

Network address :- 10.100.128.0/17

①

Given subnet = 11

= (1011) 4 bit

$$\therefore \overset{\text{subnet}}{\text{Host}} = 2^4 = 16$$

\therefore need to borrow 4 bits from Host bit address

$$\text{Network bit} = 17 + 4 \quad \text{host} = 11$$

②

subnet mask

117

$$17 + 4 = 21$$

$$\begin{array}{ccccccc} 11111111 & \cdot & 11111111 & \cdot & 11110000 & \cdot & 00000000 \\ 255 & & 255 & & 248 & & 0 \end{array}$$

$$\text{subnet mask} = 255.255.248.0$$

③ 10. 100, 128. 0 / 21

|||| |||| . |||| |||| . |||| 0000 . 0000000000

Hostbit

octet = 3
subnet generation
 $= 2^3 = 8$

$$\text{No. Host} = 2^{11}$$
$$= 2048$$
$$\text{usable} = 2048 - 2$$
$$= 2046$$

Subnet 1 :- 10.100.128.0 / 21

∴ Host address range :-

10.100.128.1 - 10.100.135.255

First address :- 10.100.128.0

Broadcast address :- 10.100.135.255

Subnet 2:- 10.100.136.0 / 21

subnet 3 :- 10.100. .144. 0/21

Subnet 4 :- 10.100.152.0/21

subnet 5 :- 10.100.160.0 / 21

subnet 6 \Rightarrow 10.100.168.0/21

subnet 7 \Rightarrow 10.100.176.0/21

subnet 8 \Rightarrow 10.100.184.0/21

subnet 9 \rightarrow 10.100.192.0/21

subnet 10 \rightarrow 10.100.200.0/21

subnet 11 \rightarrow 10.100.208.0/21

(3) \therefore CIDR notation 11th subnet network address

$$= 10.100.208.0/21$$

(5) \therefore Host address range

$$10.100.208.1 - 10.100.215.254$$

Before

$$10.100.128.0/17$$

$$\therefore \text{usable Host} = 2^{32-17} - 2 = 32766$$

After

$$10.100.128.0/21$$

$$\therefore \text{usable Host} = 2^{32-21} - 2 = 2046$$

\therefore Host address lost

$$\text{on subnetting process} = 32766 - 2046 = 30720$$

⑤

10.100.128.0 / 21

No of host = 2
(10) 2bit

∴ Network bit = 32 - 2 = 30 bit

new network address
= 10.100.128.0 / 30

||||| . ||||| . ||||| . ||||| 00
↳ $2^2 = 4$ host

∴ new subnetmask :-

255.255.255.252 / 30

Two usable IP address are

① 10.100.128.1

② 10.100.128.2

10.100.128.0 → first address

10.100.128.3 → broadcast

Port addressing :- is a mechanism used in computer networking to identify specific services/processes running on a device within a network.

why do we need ?

- ① multiplexing
- ② TCP/IP networking connection establishment
- ③ ~~uniquely identify a process~~ help differentiate between various services/protocols running on device

① well-known port :- 0 - 1023

- HTTP → 80
- HTTPS → 443
- FTP → 21

② Registered port :- 1024 - 49151

③ Dynamic/private port :- 49151 - 65535

What is default gateway?

→ is a device that serves as the exit point for network traffic from a local network to other network. It acts as a router to connect local network to external network such as Internet
→ connect local network to other network

192.168.10.0/28

∴ default gateway :- 192.168.10.1

Features

- ① Traffic Routing (forwarding traffic)
- ② Internet Access (can route to other network)
- ③ Network Address Translation (NAT)
- ④ Firewall functionality
- ⑤ act DHCP services
- ⑥ supports QoS (Quality of service)

Host Forwarding Decision technique :-

(local routing)

→ is a method used by individual hosts to determine how to forward network traffic destined for different network.

- ① Packets are always created at source
- ② Routing Table :- each host device create their own routing table
- ③ Destination IP :- a host can send packet to
 - ④ Itself :- 127.0.0.1
 - ② Local host :- (another host on same LAN)
 - ③ Remote host :- not in same LAN

Next hop determination :-

- ④ source device determine where the destination is Local or remote
For determination it use own IP address and subnetmask with destination IP address
- ⑤ Local traffic handled by host interface
Remote traffic " " by default gateway of LAN

Point to point

refers to a communication link that connects two nodes directly with a dedicated link, without any intermediary device.

peer to peer

refers to network architecture where all peers (nodes) have equal capabilities and responsibility. Each node can act as both client and server, sharing resources directly.

what are the key elements of network protocol?

① Syntax :- define the structure and format of data being transmitted

Packet header, data field

② Semantics :- define the meaning and Interpretation of ^{data} exchanged between device

③ Timing :- coordination & synchronization between devices.

what are functions provided by network protocol?

① Addressing & Identification

② Data encapsulation

③ packet forwarding - routing

④ error detection - correction

⑤ flow control

⑥ network management

⑦ security & Encryption

⑧ Reliability
(guaranteed delivery)

⑨ sequencing

what are the network protocol requirements?

- ① an identified sender - receiver
- ② common language - grammar
- ③ speed - timing of delivery
- ④ Acknowledgement and confirmation of requirements.

what are the four fundamental characteristics of data communication

- ① Delivery :- must deliver to correct destination
- ② Accuracy :- must deliver accurate data
- ③ Timeliness :- timely manner deliver
- ④ Jitter :- refers to the variation in packet arrival time.

Q) What are the four characteristics of Reliable Network?

① fault tolerance :- refers to the ability of Network to continue operating & providing service even in the presence of failure

② scalability

③ QoS (Quality of service) :- prioritize and manage network traffic to ensure specific level of performance, reliability, service, delivery

④ Network security

What are the benefits of layered model?

- ① Modular Design :- divide complex task into separate layers
- ② Interoperability
- ③ Easier Design & simplified design implementation
- ④ Flexibility and Extensibility
- ⑤ Easy troubleshooting and debugging
- ⑥ standardization value

— • —

Physical Layer

- ① physical characteristics of interface and transmission medium
- ② Representation of bits
- ③ Data/Bit rate
- ④ Synchronization of bit
- ⑤ physical topology
- ⑥ Line configuration
- ⑦ Transmission mode
- ⑧ Signal encoding and modification

Ethernet
WLAN
SONET
SDH

bits

Data Link Layer

- ① Framing & defining bits
- ② provide physical address
- ③ Error detection
- ④ flow control
- ⑤ access control
- ⑥ hop to hop delivery

Frame Header	packet (data)	Frame Trailer
--------------	---------------	---------------

frame start	addressing	Type	control	Data	Error detection	Frame stop
-------------	------------	------	---------	------	-----------------	------------

subLayer

LLC (Logical link control) sublayer

- ① Framming
- ② Error control
- ③ flow control
- ④ sequencing
- ⑤ Link management

MAC (Media Access Control) sublayer

- ① Addressing
- ② Medium access control
- ③ Frame transmission

Network Layer

- ① Host to host packet delivery
- ② logical Addressing
- ③ Routing (Route determination, selection)
- ④ provides best effort service

IPv4
IPv6
ICMPv4
ICMPv6

Transport Layer

- ① TCP, UDP
- ② Reliable process to process delivery
- ③ port addressing
- ④ Error detection
- ⑤ flow control
- ⑥ connection control
- ⑦ Data segmentation and reassemble
- ⑧ Describe the format of request/response in between client-server
- ⑨ connection establishment and termination
- ⑩ data multiplexing

Session Layer

- ① Dialog control
- ② synchronization
- ③ Login - logout
- ④ session establishment & manging

Presentation Layer

- ① Translation, Formatting PNG
JPG
- ② Compression GIF
- ③ Encryption MKV

Application Layer

- ① providing service / access to user
- ② file transfer, access, management
- ③ mail (email) and directory Services -

FTP, HTTP, HTTPS, DNS

CSE

192.168.40.0 / 21

11111111 . 11111111 . 11111000 . 00000000

subnet mask :- 255.255.248.0

subnets :- 32

Host :- $2^{11} = 2048$

subnet :-
-1

192.168.40.0 / 21

192.168.40.1 — 192.168.47.254

— 0 —

fields		Destination		Destination	
00-07-E9-42-AE-28	00-07-E9-00-BC-70	192.168.1.27	192.168.1.7	1022	8080
Destination mac	Source mac	Source IP	IP	Source Port	Host port

Data	CRC
------	-----

Data Link
Layer
Ethernet frame

source socket :- IP + port
192.168.1.27:1022

What is NAT?

NAT is network address translation which works by translating IP (private) address used within a local network into a public IP address assigned by ISP (Internet Service Provider).

→ allows device with private ~~IP~~ IP address to communicate with device outside the local ~~IP~~ network using the public IP.

How NAT works

- ① In local network, device are assigned private IP address. (which are not routable in Internet)
- ② NAT act as gateway between local network and Internet.

③ It has both private IP address with local network and a public IP assigned by ISP

The NAT router maintains a ^{mapping} table that keeps track of private IP address and their corresponding public IP address translation.

④ when a device from local network wants to communicate with a device on Internet, NAT router modifies the source IP of outgoing packets to its own public IP

It allows multiple device within ~~a single~~ local network to connect internet using a single internet connection (public IP address)

Advantage

- ① allows a single IP address for multiple device
- ② Enhanced Security
- ③ simplified network configuration

disadvantage

- ① limited ^{to} Peer-to-peer connectivity
- ② Increases complexity for network administration
- ③ fully dependent on public IP availability.