Chapter 5
Internet/Network Layer

Contents

- Network Layer
- IPV4
- IPV6
- Routing Protocols

Network Layer

- The Network layer receives the segments and converts them into packets and adds header information (logical addressing) and sends them to the Data Link Layer
- The data link layer is very similar to the network layer, except the data link layer facilitates data transfer between two devices on the same network. The data link layer takes packets from the network layer and breaks them into smaller pieces called frames

Function of Network Layer

- **Routing**: Determines the best path for data to reach its destination based on network conditions and other factors.
- **Forwarding**:
  - Forwards packets to network routers, which use algorithms to determine the best paths for data to travel.
  - Source to destination delivery of packets
- **Addressing**: Assigns unique logical addresses to each device, such as IP addresses.
- **Error handling**: Uses protocols like the Internet Control Message Protocol (ICMP) to handle errors and diagnostics.
- **Quality of Service** (QoS): Prioritizes certain traffic over other traffic

What is an IP address?

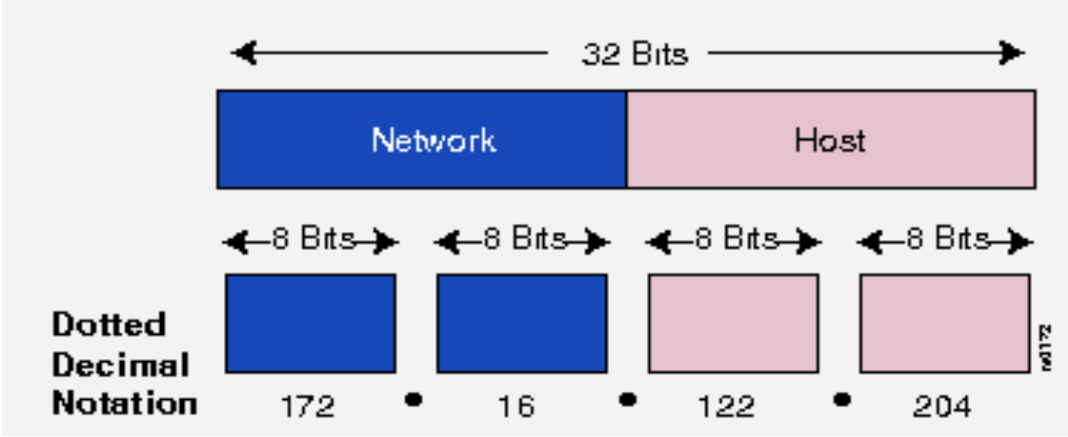
- An **Internet Protocol address** is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication
- IP address is a logical address
- An IP address serves two principal functions: host or network interface identification and location addressing

What is an IP address?

- An IP address, or Internet Protocol address, is a unique number that identifies a device connected to the internet:
- IP addresses allow devices to communicate with each other by sending and receiving data over the internet. They also identify and locate network devices.
- IP addresses are used to access data and information on the web. When a device sends a request to a server, its IP address is used to pass the request through routers, hubs, and other network nodes.
- There are two versions of IP addresses:
  - **IPv4:** The older version, which has space for up to 4 billion IP addresses.
  - **IPv6:** The newer version, which has space for trillions of IP addresses.

IPV4

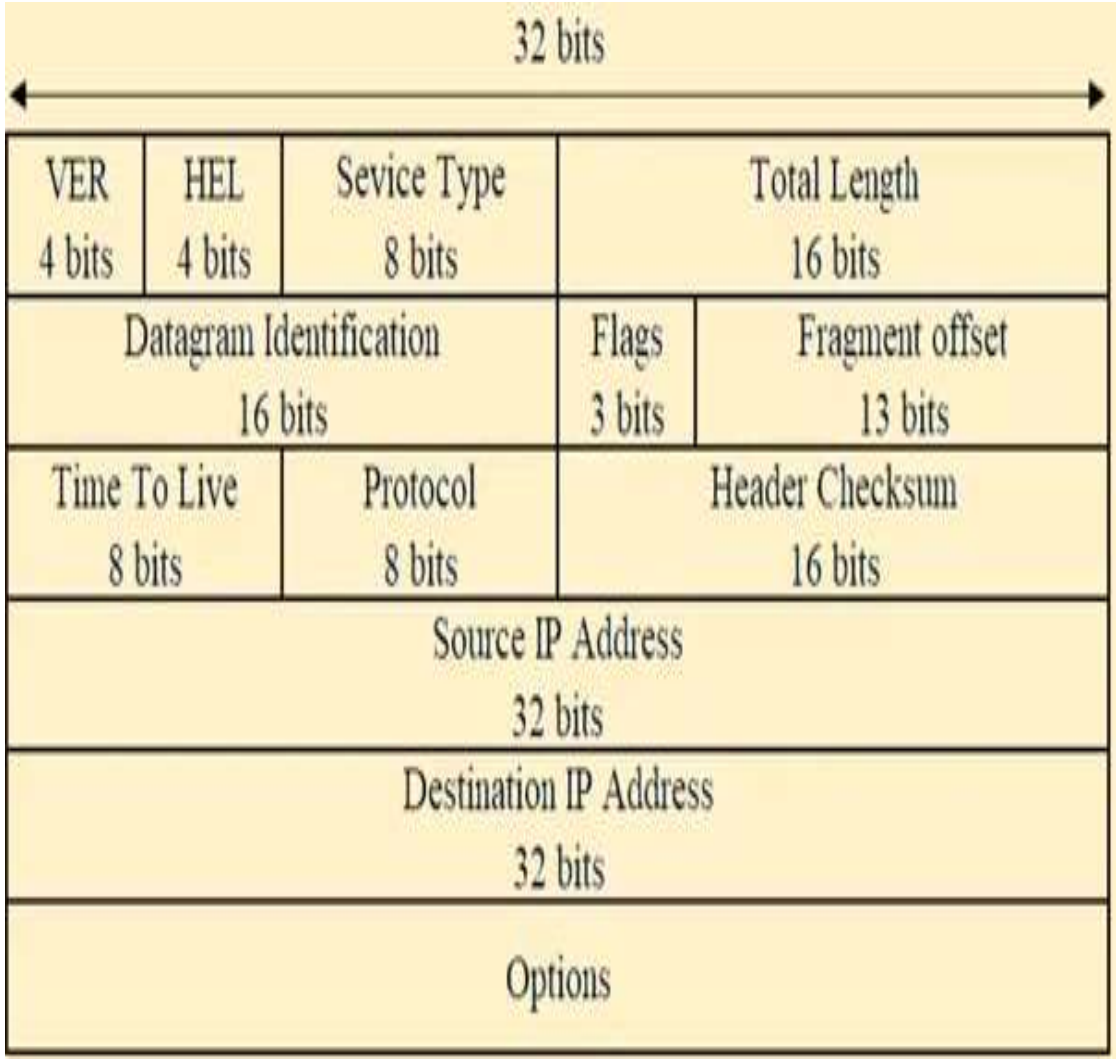
- The 32-bit IP address is grouped 8 bits at a time, each group of 8 bits is an octet. Each of the four octets are separated by a dot, and represented in decimal format, this is known as dotted decimal notation.
- Each bit in an octet has a binary weight (128, 64, 32, 16, 8, 4, 2, 1). The minimum value for an octet is 0 (all bits set to 0), and the maximum value for an octet is 255 (all bits set to 1)



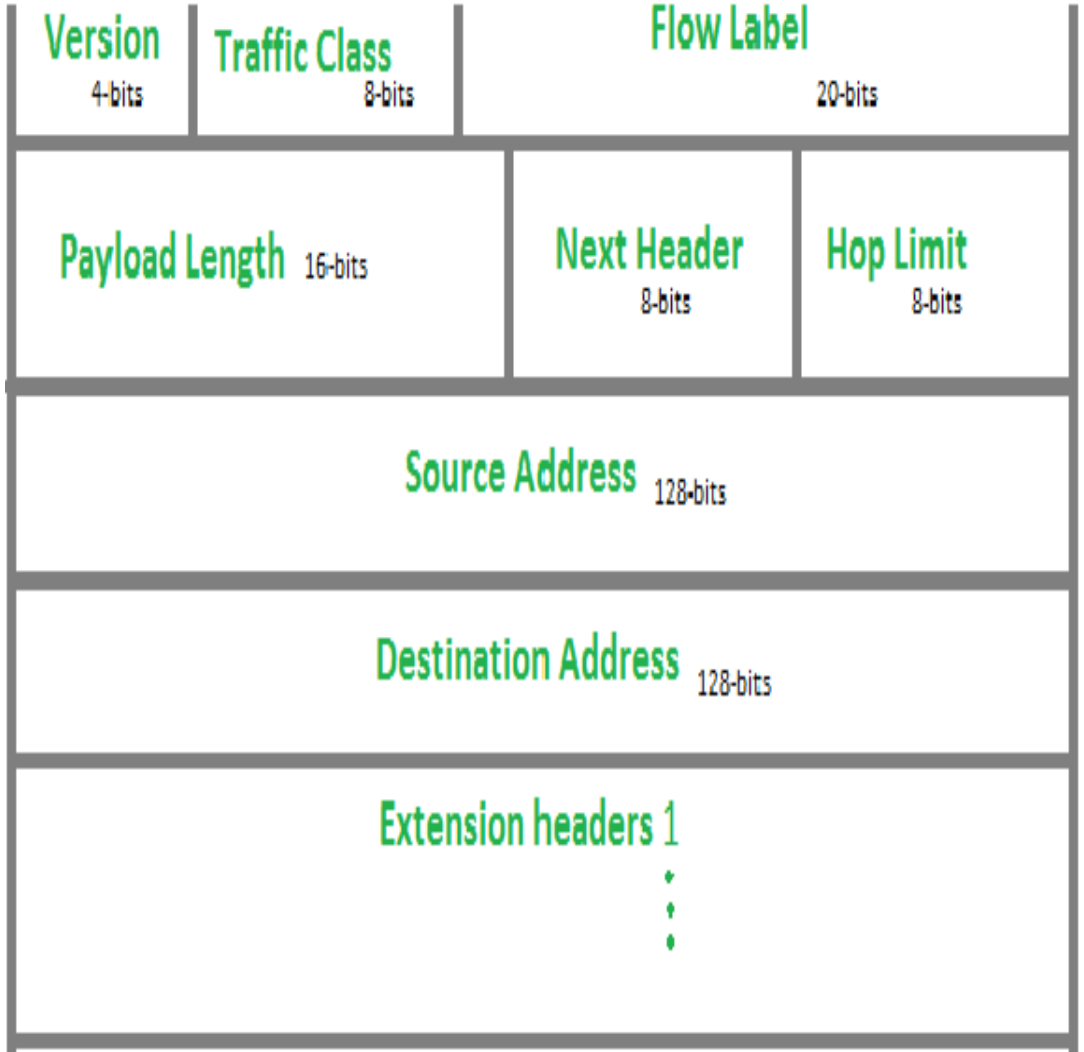
IPV6

- IPv6, or Internet Protocol version 6, is the latest version of the Internet Protocol (IP)
- IPv6 addresses are 128 bits long and are usually written as sequences of hexadecimal digits separated by colons.
- IPv6 can support 340 trillion addresses, which is enough for every networked device on the planet.
- The IPv6 address size is 128 bits. The preferred IPv6 address representation is: x:x:x:x:x:x:x:x , where each x is the hexadecimal values of the eight 16-bit pieces of the address. IPv6 addresses range from 0000:0000:0000:0000:0000:0000:0000:0000 to ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

IPV4 header format



IPV6 header format



Five different Classes of IPV4

- **Class A**: Used by large enterprises, government organizations, and ISPs. The first octet of a Class A address is 0-127, and the default subnet mask is 255.0.0.0.
- **Class B**: Used by universities, large schools, and mid-sized companies. The first two bytes of a Class B address specify the network prefix, and the default subnet mask is 255.255.0.0.
- **Class C:** Used by small businesses, home networks, and small organizations. The default subnet mask of a Class C address is 255.255.255.0.
- **Class D:** Used for multicast groups.
- Class E: Reserved for experimental use.

Five different Classes of IPV4

Class	First Octet decimal (range)	First Octet binary (range)	IP range	Subnet Mask	Hosts per Network ID	# of networks
Class A	0 – 127	**0**XXXXXXX	0.0.0.0-127.255.255.255	255.0.0.0	$2^{24}-2$	2^{7}
Class B	128 – 191	**10**XXXXXX	128.0.0.0-191.255.255.255	255.255.0.0	$2^{16}-2$	2^{14}
Class C	192 – 223	**110**XXXXX	192.0.0.0-223.255.255.255	255.255.255.0	$2^{8}-2$	2^{21}
Class D (Multicast)	224 – 239	**1110**XXXX	224.0.0.0-239.255.255.255			
Class E (Experimental)	240 – 255	**1111**XXXX	240.0.0.0-255.255.255.255			

How to recognize the network portion?

IP address = 192 . 100 . 10 . 33

Address Class = C

Network Portion = 192 . 100 . 10 . 33

Host Portion = 192 . 100 . 10 . 33

IP address = 11000000 . 01100100 . 00001010 . 00100001

Default subnet mask = 11111111 . 11111111 . 00000000 . 00000000

Bitwise AND operation = 11000000 . 01100100 . 00001010 . 00100001

Network Address

- First IP address of the range
- All zeros in the host portion
- Reserved for identifying complete network
- Cannot assign this address to any device in the network
- Only valid IP address are assigned to the hosts/clients

Broadcast Address

- Last IP address of the range
- All ones in the host portion
- Used to send broadcast to all within the same network
- Cannot assign this address to any device in the network
- Only valid IP address are assigned to the hosts/clients

Types of Communication

- Unicast
- Broadcast
- Multicast

Private IP and Public IP

- The main difference between a public IP address and a private IP address is their scope: public IP addresses are visible on the internet, while private IP addresses are only used within a local network:
- **Private IP addresses**
  - Has local reach. These addresses are only used within a local network, such as a home or office network.
  - Communicates within your private network with other devices in your home or office. They are assigned to devices by a router within the network.
  - A non unique numeric code that may be re-used by other device in other private network. Private IP addresses allow devices within a network to communicate securely with each other.
  - Free of charge
- **Public IP addresses**
  - Has global reach
  - Communicates outside your private network over the internet. These addresses are unique and visible to everyone on the internet. They are assigned by an ISP and allow devices to communicate with the internet. For example, your home address is like your public IP address, as it allows people to find you on the internet.
  - Unique numeric code never used by other device.
  - Not free, it should be payed

Subnetting

- Division of Network into multiple manageable parts
- It is the process of creating logical groups inside the network

Benefits of Subnetting

- Broadcast control
- Security improvement
- Traffic management
- Network management

Subnetting is a logical subdivision of one single network into multiple smaller networks. Hereby subnetting helps in minimizing the wastage of IP address

Tutorial

1. Perform the subnetting of 192.168.0.0 using CIDR value 25

Tutorial

2. Perform the subnetting of 192.168.0.0 using CIDR value 26

Tutorial

3. Perform the subnetting of 172.168.0.0 using CIDR value 17

Tutorial

4. Perform the subnetting of 172.168.0.0 using CIDR value 26

Tutorial

5. Perform the subnetting of 10.0.0.0 using CIDR value 9

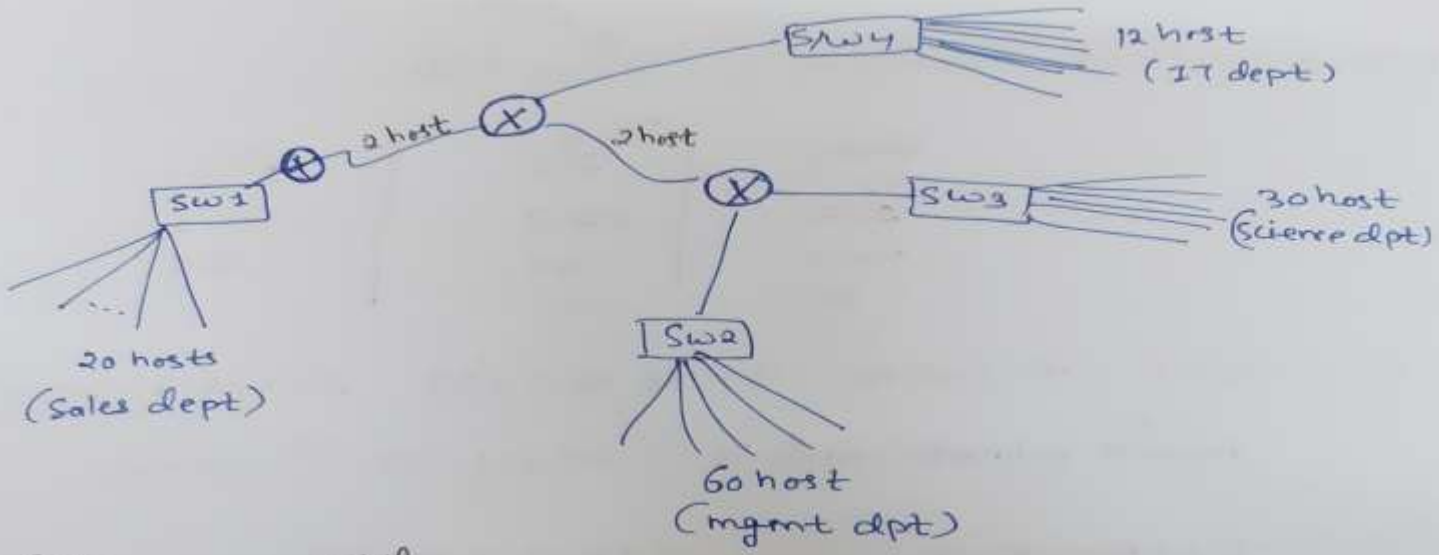
Tutorial

6. Perform the subnetting of 10.0.0.0 using CIDR value 11

Variable Length Subnet Mask (VLSM)

- In subnetting, we divided one large network into small networks but a subnet mask of same length
- But here in VLSM, we divide one large network into subnets with subnet mask of different length and we choose the length of mask according to the no of host required in our network

Consider a scenario as under



Soln.

Here total host = 20 + 60 + 30 + 12 + 2 + 2 = 126. (valid)

note

0-127 → Class A
128-191 → Class B
192-223 → Class C.

→ for class C ⇒ 192.168.16.0
192.168.16.1
⋮
192.168.16.254
192.168.16.255

} 254 valid IP

for our case, we have 126 host, so, our requirement is gained if we use Class C IP address.

For 60 valid host

① No. of valid host per network is $2^{6\text{ offbit}} - 2 = 60$

Since,

$2^5 - 2$
$= 32 - 2$
$= 30$

$2^6 - 2$
$= 64 - 2$
$= 62$ ✓

$2^7 - 2$
$= 128 - 2$
$= 126$

For 6 offbit, it implies 192.168.16.0 /26 ∴ CIDR is /26

new ~~default~~ subnet mask is 255.255.255.$\overset{2\,1}{11}$000000

② No. of network is
$2^{\text{m-bit}}$
$= 2^2$
$= 4$

③ Subnet mask is
255.255.255.192

④ Block size is 256 − 192 = 64

⑤ Subnetting table is

network id	1st IP	last IP	Broadcast IP
192.168.16.0	192.168.16.1 - - -	192.168.16.60	192.168.16.63
192.168.16.64	192.168.16.65 - - -	192.168.16.126	192.168.16.127
192.168.16.128	192.168.16.129 - - -	192.168.16.190	192.168.16.191
192.168.16.192	192.168.16.193 - - -	192.168.16.254	192.168.16.255
192.168.16.256			

for 30 valid host, CIDR is /26.

① No. of valid host per n/w is

$2^{n\text{ of bit}} - 2$

$2^5 - 2$ | $2^6 - 2$

$32 - 2$ | $64 - 2$

30 | 62

is OK.

② no. of network

$2^{\text{on bit}}$

2^2

$= 4$

③ new subnet mask is 255.255.255.192

④ Block size $256 - 192$

64.

for 20 valid host, CIDR is /27

① No. of valid host per n/w

$2^{\text{host bit}} - 2$

$2^4 - 2$ $2^5 - 2$

16-2   32-2

(14)   (30) is ok.

② No. of n/w

⇒ 2^3

⇒ 8

③ Subnet mask.

⇒ 255.255.255.11100000

⇒ 255.255.255.224.

④ Block size

256-224

⇒ 32

⑤ Calculate Subnetting table.

Network ID.	1st IP --- last IP	Broadcast IP
192.168.16.0	192.168.16.1 --- 192.168.16.30	192.168.16.31
192.168.16.32	192.168.16.33 --- 192.168.16.62	192.168.16.63
192.168.16.64	192.168.16.65 --- 192.168.16.94	192.168.16.95
192.168.16.96	192.168.16.97 --- 192.168.16.126	192.168.16.127
192.168.16.128	192.168.16.129 --- 192.168.16.158	192.168.16.159
192.168.16.160	192.168.16.161 --- 192.168.16.190	192.168.16.191
192.168.16.192	192.168.16.193 --- 192.168.16.222	192.168.16.223
192.168.16.224	192.168.16.225 --- 192.168.16.254	192.168.16.255
~~192.168.16.255~~		

for 12 valid host : CIDR is /28

① No. of valid host per nw is

$2^{off\ bit} - 2$

$2^4 - 2$

14

[illegible] 12 [illegible]
+1 gateway [illegible]
+1 extra reserve [illegible]

② No. of Subnet/network.

$2^{on\ bit}$

2^4

16

③ New Subnet mask is

255.255.255.11110000

255.255.255.240

④ Block size

256 − 240

16

⑤ Subnetting table

Network ID	1st IP	Last IP	Broadcast IP
192.168.16.0	192.168.16.1 ----	192.168.16.14	192.168.16.15
192.168.16.16	192.168.16.17 ----	192.168.16.30	192.168.16.31
192.168.16.32	192.168.16.33 ----	192.168.16.46	192.168.16.47
192.168.16.48	192.168.16.49 ----	192.168.16.62	192.168.16.63
192.168.16.64	192.168.16.65 ----	192.168.16.78	192.168.16.79
192.168.16.80	192.168.16.81 ----	192.168.16.94	192.168.16.95
192.168.16.96	192.168.16.97 ----	192.168.16.110	192.168.16.111
192.168.16.112	192.168.16.113 ----	192.168.16.126	192.168.16.127
192.168.16.128	192.168.16.129 ----	192.168.16.142	192.168.16.143
192.168.16.144	192.168.16.145 ----	192.168.16.158	192.168.16.159
192.168.16.160	192.168.16.161 ----	192.168.16.174	192.168.16.175
192.168.16.176	192.168.16.177 ----	192.168.16.190	192.168.16.191
192.168.16.192	192.168.16.193 ----	192.168.16.206	192.168.16.207
192.168.16.208	192.168.16.209 ----	192.168.16.222	192.168.16.223
192.168.16.224	192.168.16.225 ----	192.168.16.238	192.168.16.239
192.168.16.240	192.168.16.241 ----	192.168.16.254	192.168.16.255

192.168.~~16.256~~

(5) for 2 Host / cidr value is /30

① No. of Valid host per n/w ⇒ $2^{\text{no. of host bit}} - 2$

⇒ $2^2 - 2$

⇒ 4 - 2

⇒ 2.

② no. of n/w ⇒ $2^{\text{n-bit}}$

⇒ 2^6

⇒ 64.

③ Subnet mask.

255.255.255.11000000

255.255.255.252

④ Block size

256-252

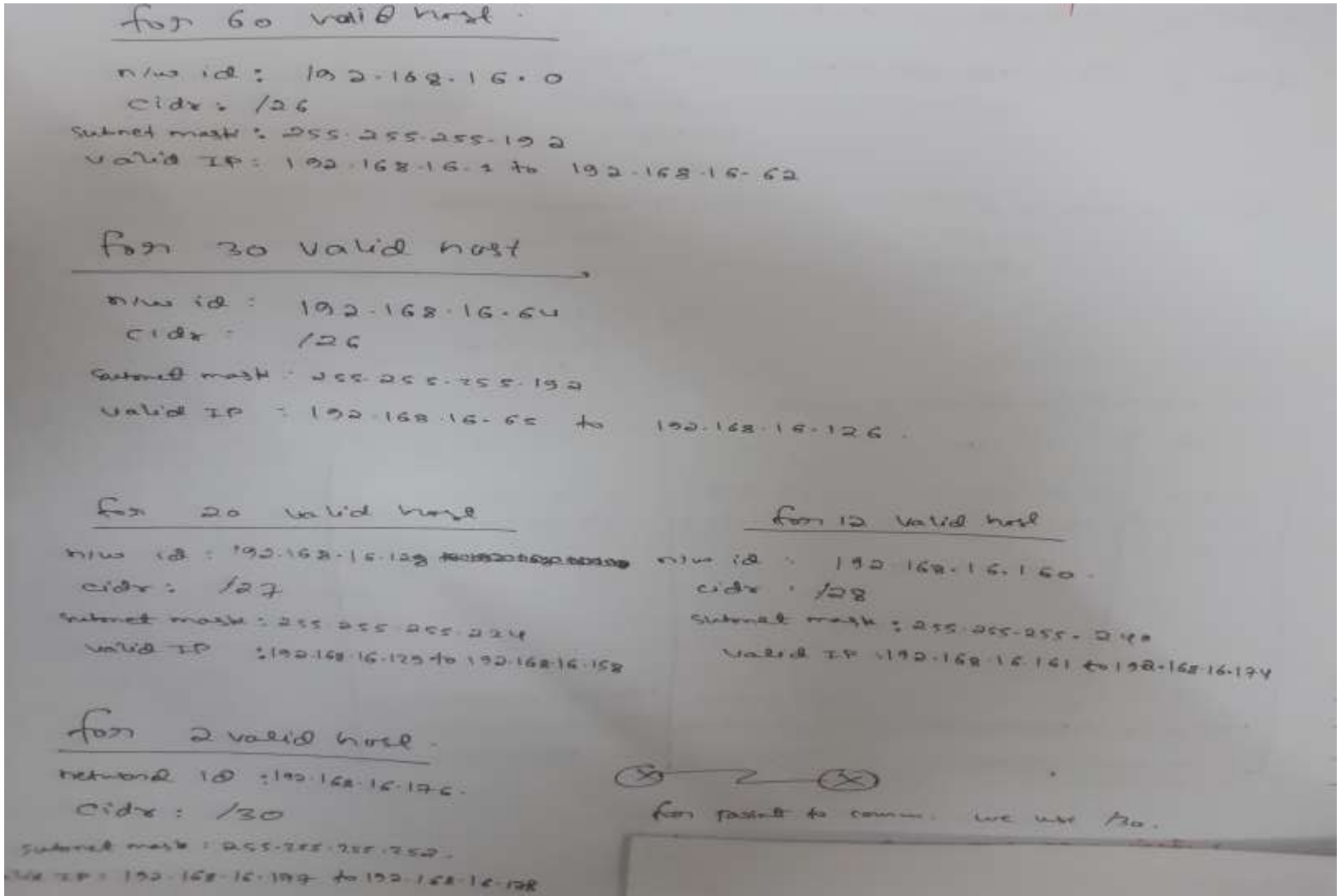
⇒ 4.

⑤ Calculate subnetting table.

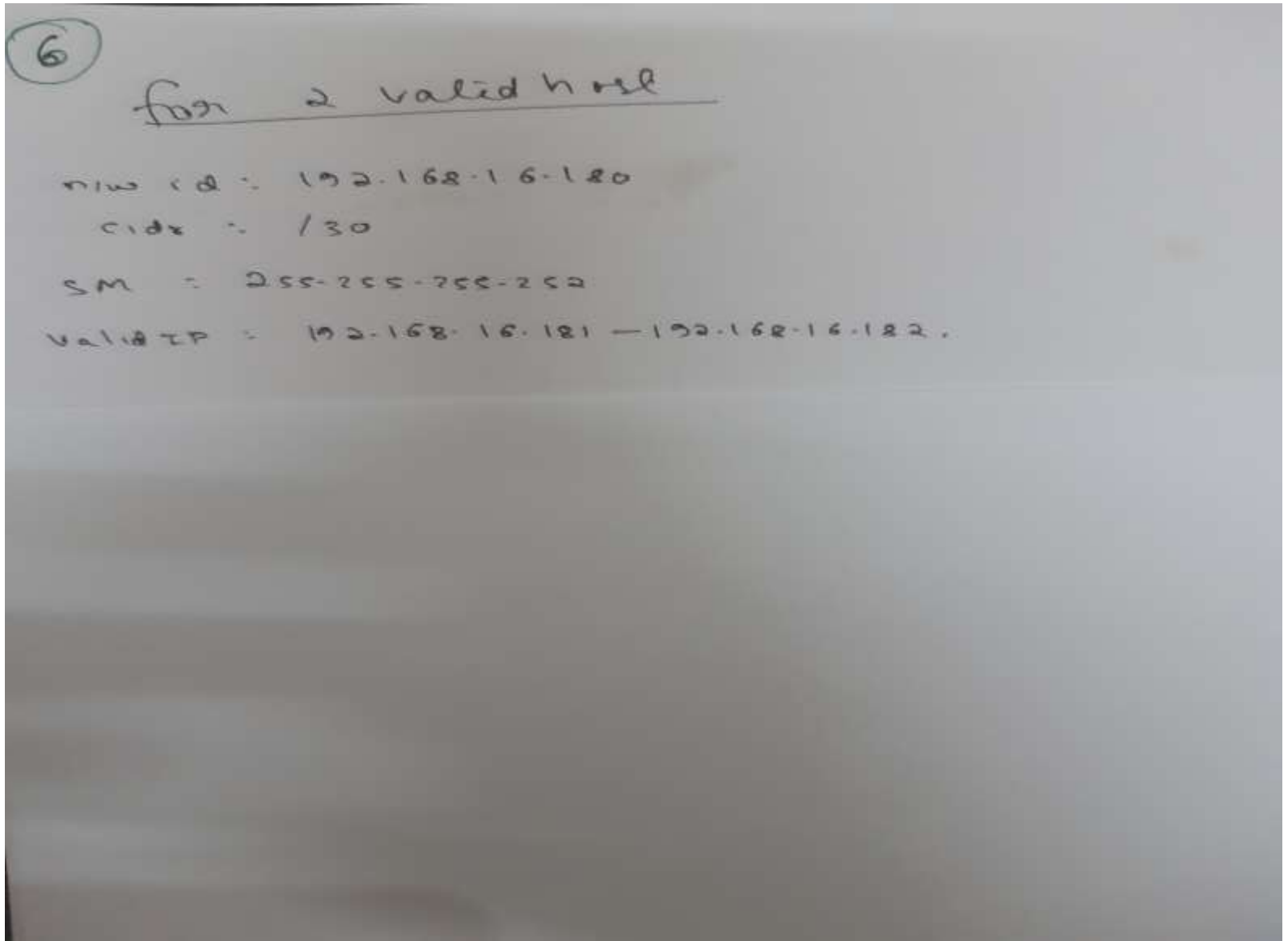
n/w id	1st IP ---- last IP.	Bid
192.168.16.0	192.168.16.1 ---- 192.168.16.2	192.168.16.3
192.168.16.4	192.168.16.5 ---- 192.168.16.6	192.168.16.7
192.168.16.8	.	
		192.168.16.247
192.168.16.248	192.168.16.249 ---- 192.168.16.250	192.168.16.251
192.168.16.252	192.168.16.253 ---- 192.168.16.254	192.168.16.255

192.168.16.256

Documentation report of the given network



Documentation report of the given network



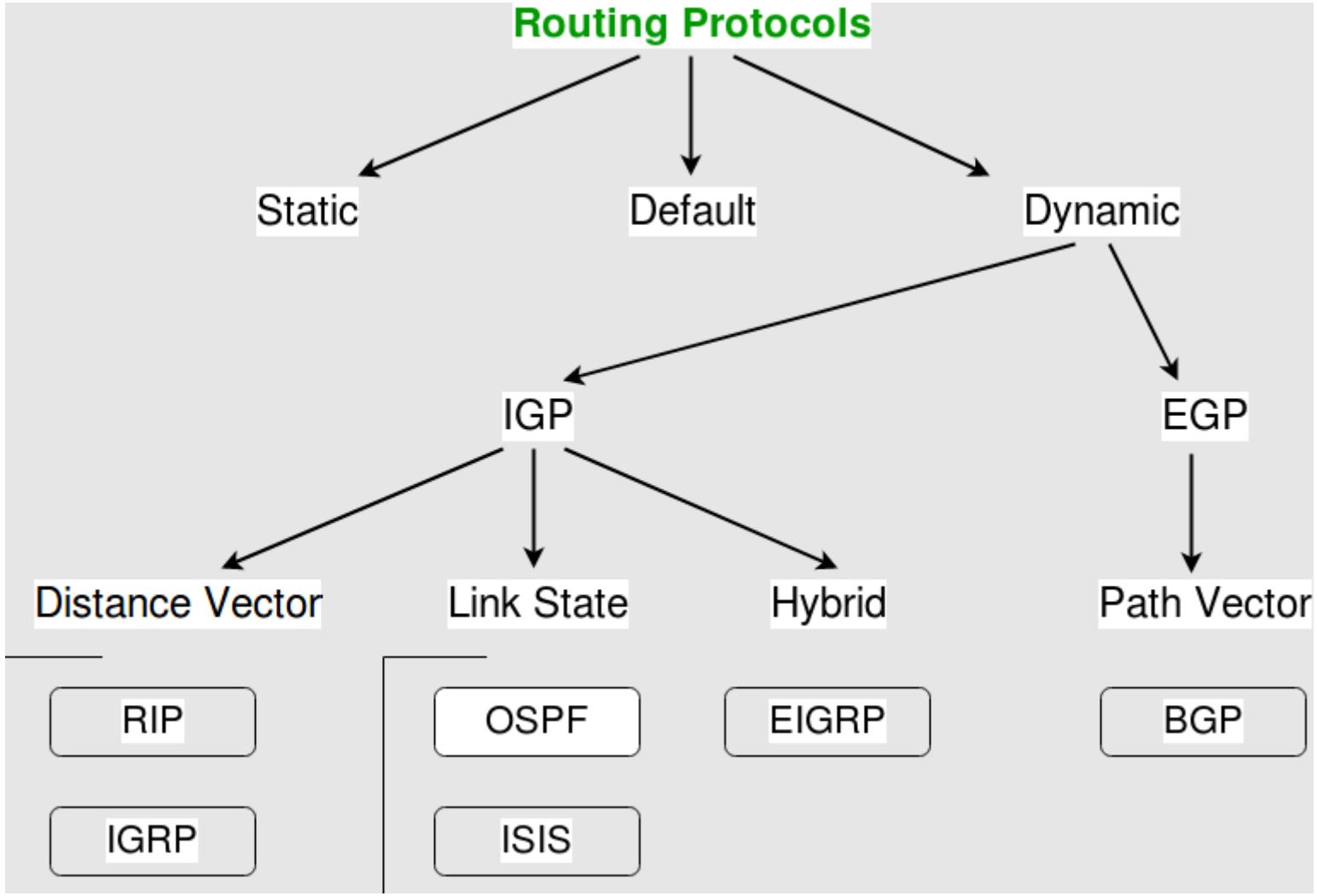
Why is routing essential?

- Routing is essential in computer network to give a least cost path
- Least cost path = least hop
- Hence different routing algorithms are applied in order to route the packets to the destination for searching the least cost path
- Router contains the routing table which has the information regarding the cost or distance, destination, maximum hop

- Static Routing / non-adaptive routing
  - Static routing do not base their routing decision on the measurement and estimation of the current traffic and topology.
  - Instead the choice of the route is computed in advance, off line and downloaded to the routers when the network is booted
- Dynamic Routing / adaptive routing
  - In contrast to static routing, dynamic routing change their routing decision to reflect changes in the topology and usually the traffic as well

Unicast and multicast routing

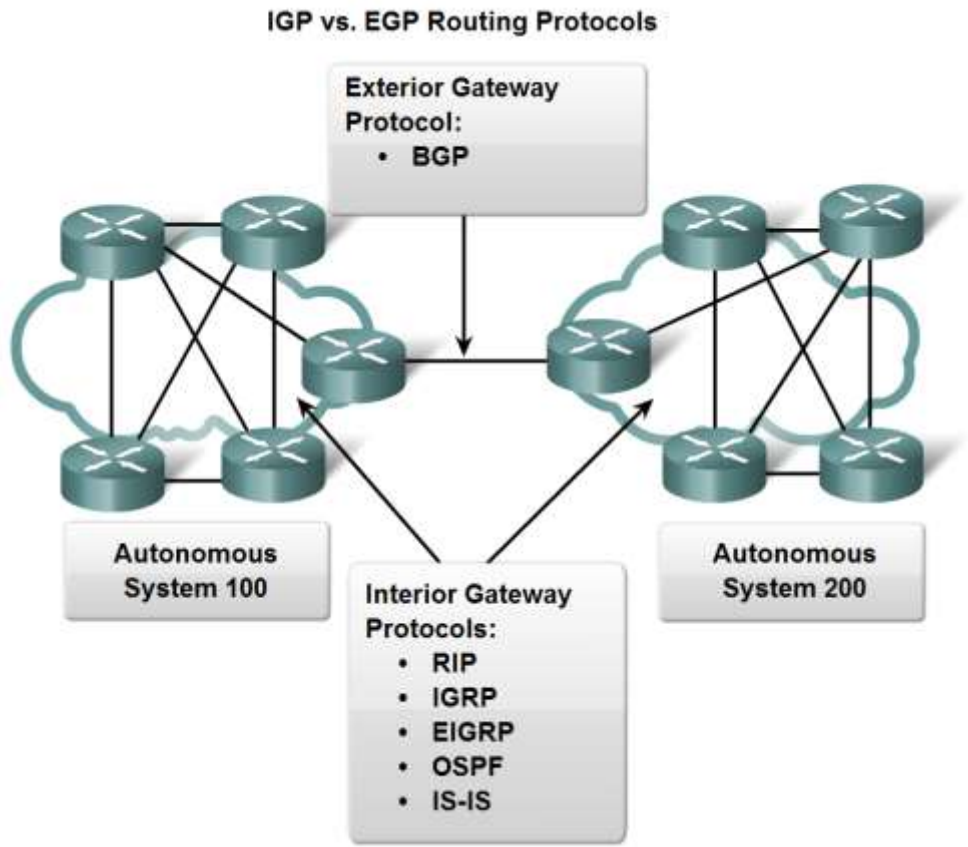
- A unicast transmission/stream sends IP packets to a single recipient on a network
- A multicast transmission send IP packets to a group of host on a network
- Multicasting routing is a networking method for efficient distribution of one-to-many traffic
- A multicast source, such as live video conference sends traffic to a multicast group
- The multicast group contains receivers such as computers and other devices


Routing Protocols
Static
Default
Dynamic
IGP
EGP
Distance Vector
Link State
Hybrid
Path Vector
RIP
IGRP
OSPF
ISIS
EIGRP
BGP

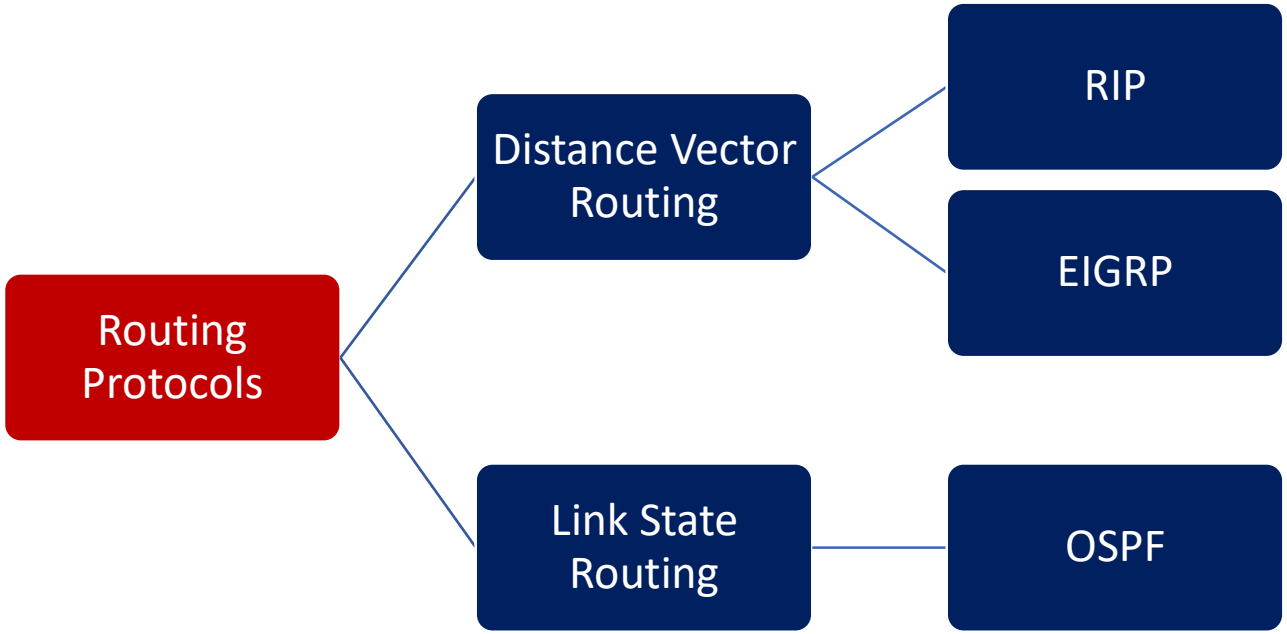
Routing Protocols

- Interior Gateway Routing Protocols
  - ✓ Used for Routing Inside an Autonomous System (AS).
  - ✓ AS => Network under Common Administration.
  - ✓ Examples => RIP, EIGRP and OSPF
- Exterior Gateway Routing Protocols
  - ✓ Used for Routing between Autonomous System (AS)

Routing Protocols: Example



Routing Protocols: Classification



Routing Protocols

- Distance Vector Routing Protocols
  - ✓ Incomplete View of Topology.
  - ✓ Routes are advertised as Vectors of Distance and Direction.
  - ✓ Generally Periodic Updates.
- Link State Routing Protocols
  - ✓ Complete View of Network Topology.
  - ✓ Updates are Not Periodic. (Bounded and Triggered Updates).

Distance Vector Routing	Link State Routing
Bandwidth required is less due to local sharing, small packets and no flooding.	Bandwidth required is more due to flooding and sending of large link state packets.
Based on local knowledge, since it updates table based on information from neighbours.	Based on global knowledge, it have knowledge about entire network.
Make use of Bellman Ford Algorithm.	Make use of Dijakstra's algorithm.
Traffic is less.	Traffic is more.
Converges slowly i.e, good news spread fast and bad news spread slowly.	Converges faster.
Count of infinity problem.	No count of infinity problem.
Persistent looping problem i.e, loop will be there forever.	No persistent loops, only transient loops.
Practical implementation is RIP and IGRP.	Practical implementation is OSPF and ISIS.

Tutorial

- What are the drawbacks of IPV4? Which of the drawbacks do IPV6 solve? Explain
- Explain briefly IPV4 and IPV6 header protocol format
- Perform sub netting of 92.168.0.0 using CIDR value26. What is VLSM and why do we use it?
- What are the benefits of sub netting? Perform the sub netting of 10.0.0.0 using CIDR value 11
- Pokhara university has three different departments namely Computer, Software, Civil Engineering with 60, 30 and 10 network devices. Design a network using suitable IP address to compute the network address, broadcast address and usable IP Pool
- What is routing table? Illustrate with a suitable example
- What is the significance of routing in computer network? Differentiate between link state routing and distance vector routing.
- Write short notes on.
  - Classful and Classless Routing
  - Adaptive and non-adaptive routing
  - Unicast and multicast routing