A-Level
Computer Science

Network protocols and
IP address

Lesson Objectives

Students will learn about:

- How devices are addressed in networks
- Various protocols used in networking
- Concept of layering and how it is applied to networks
- Transmission of data using TCP/IP suite of protocols

1.

Content

Network Protocols

- Networking protocols define rules and conventions for communication.
- Protocols determine the speed of transmission, size of the message, error checking methods and type of transmission (synchronous or asynchronous).

Handshaking

- The protocols are established between sender and receiver before starting communication.
- This is done by handshaking, which is the process of negotiation between the sender and receiver by an exchange of messages.
- Once handshaking is complete, data packets travel from sender to receiver through various routers.
- Data packets are exchanged between various routers; this is called packet switching.

Network Addressing

- A data packet contains the sender’s and receiver’s address.
- Each device in the network is assigned a unique address, which is called an IP address.
- IP addresses consist of binary numbers and are usually represented in decimal or hexadecimal format.

IP address vs. MAC address

- An IP address should not be confused with a MAC address.
- A MAC address is the address provided by the manufacturer that uniquely identifies the network interface card.
- IP addresses are provided by a network administrator and define the connection between network and device.

IPv4 and IPv6

IPv4

In IPv4 (Internet Protocol version 4), each device is assigned a 32-bit address.

For example: 197.154.13.145.

With 32 bits, around 4 billion unique IP addresses can be assigned.

8 bits form an octet. Each octet may represent any number between 0 to 255.

IPv6

In IPv6 (Internet Protocol version 6), each device is assigned a 128-bit address.
For example: 2001: db8: ac10: fa03: 1528: 11: 134: 2.

IPv4 reserved addresses

Some reserved IP addresses that cannot be used for individual networks or hosts are:

- 127.x.x.x represents private, non-routable addresses that are used within local networks for diagnostics purposes.
- x.x.x.0 represents a network identifier
- x.x.x.1 represents a default router address
- x.x.x.255 represents a broadcast address on a subnet

IPv4 addresses

- IPv4 addresses consist of two parts: network ID and host ID.
- A network ID represents the individual network, and the host ID represents the host computer within the network.
- As the network ID is represented by the first bits of the IPv4 address, its size determines the remaining bits for host IDs.

Classful addressing

- Initially, a network consisted of different classes.
- Each class has a different structure of addressing.
- Consider a large organisation; it will require class A addressing. In a single network, 2^{24} hosts can be used. In total, only 2^{7} such organisations can be addressed.

Class	Class identifier	network ID (number of bits)	host ID (number of bits)
A	0	7	24
B	10	14	16
C	110	21	8

Classful addressing

- In class C addressing, 2^{21} organisations could be addressed, but each organisation may have only 2^8 hosts.
- Due to a fixed number of hosts, classful addressing is not preferred. Instead, classless addressing was designed to overcome this problem.

Class	Class identifier	network ID (number of bits)	host ID (number of bits)
A	0	7	24
B	10	14	16
C	110	21	8

Classless addressing

- In classless addressing, an IP address has an 8-bit suffix that specifies the number of bits allocated for network ID.
- For example, if the 8-bit suffix represents the number 14, then network ID consists of 14 bits and the remaining 18 bits represents the host ID.
- For example, 172. 45. 9. 3/14 is represented in binary as given. The network ID is highlighted:

10101100001011010000100100000011/00001110

Subnet masking

- A subnet mask is used to identify the two parts of an IP address.
- For example, a subnet mask 255.0.0.0 represents a network ID of 8 bits and a host ID of 24 bits. This is equivalent to a suffix /8 in classless addressing.
- When AND operation is performed between an IP address and its subnet mask, its network ID is obtained.
- Using the source address, destination address and subnet mask, it can be found whether the source and destination nodes are present in the same subnetwork or not.

Subnet masking

- For example, consider a subnet mask of 255.255.255.0.
- Its binary equivalent is: 11111111. 11111111. 11111111. 00000000.
- Consider the source and destination addresses, 192.134.81.7 and 192.134.81.57. To find out whether the source and destination nodes are present on the same subnetwork, the given steps are followed.

Subnet masking

- Find the network ID of the source computer by performing AND operation of the source IP address and subnet mask.

Source IP address	11000000	10000110	01010001	00000111
subnet mask	11111111	11111111	11111111	00000000
Network ID	11000000	10000110	01010001	00000000

Subnet masking

- Find the network ID of the destination computer by performing AND operation of the destination IP address and subnet mask.

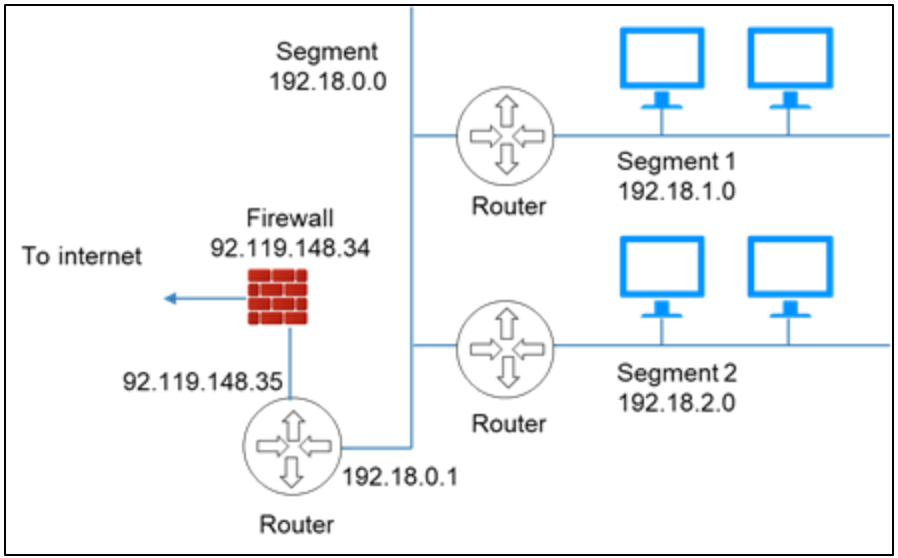
Destination IP address	11000000	10000110	01010001	00111001
subnet mask	11111111	11111111	11111111	00000000
Network ID	11000000	10000110	01010001	00000000

Subnet masking

- The network IDs for source and destination IP addresses are the same, which means that both computers are in the same subnetwork.
- Alternatively, if the network IDs were not same, we require a router to forward the data packet to the subnet in which destination computer is present.

Subnetting

- The network of a large organisation may be divided into several segments using subnet IDs.
- This improves ease in management and efficiency in routing.
- As the main network is now subdivided, collisions are reduced. Also, the speed, reliability and security of the network improves.



Subnet ID

- A subnet ID is formed by using the most significant bits of the host ID of an IP address.
- The first 8 bits of the host ID is used as subnet ID in this example.
- Using 8 bits, 254 (excluding 0 and 255 as reserved IP address), different host addresses are possible in the $2^8 = 256$ different subnetworks.

IP address	11000000	00010010	00000001	00000000
subnet mask	11111111	11111111	11111111	00000000
	11000000	00010010	00000001	00000000
	Network ID		subnet ID	host ID

Public and private IP addresses

Public addresses

Also called routable, an IP address is globally unique.

The public address of a computer can be globally addressed by any computer in the world.

Examples of public IP addresses include the address of a company's web server and the address of an internet router.

Private addresses

Also called non-routable, IP addresses are addresses used within a local network.

The router forwards data to the correct node using this address. This type of address is unique only within the local network and need not be unique globally.

Public and private IP addresses

Public addresses

Some public IP addresses are also identified using domain names.

A Domain Name Server (DNS) translates the domain name to IP address.

Private addresses

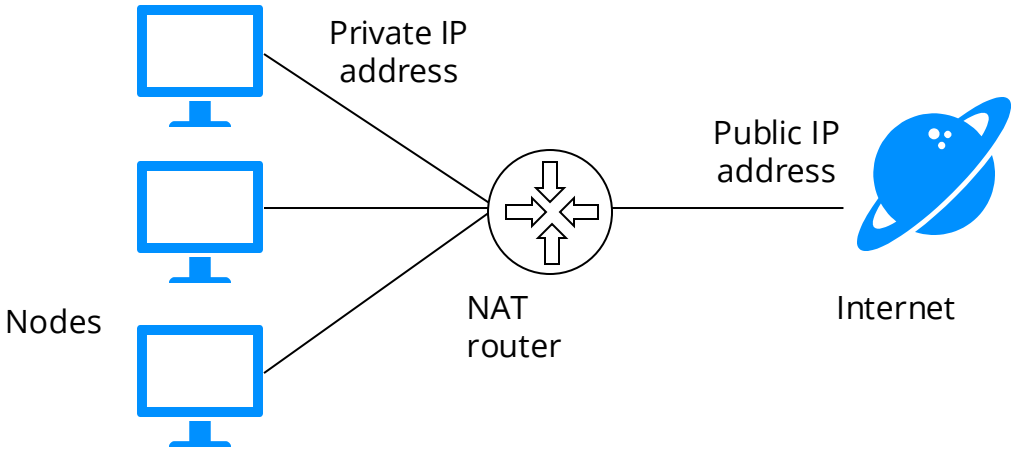
These addresses need not be registered on the Internet registry.

The commonly used Class C private addresses range from 192.168.0.0 to 192.168.255.255.

Private addressing for internal networks saves unique IPv4 addresses that can be used for routers and web servers that connect to the Internet directly.

NAT router

A Network Address Translator (NAT) router provides external access to a privately addressed network as shown in the figure.



Let’s review some concepts

Network Addressing

Each device in the network is assigned a unique address, which is called an IP address.

IPv4 →32-bit address.

IPv6 →128-bit address.

Subnet masking:

Used to identify the two parts of an IP address.

Network ID = IP address AND subnet mask.

A subnet ID is formed by using the most significant bits of the host ID of an IP address.

Static and dynamic addressing

Static: When the device is not in use, this address remains unused too.

Dynamic: IP addresses could be reused using DHCP.

Public and private IP addresses

Public IP address: globally unique

Private IP address: non-routable IP addresses are addresses used within a local network.

Classful addressing

Class A, Class B & Class C) to specify the number of bits for a network ID.

Classless addressing

8-bit suffix that specifies the number of bits allocated for a network ID.

NAT

Network Address Translation is a system that matches the private IP addresses to public addresses.

Port forwarding: A method of routing data through additional ports.

Let’s review some concepts

Protocols
HTTP: viewing web pages
STMP, POP3, IMAP: emails
VoIP: voice calls over the Internet
FTP: transferring files
DHCP: Dynamic addressing
SSH: Remote access

Layering:

Layering is the process of breaking a complex process into several processes or layers in a particular order.

Network layers:

- Application layer: user interface
- Transport layer: data is segmented to packets (port num)
- Internet layer: adds the sender’s and receiver’s IP addresses (socket num)
- Link layer: MAC addresses

TCP/IP

TCP/IP is a suite of communication protocols used to interconnect network devices of different manufacturers on the Internet.

Encapsulation

Each layer of the TCP/IP stack adds information to the data. This process is called an encapsulation.

2.

Activity

Activity-1

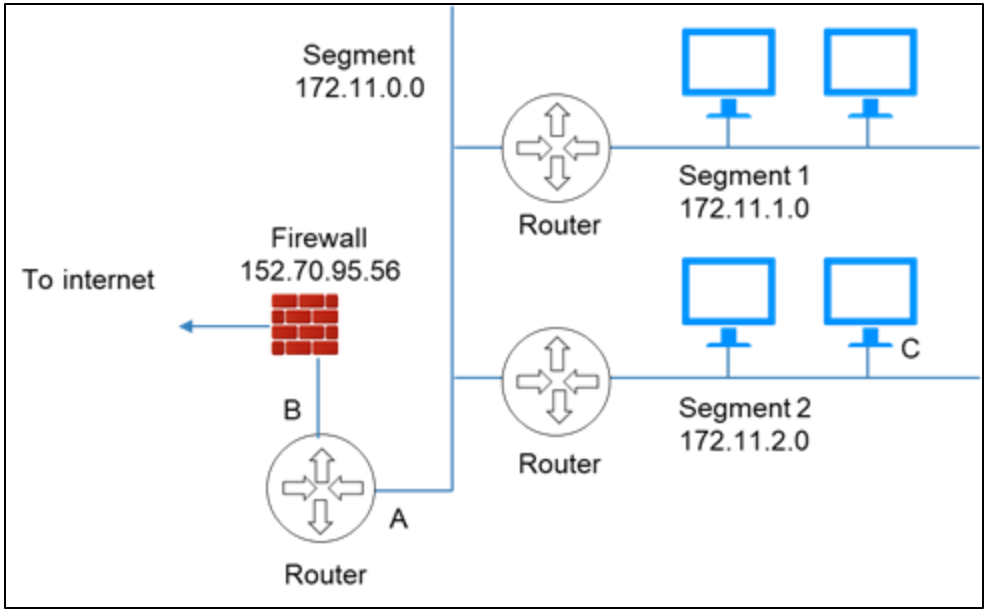
Duration: 15 minutes

1. Physical topology of a LAN network that is connected to the Internet is given. This network uses IPv4 protocol.

   a) State suitable IP address for router connection marked A.

   b) State suitable IP address for router connection marked B.

   c) State suitable IP address for NIC of terminal C.



3.

End of topic questions

End of topic questions

1. What is the difference between public and private IP address?
2. What are the advantages of subnetting? If the first 20 bits of a public IP address are used as the network ID, the next 3 bits represent the subnet ID and the nodes of the network are configured using subnet mask 11111111. 11111111. 11111110. 00000000, how many IP addresses are available for devices in the network?
3. Briefly explain how port forwarding works.
4. How is an IP address allocated to a client using dynamic host control protocol (DHCP)? What are the advantages of using DHCP?