CMR Institute of Technology
Department of Information Science & Engineering
Improvement Test Solutions
10CS64 – Computer Networks-2

1. a] Define routing algorithm. Explain Bellman-Ford algorithm with the help of an example. [6] CO2 L2

ROUTING

• Routing means determining feasible paths for packets to follow from each source to each destination.

BELLMAN-FORD ALGORITHM

• If each neighbor of node-A knows the shortest path to node-Z, then node-A can determine its shortest path to node-Z by calculating the cost to node-Z through each of its neighbors and picking the minimum.

• Let D_j = current estimate of the minimum cost from node-j to the destination

Let C_{ij} = link cost from node-i to node-j. (For example $C_{13}=C_{31}=2$) The link cost from node-i to itself is defined to be zero ($C_{ii}=0$).

The link cost between node-i & node-k is infinite if node-i & node-k are not directly connected.(for example $C_{15}=C_{23}=\sim$)

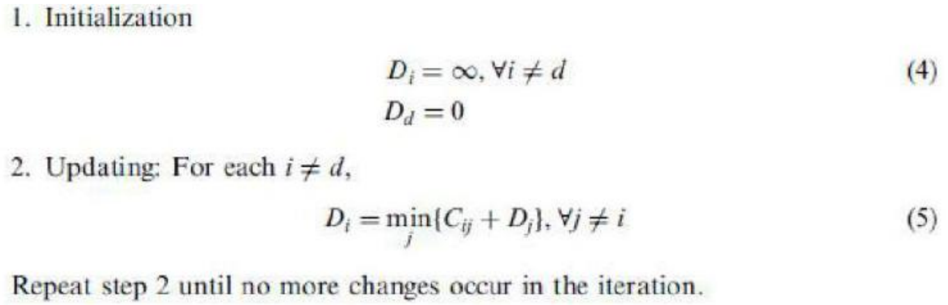
• If the destination node is node-6, then the minimum cost from node-2 to the destination node-6 can be calculated in terms of distances through node-1, node-4 or node-5(Fig 7.29):

$D_2 = \min\{C_{21}+D_1, C_{24}+D_4, C_{25}+D_5\}$

$= \min\{3+3, 1+3, 4+2\}$

$= 4$

Algorithm is as follows:



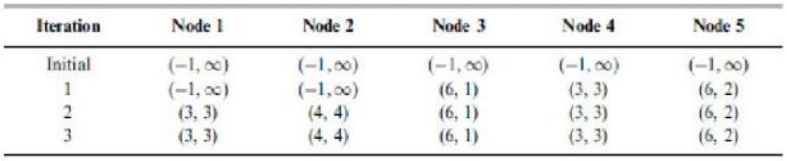
1. Initialization

$$D_i = \infty, \forall i \neq d \qquad (4)$$
$$D_d = 0$$

2. Updating: For each $i \neq d$,

$$D_i = \min_j\{C_{ij} + D_j\}, \forall j \neq i \qquad (5)$$

Repeat step 2 until no more changes occur in the iteration.



Iteration	Node 1	Node 2	Node 3	Node 4	Node 5
Initial	$(-1, \infty)$	$(-1, \infty)$	$(-1, \infty)$	$(-1, \infty)$	$(-1, \infty)$
1	$(-1, \infty)$	$(-1, \infty)$	(6, 1)	(3, 3)	(6, 2)
2	(3, 3)	(4, 4)	(6, 1)	(3, 3)	(6, 2)
3	(3, 3)	(4, 4)	(6, 1)	(3, 3)	(6, 2)

TABLE 7.1 Sample processing of Bellman-Ford algorithm. Each entry for node *j* represents the next node and cost of the current shortest path to destination 6.

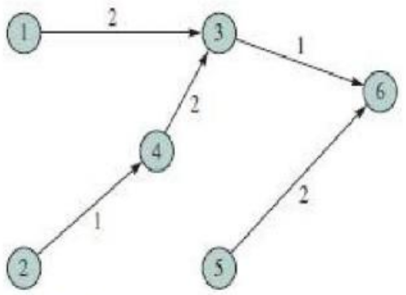


FIGURE 7.29 Shortest-path tree to node 6

b] Explain the structure of a typical sensor node. **[4] CO6 L2**

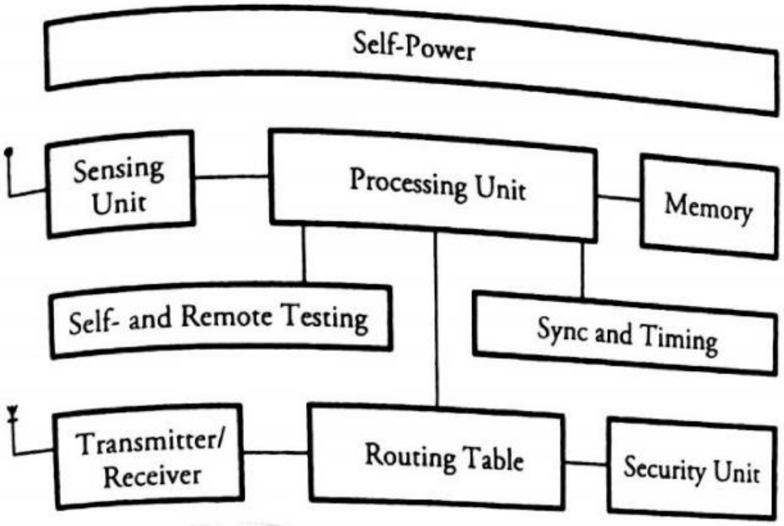


Figure 20.3 A typical wireless sensor node

as well as a self- and remote-testing unit, a synchronizing and timing unit, a routing table, and security units. Since nodes in a network are not physically accessible once they are deployed in the field, they are not worth being brought under test. An option is an on-board remote self-testing unit for the node on a routine basis.

Each node must determine its location. This task is carried out by a location-finding system based on the *global positioning system* (GPS). All the processes within the sensor node are synchronized by a local clocking and synchronizing system. The communication and security protocol units are in fact part of the processing unit. These two units are responsible for computing the best path for networking and security of the data being transmitted. The three main blocks of the sensor node—sensing unit, processing and memory unit, and power unit—are described in more detail in the following subsections.

Sensing Unit

The sensing unit consists of a sensor and an analog-to-digital converter. A smart sensor node consists of a combination of multiple sensors. The analog signals produced by the sensors, based on the observed event, are converted to digital signals by the converter and then fed into the processing unit. The sensing unit collects data externally and interacts with the central processor at the heart of the node.

Processing and Memory Unit

The *processing unit* performs certain computations on the data and, depending on how it is programmed, may send the resulting information out to the network. The processing unit, which is generally associated with memory, manages the procedures

2. a] Explain datagram and virtual packet switching with delay calculations. [5] CO1 L2

DATAGRAM PACKET SWITCHING

- Let transmission delay of message = p seconds.
- Let transmission time of message = T seconds.

- Let the message is broken into 3 separate packets.
- As shown in figure 7.16, the first packet arrives at the switch after p+P seconds.
  The first packet is received at the second switch at time 2p+2P.
  The first packet is received at the third switch at time 3p+3P.

The final packet will arrive at the destination at time 3p+3P+2P=3p+5P=3p+t+2p.

- In general, if the path followed by a sequence of packets consists of L hops with identical propagation delays and transmission speeds, then the delay incurred by a message that consists of k packets is given by

Lp+LP+(k-1)P

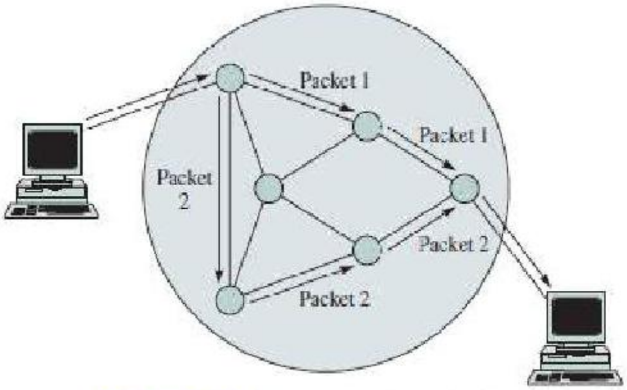


FIGURE 7.15 Datagram packet switching

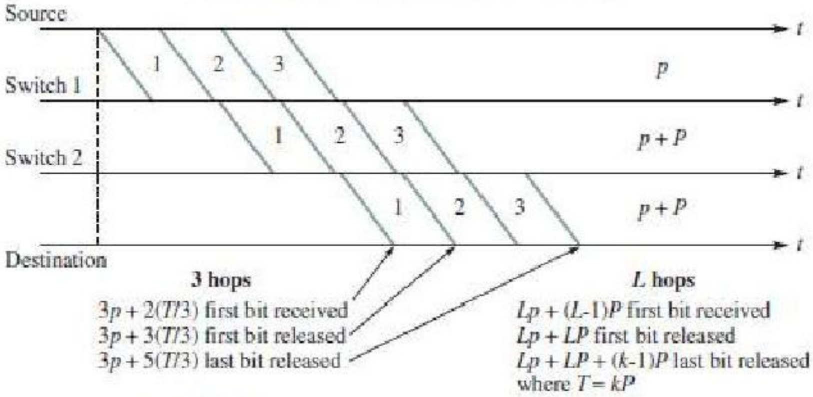
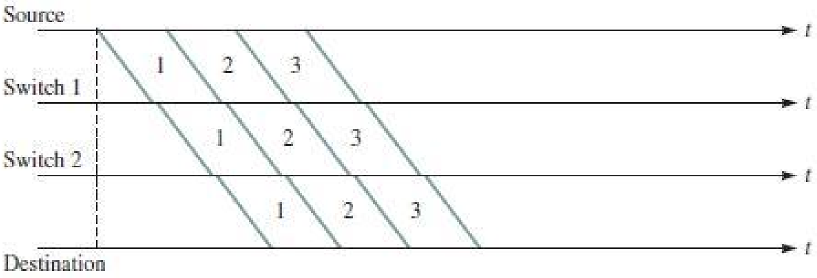

Source
Switch 1
Switch 2
Destination
t
t
t
t
1
2
3
1
2
3
1
2
3
p
$p + P$
$p + P$
3 hops
$3p + 2(T/3)$ first bit received
$3p + 3(T/3)$ first bit released
$3p + 5(T/3)$ last bit released
L hops
$Lp + (L-1)P$ first bit received
$Lp + LP$ first bit released
$Lp + LP + (k-1)P$ last bit released
where $T = kP$

FIGURE 7.16 Delays in packet switching

VIRTUAL CIRCUIT PACKET SWITCHING

- A modified form of virtual-circuit packet switching, called cut-through packet stitching, can be used when retransmissions are not used in the underlying data link control (Figure 7.22).

- The minimum delay in transmitting the message is approximately equal to the sum of the propagation delays in the various hops plus the one-message transmission time.



Minimum delay = $3p + T$

FIGURE 7.22 Cut-through packet switching

b] Explain the DEEP clustering algorithm. [5] CO6 L2

DEEP (Decentralized Energy Efficient Propagation)

- The protocol that establishes clusters with uniformly distributed cluster heads.

- This protocol balances the load among all the cluster heads by keeping the clusters' radii fairly equal.

- This protocol is completely decentralized, and there is no need for any location-finder device or hardware.

- The protocol starts with initial cluster head and forms new cluster-head candidates gradually by controlling the relative distance between a pair of cluster heads and the circular radius of each cluster.

Clustering Algorithm

1) Initialize: Initial cluster head finds cluster members by sending "cluster-head declaration."

2) Initial cluster head finds new cluster-head candidates by sending "cluster-head exploration signal."

3) Repeat: Cluster-head candidates that are placed on the (d_{r1},d_{r2}) ring find cluster members.

4) Nodes that receive more than one cluster-head declaration choose the closest cluster head, based on the received signal energy.

5) Cluster-head candidates that receive a cluster-head declaration signal negotiate with the sender, and one of them gets eliminated.

6) Confirmed cluster heads send "cluster-head exploration" signals to find new cluster-head candidates (Go to step 4).
7) Finalize: If the number of members in a cluster is less than m_n , all the members find new clusters by sending the membership-search signal.

8) At the end, a node that has not received any control signal sends the membership-search signal.

3. a] With neat diagram explain leaky bucket algorithm used for policing [7] CO2 L2

LEAKY BUCKET ALGORITHM

• The process of monitoring & enforcing the traffic-flow is called the policing.

• When traffic-flow violates agreed-upon contract, the network may choose to tag (or discard) the nonconforming traffic.

• Tagging essentially lowers priority of nonconforming traffic.
• When network resources are exhausted, tagged traffic is the first to be discarded.
• Policing-device can be implemented based on the concept of a leaky bucket.

• Imagine the traffic-flow to a policing-device as water being poured into a bucket that has a hole at the bottom.
• Bucket leaks at a constant rate (Figure 7.53).

• When bucket is full, a new portion of water is said to be nonconforming and the water can be discarded.

When water is poured into bucket & overflow does not occur, a new portion of water (i.e. packet) is said to be conforming.

• The hole ensures that bucket will never overflow as long as drain-rate is higher than rate water is being poured in.

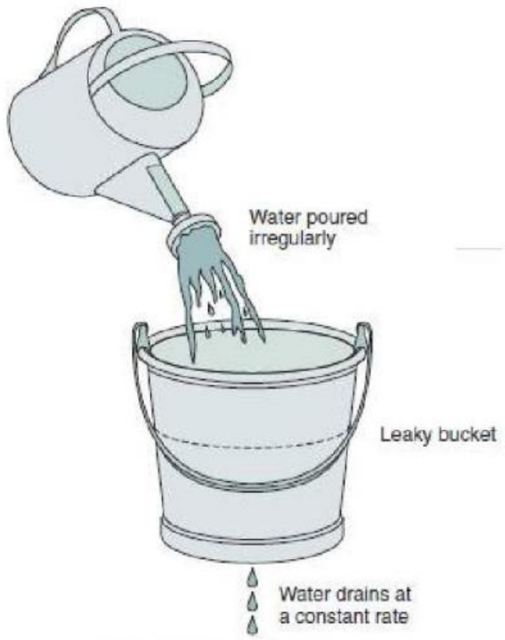


FIGURE 7.53 A leaky bucket

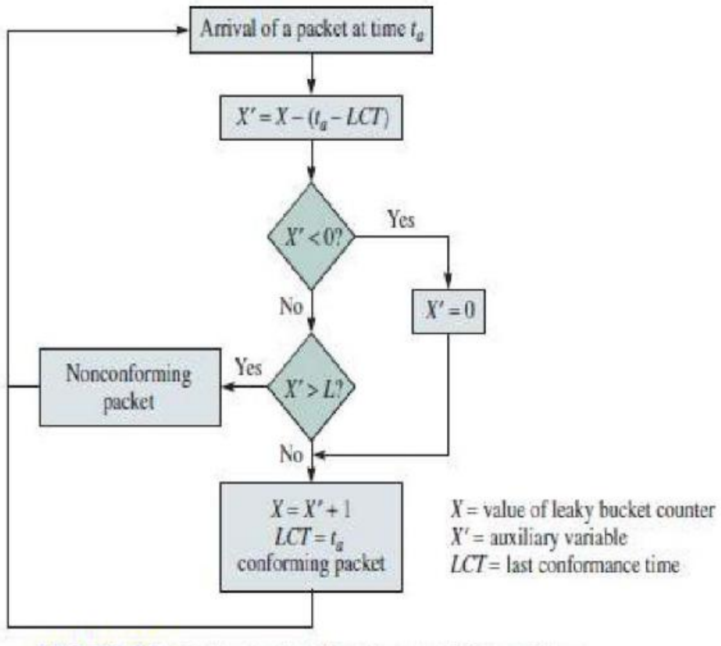

Arrival of a packet at time t_a
$X' = X - (t_a - LCT)$
$X' < 0$?
Yes
$X' = 0$
No
$X' > L$?
Yes
Nonconforming packet
No
$X = X' + 1$
$LCT = t_a$
conforming packet
X = value of leaky bucket counter
X' = auxiliary variable
LCT = last conformance time

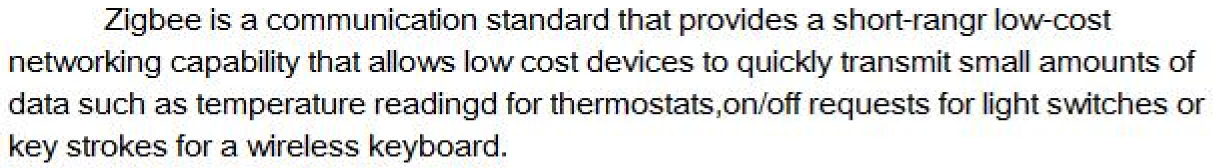
FIGURE 7.54 Leaky bucket algorithm used for policing

• The inverse of I is called the sustainable rate, which is the long-term average rate allowed for the conforming traffic.
• Suppose the peak rate of a given traffic flow is denoted by R and its inverse is T, that is,

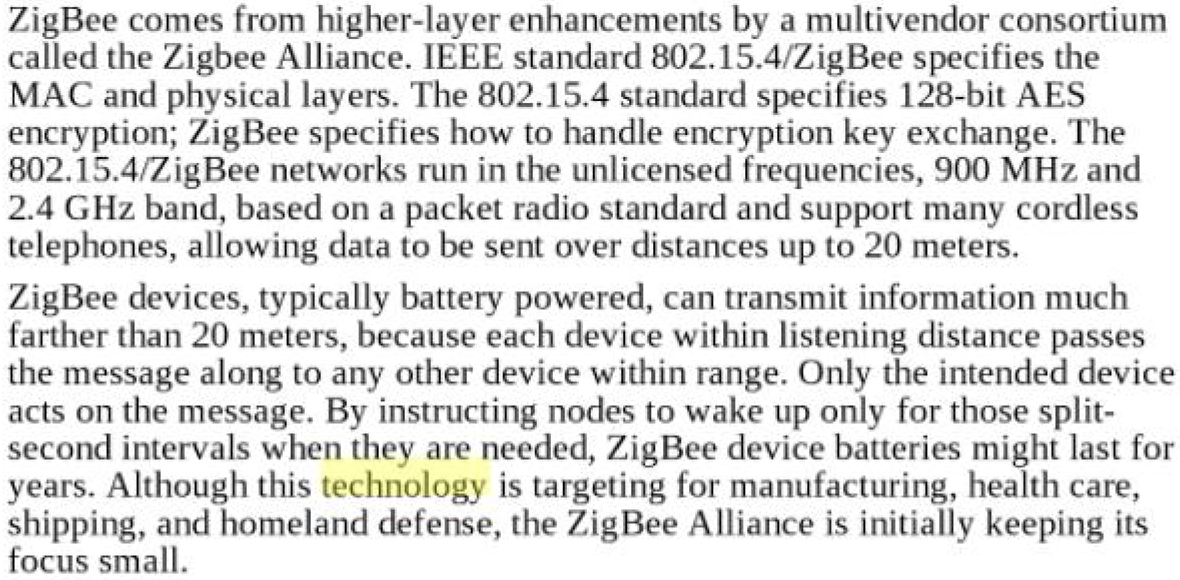
T=1/R. Then, the maximum burst size is given by

$$MBS = 1 + \left[\frac{L}{1 - T}\right]$$

b] Write a note on Zig-bee technology. **[3] CO6 L2**



Zigbee is a communication standard that provides a short-rangr low-cost networking capability that allows low cost devices to quickly transmit small amounts of data such as temperature readingd for thermostats,on/off requests for light switches or key strokes for a wireless keyboard.



ZigBee comes from higher-layer enhancements by a multivendor consortium called the Zigbee Alliance. IEEE standard 802.15.4/ZigBee specifies the MAC and physical layers. The 802.15.4 standard specifies 128-bit AES encryption; ZigBee specifies how to handle encryption key exchange. The 802.15.4/ZigBee networks run in the unlicensed frequencies, 900 MHz and 2.4 GHz band, based on a packet radio standard and support many cordless telephones, allowing data to be sent over distances up to 20 meters.

ZigBee devices, typically battery powered, can transmit information much farther than 20 meters, because each device within listening distance passes the message along to any other device within range. Only the intended device acts on the message. By instructing nodes to wake up only for those split-second intervals when they are needed, ZigBee device batteries might last for years. Although this technology is targeting for manufacturing, health care, shipping, and homeland defense, the ZigBee Alliance is initially keeping its focus small.

4. a] Explain the three way handshake protocol for establishing connection. **[6] CO3 L2**

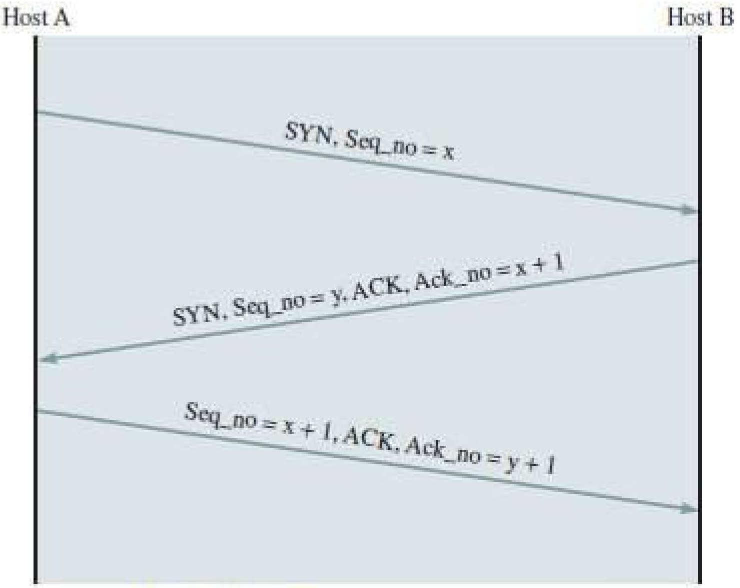
TCP CONNECTION ESTABLISHMENT

• To establish a connection, TCP uses a three-way handshake.

• Before a client attempts to connect with a server, the server must first bind to a port to open it up for connections: this is called a passive open.

• Once the passive open is established, a client may initiate an active open.
• To establish a connection, the three-way (or 3-step) handshake occurs:
1) The active open is performed by the client sending a SYN to the server.
2) In response, the server replies with a SYN-ACK.

3) Finally the client sends an ACK back to the server.
• At this point, both the client and server have received an acknowledgment of the connection.


Host A
Host B
SYN, Seq_no = x
SYN, Seq_no = y, ACK, Ack_no = x + 1
Seq_no = x + 1, ACK, Ack_no = y + 1

- Each SYN message during connection establishment can specify options such as maximum segment size (MSS), window scaling and time stamps.

- The three way handshake procedure ensures that both host’s agree on their initial sequence numbers.

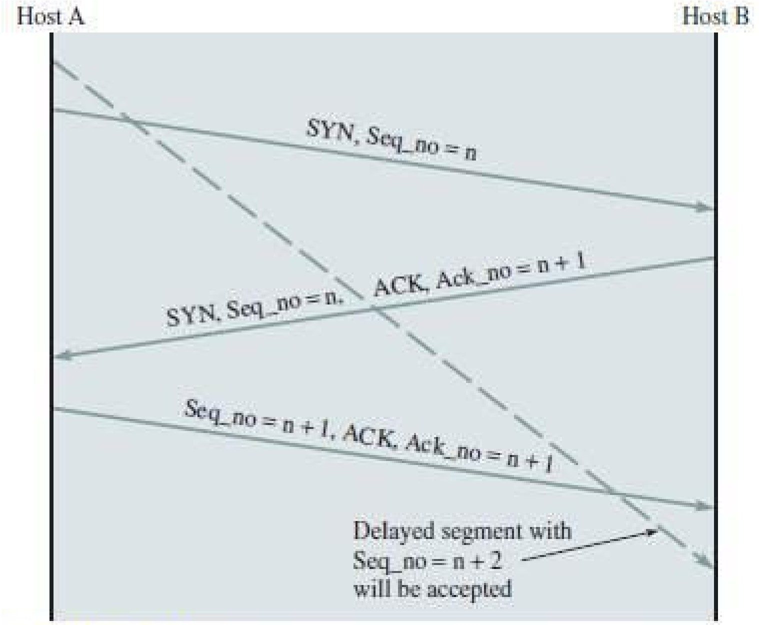


FIGURE 8.23 If a host always uses the same initial sequence number, old segments cannot be distinguished from the current ones

b] Write short notes on mobile IP. [4] CO3 L2

MOBILE IP

- This allows location-independent routing of IP datagrams on the Internet.
- Each mobile node is identified by its home address disregarding its current location in the Internet.

- While away from its home network, a mobile node is associated with a care-of address which identifies its current location and its home address is associated with the local endpoint of a tunnel to its home agent.

- Mobile IP allows portable devices called mobile hosts (MHs) to roam from one area to another.

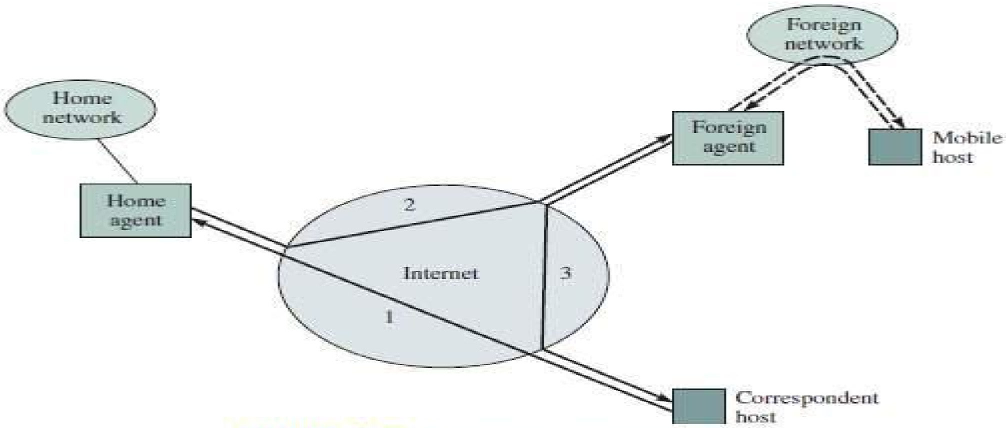


FIGURE 8.29 Routing for mobile hosts

Mobile IP operates as follows

- When a correspondent host (CH) wants to send a packet to MH, the CH transmits the standard IP packet with its address as the source IP address and MH's address as destination IP address.

- This packet will be intercepted by the mobile host's router called home agent (HA). The HA keeps track of the current location of the MH. The HA manages all MHs in its home network that use the same address prefix.

- If the MH is located in the home network, the HA simply forwards the packet to its home network.

- When an MH moves to a foreign network, the MH obtains a care of address from the foreign agent (FA) and registers the new address with its HA. The care-of-address reflects the MH's current location and is typically the address of FA.

- Once the HA knows the care-of-address of the MH, the HA can forward the registration packet to the MH via the FA.

5. a] Write a note on P2P connection in context with overlay networks. [5] CO5 L2

OVERLAY NETWORK

- This is an application specific computer network built on top of another network (Fig 16.11).
- This creates a virtual topology on top of the physical topology of the public network.

- This type of network is created to protect the existing network structure from new protocols whose testing phases requires Internet use.

- These have no control over how packets are routed in the underlying network between a pair of overlay source/destination nodes.

- However, these can control a sequence of overlay nodes through a message passing function before reaching destination.

- These are self-organized. When a node fails, the overlay-network algorithm should provide solutions that let the network recover and recreate an appropriate network structure.

- These permit routing messages to destinations when the IP address is not known in advance.

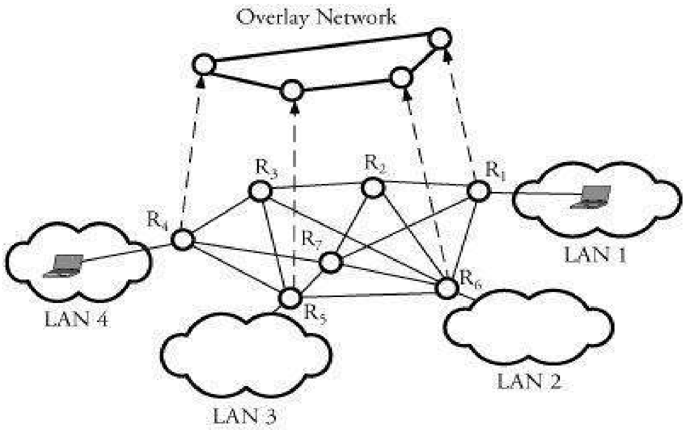


Figure 16.11. An overlay network for connections between two LANs associated with routers R1 and R4

b] Explain MPLS with its packet format. [5] CO5 L2

MPLS (MULTI PROTOCOL LABEL SWITCHING)

- MPLS transmission is a special case of tunneling.
- Features:
  1) Connection-oriented forwarding mechanism

  2) Has layer 2 label-based lookups
  3) Enables traffic engineering to implement peer-to-peer VPNs effectively
  4) Supports other applications, such as IP multicast routing and QoS extension.
- This uses a small label appended to packets and typically makes efficient routing decisions.

MPLS OPERATION

- MPLS network consists of nodes called label-switch-routers (LSR).
- An LSR switches labeled packets according to particular switching tables (Figure 16.5).

- An LSR has 2 functional components: i) Control component & ii) Forwarding component.
  1) The control component: uses routing protocols such as OSPF and BGP.

  • The control component also facilitates the exchange of information with other LSRs to build and maintain the forwarding table.

  • A label is a header used by an LSR to forward packets.

  • When a packet arrives, the forwarding component uses the label of the packet as an index to search the forwarding table for a match.

  2) The forwarding component: then directs the packets from the input interface to the output interface through the switching fabric.

- Key to scalability of MPLS: Labels have only local significance between two devices that communicate.

MPLS Packet Fields

1) Label value: This is significant only locally (Figure 16.6).

2) Exp: This is reserved for future experimental use.

3) S is set to 1 for the oldest entry in the stack and to 0 for all other entries.

4) TTL: This is used to encode a hop-count value to prevent packets from looping forever in the network.

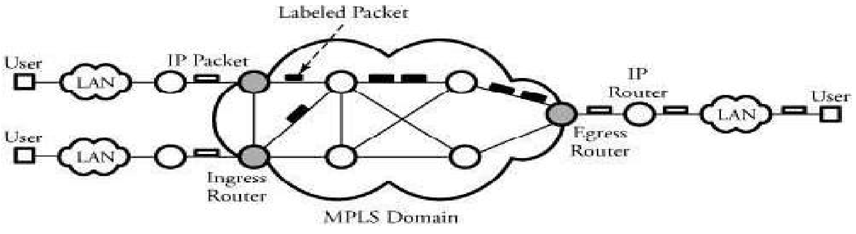


Figure 16.5. An MPLS network

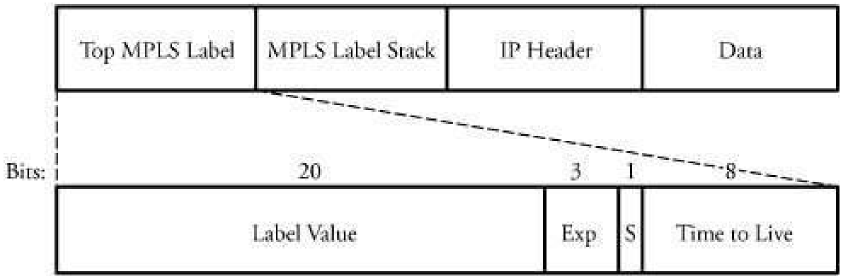


Figure 16.6. MPLS header encapsulation for an IP packet

6. Explain OSPF protocol and its operation. **[10] CO4 L2**

OSPF (OPEN SHORTEST PATH FIRST)

• This is a Link State protocol based on cost rather than hops.

• This is an Interior Gateway Protocol (IGP) Protocol, uses flooding of link state information and Dijkstra’s least-cost path algorithm.

• Router constructs a complete topological map of the entire autonomous system.

• The router then locally runs the Dijkstra’s shortest-path algorithm to determine shortest-path tree to all networks with itself as root node.
• The router’s routing table is then obtained from this shortest-path tree.

• At steady state: All routers have same LS database, Know how many routers in network, interfaces & links between routers, Cost of each link.
• Occasional Hello messages (10 sec) & LS updates sent (30 min).

The operation of OSPF can be explained in 3 steps:

Step1: Discovery of neighbors can be done by sending hello packets in point-to-point links and designated routers in multi-access networks (Figure 8.35).

• To discover, establish and maintain relationships, the OSPF transmit hello packet to each interface periodically, typically for every 10 to 30 sec.
• When a router receives a hello packet, it replies with a hello packet containing router ID of each neighbor it has seen.

• When a router receives a hello packet containing its router ID in one of the neighbor fields, the router is assured that communication to sender is bidirectional.

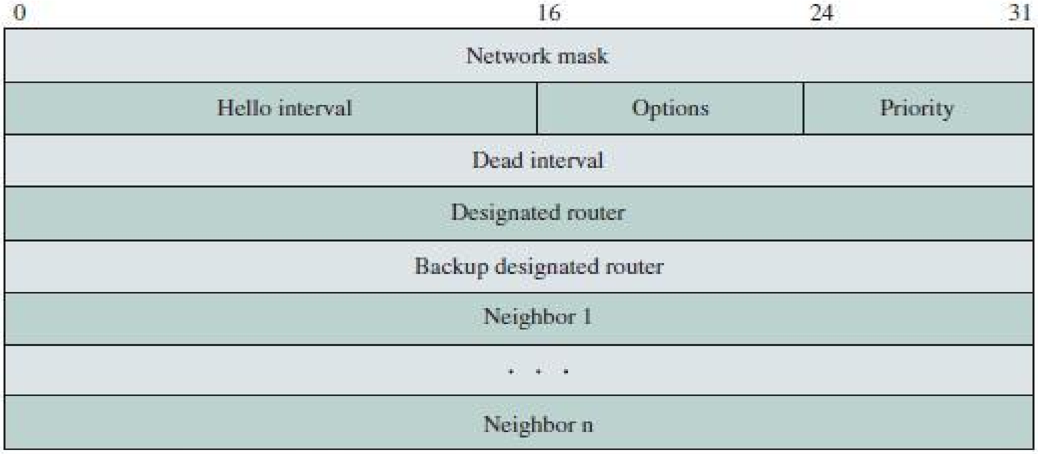


FIGURE 8.35 OSPF Hello packet format

Step 2: Establishment of adjacent and synchronization of link-state databases

- Once the connection is established between two neighbor routers, the database description packet is used to synchronize their link-state databases

- One router acts as master and other as slave (Figure 8.36).

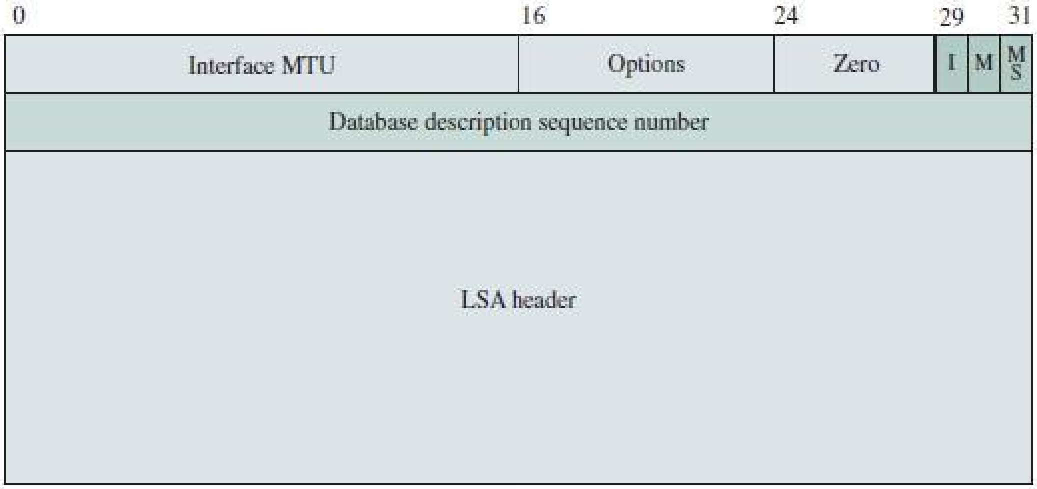


FIGURE 8.36 OSFP database description packet

Step 3: Propagation of OSPF Link State Request and building routing tables

- When a router wants to update the link-state database, it sends a LS request packet to neighbor to update part of its link-state database (Figure 8.38).

- Each LSA request is specified by the link state type, link state ID, and the advertising router.

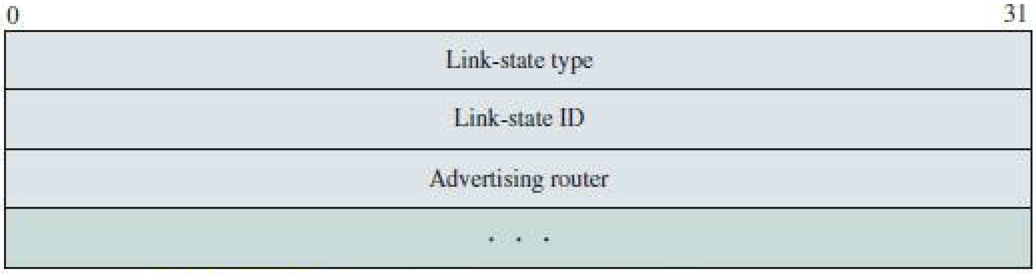
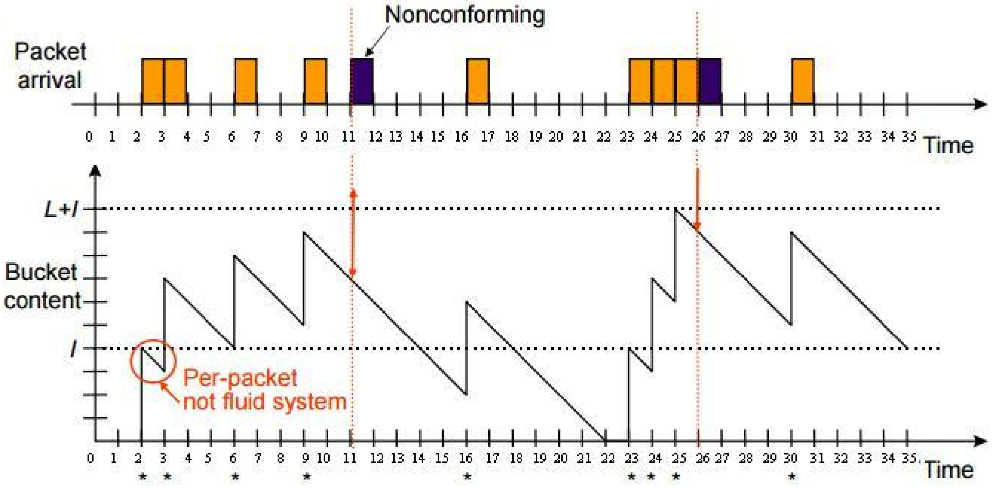


FIGURE 8.38 OSPF link-state request packet

7. a]Suppose that ATM cells arrive at a leaky bucket policer at times t=2,3,6,9,11,16,23,24,25,26 and 30. Assume I=4 and L=6. Plot the bucket content and identify any non-conforming cells. [6] CO2 L3



b] Write a note on RIP. **[4] CO4 L2**

RIP (ROUTING INFORMATION PROTOCOL)

- This is a dynamic routing protocol used in LAN and WAN.

- It is classified as an interior gateway protocol (IGP) using the distance-vector routing algorithm.
- A RIP run on top of UDP, port number 520 is used.

- RIP is a distance-vector routing protocol, which employs the hop count as a routing metric.
- Suitable for small networks (local area environments).

- The maximum number of hops allowed with RIP is 15, and the hold down time is 180 seconds.

- Value of 16 is reserved to represent infinity, i.e. node is not reachable.
- Small number limits the count-to-infinity problem.
- Originally each RIP router transmits full updates every 30 seconds by default.

- A router expects to receive an update message from each of its neighbors within 180 seconds in the worst case.

- If router does not receive update message from neighbor X within this limit, it assumes the link to X has failed and sets the corresponding minimum cost to 16 (infinity).

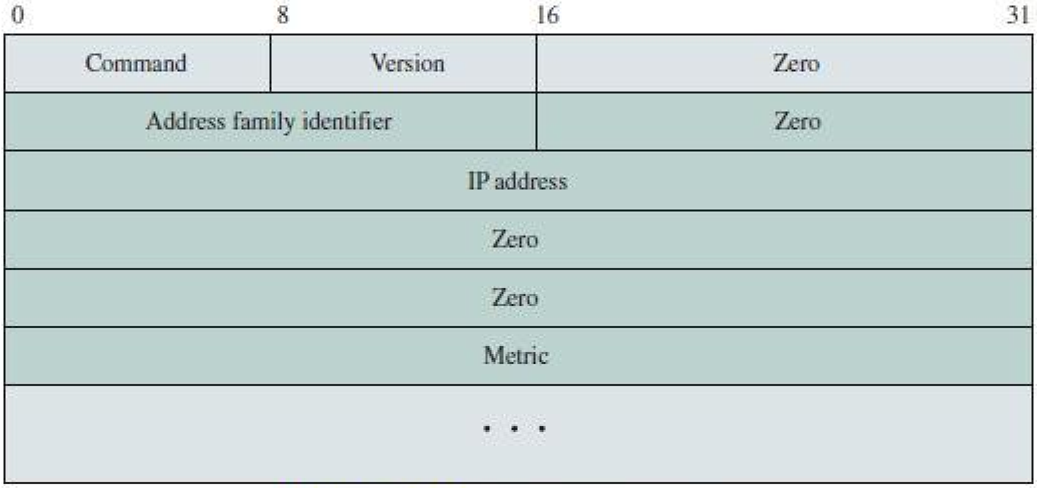


FIGURE 8.32 RIP message format

RIP Message Fields

1) Command: specifies the purpose of the message, two values are defined value 1 requests the system to send its routing information and values 2 indicates a response containing the routing information.

2) Version: two versions, RIPV1 and RIPV2

3) Address Family Identifier: identifies type of address used currently only IP address is defined

4) IP address: indicates the address of destination, which can be network or host address.

8. Explain the intra cluster and inter cluster routing protocols. [10] CO6 L2

INTRA CLUSTER ROUTING

- If the routing is happening within a cluster, then the protocol is called as intra cluster routing.
- In intra cluster routing, the packets are transmitter with in a cluster.

- It can be of 2 types.

1) Direct Routing

- The cluster head as the destination for all cluster nodes is located in the center of the cluster, so all nodes can communicate with the cluster head directly.

2) Multihop Routing

- A node can face multiple hops in order to reach the destination.

INTER CLUSTER ROUTING

- If the routing is happening between the nodes of different clusters it is called as inter cluster routing.

- These protocols are not typically different from the multihop ones for intradomain cases.

- Interdomain protocols are available for

1) Intercluster energy conscious routing (ICR)
2) Energy-aware routing (EAR)

3) Direct diffusion

- It is a destination initiated reactive routing algorithm.

- The destination is called as local base station [LBS] it will start the route discovery by creating interest signal and following them.
- ICR works in two phases, Route discovery and data acquisition.

1. Route Discovery Phase: In this phase, the LBS initiates route discovery by sending an interest signal within the range R_i,

1. All the nodes which are in the range R_i will receive the interest signal.
2. Upon receiving the interest signal, it will be stored and flooding continues.

3. If an intermediate node receive already processed interest signal, it will be discarded
4. Before flooding the interest signal, the cost value will be updated.

2. Data-acquisition phase: occurs after each cluster head collects the requested information from sensor nodes and compresses it into a packet with fixed length, searches for the neighbor’s address in memory, and relays the packet to that neighbor.

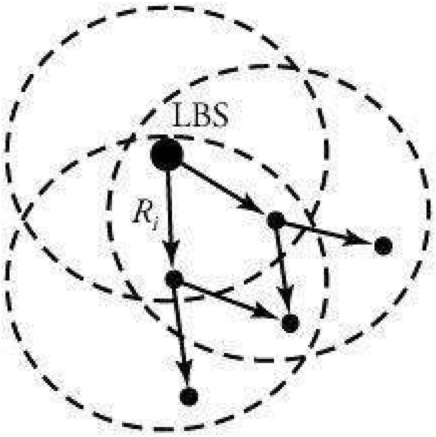


Figure 20.11. LBS starts route discovery by generating interest signals.