Network Layer

review

ISO/OSI's network model

How many layers have the OSI's model divided the network architecture into?

Seven layers

What are they from the bottom to the top?

Description of the network layer

a) **The network layer is concerned with getting p-ackets from the source all the way to the desti-nation.**

- **To achieve its goals, the network layer must know about the topology of the communica-tion subnet and choose appropriate paths th-rough it. It must also take care to choose routes to avoid overloading some of the commun-ication lines and routers while leaving others idle.**

The Network Layer

5.1 Network Layer Design Issues

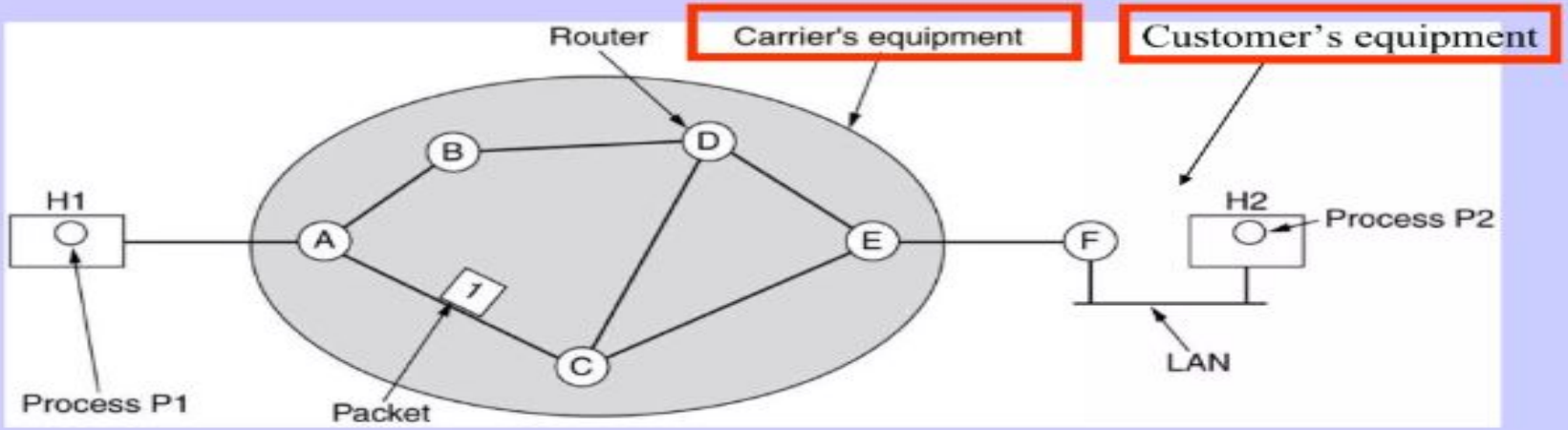
5.2 Routing Algorithms

5.6 The Network Layer in the Internet

5.1 Network Layer Design Issues

a) **Store-and-Forward Packet Switching**
b) Services Provided to the Transport Layer
c) Implementation of Connectionless Service
d) Implementation of Connection-Oriented Service
e) Comparison of Virtual-Circuit and Datagram Subnets

Store-and-Forward Packet Switching



The environment of the network layer protocols.

- This equipment is used as follows:

a) A host with a packet to send transmits it to the nearest router, either on its own LAN or over a point-to-point link to the carrier. The packet is stored there until it has fully arrived so the checksum can be verified. Then it is forwarded to the next router along the path until it reaches the destination host, where it is delivered. This mechanism is store-and-forward packet switching, as we have seen in previous chapters.

5.1 Network Layer Design Issues

a) Store-and-Forward Packet Switching
b) Services Provided to the Transport Layer
c) Implementation of Connectionless Service
d) Implementation of Connection-Oriented Service
e) Comparison of Virtual-Circuit and Datagram Subnets

Services Provided to the Transport Layer

What kind of services the network layer provides to the transport layer ?

- **The network layer services have been designed with the following goals:**

1. **The services should be independent of the router technology.**
2. **The transport layer should be shielded from the number, type, and topology of the routers present.**
3. **The network addresses made available to the transport layer should use a uniform numbering plan, even across LANs and WANs.**

5.1 Network Layer Design Issues

a) Store-and-Forward Packet Switching
b) Services Provided to the Transport Layer
c) Implementation of Connectionless Service
d) Implementation of Connection-Oriented Service
e) Comparison of Virtual-Circuit and Datagram Subnets

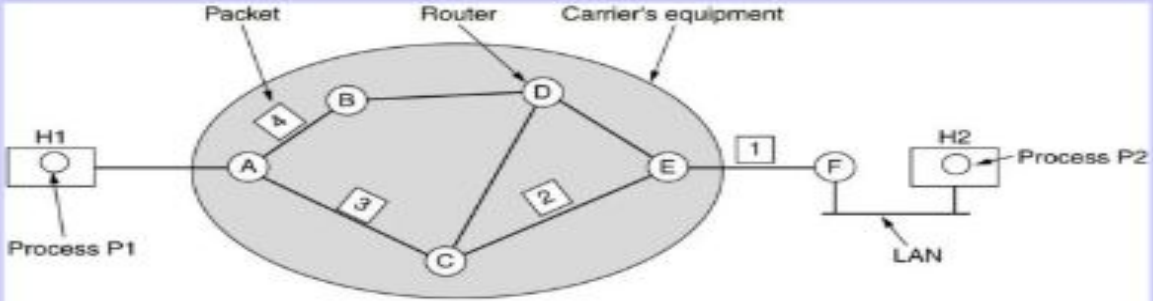
a) Two different organizations are possible, depending on the type of service offered.

b) If connectionless service is offered, packets are injected into the subnet individually and routed independently of each other. No advance setup is needed. In this context, the packets are frequently called datagrams and the subnet is called a datagram subnet.

c) If connection-oriented service is used, a path from the source router to the destination router must be established before any data packets can be sent. This connection is called a VC (virtual circuit) and the subnet is called a virtual-circuit subnet.

Implementation of Connectionless Service

P346



A's table

Dest	initially	later
A	–	–
B	B	B
C	C	C
D	B	B
E	C	B
F	C	B

Dest Line

C's table

Dest	Line
A	A
B	A
C	–
D	D
E	E
F	E

E's table

Dest	Line
A	C
B	D
C	C
D	D
E	–
F	F

The question is: a packet with a destination D arrives at router A. then which router will router A send this packet to?

5.1 Network Layer Design Issues

a) Store-and-Forward Packet Switching
b) Services Provided to the Transport Layer
c) Implementation of Connectionless Service
d) Implementation of Connection-Oriented Service
e) Comparison of Virtual-Circuit and Datagram Subnets

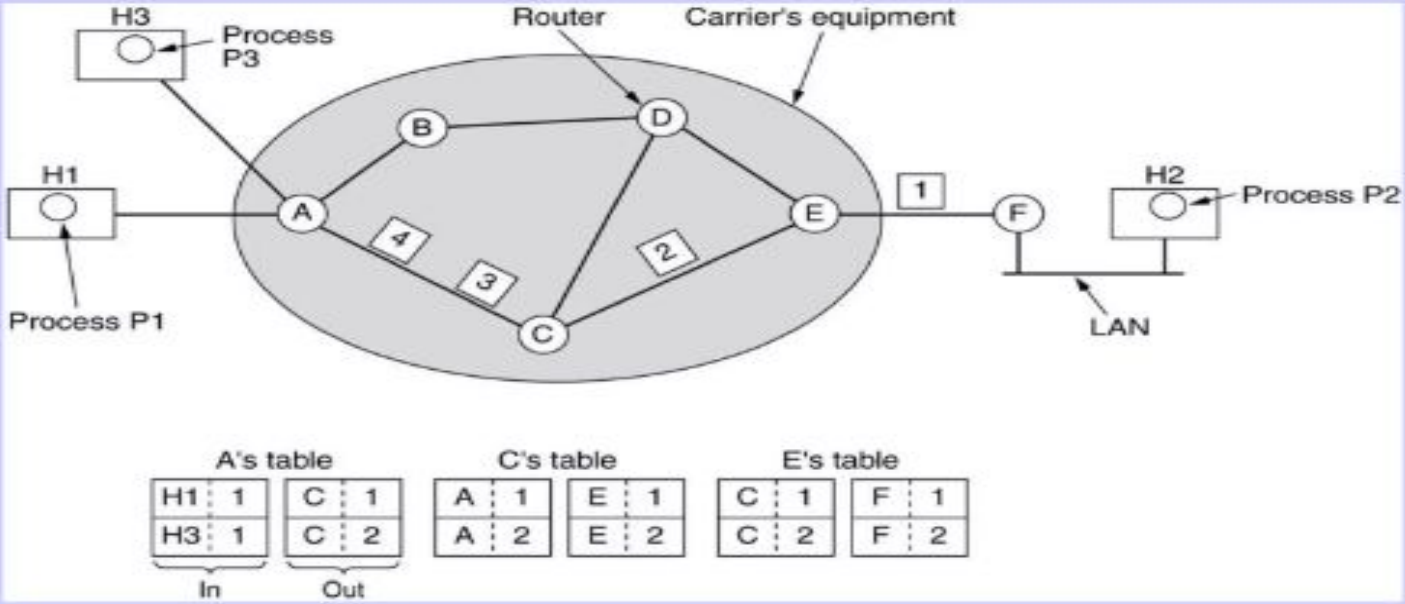
a) For connection-oriented service, we need a virtual-circuit subnet.

b) The idea behind virtual circuits is to avoid having to choose a new route for every packet sent. Instead,when a connection is established, a route from the source machine to the destination machine is chosen as part of the connection setup and stored in tables inside the routers. That route is used for all traffic flowing over the connection, exactly the same way that the teleph-one system works. When the connection is released, the virtual circuit is also terminated.

c) With connection-oriented service, each packet carries an identifier telling which virtual circuit it belongs to.

Implementation of Connection-Oriented Service

P347



Routing within a virtual-circuit subnet.

5.1 Network Layer Design Issues

a) Store-and-Forward Packet Switching
b) Services Provided to the Transport Layer
c) Implementation of Connectionless Service
d) Implementation of Connection-Oriented Service
e) Comparison of Virtual-Circuit and Datagram Subnets

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

Chapter 5 The Network Layer

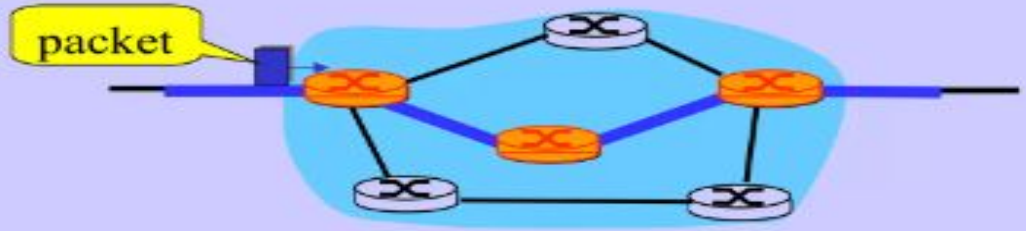
5.1 Network Layer Design Issues

5.2 Routing Algorithms

5.6 The Network Layer in the Internet

Description of Routing Algorithms

1 **Definition**: The routing algorithm is that part of the network layer software responsible for deciding which output line an incoming packet should be transmitted on.



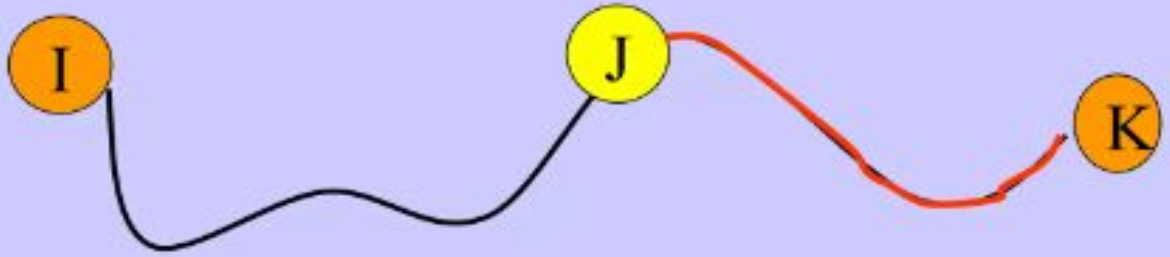
2 **Properties of routing algorithm**: correctness, simplicity, robustness, stability, fairness, and optimality.

5.2 Routing Algorithms

- The Optimality Principle
- Shortest Path Routing
- Flooding
- Distance Vector Routing
- Link State Routing
- Hierarchical Routing
- Broadcast Routing

5.2.1 The Optimality Principle

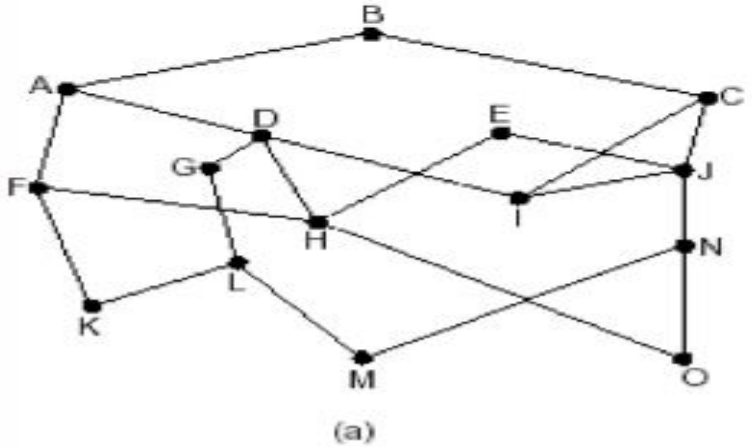
a) **The Optimality Principle**: if router J is on the optimal path from router I to router K, then the optimal path from J to K also falls along the same route.



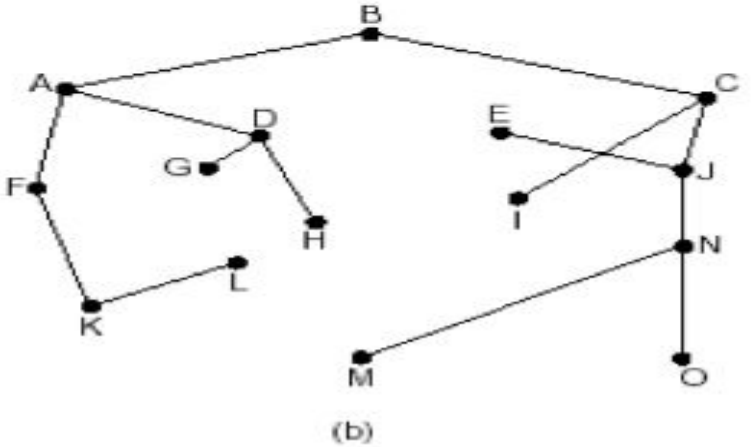
5.2.1 The Optimality Principle

a) The set of optimal routes from all sources to a given destination form a tree rooted at the destination. Such a tree is called a **sink tree**.

b) Figure (a) A subnet. (b) A sink tree for router B.



(a)



(b)

5.2.1 The Optimality Principle

a) **Note**: A sink tree is not necessarily unique; other trees with the same path lengths may exist.

b) The goal of all routing algorithms is to discover and use the sink trees for all routers.

5.2.2 Shortest Path Routing

a) A technique to study routing algorithms: The idea is to build a graph of the subnet, with each node of the graph representing a router and each arc of the graph representing a communication line (often called a link).

b) To choose a route between a given pair of routers, the algorithm just finds the shortest path between them on the graph.

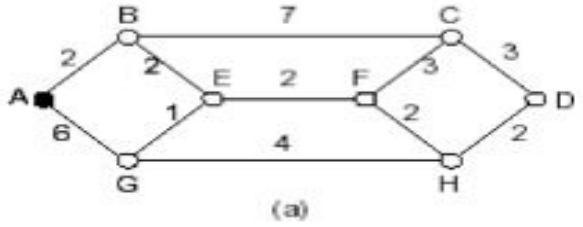
c) One way of measuring path length is the number of hops. Another metric is the geographic distance in kilometers . Many other metrics are also possible. For example, each arc could be labeled with the mean queuing and transmission delay for some standard test packet as determined by hourly test runs.

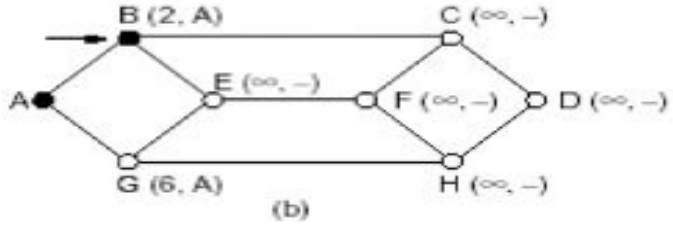
d) In the general case, the labels on the arcs could be computed as a function of the distance, bandwidth, average traffic, communication cost, mean queue length, measured delay, and other factors. By changing the weighting function, the algorithm would then compute the "shortest" path measured according to any one of a number of criteria or to a combination of criteria.

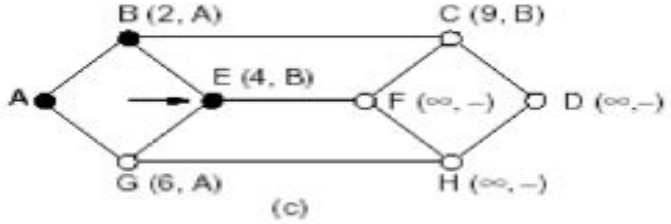
5.2.2 Shortest Path Routing

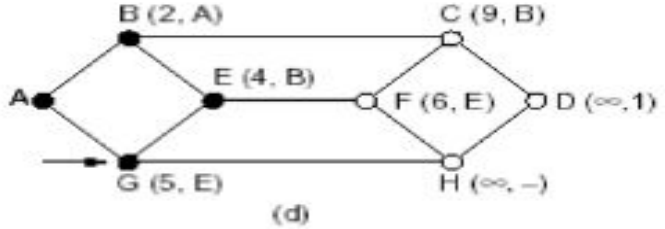
a) **Dijkstra algorithm**:Each node is labeled (in parentheses) with its distance from the source node along the best known path. Initially, no paths are known, so all nodes are labeled with infinity. As the algorithm proceeds and paths are found, the labels may change, reflecting better paths. A label may be either **tentative** or **permanent**. Initially, all labels are tentative. When it is discovered that a label represents the shortest possible path from the source to that node, it is made permanent and never changed thereafter.

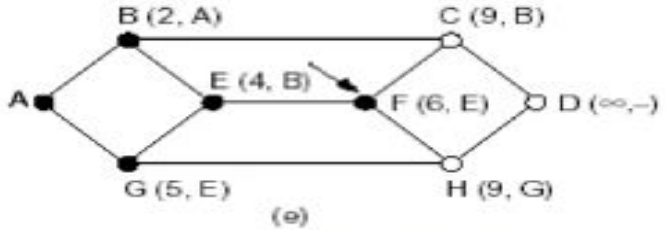
（1930 年 5 月 11 日～ 2002 年 8 月 6 日）

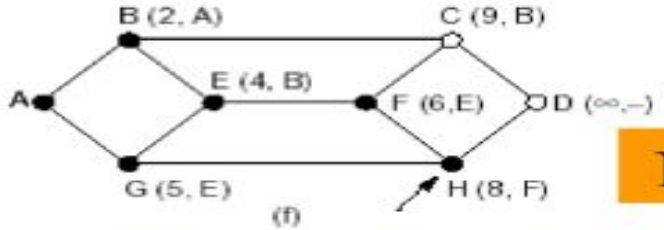












P353

Next steps?

- Figure. The first five steps used in computing the shortest path from A to D. The arrows indicate the working node.

The shortest path from A to D ABEFHD

5.2.3 Flooding

a) **Flooding algorithm**:every incoming packet is sent out on every outgoing line except the one it arrived on.

b) Flooding obviously generates vast numbers of duplicate packets, in fact, an infinite number unless some measures are taken to damp the process.

c) One such measure is to have a hop counter contained in the header of each packet, which is decremented at each hop, with the packet being discarded when the counter reaches zero.

d) An alternative technique for damming the flood is to keep track of which packets have been flooded, to avoid sending them out a second time.

- How to implement that? (**P**355)

5.2.3 Flooding

a) A variation of flooding that is slightly more practical is **selective flooding**.In this algorithm the routers do not send every incoming packet out on every line, only on those lines that are going approximately in the right direction.

b) Applications of flooding algorithm:

1. military applications
2. distributed database applications
3. wireless networks
4. as a metric against which other routing algorithms can be compared

5.2.4 Distance Vector Routing

a) A dynamic routing algorithm

b) **Distance vector routing algorithms** operate by having each router maintain a table (i.e, a vector) giving the best known distance to each destination and which line to use to get there. These tables are updated by exchanging information with the neighbors. (also named the distributed Bellman-Ford routing algorithm and the Ford-Fulkerson algorithm)

August 26, 1920 ~ March 19, 1984

Lester Randolph Ford

NO PHOTO

September 23,1927 ~

Delbert Ray Fulkerson

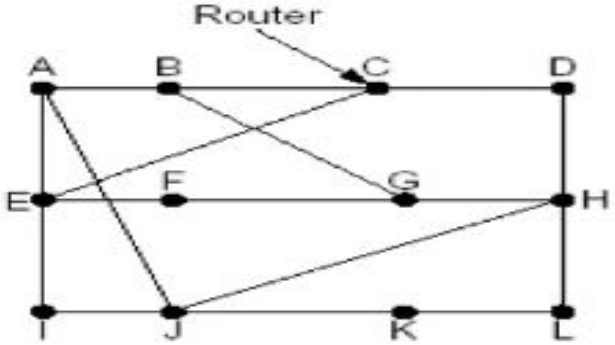
NO PHOTO

August 14, 1924 ~ January 10, 1976

5.2.4 Distance Vector Routing

a) **Table content:** 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.

b) **Table updating method**:Assume that the router knows the delay to each of its neighbors. Once every T msec each router sends to each neighbor a list of its estimated delays to each destination. It also receives a similar list from each neighbor. Imagine that one of these tables has just come in from neighbor X, with X_i being X's estimate of how long it takes to get to router i. If the router knows that the delay to X is m msec, it also knows that it can reach router i via X in X_i + m msec. By performing this calculation for each neighbor, a router can find out which estimate seems the best and use that estimate and the corresponding line in its new routing table. Note that the old routing table is not used in the calculation.



(a)

New estimated delay from J

To	A	I	H	K	Line
A	0	24	20	21	8 A
B	12	36	31	28	20 A
C	25	18	19	36	28 I
D	40	27	8	24	20 H
E	14	7	30	22	17 I
F	23	20	19	40	30 I
G	18	31	6	31	18 H
H	17	20	0	19	12 H
I	21	0	14	22	10 I
J	9	11	7	10	0 —
K	24	22	22	0	6 K
L	29	33	9	9	15 K
	JA delay is 8	JI delay is 10	JH delay is 12	JK delay is 6	New routing table for J

Vectors received from J's four neighbors

(b)

- Part (a) shows a subnet. The first four columns of part (b) show the delay vectors received from the neighbors of router J. Suppose that J has measured or estimated its delay to its neighbors, A, I, H, and K as 8, 10, 12, and 6 msec, respectively.

Link state Routing

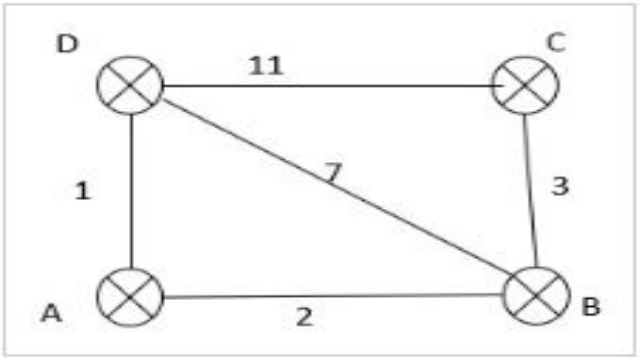
Link State Routing

- In the Link - State Routing Protocol, the router attempts to construct its own internal map of the network topology. It provides the information about whether the link to reach the router is active or not.
- Every router will create something called Link state packets.
- In the first round every node creates link state packets with the help of “Hello packets”.
- **Step 1 − Prepare the link state packet at every router.**

- **Step 1 − Prepare the link state packet at every router.**

D	
Seq	
TTL	
C	11
B	7
A	1

C	
Seq	
TTL	
D	11
B	3



A	
Seq	
TTL	
B	2
D	1

B	
Seq	
TTL	
A	2
D	7
C	3

Step 2 – Every router flood the link state packets to every offer router

At A –

Link state packet B, C, D

From B

A	2
C	3
D	7

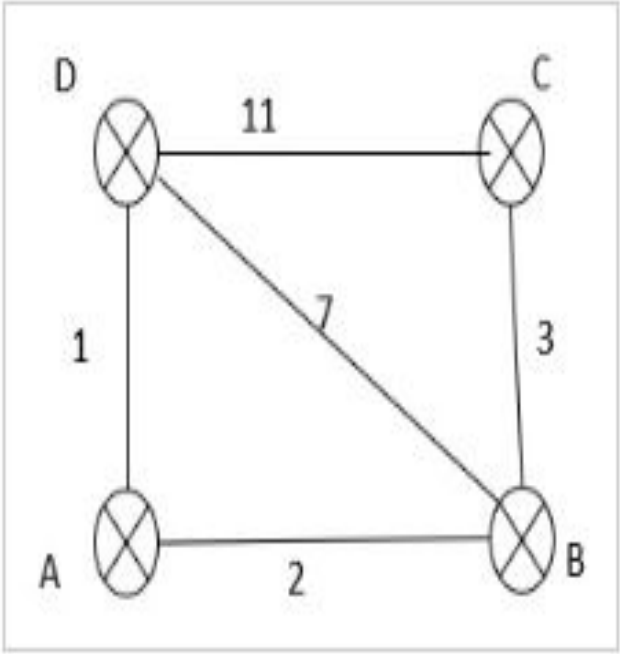
From C

B	3
D	11

From D

A	1
B	7
C	11

Now A can construct the entire graph using the received link protocol.



Like this, every node is able to construct the graph in its own memory. Every node has an entire graph. So every router can apply the Dijkstra algorithm to find the shortest path.

Advantages

The advantages of link-state routing protocol are as follows –

- Fast Network Convergence: It is the main advantage of the link-state routing protocol. Because of receiving an LSP, link-state routing protocols immediately flood the LSP out of all interfaces without any changes except for the interface from which the LSP was received.
- Topological Map: Link-state routing uses a topological map or SPF tree for creating the network topology. Using the SPF tree, each router can separately determine the shortest path to every network.
- Hierarchical Design: Link-state routing protocols use multiple areas and create a hierarchical design to network areas. The multiple areas allow better route summarization.
- Event-driven Updates: After initial flooding of LSPs, the LSPs are sent only when there is a change in the topology and contain only the information regarding that change. The LSP contains only the information about the affected link. The link-state never sends periodic updates.

Disadvantages

The disadvantages of link-state routing protocol are as follows –

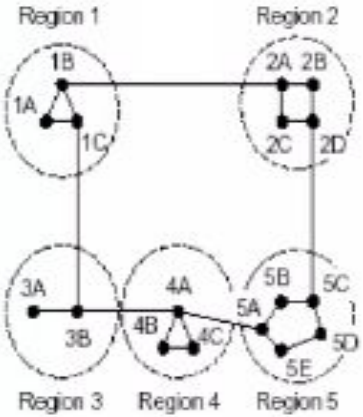
- **Memory Requirements** – The link-state routing protocol creates and maintains a database and SPF tree. The database and SPF tree required more memory than a distance vector protocol.
- **Processing Requirements** – Link-state routing protocols also require more CPU processing because the SPF algorithm requires more CPU time than distance-vector algorithms just like Bellman-Ford because link-state protocols build a complete map of the topology.
- **Bandwidth Requirements** – The link-state routing protocol floods link-state packet during initial start-up and also at the event like network breakdown, and network topology changes, which affect the available bandwidth on a network. If the network is not stable it also creates issues on the bandwidth of the network.

5.2.6 Hierarchical Routing

- The routers are divided into what we will call regions, with each router knowing all the details about how to route packets to destinations within its own region, but knowing nothing about the internal structure of other regions.
- For huge networks, a two-level hierarchy may be insufficient; it may be necessary to group the regions into clusters, the clusters into zones, the zones into groups, and so on, until we run out of names for aggregations.

5.2.6 Hierarchical Routing

- The full routing table for router 1A has 17 entries, as shown in (b). When routing is done hierarchically, as in (c), there are entries for all the local routers as before, but all other regions have been condensed into a single router, so all traffic for region 2 goes via the 1B -2A line, but the rest of the remote traffic goes via the 1C -3B line. Hierarchical routing has reduced the table from 17 to 7 entries.



(a)

Full table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2A	1B	2
2B	1B	3
2C	1B	3
2D	1B	4
3A	1C	3
3B	1C	2
4A	1C	3
4B	1C	4
4C	1C	4
5A	1C	4
5B	1C	5
5C	1B	5
5D	1C	6
5E	1C	5

(b)

Hierarchical table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2	1B	2
3	1C	2
4	1C	3
5	1C	4

(c)

5.2.6 Hierarchical Routing

- Unfortunately, these gains in space are not free. There is a penalty to be paid, and this penalty is in the form of increased path length. For example, the best route from 1A to 5C is via region 2, but with hierarchical routing all traffic to region 5 goes via region 3, because that is better for most destinations in region 5.

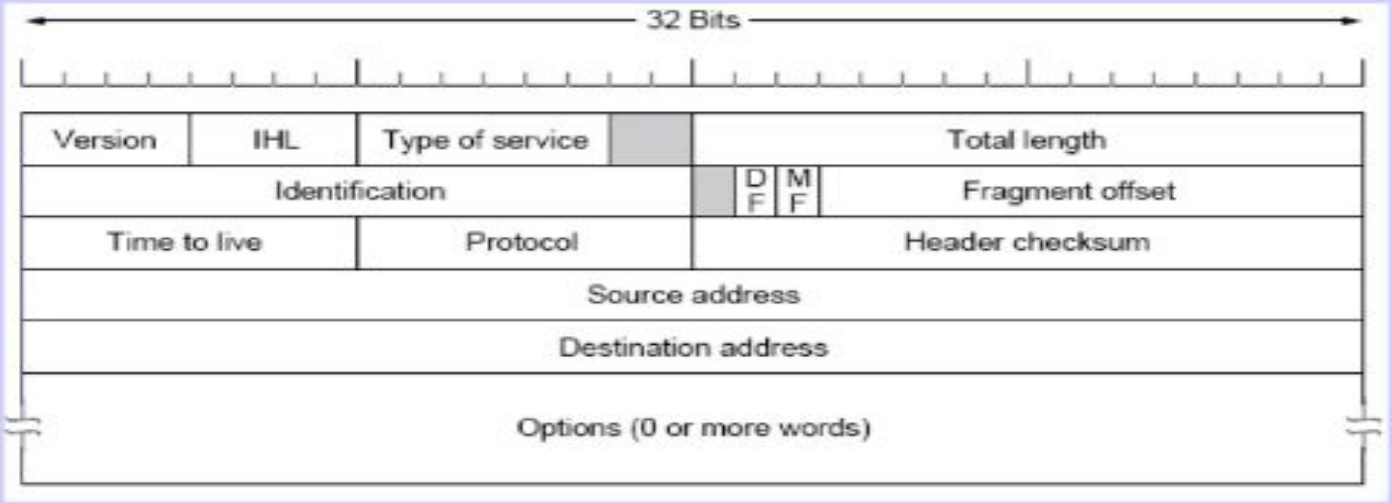
5.6 The Network Layer in the Internet

- The IP Protocol
- IP Addresses
- Internet Control Protocols

5.6.1 The IP Protocol

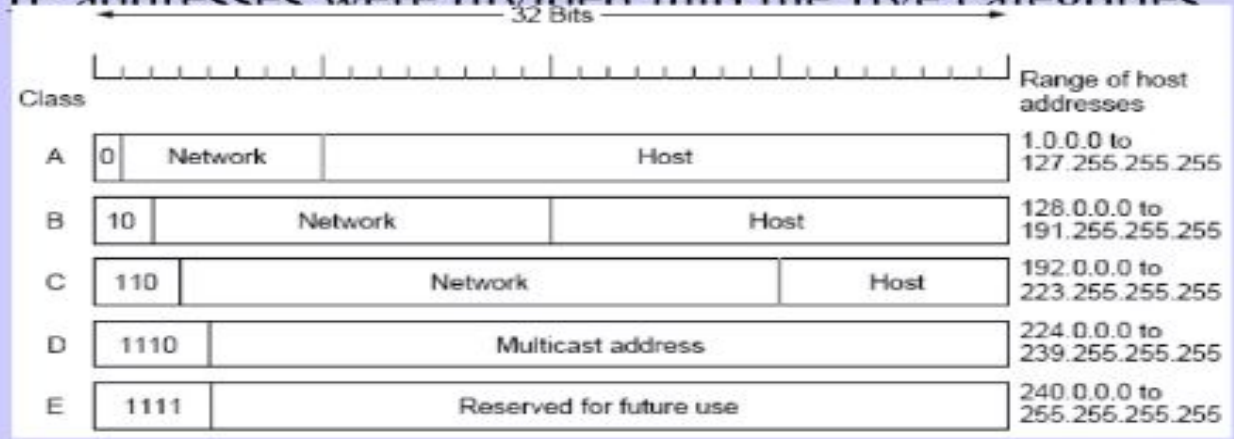
- An IP datagram consists of a header part and a text part. The header has a 20-byte fixed part and a variable length optional part.

P434



5. 6. 2 IP Addresses

- Every host and router on the Internet has an IP address, which encodes its network number and host number.
- All IP addresses are 32 bits long. It is important to note that an IP address does not actually refer to a host. It really refers to a network interface, so if a host is on two networks, it must have two IP addresses.
- IP addresses were divided into the five categories



network mask

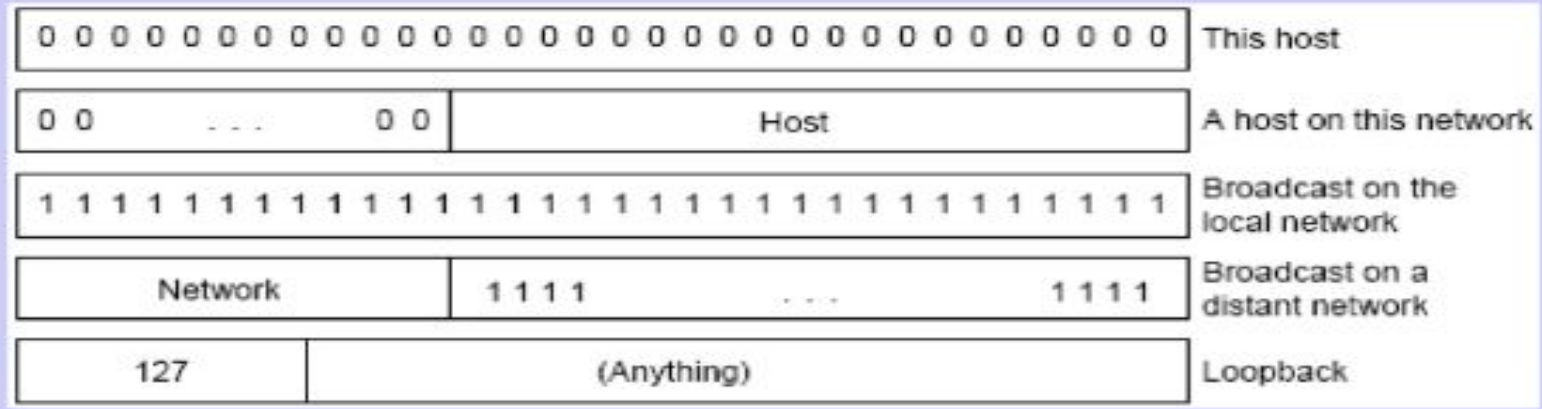
255.0.0.0

255.255.0.0

255.255.255.0

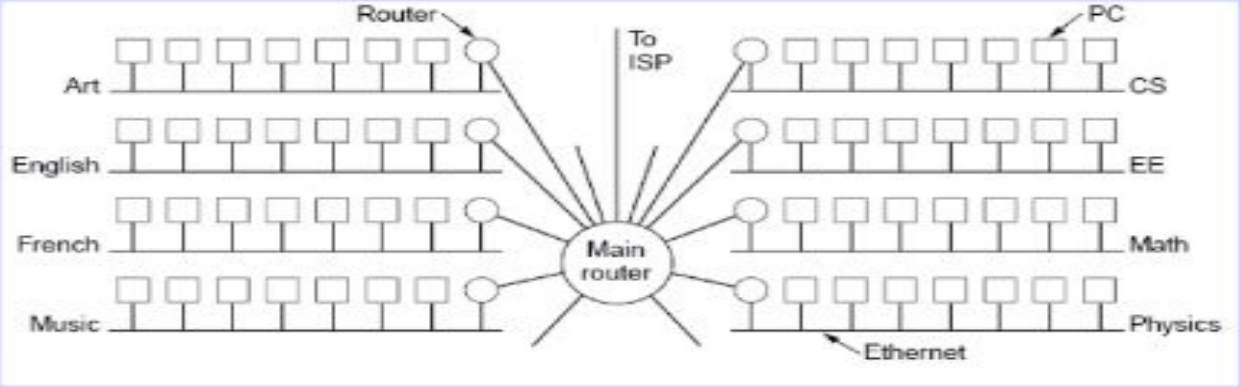
5. 6. 2 IP Addresses

- The values 0 and -1 (all 1s) have special meanings. The value 0 means this network or this host. The value of -1 is used as a broadcast address to mean all hosts on the indicated network.



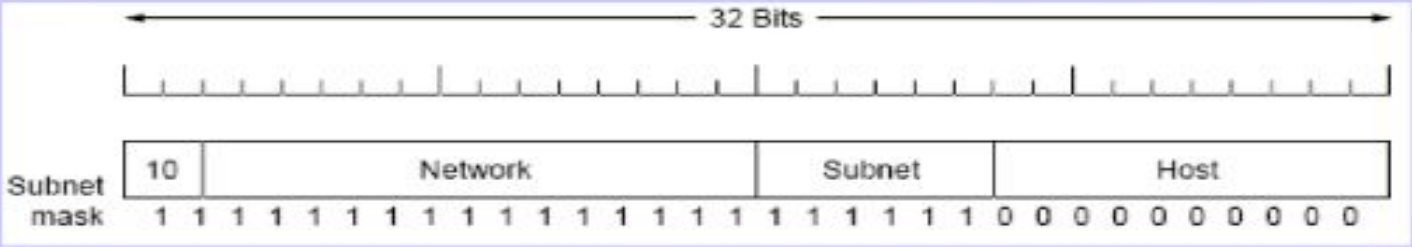
5. 6. 2 IP Addresses

- All the hosts in a network must have the same network number. This property of IP addressing can cause problems as networks grow. For example……
- The problem is the rule that a single class A, B, or C address refers to one network, not to a collection of LANs.
- The solution is to allow a network to be split into several parts for internal use but still act like a single network to the outside world.



5. 6. 2 IP Addresses

- To implement subnetting, the main router needs a subnet mask that indicates the split between network + subnet number and host.
- For example, if the university has a B address(130.50.0.0) and 35 departments, it could use a 6-bit subnet number and a 10-bit host number, allowing for up to 64 Ethernets, each with a maximum of 1022 hosts.



- The subnet mask can be written as 255.255.252.0. An alternative notation is /22 to indicate that the subnet mask is 22 bits long.

5.6.3 Internet Control Protocols

1、The Internet Control Message Protocol

- The operation of the Internet is monitored closely by the routers. When something unexpected occurs, the event is reported by the ICMP (Internet Control Message Protocol), which is also used to test the Internet.
- Each ICMP message type is encapsulated in an IP packet

Message type	Description
Destination unreachable	Packet could not be delivered
Time exceeded	Time to live field hit 0
Parameter problem	Invalid header field
Source quench	Choke packet
Redirect	Teach a router about geography
Echo	Ask a machine if it is alive
Echo reply	Yes, I am alive
Timestamp request	Same as Echo request, but with timestamp
Timestamp reply	Same as Echo reply, but with timestamp