- Now Check the connectivity between these devices by using "**Ping**" command.



- Router Device has Two Ports, if we want to increase this number then follow these steps:
 - 1- Double Click on the **Router** Device.
 - 2- Turn off the Router.
 - 3- Drag and drop "HWIC-4ESW" port in the Version7 or " WIC-1ENET " port in the previous versions.



- The Figure above highlights the steps of adding ports to the Router.
- You should power off the device before and power on after the process.

- In these two examples we will illustrate the procedure of the design of any network because each network has router and switch and end devices (main devices of each network).

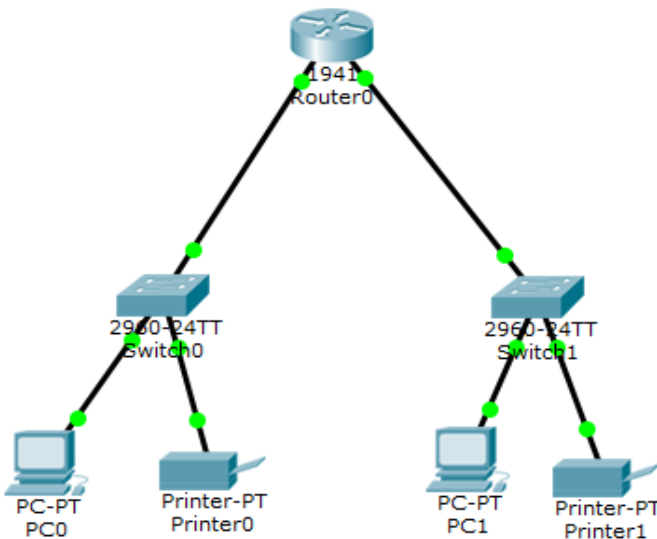
Example Three: Design Two LANs with one Router, each LAN has 1 Pc and 1 Printer. Use these IP-address:

LAN1:192.168.1.0/24

LAN2:10.0.0.0/8

Solution:

- 1- We will need 1Router, 2 Switches, 2 Pcs and 2 Printer



- 2- Set the information in each device after the designing as we did in the previous examples.
- 3- Check the connectivity.

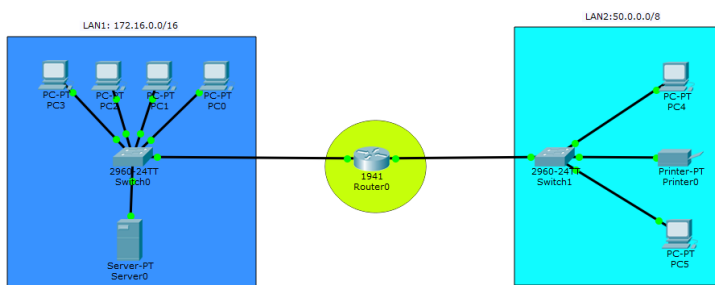
Example Four: Design a Network that has Two LANs, In the first LAN there are four PCs with One Server and in the second LAN there is two Pcs and one printer. The LANs connects to the Router. Use these IP-addresses:

LAN1: 172.16.0.0/16

LAN2:50.0.0.0/8

Solution:

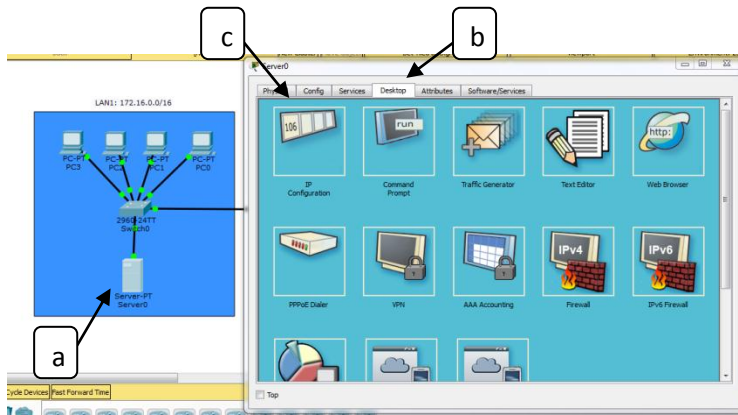
At the beginning design the networks and put all devices then connect them as shown in figure bellow:



Now set the IP-address for each device in LAN2, but in the LAN1 there is a DHCP server, thus it will be different.

To set the DHCP in the Network there are 3 steps, these steps are:

1- Set an IP-address to the server:

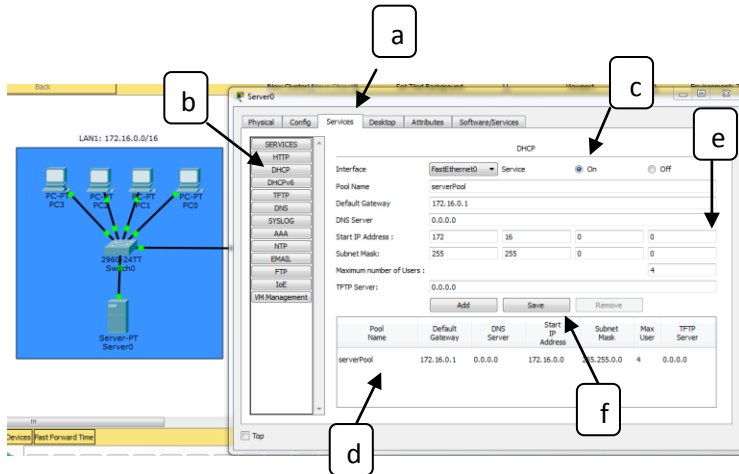


*a) Double click on **Server***

*b) Choose **Desktop***

*c) Choose **IP configuration** to set the information*

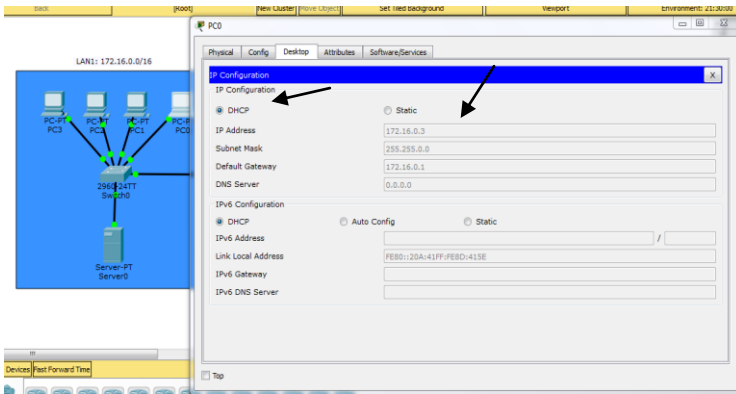
2- Set the DHCP information.



- a) Choose **Services**.
- b) Choose **DHCP**.
- c) Choose **On** to activate the DHCP.
- d) Choose the **Server pool** that already exist in the DHCP setting
- e) Set the Information that you want(Default gateway, start IP-address, Subnet mask and maximum number of users).
- f) Choose **Save**.

To add another Server pool, choose **Add** instead of **Save**.

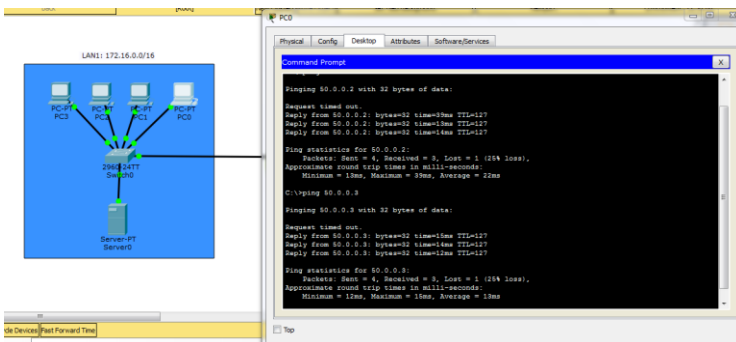
3- Set the IP-address of each Pc to **DHCP** not **Static**, thus the result will be like the figure bellow:



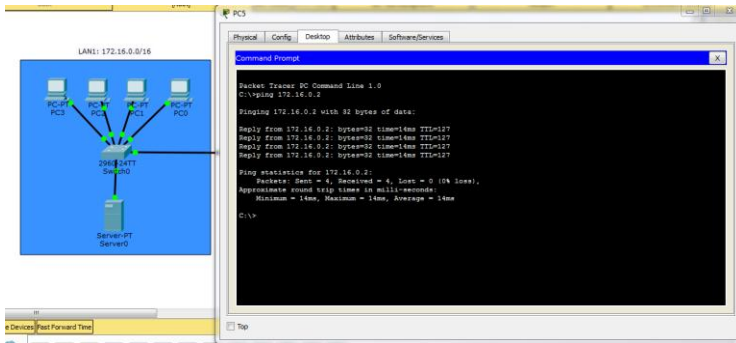
As you see in the figure above, we cannot modify the IP-address or other information in this window because it is under the DHCP control.

*Now we can check the connectivity between devices by using **Ping** command. Like the figure bellow:*

✓ **Ping from PC0 in LAN1 to PC4 in LAN2**



✓ *Ping from PC5 in LAN2 to the Server in LAN1*



Example Five: Design a network that has two routers each router has two LANs each LAN has Two PCs. Use this IP-addresses:

LAN1:20.0.0.0/8 LAN3:170.20.0.0/16

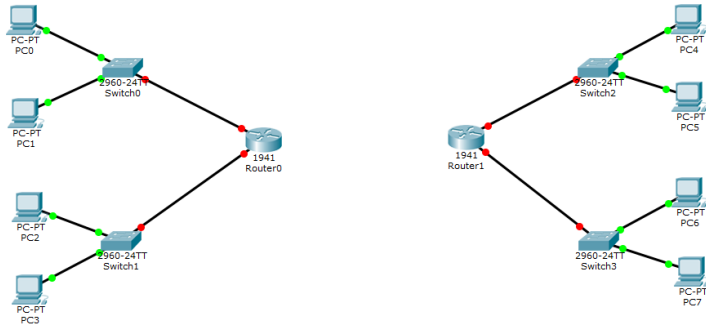
LAN2:30.0.0.0/8 LAN4:180.10.0.0/16

LAN5:192.168.10.0/24

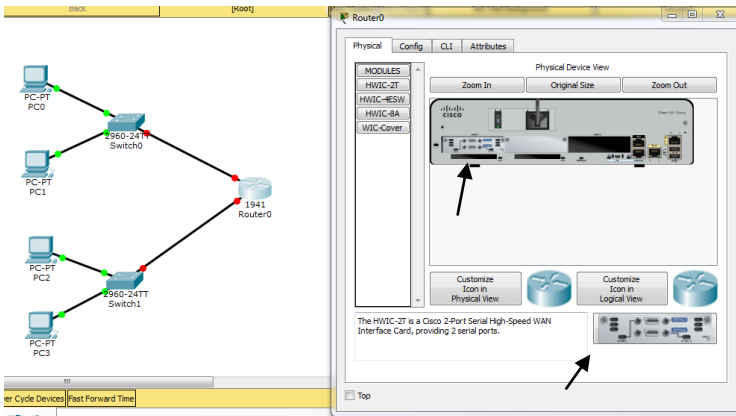
Solution:

*Because there are two **Routers** in the network, So we must activate **Routing** between them.*

At the beginning connect the network as shown below:

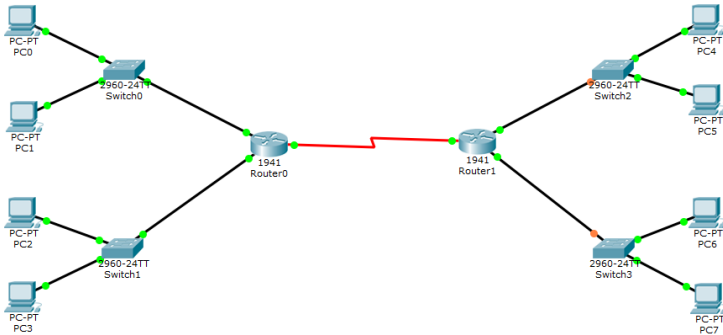


To connect these routers we need to add Serial port to each router. As we mentioned before.

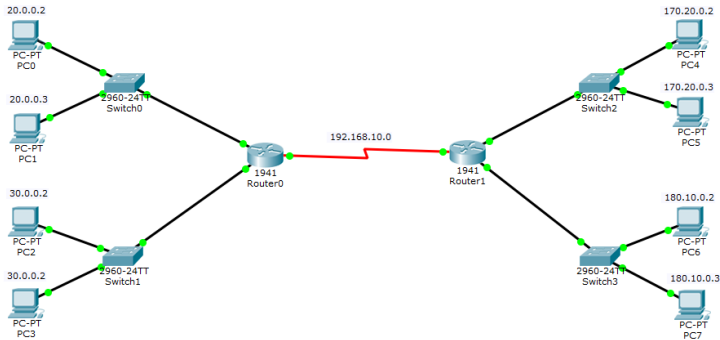


- *Power off the Router.*
- *By dragging and dropping the "HWIC-2T" port.*
- *Repeat this step on the router2.*

Now we can connect the Routers with each other.



Now, set the IP-address to each device as shown in figure below:



Now you can check the connectivity between each devices in the one side(LAN1-LAN2 or LAN3-LAN4), but the connectivity between LAN1 and LAN3 in off, also between LAN2 and LAN4 because the Router0 doesn't know about the LANs in the Router1. We should active **Routing** service to let the Routers know about all LANs in the Network.

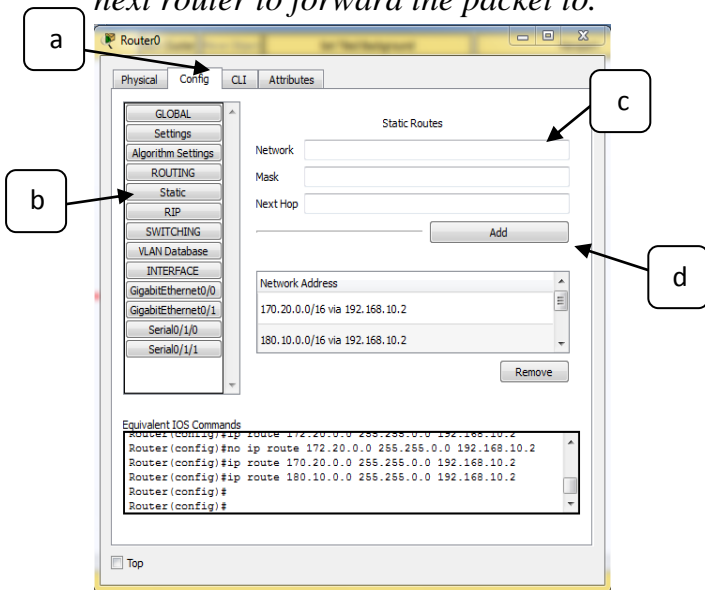
To activate Routing service follow these steps:

Double Click on Router0

- a) Choose **Config**
- b) Choose **Static**
- c) Set the **NETWORK** and it's **MASK** and **NEXT HOP**

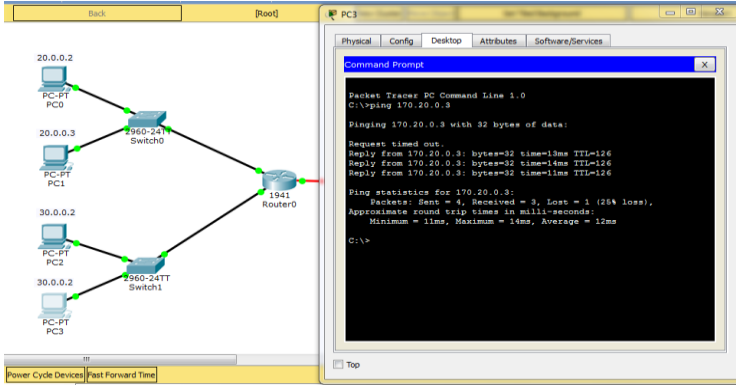
Network: Identifies the address of the remote network.

NEXT HOP: Identifies the IPv4 address of the next router to forward the packet to.



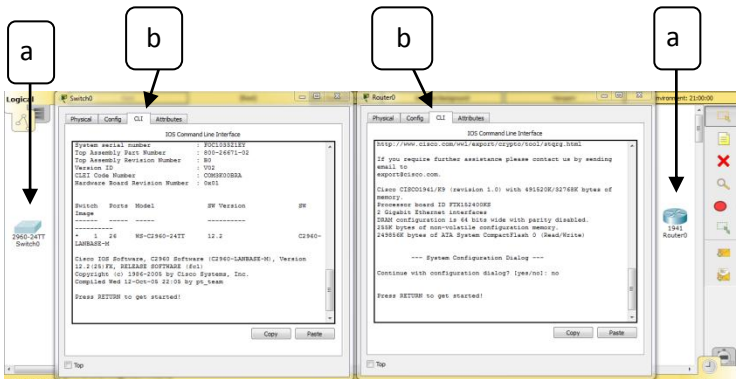
- d) Click **Add** to add this network to the Router and save it.

Repeat these steps (c & d) on the Router0, and repeat all steps on the other Router. Now we can check the connectivity between all devices.



5.4 Configuration of Router and Switch

The user needs an environment to configure these two devices, in this book will use only (Cisco Packet Tracer).

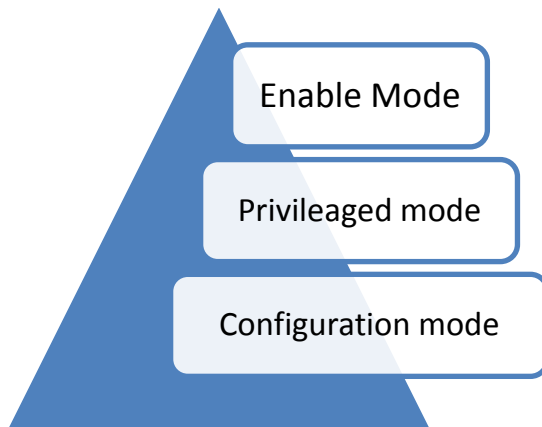


As shown in the figure above, there is no different between the Switch and Router in the program. But there is many differences between them in the **Commands**.

- a) Double Click on (Switch or Router)
- b) Choose **CLI** to write your command.

5.4.1 The Mode of Configuration

There is three Main modes in Cisco IOS, these mods are (**Enable**, **Privileged** and **Configuration mode**) as shown below:



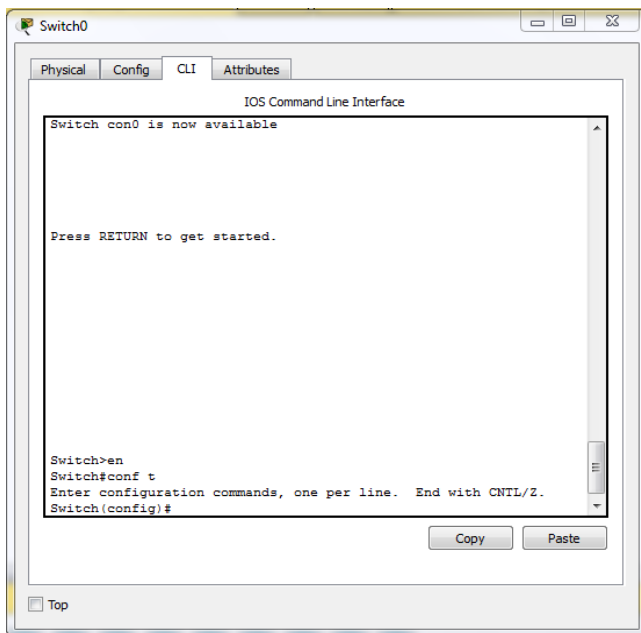
- 1- **Enable mode:** (en) allows to move from user mode to Privileged mode, in this mode there is a limited visibility of IOS. "**Switch >**"
- 2- **Privileged mode:** this is where the admin, in this mode the user can't really configure anything. "**Switch#**"

- 3- Configuration mode:** Start with global, it means everything will do will be in the global, like changes the host name. "**Switch(config)#**".

5.4.2 Configuration Steps

- ✓ Double click on Switch or Router.
- ✓ Choose CLI window to write commands.
- ✓ Write "enable" to go to the next mode
Privileged mode.
- ✓ Write "conf t" to go to the **Configuration mode.**

These three steps can be used in Switch and Router:



Now the user can change and do anything in the switch or router.

5.4.3 Basic Commands

There is many commands used in both switches and routers like:

- 1- Host name of devices.
- 2- Passwords.
- 3- Save works.

1) How to change host name

```
Switch> enable
Switch#conf t
Switch(config)#hostname S1
S1(config)#
```

: There is **One** space here.

2) How to set Passwords

```
S1> enable
S1#conf t
S1(config)#line Con 0
S1(config-line)#Password 0000
S1(config-line)#logging synchronous
S1(config-line)#login
```

Console password

```
S1> enable
S1#conf t
S1(config)#line vty 0 15
S1(config-line)#Password 1111
S1(config-line)#login
```

Telnet
password

```
S1> enable
S1#conf t
S1(config)#enable password 1234
```

Enable
password
(less Sec.)

```
S1> enable
S1#conf t
S1(config)#enable secret 1234
```

Enable
password
(more Sec.)

To encrypt all enable passwords use this command

```
S1(config)#service password encryption
```

3) Save the work

```
S1> enable
```

```
S1#conf t
```

```
S1(config)#copy running-config startup-config
```

```
S1#End
```

To back two
steps

```
S1#Exit
```

To back one
step

5.5 Active IP on the Switch

The Switch device usually deals with MAC address, but sometimes the Switch need an IP-address, because of network infrastructure devices require IP addresses to enable remote management. Using the device IP address, the network administrator can remotely connect to the device using Telnet, SSH, HTTP, or HTTPS.

A switch does not have a dedicated interface to which an IP address can be assigned. Instead, the IP address information is configured on a virtual interface called a switched virtual interface (SVI).

```
S1> enable
S1#conf t
S1(config)#interface VLAN 1
S1(config-if)#IP address 10.0.0.2 255.0.0.0
S1(config-if)#No shutdown
S1(config-if)#exit
S1(config-if)#IP default-gateway 10.0.0.1
```

Interface VLAN 1: to active vlan1.

no shutdown: to active vlan1 from down to up.

- To set any interface to the VLAN1

```
S1> enable
S1#conf t
S1(config)#interface fa0/1
S1(config-if)#Switchport mode access
S1(config-if)#Switchport access VLAN 1
```

We can repeat this steps many times, if we have more than one interface (port).

5.6 Configuration of Router

In the Router Device there are many important things that can be configured such as:

- 1- Set IP-address
- 2- Static Routing

5.6.1 Set IP-address

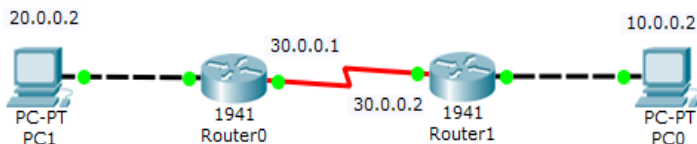
To set an IP-address for each port on the Router:

```
R1> enable
R1#conf t
R1(config)#interface gi0/0
R1(config-if)#IP address 10.0.0.2 255.0.0.0
R1(config-if)#IP default-gateway 10.0.0.1
R1(config-if)#no shutdown
R1(config-if)#end
R1#copy running-config startup-config
Press Enter
```

Interface gi0/0: To inter to the interface gigabit fast Ethernet 0/0.

5.6.2 Static Routing

To configure the Routing service on the router, follow these steps:



✓ From Pc1 to Pc0

```
R0> enable
```

```
R0#conf t
```

```
R0(config)#IP route [network][Subnet mask][next hop]
```

```
R0(config)#IP route 10.0.0.0 255.0.0.0 30.0.0.2
```

✓ From Pc0 to Pc1

```
R1> enable
```

```
R1#conf t
```

```
R1(config)#IP route [network][Subnet mask][next hop]
```

```
R1(config)#IP route 20.0.0.0 255.0.0.0 30.0.0.1
```

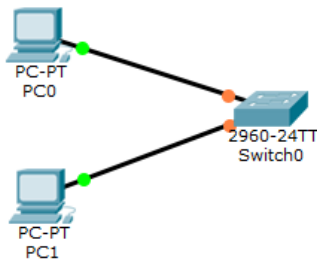
- Repeat this steps if there is another networks.

- **Show Command:** It use to view parts of the configuration that happened, it use in both switch and router, here will list some of its commands:
 - **#show IP interface brief**
It used to view a summary of the interfaces.
 - **#show VLAN**
It used to view all information about VLAN.
 - **#Show running-config**
It used to view all information that configured.
 - **#Show IP interface**
It used to view the information of interfaces.
 - **#Show History**
It used to view the information about the device, like IOS model.
 - **#Show interface fa0/10**
It used to view all information about this interface, such as (speed, duplex and physical case).

This configuration is the main configuration to the beginner that wants to inter to the World of Routers and Switches.

Check Point

- Configure this Switch with the following information:
 - The Name of Switch "**SS**"
 - Create VLAN with IP (10.0.0.2/8) and default gateway (10.0.0.1).
 - Set the Interface (0/1 and 0/2) in the switch to the VLAN.



- Configure this Router with the following information:
 - The name of the Router "**R1**"
 - Set Console Password.
 - Set these IP-addresses to its ports (30.0.0.1/8) (175.14.0.1/16).



References

- [1] Andrew S. Tanenbaum and David J. Wetherall, “Computer Networks”, Fifth edition, 2012
- [2] Internet Protocol DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION, Advance Research project, Information Sciences Institute University of Southern California 4676 Admiralty Way Marina del Rey, California 90291.
- [3] Tutorial point (I) PVT. LTD., “IPv4 internet protocol version-4”, 2014.
- [4] Wendell Odom, "CCENT/CCNA ICND 100-105", First Printer MAY 2016.
- [5] Wendell Odom, "CCNA Routing and Switching ICND2 200- 205", First Printing July 2016.
- [6] Todd Lammle, "CCNA Fast Pass", 2004.



"This book is well organized with very good detailed examples for beginners. "

Dr. Faris Muhammad

*Senior Director of Engineering Operation TM /E500
& Legacy – Cobham Wireless*



special copy

you cannot upload it or sale it.

God is watching

