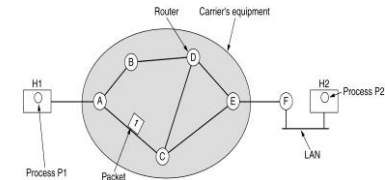


Chapter - 5 Network Layer

Prepared By:
Prof. Vishal A. Polara
Assistant Professor
Information Technology Department
Birla Vishvakarma Mahavidyalaya Engineering College

Store-and-Forward Packet Switching

In this type of network router stores packet and forward it to the appropriate destination.



Prof. Vishal A. Polara

Outline

- Design Issues
- Routing Algorithms: Shortest Path routing, Flooding, Distance vector routing, Link state routing, Broadcast, multicast routing
- Congestion Control Algorithms
- Quality of Service, Internetworking
- IPv4 and IPv6.

Prof. Vishal A. Polara

Services Provided to the Transport Layer

- Services should be *independent of router technology*.
- The transport layer should be *shielded from (covered with) number, type and topology of routers present*.
- The network addresses made available to transport layer should *use a uniform numbering plan*, even across LANs and WANs.

Prof. Vishal A. Polara

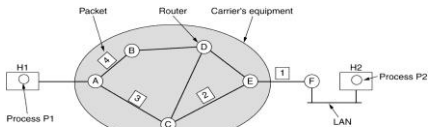
1. Network Layer Design Issues

- Following issues are possible while designing network
- Store-and-Forward Packet Switching
- Services Provided to the Transport Layer
- Implementation of Connectionless Service
- Implementation of Connection-Oriented Service
- Comparison of Virtual-Circuit and Datagram Subnets

Prof. Vishal A. Polara

Implementation of Connectionless Service

Routing within a diagram subnet.



A's table		C's table		E's table	
Initially	later				
A: -	A: -	A: A	A: C	A: C	
B: B	B: B	B: A	B: D	B: D	
C: C	C: C	C: -	C: C	C: C	
D: B	D: B	D: D	D: D	D: D	
E: C	E: B	E: E	E: E	E: -	
F: C	F: B	F: E	F: F	F: F	

Prof. Vishal A. PolaraDest.Line

Implementation of Connection-Oriented Service

Routing within a virtual-circuit subnet.

A's table

H1	1	C	1
H3	1	C	2

C's table

A	1	E	1
A	2	E	2

E's table

C	1	F	1
C	2	F	2

7

Prof. Vishal A. Polara

2.1 Shortest Path Routing

- Also known as *Dijkstra algorithm*
- Path length is measured using:
 - Number of hops
 - Geographic distance
 - Other metrics like mean queueing and transmission delay

```
graph TD
    Start([Start]) --> SetRoot[Set root to local node and move it to tentative list.]
    SetRoot --> TentativeEmpty{Tentative list is empty?}
    TentativeEmpty -- Yes --> Stop([Stop])
    TentativeEmpty -- No --> MoveShortest[Among nodes in tentative list, move the one with the shortest path to permanent list.]
    MoveShortest --> AddNeighbors[Add each unprocessed neighbor of last moved node to tentative list if not already there. If neighbor is in the tentative list with larger cumulative cost, replace it with new one.]
    AddNeighbors --> TentativeEmpty
```

10

Prof. Vishal A. Polara

Comparison of Virtual-Circuit and Datagram Subnets

Issue	Datagram subnet	Virtual-circuit subnet
Circuit setup	Not needed	Required
Addressing	Each packet contains the full source and destination address	Each packet contains a short VC number
State information	Routers do not hold state information about connections	Each VC requires router table space per connection
Routing	Each packet is routed independently	Route chosen when VC is set up; all packets follow it.
Effect of router failures	None, except for packets lost during the crash	All VCs that passed through the failed router are terminated
Quality of service	Difficult	Easy if enough resources can be allocated in advance for each VC
Congestion control	Difficult	Easy if enough resources can be allocated in advance for each VC

8

Prof. Vishal A. Polara

Steps

- It is non adaptive (static) routing algorithm.
- In this algorithm initially distance from each node is infinite.
- In this algorithm nodes divide into two sets: tentative and permanent.
- It finds the neighbors of a current node, makes them tentative, examines them and if they pass the criteria makes them permanent.
- After reaching the destination algorithm stop.

11

Prof. Vishal A. Polara

2. Routing Algorithm

- Static Algorithms (Non-Adaptive)
 - Shortest-path routing.
 - Flooding.
- Dynamic Routing (Adaptive Routing)
 - Distance vector routing.
 - Link state routing.

9

Prof. Vishal A. Polara

Shortest Path Routing

Links: solid line, dashed line, dotted line
Nodes: solid circle, open circle
+ means newly added or changed

a) b) c) d) e) f) g) h) i)

12

Prof. Vishal A. Polara

2.2 Flooding

- It is static routing algorithm.
- Each router must have details of adjacent router.
- Sends data packet to all router except the one from where data come.
- Many duplicate packet will be arrived at destination end to eliminate this use counters at hops
- Problem: duplicates
- Constraining the flood:
 - **Sequencing** – Each packet is uniquely numbered at the source.
 - **Hop count** – Each time a node passes on a packet, it decrements the value by one. When its value becomes '0', the packet is discarded. Hop count is equal to total numbers of node from source to destination.
 - **Selective flooding** – Exclude unreasonable links

13

Prof. Vishal A. Polara

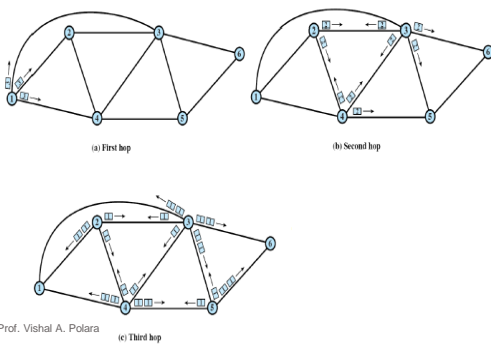
2.3 Distance Vector Routing

- It has three step: initialization, sharing, updating
- During initialization each node know how to reach all other node which is immediately connected to it.
- During sharing phase each node share their routing table to other node so other node can decide how to reach all the node which is not directly connected to it.
- During updating phase each node update distance to the node which is not directly connected to it and add entry in third column (it will add entry of source node).
- Node will create modified table from neighbor node and compare with old one and keeps the shortest one.

16

Prof. Vishal A. Polara

Flooding Example



14

Prof. Vishal A. Polara

2.3 Distance Vector Routing

- When to share?
- Periodic update: a node sends its routing table, normally every 30s, in a periodic update.
- Triggered update: a node sends its two column routing table to its neighbors anytime there is a change in its routing table. This is called triggered update.
 - A node receives a table from a neighbor, resulting in changes in its own table after updating.
 - A node detects some failure in the neighboring links which results in a distance change to infinity.

17

Prof. Vishal A. Polara

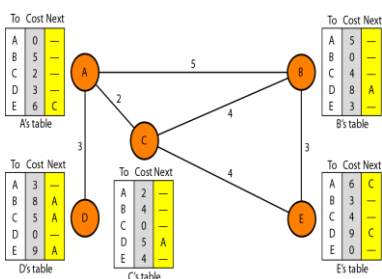
2.3 Distance Vector Routing

- It is dynamic routing (adaptive) algorithm.
- In this algorithm each router maintain routing table. This tables are updated by exchanging information with the neighbors.
- It is also known as **bell men ford** and **ford-fulkerson** algorithm.
- In distance vector routing, each router maintains a routing table indexed by, and containing one entry for, each router in the subnet. This entry contains two parts: the preferred outgoing line to use for that destination and an estimate of the time or distance to that destination.
- Metric is hop, queue and delay.

15

Prof. Vishal A. Polara

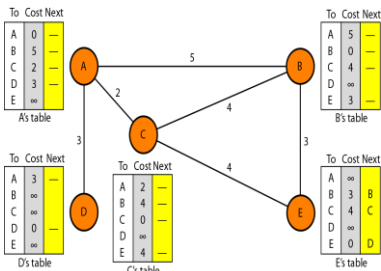
Figure Distance vector routing tables



18

Prof. Vishal A. Polara

Figure Initialization of tables in distance vector routing



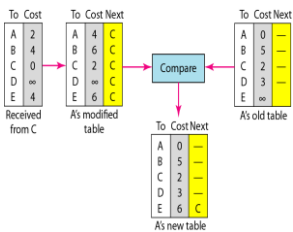
Prof. Vishal A. Polara

2.3 Distance Vector Routing solution

- **Split Horizon:** Another solution is called split horizon. If according to its table node B think that optimum path to reach X from A then it will not advertise this information to A. it comes from A.
- **Split Horizon and poison reverse:**
- The distance vector protocol uses a timer, and if there is no news about a route, the node deletes the route from its table. when node B in the previous scenario eliminate the route to X from its advertisement to A. here node B still advertise the value for X but with value as infinite that means value comes from A.

Prof. Vishal A. Polara

Figure Updating in distance vector routing



Prof. Vishal A. Polara

2.3 Distance Vector Routing prob & sol.

- **Three node instability:** in this case no guarantee of stability.
- X—A---B ---C---A
- If X is not reachable node A send this to B and C , B will receive and update table but C will not receive so it assume that there is a path to X . C sends its routing table to B, B is fooled here so it update table there is a route from C, after a while B advertise to A and A will be fooled.
- Now loop continues. The loop stops when the cost in each node reaches infinity.

Prof. Vishal A. Polara

2.3 Distance Vector Routing Problem &sol.

- **Two Node instability:**
- If there are two node at the A and B who knows how to reach X at beginning. Now the link between A and X fails. Node A changes its table , if A can send its table to B immediately, everythin is fine.
- For ex. X---A---B is connection
- But if B sends its routing table to A it will create a problem , here A assumes that there is a path from B to X. now A send its routing table to B so cost of reaching X increases gradually until it reaches infinity.
- **Solution:**
- **Defining Infinity:**
- Define distance between each node is 1 and 16 as infinity that means it cannot use for large system. The size of the network in each direction cannot exceed 15 hops.

Prof. Vishal A. Polara

2.4 Link State Routing

Each router must do the following:

1. Discover its neighbors, learn their network address.
2. Measure the delay or cost to each of its neighbors.
3. Construct a packet telling all it has just learned.
4. Send this packet to all other routers.
5. Compute the shortest path to every other router.

Dijkstra's algorithm is run to find the shortest path to each routers.

Prof. Vishal A. Polara

1.Learning About the neighbors

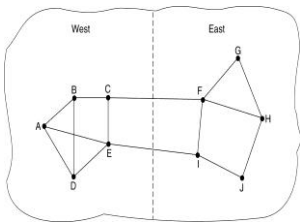
- In this step router will learn about its neighbors.
- It send hello message to all other node on point to point line. Then the router on the other end is expected to send back a reply telling who it is.
- These names must be globally unique because when a distant router later hears that three routers are all connected to F, it is essential that it can determine whether all three mean the same F.
- When two or more routers are connected by a LAN, the situation is slightly more complicated.

25

Prof. Vishal A. Polara

Measuring Line Cost

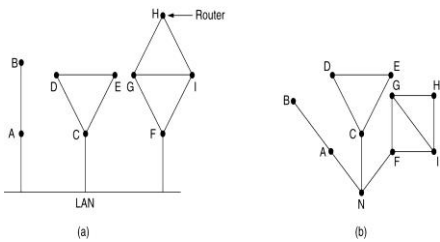
A subnet in which the East and West parts are connected by two lines.



28

Prof. Vishal A. Polara

Learning about the Neighbors



(a) Nine routers and a LAN.
(b) A graph model of (a).

26

Prof. Vishal A. Polara

3. Building Link State packets

- After Collecting all the information each router to build packet containing data.
- Packet start with identity of sender, followed by sequence number and age, and list of neighbors. For each neighbor delay is also given.
- It is easy to build packet but it is difficult to determine when to build.
- Normally it is build periodically at regular intervals. Another way to build them when some significant event occurs. Such as line or neighbor going down.

29

Prof. Vishal A. Polara

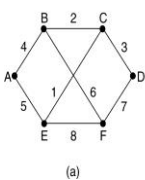
2.Measuring line cost

- In this step router will calculate delay to its neighbors.
- Each router will send ECHO packet to calculate delay. When this packet comes back at source it will divide total time by 2 and note down the time as delay.
- It is also calculated based on delay between to two line heavily loaded and lightly loaded. It will select line which is lightly loaded.
- In the figure CF path is longest and EI is smallest so all traffic follows EI path.

27

Prof. Vishal A. Polara

Building Link State Packets



Link		State		Packets	
A	B	C	D	E	F
Seq.	Seq.	Seq.	Seq.	Seq.	Seq.
Age	Age	Age	Age	Age	Age
B 4	A 4	B 2	C 3	A 5	B 6
E 5	C 2	D 3	F 7	C 1	D 7
	F 6	E 1		F 8	E 8

(a) A subnet. (b) The link state packets for this subnet.

30

Prof. Vishal A. Polara

4. Distributing the link state packets

- Fundamentally flooding is used to distribute packets. It keeps track of all packet and source. It will check packet if it is new then it will forward to all except one from whom it comes. If duplicate it is discarded.
- First problem is sequence number wrap around or completed.
- Second problem if router get crashed, it will lose track of sequence numbers. If it start with 0 next packet will be rejected as a duplicate.
- Third problem is if sequence number is corrupted.
- Solution of this problem is adding age after sequence number which is decremented once per second. When age hits 0 information from that router is discarded.

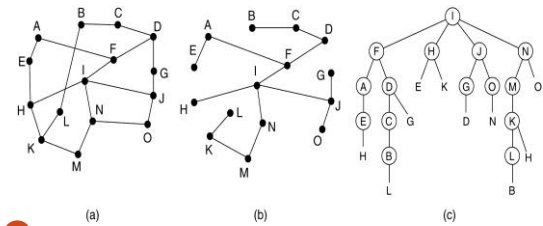
31

Prof. Vishal A. Polara

Broadcast Routing

Reverse path forwarding

(a) A subnet. (b) a Sink tree. (c) The tree built by reverse path forwarding.



34

Prof. Vishal A. Polara

5. Computing the new routes

- Once a router has accumulated a full set of link state packets, it can construct the entire subnet graph because every link is represented.
- Dijkstra's algorithm can be run locally to construct the shortest path to all possible destinations

32

Prof. Vishal A. Polara

2.6 Multicast Routing

- It is used when all are not interested to receive the message.
- In this technique there are group of router and message will be send to specific group only.

35

Prof. Vishal A. Polara

2.5 Broadcast Routing

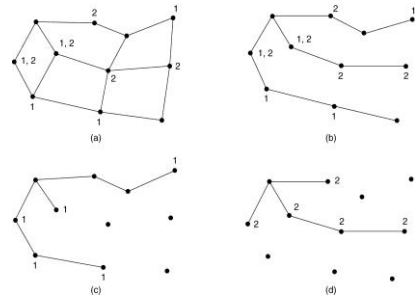
It is the process of “Sending a packet to all destinations simultaneously”. Various methods are:

- Send packet to each destination
- **Flooding** – point-to-point routing algorithm
- **Multidestination routing** – new packet for each output line to be used. (Each output line will contain the destination address that are to use that line)
- **A spanning tree** - is a subset of the subnet that includes all the routers but contains no loops
- **Reverse path forwarding**

33

Prof. Vishal A. Polara

2.6 Multicast Routing



(a) A network. (b) A spanning tree for the leftmost router. (c) A multicast tree for group 1. (d) A multicast tree for group 2.

36

Prof. Vishal A. Polara

3. Congestion Control

- Congestion control refers to techniques and mechanisms that can either prevent congestion, before it happens, or remove congestion, after it has happened.
- In general, we can divide congestion control mechanisms into two broad categories:
 1. open-loop congestion control (prevention): It is applied to prevent congestion before it happens.
 2. closed-loop congestion control (removal): it is applied to alleviate congestion after it happens.

37

Prof. Vishal A. Polara

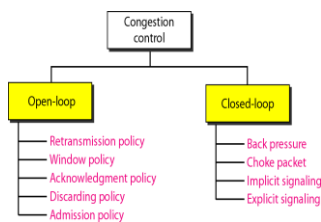
Close Loop Congestion control

- **1. Backpressure:** In this technique congested node stops receiving data from the immediate upstream node or nodes.
- Backpressure is a node to node congestion control that starts with a node and propagates, in the opposite direction of data flow.
- It is applied only to virtual circuit network. In which each node knows the upstream node from which a flow of data is coming.
- **2. Choke Packet:** A choke packet is a packet sent by a node to the source to inform it of congestion.
- In choke packet method the warning is from the router which has encountered congestion, to the source station directly.

40

Prof. Vishal A. Polara

Figure Congestion control categories



38

Prof. Vishal A. Polara

Close Loop Congestion control

- **3. Implicit Signaling:** in this technique there is no communication between the congested node or nodes and the source.
- The source guesses that there is a congestion somewhere in the network from other symptoms.
- For example if source will not get an acknowledgment for a while it assumes that there is a congestion.
- **4. Explicit Signaling:** The node that experience congestion will send signal to source or destination.
- In this technique no separate packet is used, signal is included in the packets that carry data.
 - Backward signaling: bit sent to source in reverse direction to inform congestion
 - Forward signaling: bit sent in same direction to receiver

41

Prof. Vishal A. Polara

Open Loop Congestion control

- **1. Retransmission Policy:** Retransmission can create congestion when packet get lost. To prevent it retransmission times must be designed to optimize efficiency and at the same time prevent congestion.
- **2. Window policy:** the type of window also create congestion. It is better to use selective repeat instead of go back N.
- **3. Acknowledgement Policy:** the acknowledgment by receiver also affect congestion. In this case receiver will not send acknowledgement for every packet it receive which will slow down the receiver.
- **4. Discarding Policy:** packet must be discarded by router to prevent congestion. For example in audio transmission less sensitive packets is discarded when congestion occurs.
- **5. Admission Policy:** In this case router will check all resources before establishing virtual circuit. If there is congestion it will not allow to get admission in circuit.

39

Prof. Vishal A. Polara

Figure Backpressure method for alleviating congestion

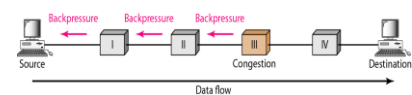
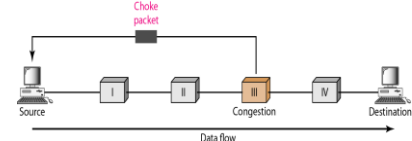


Figure Choke packet

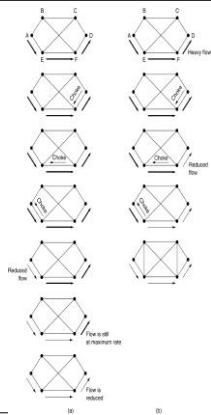


42

Prof. Vishal A. Polara

Hop-by-Hop
Choke
Packets

- (a) A choke packet that affects only the source.
- (b) A choke packet that affects each hop it passes through.



43 Prof. Vishal A. Polara

4.1 Quality of service improved technique

- 1. **Scheduling:**
- FIFO queuing:** first in, first out queuing packets wait in buffer until the node is ready to process them. If the average arrival rate λ higher than the average processing rate μ , the queue will fill up and new packets will be discarded. For example wait at bus stop.
- Priority Queuing:** In this technique priority class is assigned to packets. The packet in higher priority queue are processed first.
- there is a drawback if there is a continuous flow in high priority queue. The packets in the lower priority queues will never a chance to be processed.
- Weighted Fair Queuing:** It is like priority queue class is assigned to packet but here higher priority means weight, if weights are 3,2, and 1, there packets are processed from the first queue, two from send and one from third queue.

46 Prof. Vishal A. Polara

4. Quality of service

- Flow Characteristics:**
- 1. Reliability:** It means lose of packet. If packet lose is less than reliability is more. For example it is required in mail, file transfer etc.
- 2. Delay:** source to destination delay is not good for voice communication.
- 3. Jitter:** Jitter is the variation in delay for packets belonging to the same flow. For example if four packet sent at 1,2,3 and 4 second it arrive at 21,22,23,24 then there is a same delay 20.
- high jitter means difference between delay is large.
- 4. Bandwidth:** different applications need different bandwidths. Video conferencing require millions of bit to sent while mail doesnot.

44 Prof. Vishal A. Polara

Scheduling - FIFO

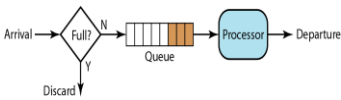
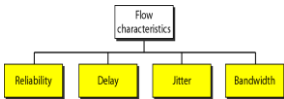


Figure FIFO queue

47 Prof. Vishal A. Polara

Figure Flow characteristics



45 Prof. Vishal A. Polara

Scheduling – Priority queuing

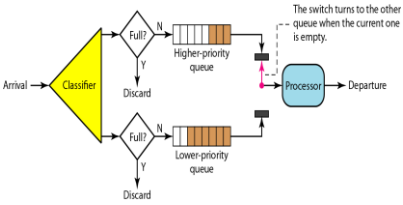


Figure Priority queuing

48 Prof. Vishal A. Polara

Scheduling – Weighted Fair queuing

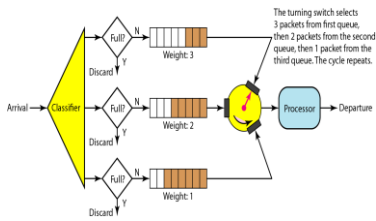
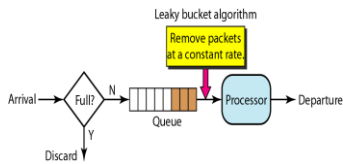


Figure Weighted fair queuing

49 Prof. Vishal A. Polara

Figure Leaky bucket implementation



52 Prof. Vishal A. Polara

4.1 Quality of service improved technique

- **2. Traffic Shaping**
- It is a mechanism to control the amount and the rate of the traffic sent to the network.
- **Leaky Bucket:** It is used to smooth out bursty traffic.
- Flow is not depend on input, output flow is constant.
- Here bursty chunks are stored in the bucket and sent out at an average rate.
- It can also prevent congestion. It is also used for FIFO queue. If the traffic consists of fixed size packets ,the process removes a fixed number of packets from the queue at each tick of the clock. If the traffic consists of variable length packets the fixed output rate must be based on the number of bytes or bits..

50 Prof. Vishal A. Polara

4.1 Quality of service improved technique

- **Token Bucket:** the leaky bucket is very restrictive. It does not credit and idle host.
- If host does not have data bucket becomes empty. If the host has bursty data the leaky bucket allows only an average rate.
- In token bucket algorithm allow idle host to accumulate credit for the future in the form of tokens.
- For each tick of the clock the system sends n tokens to the bucket. The system removes one token for every cell(or byte) of data sent.
- For example if n is 100 and the host is idle for 100 ticks. The bucket collect 10,000 tokens.
- Here host can send bursty data as long as the bucket is not empty.
- It can be easily implemented using counter. Each time token is added counter is incremented by 1 and each time data is sent counter is decremented by 1.

53 Prof. Vishal A. Polara

Traffic Shaping – Leaky bucket

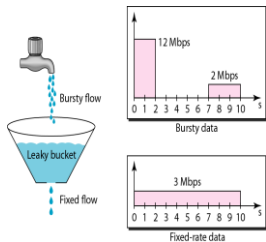


Figure 24.19 Leaky bucket

51 Prof. Vishal A. Polara

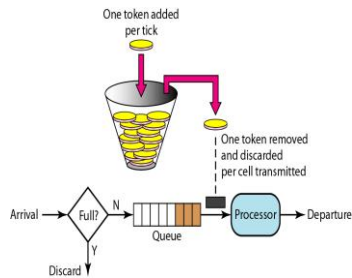


Figure Token bucket

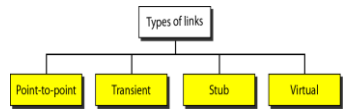
54 Prof. Vishal A. Polara

4.1 Quality of service improved technique

- **3. Resource Reservation:** A flow of data needs resources such as buffer, bandwidth, CPU time.
- Quality of service improved if resources are reserve before task.
- **4. Admission Control:** Admission control refers to the mechanism use by router or a switch to accept or reject a flow based on predefined parameters called flow specifications.
- it check the availability of new connection based on load.

55 Prof. Vishal A. Polara

Figure Types of links



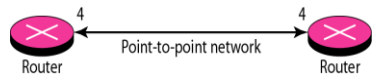
58 Prof. Vishal A. Polara

The Example Protocol – OSPF

- Open Shortest Path First
- Areas – Collection of networks, host and routers all contained within an autonomous system
- Area Border routers
- Backbone & Backbone routers
- Virtual link
- Area identification
- Metric
- Types of links

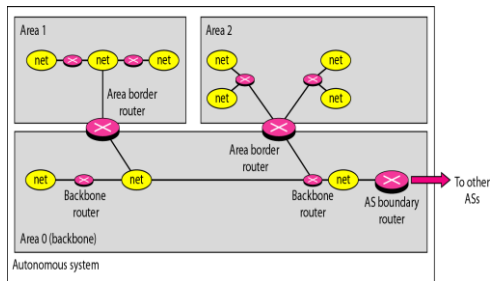
56 Prof. Vishal A. Polara

Figure Point-to-point link



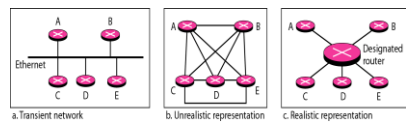
59 Prof. Vishal A. Polara

Figure Areas in an autonomous system



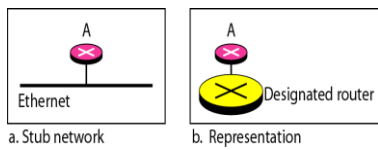
57 Prof. Vishal A. Polara

Figure Transient link



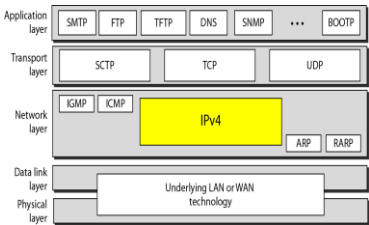
60 Prof. Vishal A. Polara

Figure Stub link



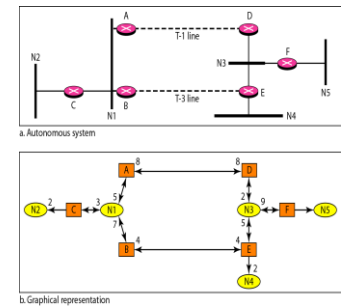
61 Prof. Vishal A. Polara

Figure Position of IPv4 in TCP/IP protocol suite



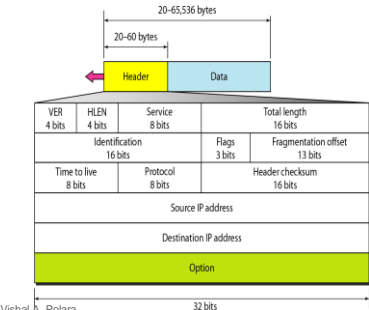
64 Prof. Vishal A. Polara

Figure Example of an AS and its graphical representation in OSPF



62 Prof. Vishal A. Polara

Figure IPv4 datagram format



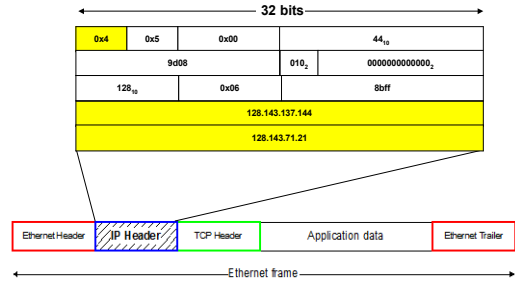
65 Prof. Vishal A. Polara

5. Internetworking (IPv4 and IPv6)

- Internetwork is made of five networks: four LANs and one WAN.
- Internet is made of four sub network 4 LAN and 1 WAN.
- IP is connection less so it will not provide reliability.
- IPv4 is also connection less it will not provide flow control and error control.
- To provide reliability it must be used with TCP.

63 Prof. Vishal A. Polara

IP Addresses



66 Prof. Vishal A. Polara

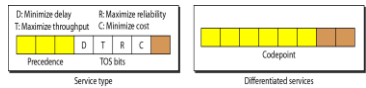
IPv4 Header

- **Version(VER):** it is a 4 bit field defines the version of the IPv4 Protocol.
- **Header Length(HLEN):** this 4 bit field defines the total length of the datagram header in 4 byte words.
- Header length is from 20 to 60 byte so when it is minimum 20 bytes, header length is 5 ($5 * 4=20$).
- **Service:** it is of 8 bit. In this interpretation first 3 bits are called precedence bits. The next 4 bits are called type of service(TOS) bits.
- Precedence is used to defined priority of datagram at the time of congestion.
- TOS bits with each bit have special meaning given in table.

67

Prof. Vishal A. Polara

Figure Service type or differentiated services



70

Prof. Vishal A. Polara

IPv4 Header

- **Total Length:** this is a 16 bit field that defines the total length of the IPv4 datagram in bytes.
- Length of data is coming from upper layer can be calculated using
- Length of data = total length – header length
- **Identification:** it is 16 bit field identifies a datagram origination from source.
- **Flags:** this is a 3 bit field. The first bit is reserved. The second bit is called the do not fragment bit. If its value is 1, don't fragment. Third bit is called more fragment bit. If its value is 1, it means the datagram is not the last fragment, there are more fragments after this one.

68

Prof. Vishal A. Polara

Table Types of service

TOS Bits	Description
0000	Normal (default)
0001	Minimize cost
0010	Maximize reliability
0100	Maximize throughput
1000	Minimize delay

71

Prof. Vishal A. Polara

IPv4 Header

- **Fragmentation offset:** this is 13 bit field shows the relative position of this fragment with respect to the whole datagram.
- Ex. Datagram 0 to 3999 first fragment 0 to 1399 offset is $0/8=0$, second fragment 1400 to 2799, offset is $1400/8=175$ same last.
- **Time to live:** A datagram has a limited lifetime in its travel through an internet. It holds the timestamp. It is discarded after completion of time stamp.
- **Protocol:** it is 8 bit filed defines the higher level protocol that uses the services of the IPv4 layer.
- **Checksum:** Use for error detection.
- **Source address and destination address:** it is 32 bit field defines the IPv4 address of source.

69

Prof. Vishal A. Polara

Table Default types of service

Protocol	TOS Bits	Description
ICMP	0000	Normal
BOOTP	0000	Normal
NNTP	0001	Minimize cost
IGP	0010	Maximize reliability
SNMP	0010	Maximize reliability
TELNET	1000	Minimize delay
FTP (data)	0100	Maximize throughput
FTP (control)	1000	Minimize delay
TFTP	1000	Minimize delay
SMTP (command)	1000	Minimize delay
SMTP (data)	0100	Maximize throughput
DNS (UDP query)	1000	Minimize delay
DNS (TCP query)	0000	Normal
DNS (zone)	0100	Maximize throughput

72

Prof. Vishal A. Polara

Table Values for codepoints

Value	Protocol
1	ICMP
2	IGMP
6	TCP
17	UDP
89	OSPF

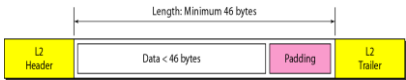
73 Prof. Vishal A. Polara

Table Protocol values

Value	Protocol
1	ICMP
2	IGMP
6	TCP
17	UDP
89	OSPF

76 Prof. Vishal A. Polara

Figure Encapsulation of a small datagram in an Ethernet frame

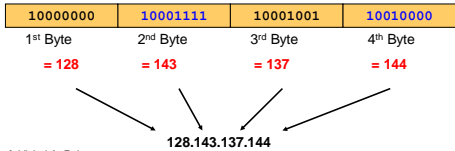


74 Prof. Vishal A. Polara

Dotted Decimal Notation

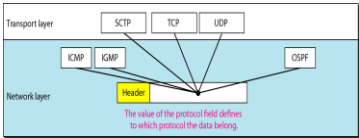
- IP addresses are written in a so-called **dotted decimal notation**
- Each byte is identified by a decimal number in the range [0..255]:

• Example:



77 Prof. Vishal A. Polara

Figure Protocol field and encapsulated data



75 Prof. Vishal A. Polara

Network prefix and Host number

- The network prefix identifies a network and the host number identifies a specific host (actually, interface on the network).



- How do we know how long the network prefix is?
 - The network prefix **used** to be implicitly defined (**class-based addressing, A,B,C,D...**)
 - The network prefix now is flexible and is indicated by a **prefix/netmask (classless)**.

78 Prof. Vishal A. Polara

Classfull IP addresses

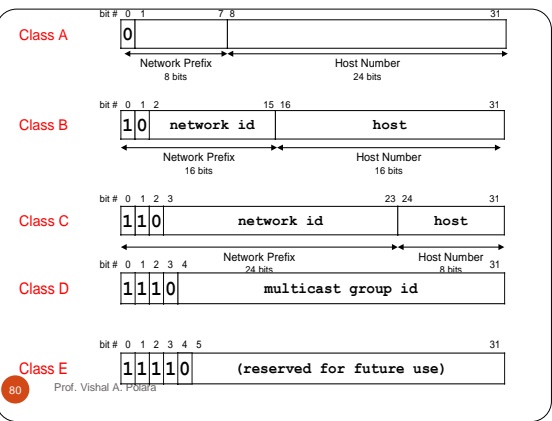
- When Internet addresses were standardized (early 1980s), the Internet address space was divided up into classes:
 - Class A:** Network prefix is 8 bits long
 - Class B:** Network prefix is 16 bits long
 - Class C:** Network prefix is 24 bits long
- Each IP address contained a key which identifies the class:
 - Class A:** IP address starts with “0”
 - Class B:** IP address starts with “10”
 - Class C:** IP address starts with “110”

79 Prof. Vishal A. Polara

Table Subnet masks for classfull addressing

Class	Binary	Dotted-Decimal	CIDR
A	11111111 00000000 00000000 00000000	255.0.0.0	/8
B	11111111 11111111 00000000 00000000	255.255.0.0	/16
C	11111111 11111111 11111111 00000000	255.255.255.0	/24

Prof. Vishal A. Polara 19.82



80 Prof. Vishal A. Polara

Example

Change the following IPv4 addresses from binary notation to dotted-decimal notation.

- a. 10000001 00001011 00001011 11101111
- b. 11000001 10000011 00011011 11111111

Solution

We replace each group of 8 bits with its equivalent decimal number (see Appendix B) and add dots for separation.

- a. 129.11.11.239
- b. 193.131.27.255

83 Prof. Vishal A. Polara

Figure Finding the classes in binary and dotted-decimal notation

	First byte	Second byte	Third byte	Fourth byte
Class A	0			
Class B	10			
Class C	110			
Class D	1110			
Class E	1111			

a. Binary notation

	First byte	Second byte	Third byte	Fourth byte
Class A	0-127			
Class B	128-191			
Class C	192-223			
Class D	224-239			
Class E	240-255			

b. Dotted-decimal notation

81 Prof. Vishal A. Polara

Example

Change the following IPv4 addresses from dotted-decimal notation to binary notation.

- a. 111.56.45.78
- b. 221.34.7.82

Solution

We replace each decimal number with its binary equivalent (see Appendix B).

- a. 01101111 00111000 00101101 01001110
- b. 11011101 00100010 00000111 01010010

84 Prof. Vishal A. Polara

Example

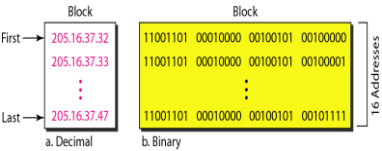
- Find the error, if any, in the following IPv4
- a. 111.56.045.78
 - b. 221.34.7.8.20
 - c. 75.45.301.14
 - d. 11100010.23.14.67

Solution

- a. There must be no leading zero (045).
- b. There can be no more than four numbers.
- c. Each number needs to be less than or equal to 255.
- d. A mixture of binary notation and dotted-decimal notation is not allowed.

85 Prof. Vishal A. Polara

Figure A block of 16 addresses granted to a small organization



88 Prof. Vishal A. Polara

Example

- Find the class of each address.
- a. 00000001 00001011 00001011 11101111
 - b. 11000001 10000011 00011011 11111111
 - c. 14.23.120.8
 - d. 252.5.15.111

Solution

- a. The first bit is 0. This is a class A address.
- b. The first 2 bits are 1; the third bit is 0. This is a class C address.
- c. The first byte is 14; the class is A.
- d. The first byte is 252; the class is E.

86 Prof. Vishal A. Polara

Problems with Classful IP Addresses

- The original classful address scheme had a number of problems
- Problem 1.** Too few network addresses for large networks
- Class A and Class B addresses are gone
- Problem 2.** Two-layer hierarchy is not appropriate for large networks with Class A and Class B addresses.
- Fix #1: Subnetting
- Problem 3.** Inflexible. Assume a company requires 2,000 addresses Class A and B addresses are overkill Class C address is insufficient (requires 8 Class C addresses)
- Fix #2: Classless Interdomain Routing (CIDR)
- Problem 4:** Exploding Routing Tables: Routing on the backbone Internet needs to have an entry for each network address. In 1993, the size of the routing tables started to outgrow the capacity of routers.
- Fix #2: Classless Interdomain Routing (CIDR)

89 Prof. Vishal A. Polara

Table Number of blocks and block size in classfull IPv4 addressing

Class	Number of Blocks	Block Size	Application
A	128	16,777,216	Unicast
B	16,384	65,536	Unicast
C	2,097,152	256	Unicast
D	1	268,435,456	Multicast
E	1	268,435,456	Reserved

Prof. Vishal A. Polara 19.87

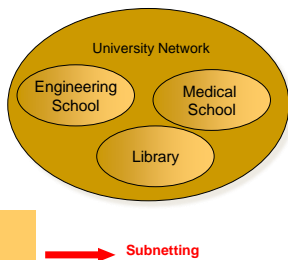
Problem 5. The Internet is going to outgrow the 32-bit addresses

Fix #3: IP Version 6

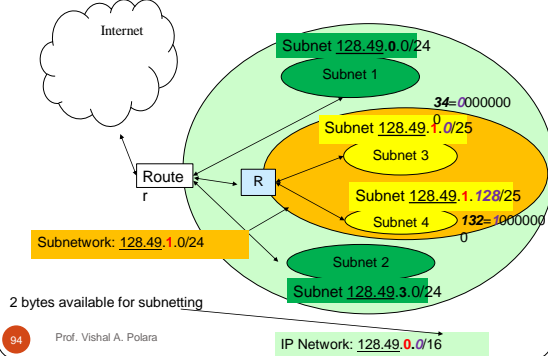
90 Prof. Vishal A. Polara

Subnetting

- **Problem:** Organizations have multiple networks which are independently managed
- **Solution 1:** Allocate an address for each network
 - Difficult to manage
 - From the outside of the organization, each network must be addressable ie have an identifiable address.
- **Solution 2:** Add another level of hierarchy to the IP addressing structure

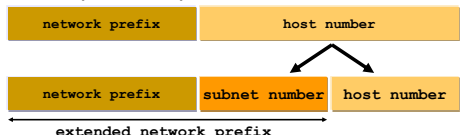


Example of a Subnetting Plan



Basic Idea of Sub netting

- Split the host number portion of an IP address into a **subnet number** and a (smaller) **host number**.
- Result is a 3-layer hierarchy



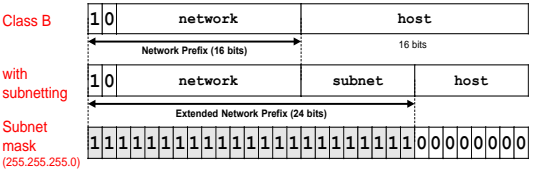
- **Then:**
 - Subnets can be freely assigned within the organization
 - Internally, subnets are treated as separate networks
 - Subnet structure is not visible outside the organization

Subnetting Example

Subnet	Network bits	Total number of host
255.255.255.0	/24	254
255.255.255.128	/25	126
255.255.255.192	/26	62
255.255.255.224	/27	30
255.255.255.240	/28	14
255.255.255.248	/29	6
255.255.255.252	/30	2

Subnet Masks

- Routers and hosts use an **extended network prefix (subnet mask)** to identify the start of the host numbers



Subnetting Example

- An organization with 4 departments has the following IP address space: 192.168.1.0/24. As the systems manager, you are required to create subnets to accommodate the IT needs of 4 departments. The subnets have to support to 100, 50, 25, and 05 hosts respectively. What are the 4 **subnet network numbers**?

- **Solution:**
 - 192.168.1.0/25 (255.255.255.128) total 126 ip
 - 192.168.1.0/26 (255.255.255.192) total 62 valid ip
 - 192.168.1.0/27 (255.255.255.224) total 30 ip
 - 192.168.1.0/29 (255.255.255.248) total 6 ip

192.203.17.0
Mask: 255.255.255.128

192.203.17.0 (.0 to .127) 192.203.17.0 (.128 to .255)

192.213.17.128 (.128 to .191) 192.213.17.128 (.192 to .255)
Mask: 255.255.255.192

97

Prof. Vishal A. Polara

Subnetting in CIDR.

20.30.40.10/25 20.30.40.0/26 20.30.40.64/26

20.30.40.0/26 20.30.40.64/26

20.30.40.64/26 20.30.40.80/26

20.30.40.80/26 20.30.40.96/26

20.30.40.96/26 20.30.40.112/26

100

Prof. Vishal A. Polara

CIDR rule

- All IP address should be continuous.
- It must be of 2^n .
- First IP address in the block should be entirely divided by size of block.
 - For example: 100.1.2.32 to 100.1.2.47

98

Prof. Vishal A. Polara

Subnetting in CIDR.

20.30.40.10/25 20.30.40.0/26 20.30.40.64/26

20.30.40.0/26 20.30.40.64/26

20.30.40.64/26 20.30.40.80/26

20.30.40.80/26 20.30.40.96/26

20.30.40.96/26 20.30.40.112/26

101

Prof. Vishal A. Polara

IP address	Subnet mask	No. of Hosts	Subnets in class A	Subnets in class B	Subnets in class C
00000000-0	255.0.0.0	$2^{24}-2$	1	—	—
10000000-128	255.128.0.0	$2^{23}-2$	2	—	—
11000000-192	255.192.0.0	$2^{22}-2$	4	—	—
11100000-224	255.240.0.0	$2^{20}-2$	16	—	—
11110000-240	255.252.0.0	$2^{16}-2$	64	—	—
11111000-248	255.254.0.0	$2^{15}-2$	128	—	—
11111100-252	255.255.0.0	$2^{14}-2$	256	—	—
11111110-254	255.255.128.0	$2^{13}-2$	512	—	—
11111111-255	255.255.255.0	2^8-2	1024	256	256

99

Prof. Vishal A. Polara

VLSM in CIDR (block)

20.30.40.10/25 20.30.40.0/26 20.30.40.64/26

20.30.40.0/26 20.30.40.64/26

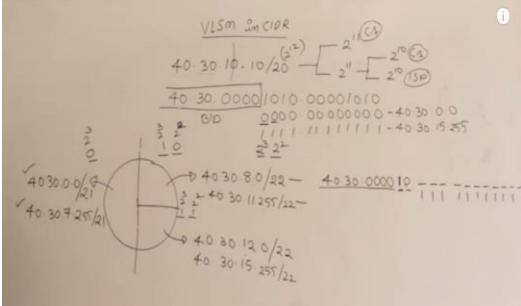
20.30.40.64/26 20.30.40.80/26

20.30.40.80/26 20.30.40.96/26

20.30.40.96/26 20.30.40.112/26

102

Prof. Vishal A. Polara



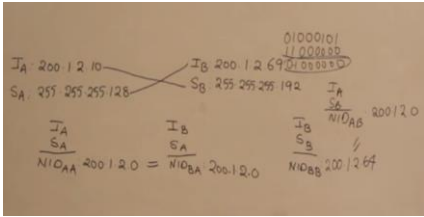
103Prof. Vishal A. Polara

192.168.10.0/24 Total No. of Networks: 16 IP Address: 16				NETWORK 1	
Network Number	Network ID	Host IP Address	Broadcast Address		
1	192.168.10.0	192.168.10.1 - 192.168.10.14	192.168.10.15		192.168.10.0
2	192.168.10.16	192.168.10.17 - 192.168.10.30	192.168.10.31		192.168.10.1
3	192.168.10.32	192.168.10.33 - 192.168.10.46	192.168.10.47		192.168.10.2
4	192.168.10.48	192.168.10.49 - 192.168.10.62	192.168.10.63		192.168.10.3
5	192.168.10.64	192.168.10.65 - 192.168.10.78	192.168.10.79		192.168.10.4
6	192.168.10.80	192.168.10.81 - 192.168.10.94	192.168.10.95		192.168.10.5
7	192.168.10.96	192.168.10.97 - 192.168.10.110	192.168.10.111		192.168.10.6
8	192.168.10.112	192.168.10.113 - 192.168.10.126	192.168.10.127		192.168.10.7
9	192.168.10.128	192.168.10.129 - 192.168.10.142	192.168.10.143		192.168.10.8
10	192.168.10.144	192.168.10.145 - 192.168.10.158	192.168.10.159		192.168.10.9
11	192.168.10.160	192.168.10.161 - 192.168.10.174	192.168.10.175		192.168.10.10
12	192.168.10.176	192.168.10.177 - 192.168.10.190	192.168.10.191		192.168.10.11
13	192.168.10.192	192.168.10.193 - 192.168.10.206	192.168.10.207		192.168.10.12
14	192.168.10.208	192.168.10.209 - 192.168.10.222	192.168.10.223		192.168.10.13
15	192.168.10.224	192.168.10.225 - 192.168.10.238	192.168.10.239		192.168.10.14
16	192.168.10.240	192.168.10.241 - 192.168.10.254	192.168.10.255		192.168.10.15

106Prof. Vishal A. Polara

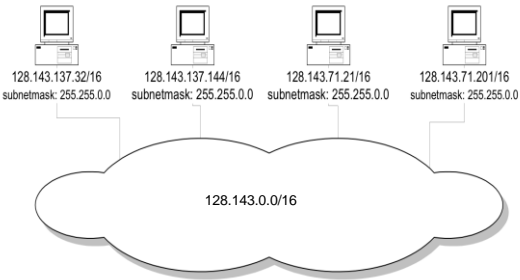
How to find ip is on same network or not

- Perform AND operation of Ip of A with subnet of B for network id.
- To find network id of A or B. perform AND operation with Ia and Sa.



104Prof. Vishal A. Polara

Network without subnets



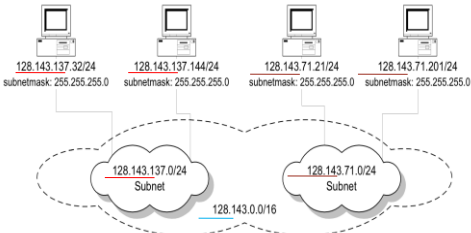
107Prof. Vishal A. Polara

Advantages of Subnetting

- With subnetting, IP addresses use a 3-layer hierarchy:
Network
Subnet
Host
- Improves efficiency of IP addresses by not consuming an entire address space for each physical network.
- Reduces router complexity. Since external routers do not know about subnetting, the complexity of routing tables at external routers is reduced.

105Prof. Vishal A. Polara

Same Network with Subnets



108Prof. Vishal A. Polara

CIDR: Prefix Size vs. Host Space

CIDR Block Prefix	# of Host Addresses
/27	32 hosts
/26	64 hosts
/25	128 hosts
/24	256 hosts
/23	512 hosts
/22	1,024 hosts
/21	2,048 hosts
/20	4,096 hosts
/19	8,192 hosts
/18	16,384 hosts
/17	32,768 hosts
/16	65,536 hosts
/15	131,072 hosts
/14	262,144 hosts
/13	524,288 hosts

109 Prof. Vishal A. Polara

Example

A block of addresses is granted to a small organization. We know that one of the addresses is 205.16.37.39/28. What is the first address in the block?

Solution

The binary representation of the given address is
11001101 00010000 00100101 00100111
If we set 32–28 rightmost bits to 0, we get
11001101 00010000 00100101 00100000
or
205.16.37.32

112 Prof. Vishal A. Polara

In IPv4 addressing, a block of addresses can be defined as
 $x.y.z.t / n$
in which $x.y.z.t$ defines one of the addresses and the $/ n$ defines the mask.

Prof. Vishal A. Polara 19.110

The last address in the block can be found by setting the rightmost
 $32 - n$ bits to 1s.

113 Prof. Vishal A. Polara

The first address in the block can be found by setting the rightmost
 $32 - n$ bits to 0s.

Prof. Vishal A. Polara 19.111

Example

Find the last address for the block in previous example.

Solution

The binary representation of the given address is
11001101 00010000 00100101 00100111
If we set $32 - 28$ rightmost bits to 1, we get
11001101 00010000 00100101 00101111
or
205.16.37.47

Prof. Vishal A. Polara 19.114

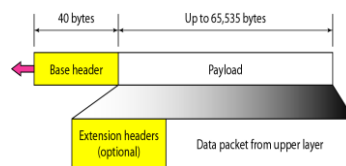
The number of addresses in the block can be found by using the formula

$$2^{32-n}$$

Prof. Vishal A. Polara

19.115

Figure IPv6 datagram header and payload



116

Prof. Vishal A. Polara

Example

Find the number of addresses in previous example

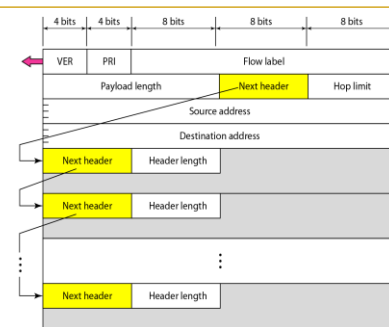
Solution

The value of n is 28, which means that number of addresses is 2^{32-28} or 16.

Prof. Vishal A. Polara

19.116

Figure Format of an IPv6 datagram



119

Prof. Vishal A. Polara

IPv6

- **IP Version 6**
 - Is the successor to the currently used IPv4
 - Specification completed in 1994
 - Makes improvements to IPv4 (no revolutionary changes)
- One (not the only !) feature of IPv6 is a significant increase in size of the IP address to **128 bits (16 bytes)**
 - IPv6 will solve – for the foreseeable future – the problems with IP addressing

117

Prof. Vishal A. Polara

IPv6 Header

- **Version:** it is the version number of IP
- **Priority:** it is 4 bit field defines the priority of the packet with respect to traffic congestion
- **Flow Label:** it is a 3 byte field that is designed to provide special handling for particular flow of data.
- **Payload length:** it is 2 byte defines the length of the ip datagram excluding the base header
- **Next header:** it is an 8 bit field defining the header that follows base header.
- **Hop limit:** it is 8 bit hop limit like TTL in ipv4.
- **Source address and destination address:** 16 byte (128 bit) internet address that identifies the original source and destination.

120

Prof. Vishal A. Polara

IPv6 Provider-Based Addresses

- The first IPv6 addresses will be allocated to a provider-based plan

010	Registry ID	Provider ID	Subscriber ID	Subnetwork ID	Interface ID
-----	-------------	-------------	---------------	---------------	--------------

- **Type:** Set to "010" for provider-based addresses
- **Registry:** identifies the agency that registered the address

The following fields have a variable length (recommended length in "() ")

- **Provider:** Id of Internet access provider (16 bits)
- **Subscriber:** Id of the organization at provider (24 bits)
- **Subnetwork:** Id of subnet within organization (32 bits)
- **Interface:** identifies an interface at a node (48 bits)

Thank
You

Table Next header codes for IPv6

Code	Next Header
0	Hop-by-hop option
2	ICMP
6	TCP
17	UDP
43	Source routing
44	Fragmentation
50	Encrypted security payload
51	Authentication
59	Null (no next header)
60	Destination option

Table Comparison between IPv4 and IPv6 packet headers

Comparison
1. The header length field is eliminated in IPv6 because the length of the header is fixed in this version.
2. The service type field is eliminated in IPv6. The priority and flow label fields together take over the function of the service type field.
3. The total length field is eliminated in IPv6 and replaced by the payload length field.
4. The identification, flag, and offset fields are eliminated from the base header in IPv6. They are included in the fragmentation extension header.
5. The TTL field is called hop limit in IPv6.
6. The protocol field is replaced by the next header field.
7. The header checksum is eliminated because the checksum is provided by upper-layer protocols; it is therefore not needed at this level.
8. The option fields in IPv4 are implemented as extension headers in IPv6.