LABORATORY WORK NO. 4

Network Layer – IPv4 Fundamentals

1. Objectives

At the end of the lab, students will be able: to explain the characteristics of the network layer, to describe the operation of the IPv4 protocol, to divide the networks into subnets, to explain the network address translation process, and to implement basic IPv4 network configurations.

2. Theoretical considerations

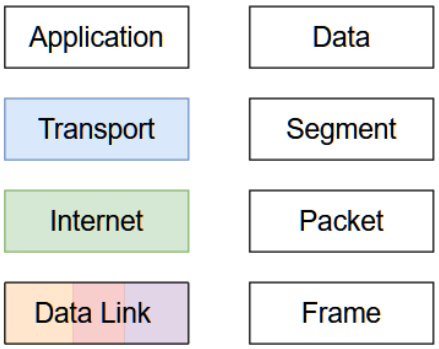
2.1 Network layer

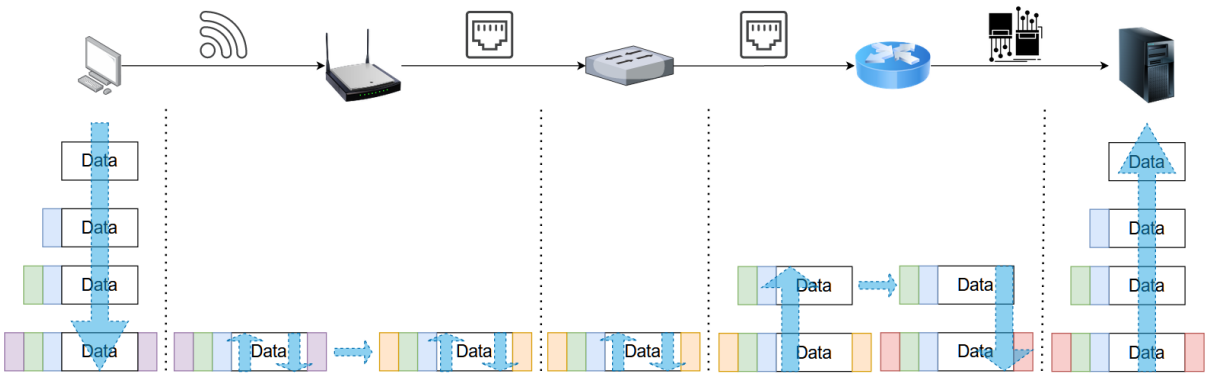
The OSI Network layer corresponds to the TCP/IP Internet layer. It provides addressing, routing and traffic control services to allow devices to exchange data across networks and contains different types of protocols:

- IP version 4 (IPv4) and IP version 6 (IPv6) routed protocols;
- routing protocols such as Open Shortest Path First (OSPF) or Border Gateway Protocol (BGP);
- messaging protocols such as Internet Control Message Protocol (ICMP).

The network layer performs four basic operations:

- Addressing
- Encapsulation
- Routing
- De-encapsulation





IP protocols have the following characteristics:

- Connectionless
  - no connection established between source and destination before data packets transmission;
  - no control information (synchronizations, acknowledgments, etc.).

- Best Effort
  - unreliable, packet delivery is not guaranteed;
  - no mechanism to resend data that is not received, reduced overhead.

- Media Independent
  - does not concern itself with the type of frame required at the data link layer or the media type at the physical layer;
  - can be sent over any media type: copper, fiber, or wireless.

2.2 IPv4

The packet header is presented below:

Octet	0								1								2								3							
Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	Version				IHL				DSCP						ECN		Total Length															
32	Identification																Flags			Fragment Offset											
64	Time To Live								Protocol								Header Checksum															
96	Source IP Address																															
128	Destination IP Address																															
160	Options																															

- Version - version field, equal to 4;
- Internet Header Length (IHL) - the size of the IPv4 header;
- Differentiated Services Code Point (DSCP) - originally defined as the type of service (ToS), specifies differentiated services (DiffServ);
- Explicit Congestion Notification (ECN) - allows end-to-end notification of network congestion without dropping packets, optional feature;
- Total Length - defines the entire packet size in bytes, including header and data;
- Identification- identification field, primarily used for uniquely identifying the group of fragments of a single IP datagram;
- Flags - used to control or identify fragments;
  - bit 0 – Reserved, must be zero;
  - bit 1 – Don't Fragment (DF)
  - bit 2 – More Fragments (MF)
- Fragment offset –specifies the offset of a fragment relative to the beginning of the original unfragmented IP datagram;
- Time to live (TTL) – limits a datagram's lifetime;
  - in practice, is used as a hop count;
  - when the datagram arrives at a router, the router decrements the TTL field by one;
  - when the TTL field hits zero, the router discards the packet and sends an ICMP time exceeded message to the sender.

- Protocol –defines the protocol used in the data portion of the IP datagram;
- Header checksum – used for error-checking of the header;
- Source address – the IPv4 address of the sender of the packet;
- Destination address – the IPv4 address of the receiver of the packet;
- Options – rarely used, if IHL is greater than 5, the options field is present.

The addresses can be assigned statically or dynamically.
The address is hierarchical, being composed of two parts: the network part and host part.

Network ID	Host ID

The number of bits assigned to the network and host depends on the class to which the address belongs:

Class	1st Octet Decimal Range	1st Octet High Order Bits	Network/Host ID (N=Network, H=Host)	Default Subnet Mask
A	1 – 126*	0	N.H.H.H	255.0.0.0
B	128 – 191	10	N.N.H.H	255.255.0.0
C	192 – 223	110	N.N.N.H	255.255.255.0
D	224 – 239	1110	Reserved for Multicasting	
E	240 – 255**	1111	Experimental; used for research	

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

** 255.255.255.255 is reserved as the IPv4 Broadcast address.

The IPv4 subnet mask is used to differentiate the network portion from the host portion of an IPv4 address. It is, like the IPv4 address, a 32 bits structure. The bits corresponding to the network portion are set to 1 and the bits corresponding to the host portion are set to 0.

Network ID	Host ID
11……..1	00……..0

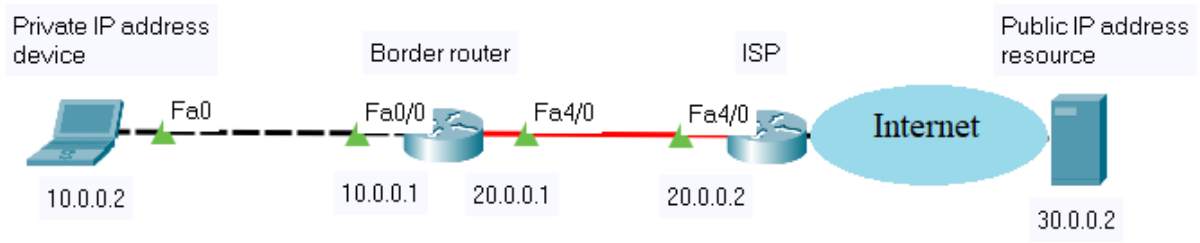
The network masks corresponding to the classes are presented below:

Class A: 255.0.0.0 or /8 (11111111.00000000.00000000.00000000)
Class B: 255.255.0.0 or /16 (11111111.11111111.00000000.00000000)
Class C: 255.255.255.0 or /24 (11111111.11111111.11111111.00000000)

Public IPv4 addresses are uniquely assigned addresses and are are globally routed between internet service provider (ISP) routers. There are also blocks of addresses, called private addresses, that are used by most organizations to assign IPv4 addresses to internal hosts. These addresses are not uniquely assigned addresses and are are not globally routed between ISP routers. These blocks of private addresses are presented below.
Class A: 10.0.0.0 - 10.255.255.255 /8
Class B: 172.16.0.0 - 172.31.255.255 /12

Class C: 192.168.0.0 - 192.168.255.255 /16

To allow a device with a private IPv4 address to access devices and resources outside of the local network, the private address must be translated to a public address. This process is called network address translation (NAT) and provides the translation of private addresses to public addresses. A NAT router typically operates at the border of a network. When a device inside the network wants to communicate with a device outside of its network, the packet is forwarded to the border router which performs the NAT process, translating the internal private address of the device to a public, outside, routable address.




```
BorderRouter#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
tcp 20.0.0.3:1027      10.0.0.2:1027      30.0.0.2:80        30.0.0.2:80
```

The network address has all the host bits set to 0 and the broadcast address has all the bits set to 1. These addresses cannot be assigned to a host. All the other addresses are valid host addresses.

Exercise
Consider the following address: 192.168.1.10/24. Calculate the network and broadcast address, the valid host range, the total number of host bits and the total number of hosts.
IP: 11000000.10101000.00000001.00001010
NM: 11111111.11111111.11111111.00000000
IP logic AND with the NM:
11000000.10101000.00000001.00001010
11111111.11111111.11111111.00000000

11000000.10101000.00000001.00000000 – Network address (all host bits are set to 0)
192.168.1.0 – Network address
11000000.10101000.00000001.11111111 – Broadcast address (all host bits are set to 1)
192.168.1.255 – Broadcast address
11000000.10101000.00000001.00000001 – First valid host address
192.168.1.1 – First valid host address
11000000.10101000.00000001.11111110 – Last valid host address
192.168.1.254 – Last valid host address
192.168.1.1-192.168.1.254 – Valid host range
Total number of host bits is 8.
Total number of hosts is 2^8-2=254.

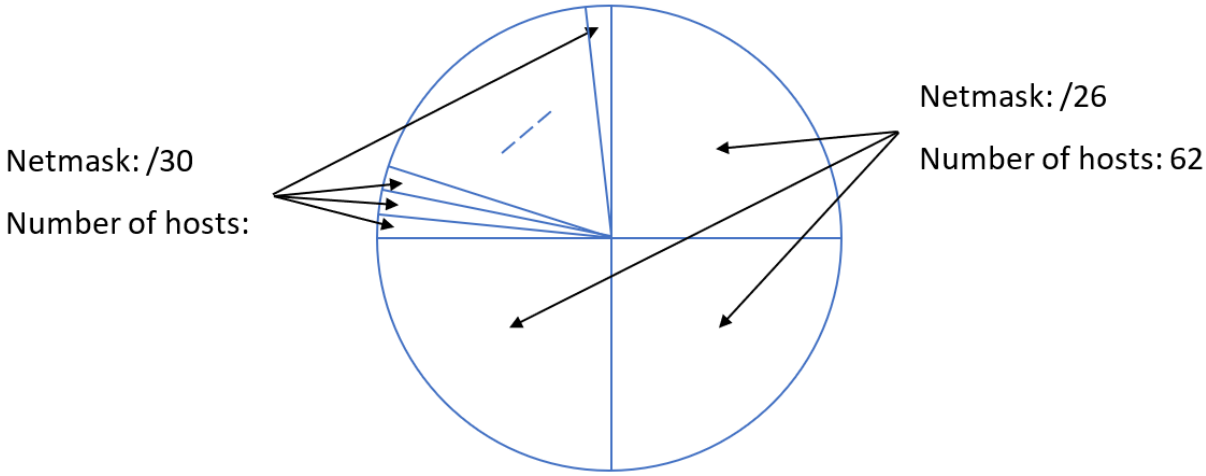
2.3 Subnetting

To create subnets, bits are borrowed from the host ID. A new network mask is created to show the new structure. In the network mask, the bits corresponding to the subnetwork portion are set to 1.

Network ID	Host ID	
11……..1	00……..0	
Network ID	Subnetwork ID	Host ID
11……..1	11……..1	00……0

Exercise
Consider the following address: 192.168.1.0/24. Divide this address in 4 subnets and further divide the fourth subnet into a maximum number of subnets. Specify for the subnets: netmask, network address, broadcast address, the number of host bits, the number of hosts and their address range.

We will borrow 2 bits to obtain 4 subnets. In order to further divide the fourth subnet into a maximum number of subnets, we will reserve for the host portion 2 bits, the minimum possible number.



First /26 subnet:

Network Subnetwork Host	
11000000.10101000.00000001.00000000	192.168.1.0/26 - Network Address
11000000.10101000.00000001.00000001	192.168.1.1/26 - First Host Address
…	…
11000000.10101000.00000001.00111110	192.168.1.62/26 - Last Host Address
11000000.10101000.00000001.00111111	192.168.1.63/26 - Broadcast Address

Netmask: /26 (255.255.255.192)
Network address: 192.168.1.0/26
Broadcast address: 192.168.1.63/26
Number of host bits: 6
Number of hosts: 2^6-2=62

Hosts address range: 192.168.1.1/26-192.168.1.62/26

First /30 subnet:

Network Subnetwork Host	
11000000.10101000.00000001.11000000	192.168.1.192/30 - Network Address
11000000.10101000.00000001.11000001	192.168.1.193/30 - First Host Address
11000000.10101000.00000001.11000010	192.168.1.194/30 - Last Host Address
11000000.10101000.00000001.11000011	192.168.1.195/30 - Broadcast Address

Netmask: /30 (255.255.255.252)
Network address: 192.168.1.192/30
Broadcast address: 192.168.1.195/30
Number of host bits: 2
Number of hosts: 2^2-2=2
Hosts address range: 192.168.1.193/30-192.168.1.194/30

3. Lab activity

3.1 Discuss the theoretical aspects.
3.2 Solve the following problems:
A. Determine the network and broadcast addresses and number of host bits and hosts for the given IPv4 addresses and prefixes:

IPv4 Address/Prefix	Network Address	Broadcast Address	Total Number of Host Bits	Total Number of Hosts
172.16.104.99/27				
198.133.219.250/24				
10.1.113.75/19				

B. Having the following information, compute subnets with the following constrains:
- A number of 62 subnets
- Host IP Address: 172.16.0.0
- Original Subnet Mask 255.255.0.0

C. Having the following information, compute subnets with the following constrains:
- A maximum number of 29 hosts/subnet
- Host IP Address: 192.168.200.0
- Original Subnet Mask 255.255.255.0

D. Having the following information, compute subnets with the following constrains:
- A number of 250 subnets
- Host IP Address: 10.0.0.0
- Original Subnet Mask 255.0.0.0

3.3 Test the following commands (using Command Prompt on Windows OS or Terminal in Linux OS):

- Command: **ipconfig /all** (on Windows OS) and **ifconfig (**on Linux OS)
- *Role: displays all network configuration values for your network interface cards*

- Command: **ipconfig /release** and **ipconfig /renew** (on Windows OS) and **dhclient (**on Linux OS)
- *Role: refreshes DHCP and DNS values*

- Command: **ping**
- *Role: troubleshoots network connectivity; verifies IP connections, using ICMP packets*

- Command: **tracert** (**traceroute** on Linux)
- *Role: troubleshoots network connectivity; resolves the path to an IP destination, using ICMP packets*

- Command: **nslookup**
- *Role: performs DNS queries*

- Command: **route print**
- *Role: displays the routing table of the host device*

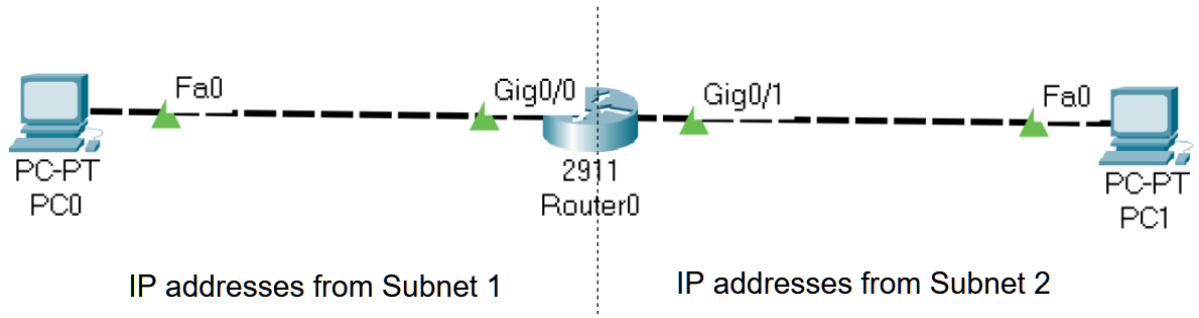
- Command: **netstat**
- *Role: network statistics tool*

- Command: **arp -a**
- *Role: displays the ARP cache (mapping of IP address to a physical addresses)*

Hint: you can use online operating systems to test various commands (e.g. https://bellard.org/jslinux/ for Alpine Linux or Windows 2000)

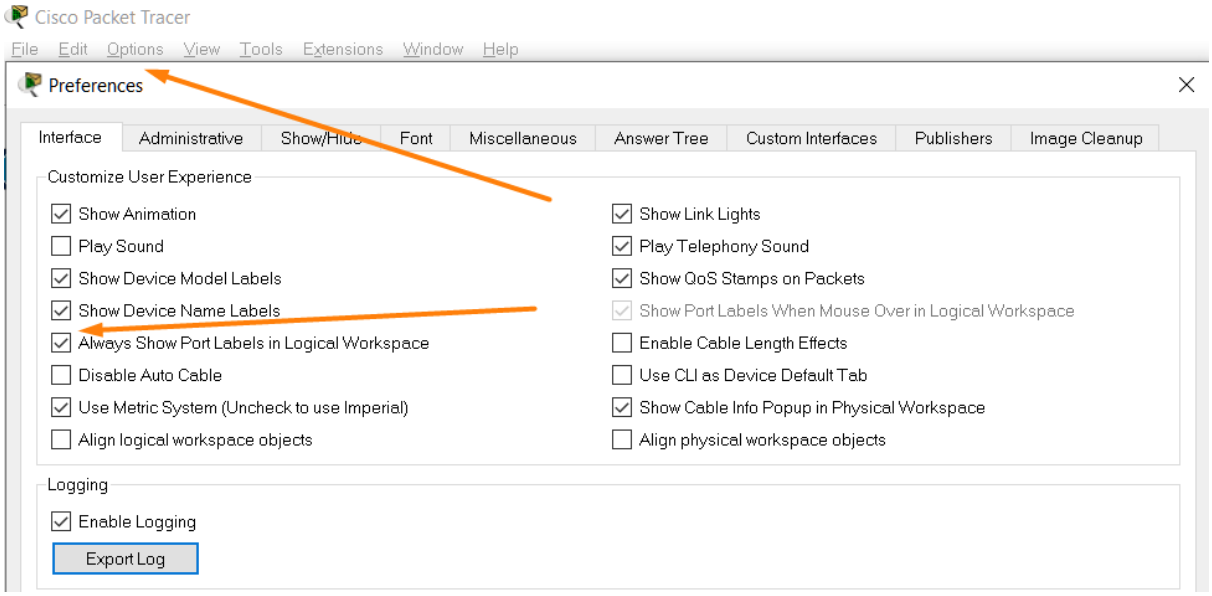
3.4 Using Wireshark, capture different types of IP packets and analyze their headers. For example:
- capture **ping** traffic by filtering the ICMP protocol filter
- capture **nsloookup** traffic by filtering the DNS protocol filter
- etc.

3.5 Configure and test the following network using Packet Tracer:



Considering IP address 172.16.0.0 /16, compute 2 subnets and assign the correct IP address to the routers' interfaces and to the host computers (PC0 and PC1).

Step 0: In order to show the interface name and numbers, go to Options -> Preferences and check "Always Show Port Labels in Logical Workspace"



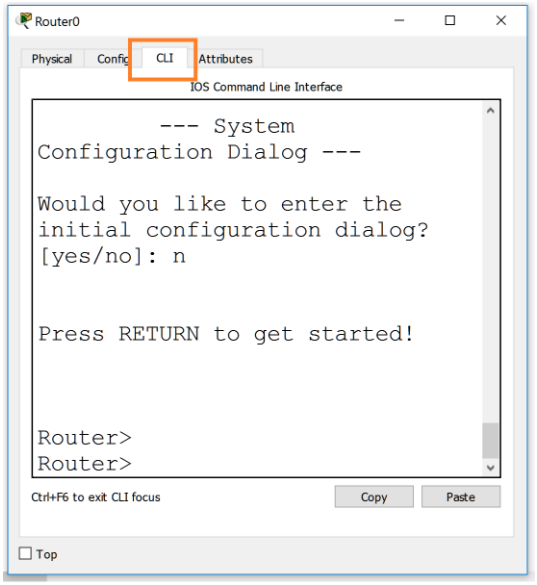
Step 1: Create the two subnets

Step 2: Before configuring the network devices, assign a unique IP address and he corresponding subnet mask to each network port:

Device	Interface	IP Address	Subnet mask
PC0	Fa0	172 . ___ . ___ . ___	___ . ___ . ___ . ___
Router0	Gig0/0	___ . ___ . ___ . ___	___ . ___ . ___ . ___
Router0	Gig0/1	___ . ___ . ___ . ___	___ . ___ . ___ . ___
PC1	Fa0	___ . ___ . ___ . ___	___ . ___ . ___ . ___

Step 3: Configure the router using the commands provided in steps **3.x** below. The commands provide sample interface names and IP addresses. You must use the interface names and the IP addresses filled in the previous table:

Example on configuring the depicted topology



Step 3.1: Enter configuration mode on the router
Router>enable
Router#configure terminal
Router(config)#

Step 3.2: Assign static IPv4 address to the router interfaces

Router(config)#interface fastethernet 0/0
Router(config-if)#ip address 192.168.0.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit

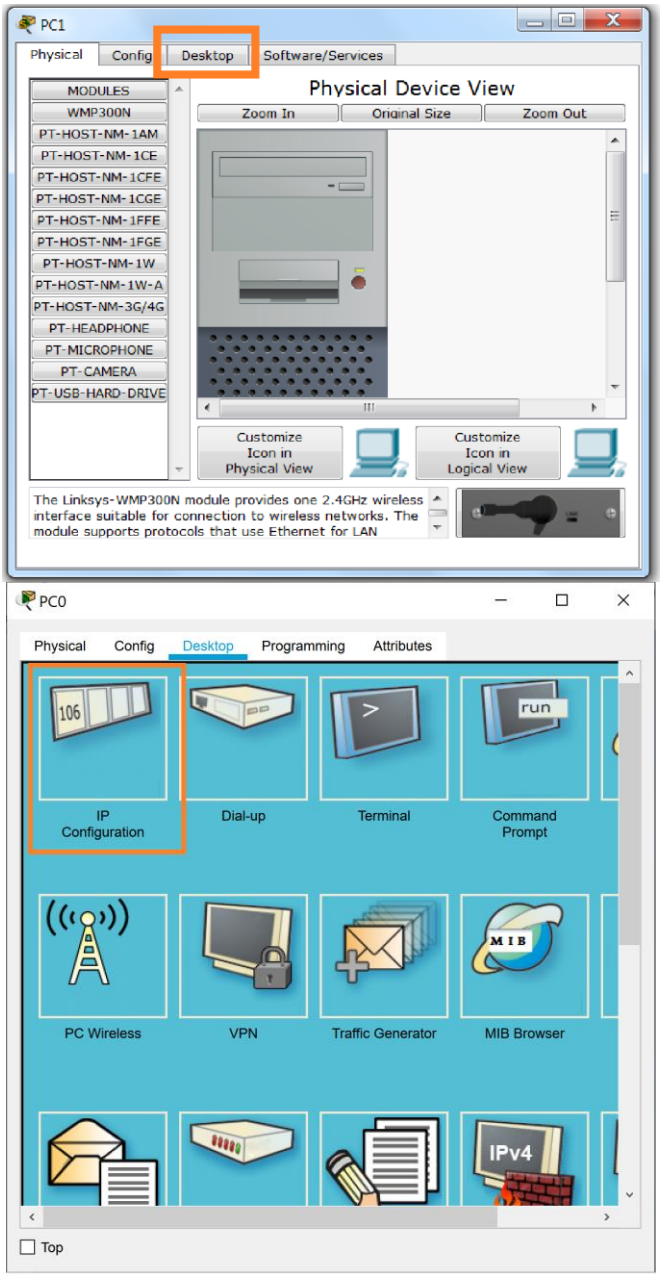
Configure the other router interface with the corresponding IP address the same for the other router interface
Router(config)# interface ___
Router(config-if)#ip address _____ _____
Router(config-if)#no shutdown

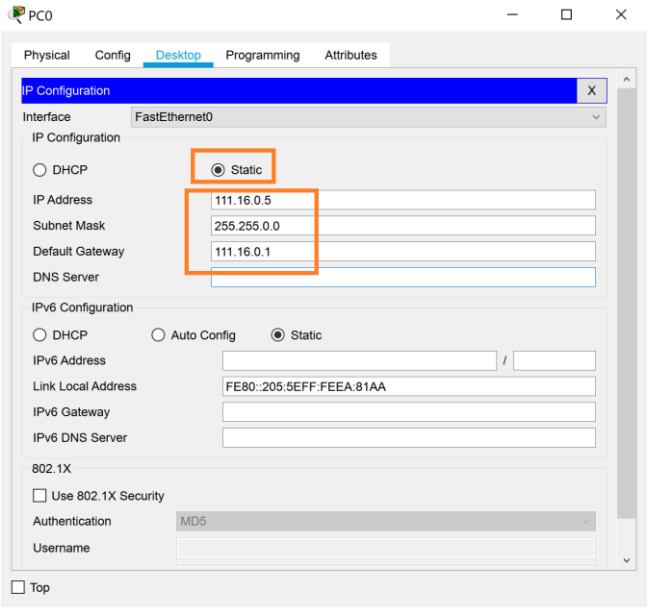
Step 3.3: Display information about the router configuration

Router#show ip interface brief
Description: Display IP information about router's interfaces

Router#show ip route
Description: Display IP routing table

Step 4: Configure IP addresses on the PCs using the following screenshots


PC1
Physical
Config
Desktop
Software/Services
MODULES
WMP300N
PT-HOST-NM-1AM
PT-HOST-NM-1CE
PT-HOST-NM-1CFE
PT-HOST-NM-1CGE
PT-HOST-NM-1FFE
PT-HOST-NM-1FGE
PT-HOST-NM-1W
PT-HOST-NM-1W-A
PT-HOST-NM-3G/4G
PT-HEADPHONE
PT-MICROPHONE
PT-CAMERA
PT-USB-HARD-DRIVE
Physical Device View
Zoom In
Original Size
Zoom Out
Customize Icon in Physical View
Customize Icon in Logical View
The Linksys-WMP300N module provides one 2.4GHz wireless interface suitable for connection to wireless networks. The module supports protocols that use Ethernet for LAN
PC0
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Dial-up
Terminal
Command Prompt
PC Wireless
VPN
Traffic Generator
MIB Browser
IPv4
Top



Test the connectivity.

a. *check IP addresses oh hosts computers: PC -> Desktop -> IP Configuration*

b. *Check connectivity between computers using the **ping <target IP>** command: PC -> Desktop -> Command prompt*

Notes