Unit-4: Network Layer

- Ankit Pangeni DATE

4.1

Introduction and Functions

The network layer is considered as the backbone of OSI model. It selects and manages the best logical path for data transfer between nodes. It is up to the Network layer to transport traffic between devices that aren't locally attached. This layer contains hardware devices such as routers, bridges, firewalls & switches. In the OSI model, the network ~~model~~ layer responds to requests from the layer above it (Transport layer) & issues requests to the layer below it. (Data link layer)

Functions:

- It translates logical network address into physical address with circuit, message or packet switching
- Routers & gateways operate in this layer
- It breaks larger packets into small packets
- Connection services are provided including network flow control, network layer error control & packet sequence control.

4.2

IPV4 Addressing

IPV4 addresses are 32 bit numbers that are typically displayed in dotted decimal notation. They are unique. They are unique in a sense that each address defines one and only one

classmate PAGE

DATE

connection to the Internet. A 32-bit address contains two primary parts: the network prefix and the host number. All hosts within a single network share the same network address and each host also has an address that uniquely identifies it. IP addresses are assigned by a central numbering authority called the Internet Assigned Numbers Authority (IANA)

The IPV4 contains the following sections:

4-3

1) IPV4 Classful Addressing

In classful addressing the address space is divided into five classes: A, B, C, D and E. Each class occupies some part of the address space. We can find the class of an address when address is given in binary notation or dotted-decimal notation.

→ If the address is given in binary notation, the first few bits can immediately tell us the class of address

→ If the address is given in decimal-dotted notation, the first byte defines the class.

Class A → Addresses use only the first byte (octet) to specify the network prefix, leaving 3 bytes to define individual host numbers

Class B → Addresses use the first 2 bytes to specify the network prefix, leaving 2 bytes to define host address

Class C → Addresses use the first 3 bytes to specify the network prefix, leaving only the last byte to identify hosts

DATE

In binary format, with an X representing each bit in the host number, the three address classes can be represented as follows

00000000	XXXXXXXX	XXXXXXXX	XXXXXXXX (class A
00000000	00000000	XXXXXXXX	XXXXXXXX (class B)
00000000	00000000	00000000	XXXXXXXX (class C)

Each bit X represents a power of 2 indicating how many host numbers can be created for a particular network prefix. Class A have 2^{24} possible host no., Class B have 2^{16} and class C have 2^8.

The 32-bit IPV4 addresses are most often expressed in dotted decimal notation, in which each octet (or byte) is treated as a separate number. Within an octet, the rightmost bit represents 2^0 (or 1) increasing to the left until the first bit in the octet is 2^7 (or 128). ex.

11010000 01100010 11000000 10101010
= 208.98.192.170

01110110 00001111 11110000 01010101 = 118.15.240.85
00110011 11001100 00111100 00110011 = 51.204.60.59

The number of networks and the number of hosts per class can be derived by this formula:

No. of networks = $2^{\text{network bits}}$

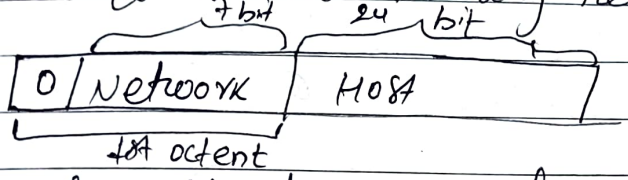
No. of Hosts/network = $(2^{\text{network bits}} - 2)$

classmate

DATE

Class A address

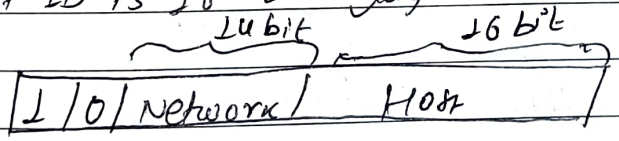
Here, the network ID is 8 bits long and the host ID is 24 bits long. Here, the MSB ie. 1st bit of the first octet is always set to 0. The remaining 7 bits in 1st octet are used to determine network ID. The 24 bits of host ID are used to determine the host in any network.



Thus, the 1st octent ranges from (00000001 - 01111111) ie (1 - 127) which means class A addresses only include Ip starting from 1.x.x.x to 126.x.x.x only. The Ip range 127.x.x.x is reserved for loopback Ip addresses. The default subnet mask for class A ip address is 255.0.0.0 which implies Class A addressing can have $2^7 - 2$ ie. 126 networks and $2^{24} - 2$ ie. 16777214 hosts. Class A Ip address formats ONNNNNNN HHHHHHHH HHHHHHHH HHHHHHHH

Class B address

Here, the network ~~ID~~ ID is 16 bits long. and the host ID is 16 bits long.



Class B Ip addresses range from 128.x.x.x to 191.255.x.x. The default subnet mask for class B is 255.255.x.x. Thus, the 1st octant ranges from 128-191 ie.

(10 000001 - 10111111)

ie. (128 - 191)

PAGE

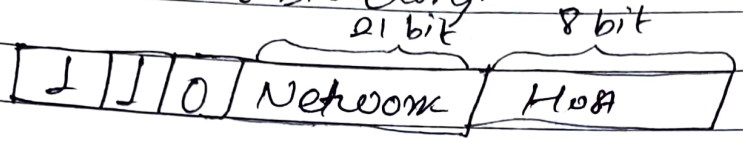
classmate Class B Ip address format is

10NNNNNN NNNNNNNN HHHHHHHH HHHHHHHH

DATE

Class C Address.

The network ID is 24 bits long and the host ID is 8 bits long.



IP addresses belonging to class C ranges from 192.0.0.X – 223.255.255.X & the default subnet mask is 255.255.255.0. The 1st octet ranges from:

11000001 – 11011111

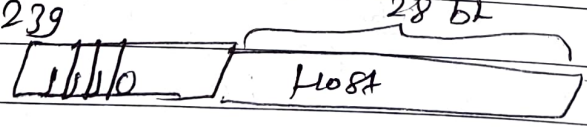
i.e. 192 – 223

Class D Address (used for multicasting)

The higher order bits of the 1st octet of IP addresses belonging to class D are always set to 1110. The remaining bits are for the address that interested hosts recognize. Class D doesn't have any subnet mask. IP address belonging to class D ranges from 224.0.0.0 – 239.255.255.255

11100000 – 11101111

i.e. 224–239



Class E Address (used for military purpose)

IP addresses of class E ranges from 240.0.0.0 – 255.255.255.254. This class doesn't have any subnet mask. Higher order bits of 1st octet of class E are always set to 1111.

i.e. 1111 0000 – 1111 1111 i.e. 240 to 255

classmate

PAGE

DATE

Rules for assigning Host ID

Host ID's are used to identify a host within a network. They are assigned based on following rules:

→ The Host ID must be unique.
→ Host ID in which all bits are 0 and all bits are 1 can't be assigned because they are used to represent network ID of the IP address & for broadcasting address to all hosts.

Rules for assigning Network ID

→ Network ID can't start with 127 because it is reserved for internal loop back functions
→ Network ID with all bits set to 0 and all bits set to 1 cannot be assigned because they are used to denote specific host on local network & reserved for an IP broadcast address

Problems / disadvantages of/with classful addressing

→ **Wastage of IP addresses:** Ex: In class A, no. of hosts in each network is $2^{24} - 1$ crore which is very huge. i.e. more than requirement. but there are very limited network of class A so, there is wastage of IP addresses & also class D & class E IP address are reserved which leads to wastage. Many of class B are wasted & class C is so small, it doesn't meet requirements
→ **Maintenance is time consuming**
→ **More prone to errors**
→ **Less flexible.**

DATE

Q. Given Ip address:
201.20.30.40
Calculate: Network ID, 4th Host ID, Last Host ID, Broadcast address

⇒ Given Ip address 201.20.30.40
This belongs to class C address Its default Subnet mask is 255.255.255.0

1) Network ID:

1st write all numbers in binary form

201.20.30.40 = 11001001 . 00010100 . 00011110 . 00101000
255.255.255.0 = 11111111 . 11111111 . 11111111 . 00000000
AND operation 11001001 . 00010100 . 00011110 . 00000000

In Decimal: 201 . 20 . 30 . 0

2) 4th Host ID: (00000000.00000000.00000000.xxxxxxxx) (4th address) (class C, host)
Total host available = $2^8 = 256$
In which we can't use two Ip addresses (1st & last)
Here, 1st Ip = 201.20.30.1 (we can't use 0)
2nd Ip = 201.20.30.2
3rd Ip = 201.20.30.3
4th Ip = 201.20.30.4
∴ 4th Host ID = 201.20.30.4

3) Last Host ID: 201.20.30.254 (because we can't use 255) (Last address)

4) Broadcast address: 201.20.30.255

4.3

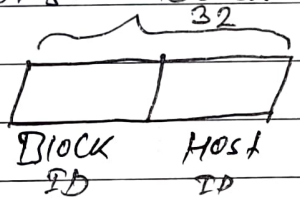
DATE

2) Classless addressing (CIDR)

Classless addressing is another concept of addressing the IPv4 addresses which was adopted ~~aft~~ in 1993 after the failure of classful addressing. The classless addressing assigns a block of address to the customer according to its requirement which prevents the wastage of addresses. It doesn't divide the address space into classes like classful addressing. It provide a variable length of blocks which have a range of addresses according to the need of users.

CIDR Notation

The classless addressing divides the IPv4 addresses into two parts: Block ID (network ID) and Host ID



The ipaddress is still 32 bit, but the msb bits represent block/network id

IP address is written in the form of x.y.z.w/n where n is the no. of bits that represent the block/network. Ex: 200.10.20.40/28.

Here, 28 represents the network ID has 28 bits and host ID has (32-28) ie. 4 bits. Its default subnet mask is 11111111.11111111.11111111.11110000 ie. 255.255.255.240

* No. of hosts = $2^4 = 16$ (no. of addresses)
* Network ID => 200.10.20.00101000 (1st address)

Now, replace last 4 bits by 0

200.10.20.00100000

ie. 200.10.20.32/28

is network / block ID

classmate

PAGE

DATE

Or you can do AND operation with default Subnet mask

200.10.20.40 = 11100100.00010100.00010100.00101000
255.255.255.240 = 11111111.11111111.11111111.11110000
AND operation ⇒ 11100100.00010100.00010100.00100000
ie 200.10.20.32

Note: If asked for last address, do AND operation with complement of mask i.e last 4 bits of network address as 1111

(property) Rules for Classless addressing

→ Addresses should be contiguous (ie. 200.10.20.32 - 33 - 34
→ No of addres in a block should be in power of 2
In above Ex, the no of hosts = 16, so we can generate 16 IP addresses, which is in divisible by 2.
→ The first address must be evenly divisible by the number of addresses.

classmate

PAGE

4.4

DATE

IPv4 Sub-netting / super-netting

Subnetting is the process of dividing the network into sub-networks. It means, creating networks within a network. Each of the small networks are called subnet and each of these subnets has its own specific address. To create additional networks, we use a subnet mask. It determines which portion of the IP address belongs to the host. The subnet address is created by dividing the host address into network & host address. The network address specifies the type of subnetwork in the network & the host address specifies the host of that subnet. Ex: ~~129~~ 172.16.1.0, 172.16.2.0, 172.16.3.0 & 172.16.4.0 are all subnets within network 127.16.0.0

Why use Sub netting?

When a network becomes too big with too much traffic, performance can begin to suffer. Breaking the network into smaller parts can help to increase network performance upto its original performance. A subnet allows router to choose the right destination for packets. Subnetting also improves network security

How to create subnets?

Creating subnetworks is essentially taking bits from the host portion of the address & reserving them to define the subnet address instead. Clearly this will result in less bits for defining hosts, which you'll always want to keep in mind.

classmate

PAGE

DATE

To create a subnet, we fulfil these three steps:

1. Determine the no. of required network IDs
   - One for each LAN subnet
   - One for each wide area connection

2. Determine the no. of required host IDs per subnet
   - One for each TCP/IP host
   - One for each router interface

3. Based on previous requirements, create the following
   - A unique subnet mask for your entire network
   - A unique subnet ID for each physical segment
   - A range of Host IDs for each subnet

Subnet Mask

A subnet mask is a 32 bit address used to distinguish a network address and host address in an IP address. The 32-bit subnet mask is composed of 1s and 0s, where the 1s represent the positions that refer to the network subnet address. Table below shows the default subnet masks for classes A, B and C

Class	Format	Default subnet mask
A	network. host. host. host	255.0.0.0
B	network. network. host. host	255.255.0.0
C	network. network. network. host	255.255.255.0

DATE

Q. If 200.100.10.66/26 is IPv4 address then answer the following questn

a) Is this a host, network or broadcast address?
b) What is the subnet mask in dotted decimal?
c) What is network address?
d) What is broadcast address?
e) What is the first usable host address?
f) What is the last usable host address?
g) How many usable hosts are in the network?
h) What is the next available network address?

=) Given, IP address 200.100.10.66/26.
It means network ID has 26 bits and host ID has 6 bits

∴ Subnet mask: 11111111.11111111.11111111.11000000.
⇒ 255.255.255.192

~~Net~~
Total hosts = $2^6 = 64$
Usable hosts = 64-2 = 62
Total subnets = $2^2 = 4$ [Here, 2 came from the no of masked bits in ~~host~~ last octet ie no of 1's.
Total hosts per subnet = $2^6 - 2 = 62$
Valid subnets = 256-192 = 64 [Here, 6 is no of unmasked bits ie 0's

Subnet	Usable IP Pool (1st host to last host)		Broadcast ID
	First host	Last host	
200.100.10.0	200.100.10.1	200.100.10.62	200.100.10.63
200.100.10.64	200.100.10.65	200.100.10.126	200.100.10.127
200.100.10.128	200.100.10.129	200.100.10.190	200.100.10.191
200.100.10.192	200.100.10.193	200.100.10.254	200.100.10.255

classmate

PAGE

DATE

a:) It is host address

b:) 255.255.255.192

c:)

200.100.10.01000010
255.255.255.11000000
AND 200.100.10.01000000

i.e. ~~255.255.25~~

i

200.100.10.01000010
255.255.255.11000000
AND 200.100.10.010.0.0000

i.e. 200.100.10.64/26

d) Subnet mask OR

200.10.10.01000010
0.0.0.00111111
200.10.10.01111111

i.e 200.10.10.127/26

(Complement) Replace last 6 bits of network address by 1111n you get 200.100.10.127

(a)

e) 200.100.10.65/26

f) 200.100.10.126/26

g) 62

h) 200.100.10.128/26

(b) (c) (d) (e) (f) (g) (h)

DATE

Classless Inter-Domain Routing (CIDR)

It is basically the method that ISPs use to allocate a number of addresses. They provide address in certain block size. We will receive a block of address from ISP like this:- 192.168.10.32/28 This is telling us what our subnet mask is. The slash notation (/) means how many bits are turned on (1's). The maximum could only be /32. But we have to keep at least 2 bits for host bits so the largest subnet mask available relevant to the Cisco exams objectives can only be a /30

Class A → /8 to /15
Class B → /16 to /23
Class C → /24 to /30

(a) Subnetting Class C Addressing

Binary (4th octet)	Decimal Dotted	CIDR
00000000	255.255.255.0	/24
10000000	255.255.255.128	/25
11000000	255.255.255.192	/26
11100000	" .224	/27
11110000	" .240	/28
11111000	" .248	/29
11111100	" .252	/30

i) No. of subnets → 2^x, where x is no. of masked bits (1's)
ii) No. of hosts per subnet → $2^y - 2$, y is no. of unmasked bits (0's)
iii) No. of usable hosts = $2^y - 2$ & no. of hosts = 2^y
iv) Block size = 256 - subnet mask.

DATE

(b) Subnetting Class B Addresses

Binary (3rd & 4th octet)	Decimal dotted	CIDR
00000000 00000000	255.255.0.0	/16
10000000 00000000	255.255.128.0	/17
⋮	⋮	⋮
11111111 00000000	255.255.255.0	/24
11111111 10000000	255.255.255.128	/25
⋮	⋮	⋮
11111111 11111100	255.255.255.252	/30

The process of subnetting a Class B is almost the same as subnetting Class C., except that we have more host bits & we start in the third octet. Use the same subnet numbers for the third octet with Class B that we used for the fourth octet with Class C, but add zero to the network portion & a 255 to the broadcast section in the fourth octet

Q. If 172.16.0.0/17 is IPV4 address then answer the following questions (same qns. as previous example)

=) Ip address: 172.16.0.0/17

Subnet Mask: 11111111.11111111.10000000.00000000
= 255.255.128.0

Total subnets = $2^1 = 2$
Total hosts = $2^{15} = 32768$

classmate

PAGE

DATE

Usable hosts = $2^{15} - 2 = 32766$
Valid subnets (3rd octet) = $256 - 128 = 128$
Valid subnets (4th octet) = $256 - 0 = 256$.

Subnet (Network IP)	Usable IP pool (First host to last host) First host	Last host.	Broadcast IP
172.16.0.0	172.16.0.1	172.16.127.254	172.16.127.255
172.16.128.0	172.16.128.1	172.16.255.254	172.16.255.255

a) => It is a network address.
b) => 255.255.128.0
c) =>

172.16.00000000.00000000
AND 255.255.1000 0000.00000000
172.16.0.0/17

Binary
127.16.01111111.11111111
=> 172.16.127.255/17

d) => 172.16.0000 0000.00000000
0.0.01111111.11111111
172.16.01111111.11111111
ie. 172.16.127.255/17

e) => 172.16.0.1/17

f) => 172.16.127.254/17

g) => 32766

h) => 172.16.128.0/17

DATE

c) Subnetting class A address

Binary (2nd, 3rd, 4th octet)	Subnet Mask	CIDR value
00000000 00000000 00000000	255.0.0.0	/8
10000000 00000000 00000000	255.128.0.0	/9
⋮	⋮	⋮
11111111 11111111 10000000	255.255.255.128	/25
11111111 11111111 11111100	255.255.255.252	/30

Table: Class A subnet mask

Subnetting class A is similar as class B or class C subnet. We must leave at least 2 bits for defining hosts. Again we have more host bits & we just use the same subnet numbers we used with class B & C but we start using these numbers in the second octet

Q. If 10.1.0.0/9 is a IPV4 address then find all network address, broadcast address, usable host, total subnets, total hosts, valid subnets.

a)
b)
c)

⇒ IP address: 10.1.0.0/9
Subnet Mask: 11111111.10000000.00000000.00000000
⇒ 255.128.0.0

a) –
b)
c)

Total subnets = $2^1 = 2$
Total hosts = $2^{23} = 8388608$

classmate

PAGE

DATE

Usable hosts = $2^{23} - 2 = 8388606$
Valid subnets (2nd octet) = 256 - 128 = 128
Valid subnets (3rd octet) = 256 - 0 = 256
Valid subnets (4th octet) = 256 - 0 = 256
Network address = 10.0.0.0/9
Broadcast address = 10.127.255.254/9

Subnet	Usable IP range (1st host to last host)		Broadcast
Network IP	First host	Last host	IP
10.0.0.0	10.0.0.1	10.127.255.254	10.127.255.255
10.128.0.0	10.128.0.1	10.255.255.254	10.255.255.255

Let's take a final example

Q Given IP address 192.168.10.0/28

a) Find the subnet mask.
b) Find the total number of network that can be created
c) Find the total number of host on each network.

⇒ Given, 192.168.10.0/28
Subnet mask: 11111111.11111111.11111111.11110000

a) Subnet Mask 255.255.255.240

b) No. of subnetwork = $2^4 = 16$ (total subnets)

c) No. IP address (hosts) on each subnetwork = 2^4 (Here 4 is no of hosts)
= 16

No. of usable host on each subnetwork: $2^4 - 2$ (4 is no of hostbit
= 14

Network address: 192.168.10.0/28, Broadcast: 192.168.10.15

CLASSMATE PAGE

DATE

	Subnet (Network ID)	HOST ID	Broadcast ID
1	192.168.10.0	192.168.10.1 - 192.168.10.14	192.168.10.15
2	192.168.10.16	192.168.10.17 - 192.168.10.30	192.168.10.31
3	192.168.10.32	192.168.10.33 - 192.168.10.46	192.168.10.47
4	192.168.10.48	192.168.10.49 - 192.168.10.62	192.168.10.63
5	192.168.10.64	192.168.10.65 - 192.168.10.78	192.168.10.79
6	192.168.10.80	192.168.10.81 - 192.168.10.94	192.168.10.95
7	192.168.10.96	192.168.10.97 - 192.168.10.110	192.168.10.111
8	192.168.10.112	192.168.10.113 - 192.168.10.126	192.168.10.127
9	192.168.10.128		192.168.10.143
10	192.168.10.144		192.168.10.159
11	192.168.10.160		192.168.10.175
12	192.168.10.176		192.168.10.191
13	192.168.10.192		192.168.10.207
14	192.168.10.208		192.168.10.223
15	192.168.10.224		192.168.10.239
16	192.168.10.240	192.168.10.241 - 192.168.10.254	192.168.10.255

classmate

PAGE

DATE

8. Given IP address 192.168.10.0/26.

⇒ Subnet mask: 11111111.11111111.11111111.11 000000.
⇒ 255.255.255.192.

Total subnets: $2^2 = 4$
Total hosts: $2^6 = 64$
Usable hosts: 64-2 = 62
valid subnet (4th octet) = 256-192 = 64

Network address ⇒ 11000000.10101000.00001010.00000000
11111111.11111111.11111111.11000000
AND
11000000.10101000.00001010.00000000
∴ Network address: 192.168.10.0/26

Broadcast address: 192.168.10.63/26
(Host Min) 1st usable host address: 192.168.10.1/26
(Host Max) last usable host address: 192.168.10.62/26

9. Given IP address 172.168.10.0/22

⇒ Subnet mask: 11111111.11111111.111111 00.00000000
⇒ 255.255.252.0.
Here, Network bits = 22, Host bits = 10
Total subnets = $2^6 = 64$
Total no. of IP (hosts) address on each subnetwork = $2^{10} = 1024$
Total no. of usable hosts on each sub network = $2^{10} - 2 = 1023$

Here, 1022 hosts isn't possible so, we use last octet borrowed from host.
i.e. $2^2 = 4$

Network address: 172.168.8.0/22
Broadcast address: 172.168.11.255/22

PAGE

DATE

S.N	Subnet (Network ID)	HOST ID	Broadcast ID.
1	172.168.0.0	172.168.0.1 - 172.168.3.254	172.168.3.255
2.	172.168.4.0	172.168.4.1 - 172.168.7.254	172.168.7.255
3.	172.168.8.0	172.168.8.1 - 172.168.11.254	172.168.11.255
4.	172.168.12.0	172.168.12.1 - 172.168.15.254	172.168.15.255
5.	172.168.16.0	172.168.16.1 - 172.168.19.254	172.168.19.255
	⋮	⋮	⋮
64.	172.168.252.0		172.168.255.255

4.4

DATE

Supernetting

Supernetting is the procedure to combine the small networks into larger space. In subnetting, Network addresses bits are increased, but in Supernetting, Host addresses bits are increased. It is implemented via variable-length subnet masking

Why Supernetting?

The routing table contains the entry of a subnet mask for every network. If there are lots of small networks then size of the routing table increases. When the router has a big routing table then it takes a lot of time for the router to process the routing table. Supernetting is used to reduce the size of the Ip routing table to improve network routing efficiency

Advantages.

- Size of router memory table is minimized
- Increases the speed of routing table lookup.
- Reduces the network traffic.

Disadvantages

- Combination of blocks should be made in power 2
- The whole network should exist in the same class.
- When merged, it leads covering different area.

DATE

* Difference between Subnetting & Supernetting.

BASIS	SUBNETTING	SUPERNETTING
BASIC	A process of dividing a network into subnetworks	A process of combining small networks into a larger network.
PROCEDURE	The number of bits of network addresses is increased	The number of bits of host addresses is increased
MASK BITS	Moved towards right of the default mask.	Moved towards left of the default mask
IMPLEMENTATION	VLSM (Variable Length Subnet Masking)	CIDR (Classless Interdomain Routing)
Purpose	Used to reduce the address depletion.	To simplify & flatten the routing process.

classmate

PAGE

U.5

DATE

* IPV6 Addressing and It's Features

Internet protocol version 6 is a new addressing protocol designed to incorporate all the possible requirements of future Internet known to us as Internet version 2. This protocol works on network layer. It is a 128-bit alphanumeric string that identifies an endpoint device in the IPV6 addressing scheme. It is arranged in eight groups, each of which is 16 bits. Each group is expressed as four hexadecimal digits & the groups are separated by colons:

Ex: FE80: CD00: 0000: 0CDE: 1257: 0000: 211E: 729C.

It can be shortened as: FE80: CD00: 0: CDE: 1257: 0: 211E: 729C.

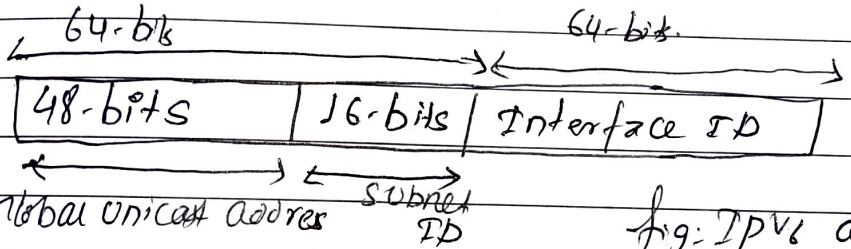


fig: IPV6 address structure.

Features of IPV6 Addressing

- Larger Address space: In contrast to IPV4, IPV6 uses 4 times more bit address to address a device on the Internet. This much of extra bits can provide approximately 3.4×10^{38} different combinations of address

- Simplified Header:- IPV6's header have been simplified by moving all unnecessary information & options (which are present in IPV4 header) to the end of IPV6 header.

DATE

- End-to-End connectivity:- Every system now has unique IP address and can traverse through the internet without using NAT or other translating components. After IPV6 is fully implemented, every host can directly reach other hosts on the Internet.

- Auto-configuration:- IPV6 supports both stateful and stateless auto configuration mode of its host devices. This way, absence of a DHCP server does not put a halt on inter segment communication.

- Mobility: IPV6 was designed keeping mobility in mind. This feature enables hosts (such as mobile) to roam in different geographical area & remain connected with the same IP address.

- No Broadcast: IPV6 doesn't have any broadcast support anymore. It uses multicast to communicate with multiple hosts.

4.6

DATE

* IPV4 and IPV6 Datagram Formats.

→ IPV4 Datagram Format

Packets in the network (internet) layer are called datagrams. A datagram is a variable-length packet consisting of two parts:- header and data. The header is 20 to 60 bytes in length and contains information essential to routing and delivery.

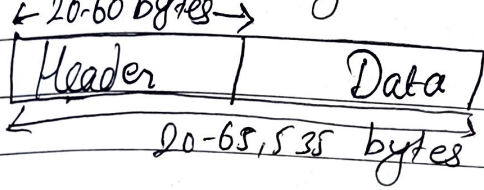


fig: Ip datagram for IPV4.

Version (4)	Header Length (4)	Type of service (8)	Total length (16 bits)
Identification (16 bits)		Flags (3 bits)	Fragmentation offset (13)
Time to Live (8 bits)	Upper layer protocol (8 bits)		Header Checksum (16 bits)
Source IP address (32 Bits)			
Destination IP address (32 Bits)			
Options + Padding (0 to 40 bytes)			
Data (16 Bits)			

fig: Header format of IPV4

- Version number: It determines the IP protocol version of the datagram. Here, we are in IPV4, so it is 4. ie 0100
- Header length: It is used to determine where in the IP datagram the data actually begins. It is 4 bits. The typical IP datagram has a minimum 20-byte to 60 byte maximum header.
- Type of service:- The TOS bits are included in IPV4 header to allow different types of IP datagrams to be distinguished from each other. Ex, it might be useful to distinguish real-time datagram from non-real time traffic (for example, FTP).

DATE

- Datagram length / Total length : This is the total length of the IP datagram (header plus data), measured in bytes. Since this is 16 bits long, the theoretical max. size of the IP datagram is 65,535 bytes. However, datagrams are rarely larger than 1,500 bytes.
  Length of data = Total length - header length.

- 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 : If IP packet is too large to handle, these flags tell if they can be fragmented or not.

- Fragmentation offset : This offset tells the exact position of the fragment in the original packet.

- Time-to-Live : To avoid looping in the network, every packet is sent with some TTL value set, which tells network how many routers this packet can cross.

- Protocol : This field value indicates the specific transport layer protocol to which the data portion of this IP datagram should be passed.

- Header Checksum : This field is used to keep checksum value of entire header. It is used for error detection.

- Source address : This 32-bit field defines the address of the sender (or source) of the packet.

classmate

PAGE

DATE

- Destination address :- This 32-bit field defines the 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.
- Data :- It contains the transport layer segment (TCP or UDP) to be delivered to destination

→ IPV6 Datagram Formats

IPV6 datagram format has a much simpler packet header compared to IPV4, by encoding only the information needed for forwarding the IP datagram. IPV6 header allows the routers to process the IPV6 datagram more efficiently.

IPV6 Header	Extension Header	Upper Layer Protocol data

fig: Structure of IPV6 datagram packet.

Version (4-bits)	Traffic Class (8-bits)	Flow Label (20 bits)
Payload length (16 bits)	Next header (8 bits)	Hop limit (8 bits)
Source IPV6 Address (128 bits)		
Destination IPV6 Address (128 bits)		
Data		

fig: Header format of IPV6.

- Version : It represents the version of IP, i.e. 0110
- Traffic Class :- Among 8 bits, the MSB 6 bits are used for type of service & LSB 2 bits are used for Explicit Congestion Notification (ECN)

classmate

PAGE

DATE

- Flow label :- This label is used to maintain the sequential flow of the packets belonging to a communication. It also helps to avoid re-ordering of data packets.
- Payload length :- This field is used to tell the routers how much information a particular packet contains in its payload
- Next header :- It identifies the protocol to which the contents of this datagram will be delivered.
- Hop limit :- This field is used to stop packet to loop in the network infinitely. It is same as TTL in IPv4
- Source Address → This field indicates the address of originator of the packet
- Destination Address → It provides the address of intended recipient of the packet
- Data :- This is the payload portion of the IPv6 datagram. When the datagram reaches its destination the payload will be removed from the IP datagram & passed on to the protocol specified in the next header field.

classmate

PAGE

4.2

DATE

Comparision of IPv4 and IPv6 Addressing

IPv4	IPv6
i) IPv4 addresses are of 32 bit length.	i) IPv6 are of 128 bit length.
ii) IPv4 addresses are binary numbers represented in decimal	ii) IPv6 addresses are binary numbers represented in hexadecimals.
iii) Internet Group Management Protocol (IGMP) is used to manage multicast group membership	iii) IGMP is replaced with Multicast Listener Discovery (MLD) messages
iv) Broadcast messages are available.	iv) Broadcast messages are not available. Link-local scope is used.
v) No packet flow identification.	v) Packet flow identification is available.
vi) Fragmentation is done by Sender & forwarding routers.	vi) Fragmentation is done only by sender.
vii) Checksum field is available in IPv4 header.	vii) No checksum field is available in IPv6 header
viii) It can generate 4.29×10^9 addresses	viii) It can generate 3.4×10^{38} addresses
ix) Ex: 192.168.1.1	ix) Ex: 2001:0db8:85a3:0000:0000:8a2e:0370:7334

4.8

DATE

* Network Address Translation (NAT)

To access the internet, one public IP address is needed, but we can use a private IP address in our private network. The idea of NAT is to allow multiple devices to access the internet through a single public address. To achieve this, the translation of a private IP address to a public IP address is required.

NAT is a process in which one or more local IP address is translated into one or more Global IP address and vice versa in order to provide Internet access to the local hosts.
NAT enables a user to have a large set of addresses internally & one address, or a small set of addresses, externally. The traffic inside can use the large set; the traffic outside can use the small set.

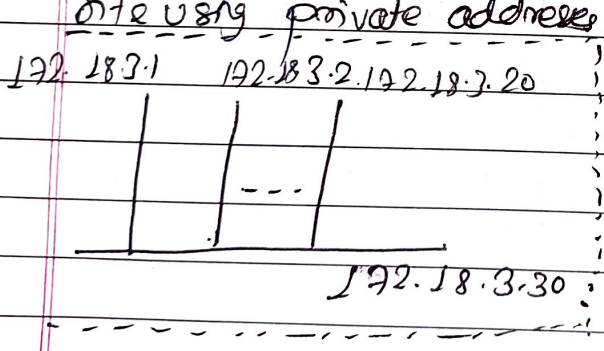


fig: NAT implementation

Advantages: i) It conserves legacy reserved IP addresses
ii) Provides privacy as the device's IP address, sending & receiving the traffic, will be hidden

Disadvantages: i) Translation results in switching path delays
ii) Certain applications won't function when NAT is enabled

classmate

PAGE

4.9

DATE

* Example addresses

→ **Unicast Addressing Mode:**

In this mode, data is sent only to one destined host. The destination field contains 32-bit IP address of the destination host. Here the client sends the data to the targeted server. This type of information transfer is useful when there is participation of single sender & single receipent. It is one-to-one transmission

→ **Broadcast Addressing Mode:**

It is one to all transmission. It is classified into two types

i) Limited Broadcasting:- This method is used when we have to send stream of packets to all the devices over the network. It will append 255.255.255.255 (called as limited broadcast address in the destination address of datagram header

ii) Direct Broadcasting:- This is useful when a device in one network wants to transfer packet stream to all the devices over the other network. This is achieved by translating all the Host ID part bits of the destination address to 1; referred as Direct Broad Cast Address in the datagram header for information transfer.

→ **Multicast Addressing Mode:-**

This mode is the mix of unicast & broadcast addressing mode. In this packet, the destination address contains a special address which starts with 224.x.x.x & can be entertained by more than one host. In multicasting one or more senders & one or more recipients participate in data transfer traffic.

CLASSMATE

PAGE

4.10

DATE

* Routing.

4.10.1 * Introduction and Definition

Routing is a process of selecting path along which the data can be transferred from source to the destination. Routing is broadly performed in many types of networks, such as the public switched telephone network (PTSN) and computer networks, such as Internet. The routing process usually directs forwarding on the basis of routing tables. Routing tables maintain a record of routes to various network destinations.

4.10.2 * Types of Routing

(a) Static vs Dynamic

Static routing → Static routing is a process in which we have to manually add routes in routing table. Static routing is used when we have very device to configure & when we know the routes which probably never change. Static routing does not handle failures & external networks well because any route configured manually must be updated or reconfigured manually to fix or repair lost connectivity.

DATE

Advantages:
- Easily implemented in a small network.
- No overheads are produced on router CPU.
- Extra resources (CPU & memory) not required

Disadvantages:-
- Unsuitable for large networks.
- Administrator must be extra careful while configuring the routes.
- Large networks increase configuration complexity & time consumption

Dynamic routing → Dynamic routing makes automatic adjustment of the routes according to the current state of the route in the routing table. Dynamic routing uses protocols to discover network destinations & routes to reach it. Automatic adjustment will be made to reach the network destination of one route goes down

Advantages:
- Suitable for all topologies.
- Network size doesn't affect the router operations
- Topologies are adapted automatically to reroute the traffic.

Disadvantages:
- Initially it could be complicated to implement.
- Routes rely on current topologies
- The broadcasting & multicasting of routing updates make it less secure.

PAGE

classmate

DATE

(b) Unicast vs Multicast

Unicast → It is the simplest form of routing because destination is already known. There is only one sender and only one receiver. When we want to send data to multiple people then unicast will waste lots of bandwidth. It doesn't perform well while streaming medias. Ex Browsing a website.

Multicast → In multicast routing, data is sent to only nodes which want to receive the packets In multicast, there is only one sender but multiple receivers. When we want to send data to multiple people then multicast will utilize the bandwidth more efficiently. It does not perform well across large networks. Ex: IP TV, Stock exchanges etc

(c) Link State vs Distance Vector:

→ In link state, bandwidth required is more due to flooding and sending of large state packets. But in distance vector, bandwidth required is less due to local sharing, no flooding & sending of small state packets.

→ Link state makes use of Dijkstra's algorithm while distance vector makes use of Bellman Ford algorithm.

→ Link state routing has more traffic while distance vector routing has less.

CLASSMATE

PAGE

DATE

→ Link State routing has ~~more traffic~~ faster coverages while distance vector routing has slower.
→ Link State routing has difficult configuration while distance vector routing has easy configuration
→ Link State routing has hierarchical structure while distance vector routing doesn't have hierarchical structure

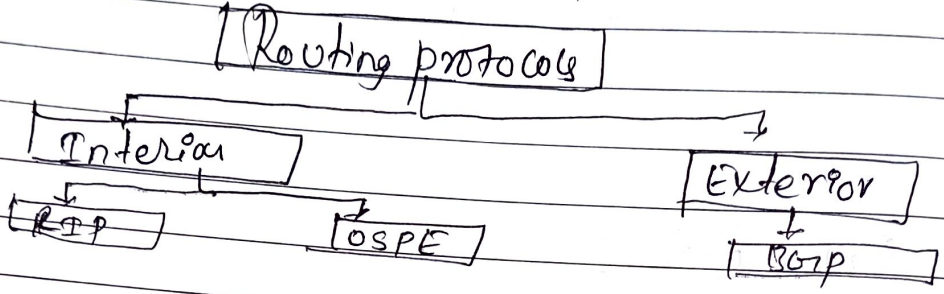
④ Interior vs Exterior

Interior routing protocols are designed for use within a contained network of limited size whereas exterior routing protocols are designed to link multiple networks together. Nearly all routing protocols are interior routing protocols. Only BGP is commonly used as an exterior routing protocol. Interior gateway protocol (IGP) used to refer to interior routing protocols and exterior gateway protocol (EGP) used to refer to exterior routing protocols.

DATE

Routing Protocols

The routing protocol specifies how routers communicate to select the routes for data transfer. Different types of routing protocols are as follows:



a) Routing Information Protocol (RIP):

In RIP, distance vector routing protocol is used for data transmission. The maximum numbers of hop in RIP is 15. Mechanism like split horizon, hold down etc. are used to prevent from incorrect or wrong routing information. RIP is a dynamic protocol used to find the best route from source to destination over a network. Compared to other routing protocols RIP is poor & limited sized network. RIP V1, RIP V2 & RIPng (next generation) are the types of routing information protocol (RIP).

b) Open Shortest Path First (OSPF)

It is the link-state routing protocol which is used to find the best path between the source & the destination. OSPF is developed by Internet Engineering Task Force (IETF) as one of the

DATE

Internet Gateway Protocol (IGP). It is a network layer protocol which works on the protocol number 89 and used AD value 110. Ospf uses multicast address 224.0.0.5 for normal communication and 224.0.0.6 for update to designated router.

c) Border Gateway Protocol (BGP).

BGP are the core routing protocol of the internet and responsible to maintain a table of Internal protocol networks with authorize network reaching capability between AS. BGP is expressed as path vector protocol. BGP is relevant to network administrators of large organizations which connect to two or more ISPs, as well as to ISPs who connect to other network providers. If we are the administrator of a small corporate network, or an end user, then we probably don't need to know about BGP

DATE

Comparison of OSPF & BGP

	OSPF	BGP
i)	OSPF is an internal gateway protocol.	i) BGP is an external gateway protocol.
ii)	OSPF is comparatively easy to implement.	ii) BGP is comparatively complex to implement.
iii)	Port number 89 is used.	iii) Port number 179 is used.
iv)	IP protocol is used.	iv) TCP protocol is used.
v)	OSPF is mainly used on smaller scale networks that are centrally administered.	v) The BGP protocol is mainly used on very large-scale networks, like the internet.
vi)	Dijkstra's algorithm is suitable to implement OSPF routing protocol.	vi) Best path algorithm is suitable to implement BGP routing protocol.

DATE

Overview of IPV4 to IPV6 Transition Mechanism:

In modern devices, both versions IPV4 & IPV6 exist simultaneously. Following are some methods that can be used when translating a network from IPV4 to IPV6.

a) Dual Stack: The process of running both IPV4 & IPV6 on the same device is called dual stack. It is the simplest method to run IPV6 on all of the devices that are currently running IPV4. It is easy to implement, however IPV6 isn't supported on all of the IPV4 devices, in this situation other methods must be considered

b) Tunneling: The process of transporting IPV6 traffic through an IPV4 network transparently is called tunneling. In this method a packet is encapsulated into a wrapper then enables its transport from a source to destination where it is decapsulated and retransmitted. The following list shows the different available tunneling methods.

- Manual IPV6 tunnels
- 6 to 4 tunnels
- Generic Routing Encapsulation (GRE) IPV6 tunnels
- IPV6 rapid deployement
- IPV4 Compatible tunnels

c) Translation: The process of converting IPV6 traffic to IPV4 traffic for transport and vice versa is called translation. When using translation, the traffic is not encapsulated but is converted to the destination type. Two methods of translation

- Network Address Translation: This method enables the ability to either statically or dynamically configure a translation of a IPV4 network address into an IPV6 network address

DATE

- NAT 64 : It offers both Stateless & Stateful option when deploying.

* Overview of ICMP / ICMP V6 :

ICMP stands for Internet Control Message Protocol which depends on internet to Provide an error control. Since, IP does not have an inbuilt mechanism for sending error & queries. It is a supporting protocol & is used by network devices like routers for sending the error messages & operations information eg: The requested service is not available.

ICMP V6 is the version 6 of ICMP which plays far more important role in the operation of IPV6. It is used for several purposes beyond simple error reporting & signaling. It is mostly used for Neighbour discovery, Router discovery, and managing hand-offs in mobile IPV6.

* Overview of Network Traffic Analysis (NTA)

NTA is the process of intercepting recording and analyzing network traffic communication patterns in order to detect and respond to security threats. This technique is used by network administrators to examine network activity manage availability, & identify unusual activity

DATE

Importance of NTA.

- Identify bottlenecks.
- Troubleshoot bandwidth issues
- Improve visibility of devices on your network.
- Detect security issues & fix them more quickly

✗ Security Concept:

- **Firewall**: A firewall is a network security device that monitors incoming and outgoing network traffic and permits or blocks data packets based on a set of security rules. Its purpose is to establish a barrier between our internal network & incoming traffic from external sources (internet) in order to block malicious traffic like viruses & hackers

Firewalls can either be a software or hardware, though it's best to have both. A software firewall is a program installed on each computer & regulates traffic through port numbers & applications, while a physical firewall is a piece of equipment installed between network & gateway. Firewalls can be divided into several different categories based on their general structure & method of operation. Following are some types:

i) Packet filtering firewalls
ii) Circuit-level-gateways
iii) Application level gateways
iv) Software firewalls
v) Hardware firewalls, etc.
vi) Stateful inspection firewalls

CLASSMATE

PAGE

DATE

- Router Access Control (ACL)

It is a set of rules defined for controlling the network traffic and reducing network attack. ACLs are used to filter traffic based on the set of rules defined for the incoming or outgoing of the network.

In a way, ACL is made up of rules that either allow access to a computer environment or deny it. It is like a guest list in an exclusive club. only those on the list are allowed in the door. This enables administrators to ensure that, unless the proper credentials are presented by the device, it cannot gain access

Types of ACLs.

- Standard ACL : Permits or denies packets based on source IP address. Valid ACL ID range: 1-99. Applied closest to destination.
- Extended ACL: Permits or denies packets based on source & destination IP addresses & also based on IP protocol information. Valid ID range: 100-199. It is applied closest to the source.

DATE

Path Computation Algorithms

Path Computation algorithms are the algorithms that helps to compute shorted path from a source to destination among several paths. Beuman Ford and Dijkstra are two main path computation algorithms.

a) Beuman Ford Algorithm :

The Beuman-Ford algorithm is an algorithm that computes shortest paths from a single source vertex to all of the other vertices in a weighted graph. It is slower than Dijkstra's algorithm but more versatile, as it is capable of handling graphs in which some of the edge weights are negative values.

Similar to Dijkstra's algorithm, this algorithm also initializes the source node to 0 and other nodes to infinity. Then we go on relaxing all the edges repeatedly for n-1 times., where n is the number of vertices.

Relaxation:-

If (u,v) is an edge between two vertices then

if(d[u] + w(u,v) < d[v])

then,

d[v] = d[u] + w(u,v)

(min cost weight recently calculated)

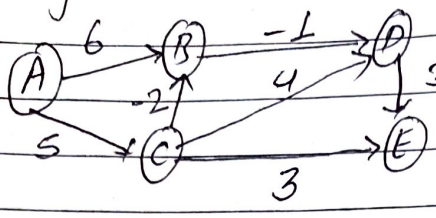
where, d[u] = weight of source vertex

d[v] = weight of destination vertex

w(u,v) = weight of edge from source to destination.

DATE

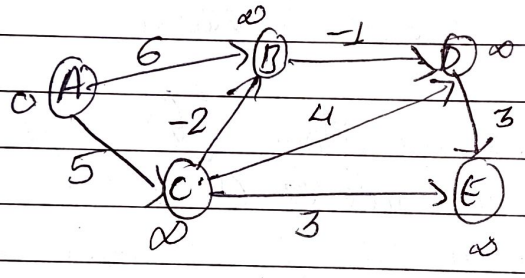
Ex: Find the shortest path of the fouowing graph by using Beuman Ford algorithm



Soln: Let the source vertex be A then we write all the edges in any order as: (A,B), (A,C), (C,B), (C,D), (C,E), (B,D), (D,E).

Since there are 5 vertices ie. n=5, So. no. of iterations for sowing problem is (n-1) = (5-1) = 4.

Now, we initialize the vertices & redraw the figure as:



ie

A	B	C	D	E
0	∞	∞	∞	∞

Iteration-1:

Now for edge AB: $d[A] + w(A,B) < d[B]$

or, $0+6 < \infty$ (True)

So, $d[B] = d[A] + w(A,B) = 0+6 = 6$

For edge AC: $d[A] + w(A,C) < d[C]$

Or, $0+5 < \infty$ (True)

So, $d[C] = d[A] + w(A,C) = 5$

For edge CB, $d[C] + w(C,B) < d[B]$

Or, $5 + (-2) < 6$ (True)

So, $d[B] = d[C] + w(C,B)$

$= 5 + (-2)$

$= 3$

classmate

PAGE

DATE

For edge CD, $d[C] + w(C,D) < d[D]$

$\Rightarrow 5 + 4 < \infty$ (True)

So $d[D] = 9$

For edge CE, $d[C] + w(C,E) < d[E]$

$\Rightarrow 5 + 3 < \infty$ [True]

$\therefore d(E) = 8$

For edge BD; $d[B] + w(B,D) < d[D]$

$\Rightarrow 3 + (-1) < 9$ (True)

So, $d[D] = 2$

For edge DE, $d[D] + w(D,E) < d[E]$

$\Rightarrow 2 + 3 < \infty$ (True)

So $d(E) = 5$

Now, we continue other iterations using table

Table	A	B	C	D	E
Initialization	0	∞	∞	∞	∞
1st Iteration		3	5	2	5
2nd Iteration		3	5	2	5
3rd Iteration		3	5	2	5
4th Iteration		3	5	2	5

Hence, shortest distance for respective vertices are

$A=0, B=3, C=5, D=2, E=5$

Note: If E is no. of edges & V is no. of vertices then time complexity is $O(E(V-1))$. Since we iterate V-1 times we can write it as $O(E \cdot V)$. If we take $E \approx V$ both as n then we can write as $O(n^2)$.

i.e. $O\left(\frac{n(n-1)}{2} \cdot (n-1)\right)$

PAGE

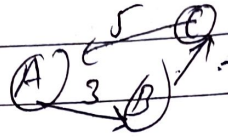
classmate

DATE

Drawback:

The main drawback of Bellman Ford algorithm is that if we have -ve weight cycle in graph then we can't get the correct solution

Ex:



Here, 5+3-10=-2 (-ve weight cycle)

b) Dijkstra's Algorithm

This is another approach of getting Single Source shortest paths. In this algorithm it is assumed that there is no negative weighted edge. It also starts with initializing Source vertex to 0 and remaining other vertex to infinity. Then we start finding shortest path for each vertex using formula as

If $(d[u] + w(u,v) < d[v])$ then
$d[v] = d[u] + w(u,v)$

Where, u = Source vertex
v = destination vertex

Algorithm:

Dijkstra_Algorithm (G, w, s)
{
for each vertex $v \in V$
$d[v] = \infty$
$d[s] = 0$
$S = \phi$
$Q = V$

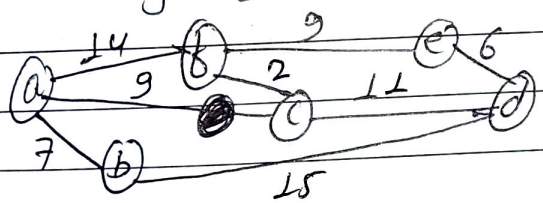
DATE

```
While(Q != Φ)
{
    u = Take minimum from Q and delete
    S = S U {u}
    for each vertex v adjacent to u
        If d[v] > d[u] + w(u,v) then
            d[v] = d[u] + w(u,v)
    }
}
```

Time Complexity : If v is the no. of vertices in the graph, then time complexity is $O(v^2)$

Disadvantage : The algorithm may not work for

Q Find the shortest paths from source node to all other vertices using Dijkstra's algorithm



=) Let source vertex be a, so we initialize initially source vertex 'a' with weight 0 & ∞ to all the other remaining vertices. Now, we construct table for faster calculations. Calculations are same as Bellman Ford algorithm. Only difference is that we use n-1 iterations there but the number of iterations are not fixed in this method.

PAGE

min(old, marked + edge)

DATE

Marked	a	b	c	d	e	f
a	[0]	∞	∞	∞	∞	∞
b	-	[7]	9	∞	∞	14
c	-	-	[9]	22	∞	14
f	-	-	-	20	∞	[11]
d	-	-	-	[20]	20	-
e	-	-	-	-	[20]	-

Hence, the shortest paths with weights for different vertex are:

Shortest path from a to b = {a, b} with weight 7
Shortest path from a to c = {a, c} with weight 9
Shortest path from a to d = {a, c, d} with weight 20
Shortest path from a to e = {a, c, f, e} with weight 20
Shortest path from a to f = {a, c, f} with weight 11.

Questions asked from this chapter

DATE

Q. Write subnet ID and broadcast address for each subnet if you divide the class B network (150.10.0.0 - 150.10.255.255) in 4 different subnets. What is the new subnet mask? (2078 - 5 marks)

Q. In a block of address, we know the Ip address of one host is 192.34.12.56/28. What are the 1st address (network address) & the last address (limited broadcast address) in this block? (2076 - 5 marks)

Q. Define routing table. Differentiate static routing table with dynamic routing table. (2076 - 5 marks) (2076 (old) - 5 marks) (2074 - 5 marks)

Q. What is NAT? How does it work? what are its benefit? (2076 - 5 marks) (2069 - 5 marks)

Q. Assume a class C and B network & divide it into eight subnet. What is the value of new subnet mask? (2074 - 5 marks) (2072 - 5 marks). (2071 - 5 marks)

Q. Explain ICMP. (2073 - 5 marks (2068 - 5 marks)

Q. What do you mean by link state routing? Differentiate between IPv4 & IPv6. (2073 - 10 marks)

Q. Explain datagram of IPv4 & IPv6. (Imp - 10 marks)