IAT-II Question paper with solution of 15CS52 Computer networks Nov-2017-Shyamasree Ghosh

Solutions-IAT-2

1. Explain the working of 'Selective Repeat' (SR) protocol by using state transition diagram. Justify the limitation on sliding window size in SR protocol with an example. (5+5)

Answer:

SR Protocol 5

- Problem with GBN:
  - ➢ GBN suffers from performance problems.
  - ➢ When the window-size and bandwidth-delay product are both large, many packets can be in the pipeline.
  - ➢ Thus, a single packet error results in retransmission of a large number of packets.
- Solution: Use Selective Repeat (SR).

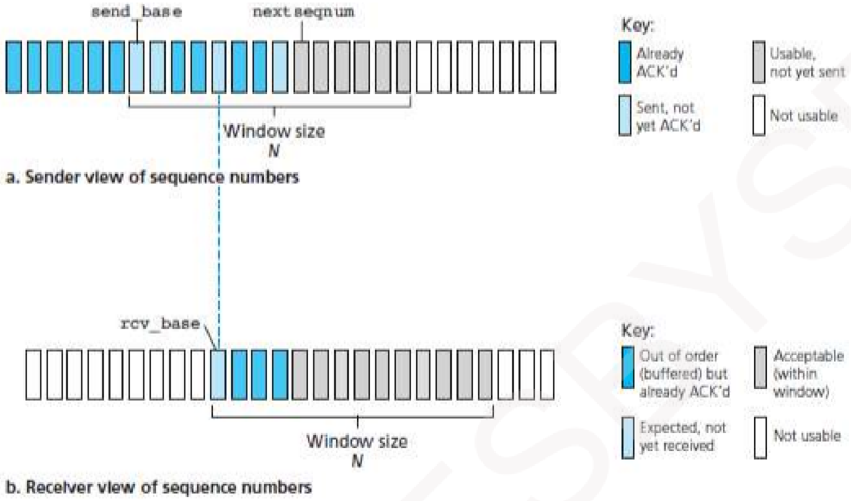

send_base
nextseqnum
Window size
N
a. Sender view of sequence numbers
Key:
Already ACK'd
Usable, not yet sent
Sent, not yet ACK'd
Not usable
rcv_base
Window size
N
b. Receiver view of sequence numbers
Key:
Out of order (buffered) but already ACK'd
Acceptable (within window)
Expected, not yet received
Not usable

Figure 2.21: Selective-repeat (SR) sender and receiver views of sequence-number space

- The sender retransmits only those packets that it suspects were erroneous.
- Thus, avoids unnecessary retransmissions. Hence, the name "selective-repeat".
- The receiver individually acknowledge correctly received packets.
- A window-size N is used to limit the no. of outstanding, unacknowledged packets in the pipeline.
- Figure 2.21 shows the SR sender's view of the sequence-number space.

SR Sender

- The various actions taken by the SR sender are as follows:

  1) Data Received from above.

  ➢ When data is received from above, the sender checks the next available sequence-number for the packet.

  ➢ If the sequence-number is within the sender's window;

  Then, the data is packetized and sent;

  Otherwise, the data is buffered for later transmission.

  2) Timeout.

  ➢ Timers are used to protect against lost packets.

  ➢ Each packet must have its own logical timer. This is because

  → only a single packet will be transmitted on timeout.

  3) ACK Received.

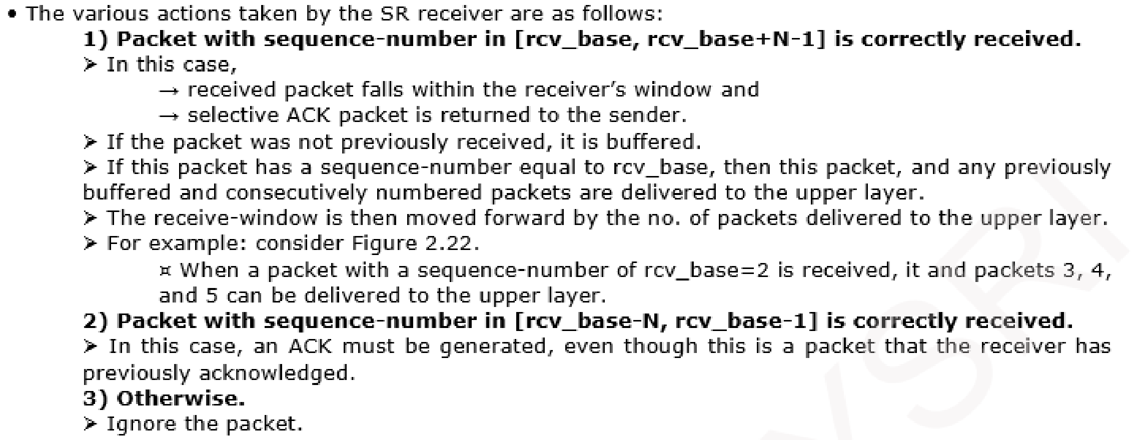
  ➢ If an ACK is received, the sender marks that packet as having been received.

  ➢ If the packet's sequence-number is equal to send_base, the window base is increased by the smallest sequence-number.

  ➢ If there are untransmitted packets with sequence-numbers that fall within the window, these packets are transmitted.

VTU NOTES BY SRI

SR Receiver



- The various actions taken by the SR receiver are as follows:

  1) Packet with sequence-number in [rcv_base, rcv_base+N-1] is correctly received.

  ➢ In this case,

  → received packet falls within the receiver's window and

  → selective ACK packet is returned to the sender.

  ➢ If the packet was not previously received, it is buffered.

  ➢ If this packet has a sequence-number equal to rcv_base, then this packet, and any previously buffered and consecutively numbered packets are delivered to the upper layer.

  ➢ The receive-window is then moved forward by the no. of packets delivered to the upper layer.

  ➢ For example: consider Figure 2.22.

  ¤ When a packet with a sequence-number of rcv_base=2 is received, it and packets 3, 4, and 5 can be delivered to the upper layer.

  2) Packet with sequence-number in [rcv_base-N, rcv_base-1] is correctly received.

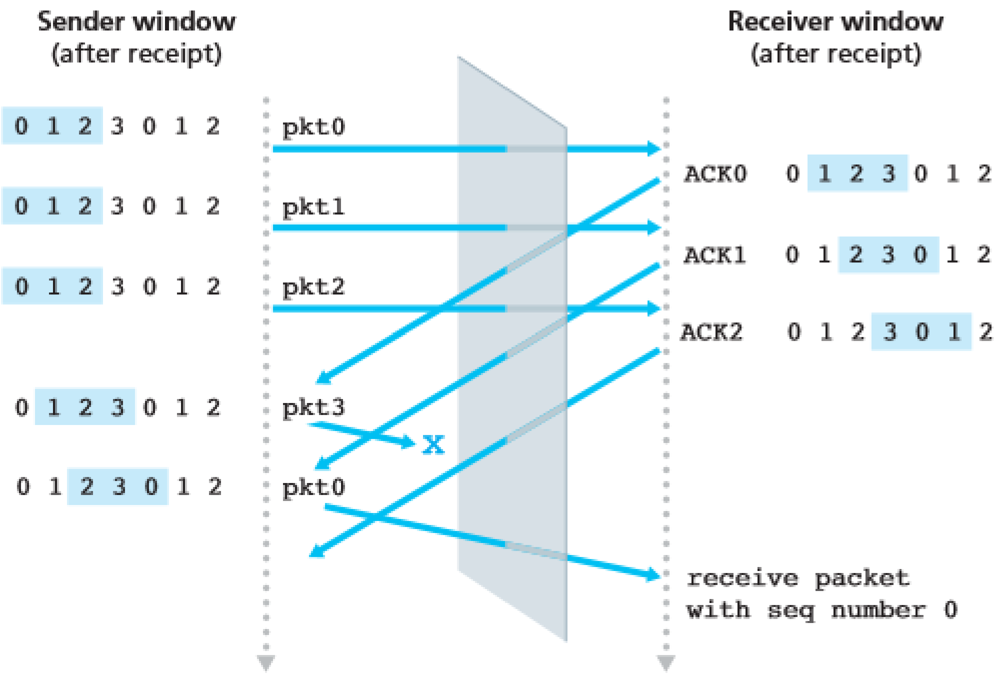
  ➢ In this case, an ACK must be generated, even though this is a packet that the receiver has previously acknowledged.

  3) Otherwise.

  ➢ Ignore the packet.

VSRI

Window size is less than 2^{m-1} **5**



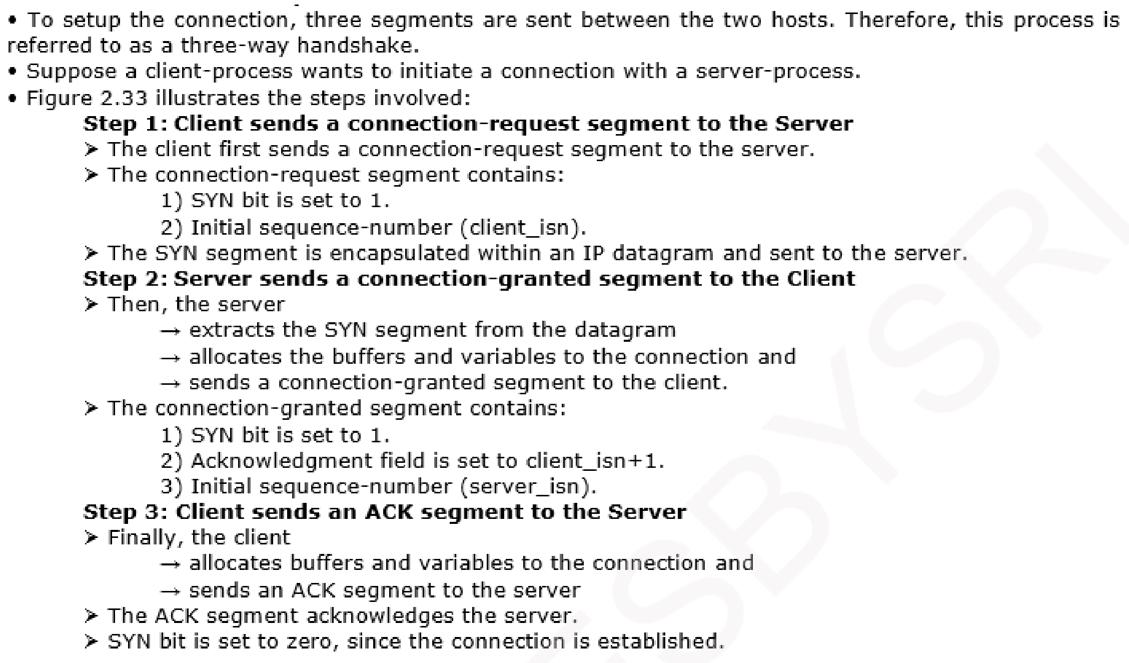
h

- In the fig above the ACKs for the first three packets are all delivered correctly. The sender thus moves its window forward and sends the fourth, fifth, and sixth packets, with sequence numbers 3, 0, and 1, respectively.
- The packet with sequence number 3 is lost, but the packet with sequence number 0 arrives—a packet containing new data.
- Now consider the receiver's viewpoint which has a figurative curtain between the sender and the receiver, since the receiver cannot "see" the actions taken by the sender.
- All the receiver observes is the sequence of messages it receives from the channel and sends into the channel.

- There is no way of distinguishing the retransmission of the first packet from an original transmission of the fifth packet.
- Clearly, a window size that is 1 less than the size of the sequence number space won't work.
- So the window size must be less than or equal to half the size of the sequence number space for SR protocols. If m is the number of bits to represent sequence number then address space is 2^m
- So the window size is $2^m/2$ i.e $\mathbf{2^{m-1}}$

2. **With state transition diagram, explain the sequence of TCP states visited by the TCP client and TCP server during client server communication session (5+5)**

Connection Setup and Data Transfer 5



- To setup the connection, three segments are sent between the two hosts. Therefore, this process is referred to as a three-way handshake.
- Suppose a client-process wants to initiate a connection with a server-process.
- Figure 2.33 illustrates the steps involved:

Step 1: Client sends a connection-request segment to the Server

➢ The client first sends a connection-request segment to the server.

➢ The connection-request segment contains:

1) SYN bit is set to 1.
2) Initial sequence-number (client_isn).

➢ The SYN segment is encapsulated within an IP datagram and sent to the server.

Step 2: Server sends a connection-granted segment to the Client

➢ Then, the server

→ extracts the SYN segment from the datagram

→ allocates the buffers and variables to the connection and

→ sends a connection-granted segment to the client.

➢ The connection-granted segment contains:

1) SYN bit is set to 1.
2) Acknowledgment field is set to client_isn+1.
3) Initial sequence-number (server_isn).

Step 3: Client sends an ACK segment to the Server

➢ Finally, the client

→ allocates buffers and variables to the connection and

→ sends an ACK segment to the server

➢ The ACK segment acknowledges the server.

➢ SYN bit is set to zero, since the connection is established.

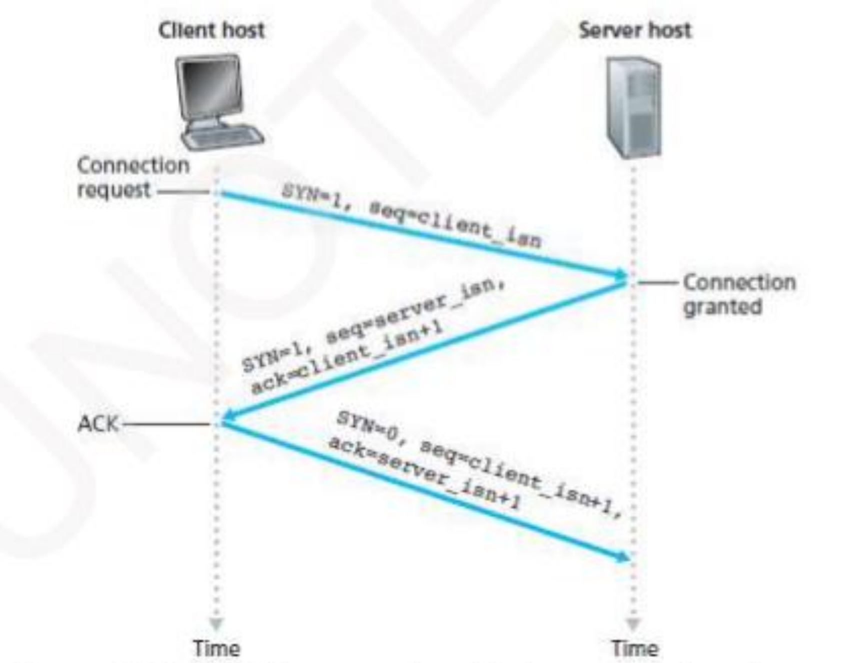


Figure 2.33: TCP three-way handshake: segment exchange

Connection Release 5

- Either of the two processes in a connection can end the connection.
- When a connection ends, the "resources" in the hosts are de-allocated.
- Suppose the client decides to close the connection.
- Figure 2.34 illustrates the steps involved:
    1) The client-process issues a close command.
        - ¤ Then, the client sends a shutdown-segment to the server.
        - ¤ This segment has a FIN bit set to 1.
    2) The server responds with an acknowledgment to the client.
    3) The server then sends its own shutdown-segment.
        - ¤ This segment has a FIN bit set to 1.
    4) Finally, the client acknowledges the server's shutdown-segment.

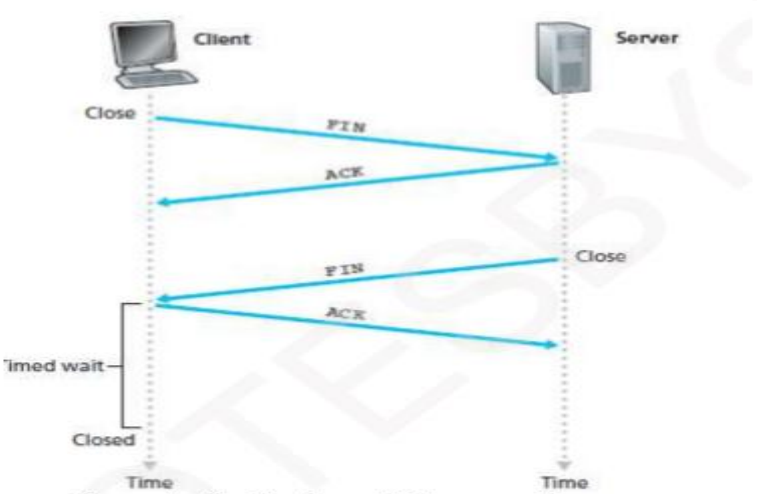
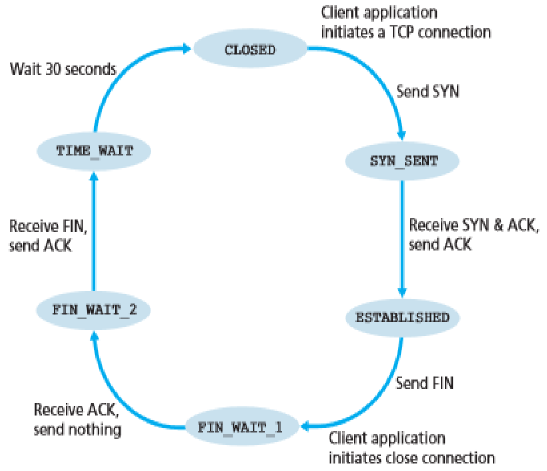
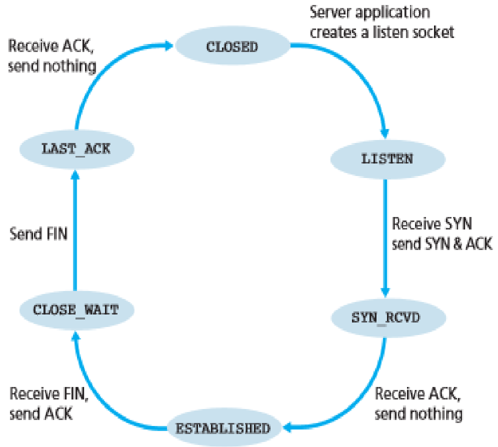


Figure 2.34: Closing a TCP connection

The state visited by server   The states visited by Client


Client application initiates a TCP connection
CLOSED
Wait 30 seconds
Send SYN
TIME_WAIT
SYN_SENT
Receive FIN, send ACK
Receive SYN & ACK, send ACK
FIN_WAIT_2
ESTABLISHED
Send FIN
Receive ACK, send nothing
FIN_WAIT_1
Client application initiates close connection


Server application creates a listen socket
Receive ACK, send nothing
CLOSED
LAST_ACK
LISTEN
Send FIN
Receive SYN send SYN & ACK
CLOSE_WAIT
SYN_RCVD
Receive FIN, send ACK
ESTABLISHED
Receive ACK, send nothing

3. With a neat diagram, explain the architecture of a router. Explain about 'Routing Management control plane' and 'Forwarding data plane'? (6+2+2)

architecture

- The router is used for transferring packets from an incoming-links to the appropriate outgoing-links.

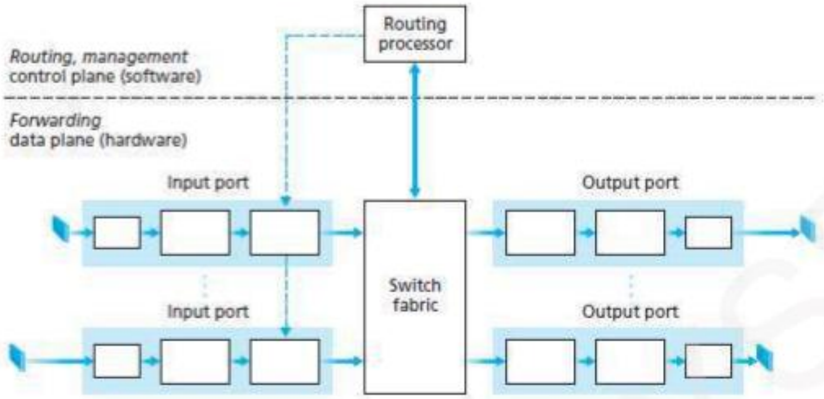
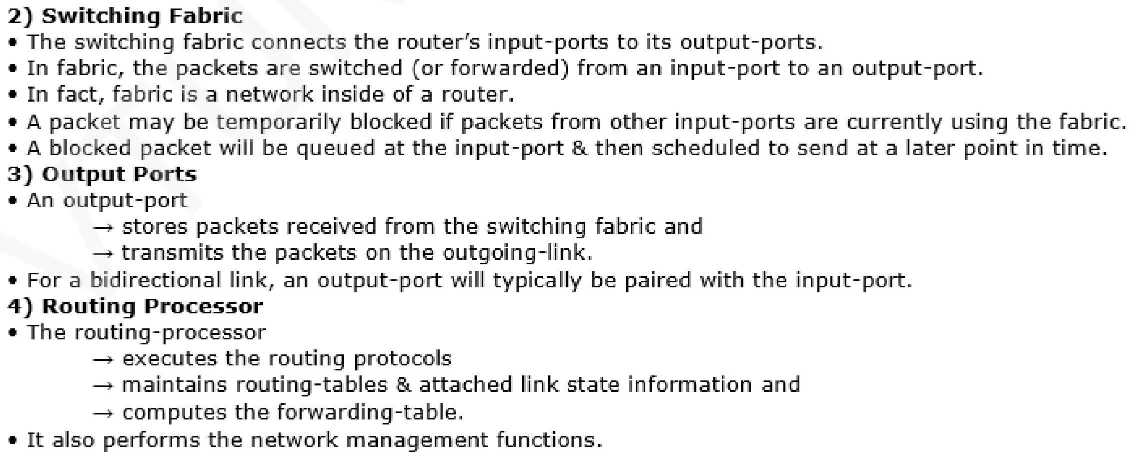

Routing processor
Routing, management control plane (software)
Forwarding data plane (hardware)
Input port
Output port
Switch fabric
Input port
Output port

Figure 3.5: Router architecture

- Four components of router (Figure 3.5):

1) Input Ports

- An input-port is used for terminating an incoming physical link at a router (Figure 3.6).
- It is used for interoperating with the link layer at the other side of the incoming-link.
- It is used for lookup function i.e. searching through forwarding-table looking for longest prefix match.
- It contains forwarding-table.
- Forwarding-table is consulted to determine output-port to which arriving packet will be forwarded.
- Control packets are forwarded from an input-port to the routing-processor.
- Many other actions must be taken:
  - i) Packet's version number, checksum and time-to-live field must be checked.
  - ii) Counters used for network management must be updated.



2) Switching Fabric

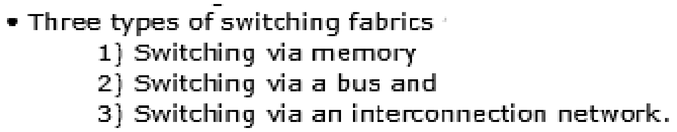
- The switching fabric connects the router's input-ports to its output-ports.
- In fabric, the packets are switched (or forwarded) from an input-port to an output-port.
- In fact, fabric is a network inside of a router.
- A packet may be temporarily blocked if packets from other input-ports are currently using the fabric.
- A blocked packet will be queued at the input-port & then scheduled to send at a later point in time.

3) Output Ports

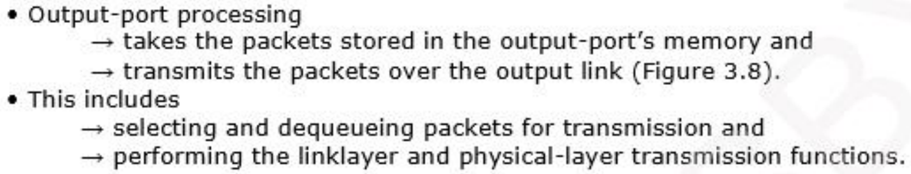
- An output-port
  → stores packets received from the switching fabric and
  → transmits the packets on the outgoing-link.
- For a bidirectional link, an output-port will typically be paired with the input-port.

4) Routing Processor

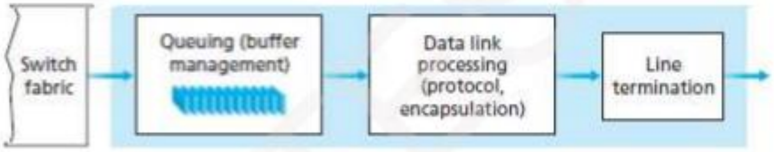
- The routing-processor
  → executes the routing protocols
  → maintains routing-tables & attached link state information and
  → computes the forwarding-table.
- It also performs the network management functions.



- Three types of switching fabrics
  1) Switching via memory
  2) Switching via a bus and
  3) Switching via an interconnection network.



- Output-port processing
  → takes the packets stored in the output-port's memory and
  → transmits the packets over the output link (Figure 3.8).
- This includes
  → selecting and dequeueing packets for transmission and
  → performing the linklayer and physical-layer transmission functions.



Switch fabric
Queuing (buffer management)
Data link processing (protocol, encapsulation)
Line termination

Figure 3.8: Output port processing

Forwarding data plane 2

- A router's input ports, output ports, and switching fabric together implement the forwarding function and are almost always implemented in hardware, These forwarding functions are sometimes collectively referred to as the router forwarding plane.
- Forwarding plane hardware can be implemented either using a router vendor's own hardware designs, or constructed using purchased merchant-silicon chips (e.g., as sold by companies such as Intel and Broadcom).
- Forwarding plane operates at the nanosecond time scale

Routing Management control plane 2

- A router's control functions—executing the routing protocols, responding to attached links that go up or down, and performing management functions are called router control plane
- These router control plane functions are usually implemented in software and execute on the routing processor (typically a traditional CPU).

IAT-II Question paper with solution of 15CS52 Computer networks Nov-2017-Shyamasree Ghosh

4. What is a routing loop? How does it lead to 'counting to infinity' problem in a network? Illustrate how 'poisoned reverse' technique is used to avoid the formation of routing loops in distance vector routing algorithm? **(2+4+4)**

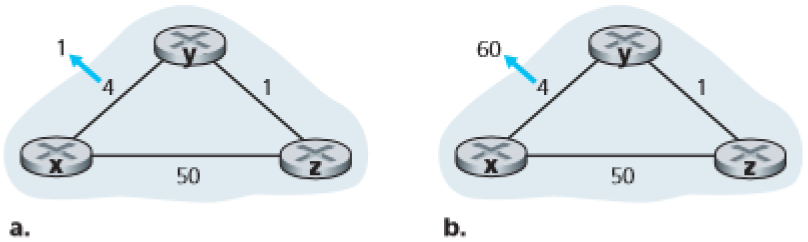
Routing loop **2**

A routing loop is a common problem with various types of networks, particularly computer networks. They are formed when an error occurs in the operation of the routing algorithm, and as a result, in a group of nodes, the path to a particular destination forms a loop.

counting to infinity **4**

The Bellman–Ford algorithm does not prevent routing loops from happening and suffers from the count-to-infinity problem.

Let's now consider what can happen when a link cost increases. Suppose that the link cost between x and y increases from 4 to 60, as shown in Figure



- Before the link cost changes, Dy(x) = 4, Dy(z) = 1, Dz(y) = 1, and Dz(x) = 5. At time t0, y detects the link-cost change (the cost has changed from 4 to 60). y computes its new minimum-cost path to x to have a cost of Dy(x) = min{c(y,x) + Dx(x), c(y,z) + Dz(x)} = min{60 + 0, 1 + 5} = 6 ,the only information node y has is that its direct cost to x is 60 and that z has last told y that z could get to x with a cost of 5. So in order to get to x, y would now route through z, fully expecting that z will be able to get to x with a cost of 5. As of t1 we have a routing loop—in order to get to x, y routes through z, and z routes through y. Arouting loop is like a black hole—a packet destined for x arriving at y or z as of t1 will bounce back and forth between these two nodes forever (or until the forwarding tables are changed).
- Since node y has computed a new minimum cost to x, it informs z of its new distance vector at time t1.
- Sometime after t1, z receives y's new distance vector, which indicates that y's minimum cost to x is 6. z knows it can get to y with a cost of 1 and hence computes a new least cost to x of Dz(x) = min{50 + 0,1 + 6} = 7. Since z's least cost to x has increased, it then informs y of its new distance vector at t2.
- In a similar manner, after receiving z's new distance vector, y determines Dy(x) = 8 and sends z its distance vector. z then determines Dz(x) = 9 and sends y its distance vector, and so on.

Poisoned Reverse **4**

- The specific looping scenario just described can be avoided using a technique known as poisoned reverse.
- The idea is simple—if z routes through y to get to destination x, then z will advertise to y that its distance to x is infinity, that is, z will advertise to y that Dz(x) = ∞ (even though z knows Dz(x) = 5 in truth). z will continue telling this little white lie to y as long as it routes to x via y. Since y believes that z has no path to x, y will never attempt to route to x via z, as long as z continues to route to x via y (and lies about doing so).

Let's now see how poisoned reverse solves the particular looping problem we encountered before in Figure 4.31(b). As a result of the poisoned reverse, y's distance table indicates Dz(x) = ∞. When the cost of the (x, y) link changes from 4 to 60 at time t0, y updates its table and continues to route directly to x, albeit at a higher cost of 60, and informs z of its new cost to x, that is, Dy(x) = 60. After receiving the update at t1, z immediately shifts its route to x to be via the direct (z, x) link at a cost of 50. Since this is a new least-cost path to x, and since the path no longer passes through y, z now informs y that Dz(x) = 50 at t2. After receiving the update from z, y updates its distance table with Dy(x) = 51. Also, since z is now on y's least-cost path to x, y poisons the reverse path from z to x by informing z at time t3 that Dy(x) = ∞ (even though y knows that Dy(x) = 51 in truth).

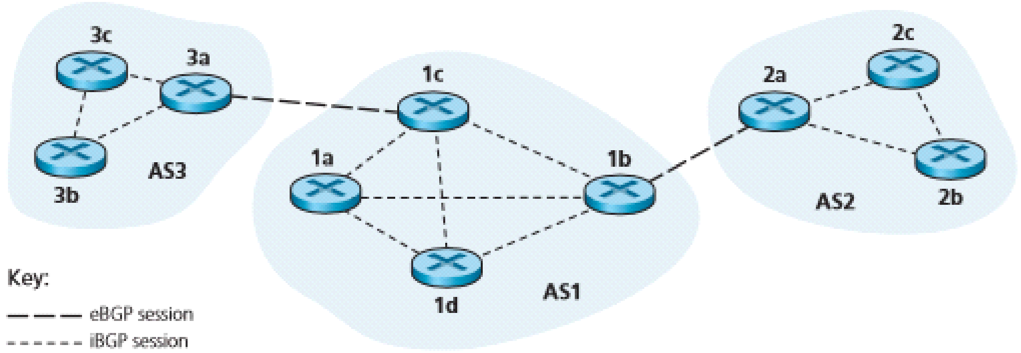
5. **Explain what is iBGP and eBGP? Demonstrate how does BGP work with path attributes and route selection policies. (2+4+4)**

Answer:

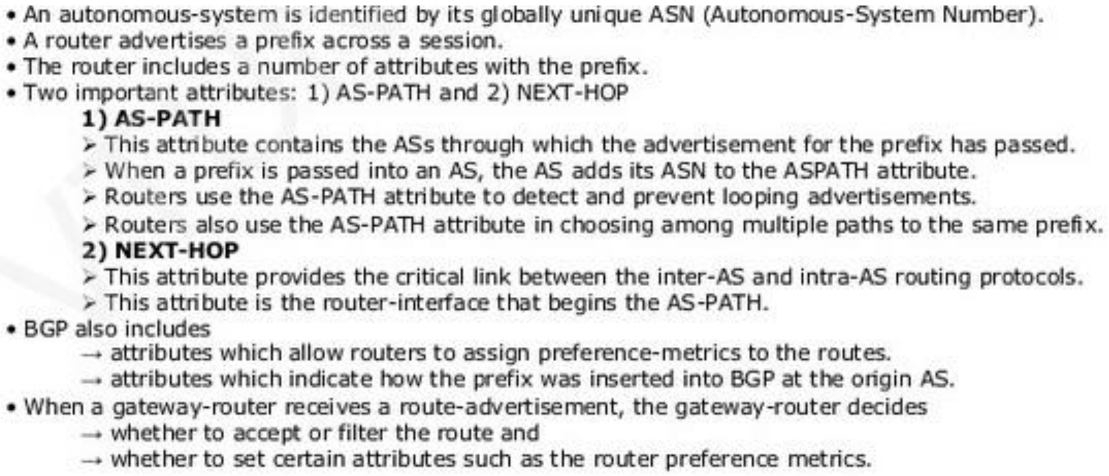
iBGP & eBGP **2**

- In BGP, pairs of routers exchange routing information over semipermanent TCP connections using port 179.
- For each TCP connection, the two routers at the end of the connection are called BGPpeers, and the
- TCP connection along with all the BGP messages sent over the connection is called a BGPsession.
- Furthermore, a BGPsession that spans two ASs is called an external BGP (eBGP) session, and a BGP session between routers in the same AS is called an internal BGP (iBGP) session.
- The eBGP sessions are shown with the long dashes; the iBGPsessions are shown with the short dashes

IAT-II Question paper with solution of 15CS52 Computer networks Nov-2017- Shyamasree Ghosh



Path Attribures: 4



- An autonomous-system is identified by its globally unique ASN (Autonomous-System Number).
- A router advertises a prefix across a session.
- The router includes a number of attributes with the prefix.
- Two important attributes: 1) AS-PATH and 2) NEXT-HOP

  1) AS-PATH

  ➢ This attribute contains the ASs through which the advertisement for the prefix has passed.
  ➢ When a prefix is passed into an AS, the AS adds its ASN to the ASPATH attribute.
  ➢ Routers use the AS-PATH attribute to detect and prevent looping advertisements.
  ➢ Routers also use the AS-PATH attribute in choosing among multiple paths to the same prefix.

  2) NEXT-HOP

  ➢ This attribute provides the critical link between the inter-AS and intra-AS routing protocols.
  ➢ This attribute is the router-interface that begins the AS-PATH.
- BGP also includes
  → attributes which allow routers to assign preference-metrics to the routes.
  → attributes which indicate how the prefix was inserted into BGP at the origin AS.
- When a gateway-router receives a route-advertisement, the gateway-router decides
  → whether to accept or filter the route and
  → whether to set certain attributes such as the router preference metrics.

Route selection: 4

A router may learn about more than one route to any one prefix, in which case the router must select one of the possible routes. The input into this route selection process is the set of all routes that have been learned and accepted by the router. If there are two or more routes to the same prefix, then BGPsequentially invokes the following elimination rules until one route remains:

- Routes are assigned a local preference value as one of their attributes. The local preference of a route could have been set by the router or could have been learned by another router in the same AS. This is a policy decision that is left up to the AS's network administrator. (We will shortly discuss BGP policy issues in some detail.) The routes with the highest local preference values are selected.

- From the remaining routes (all with the same local preference value), the route with the shortest AS-PATH is selected. If this rule were the only rule for route selection, then BGP would be using a DV algorithm for path determination, where the distance metric uses the number of AS hops rather than the number of router hops.

- From the remaining routes (all with the same local preference value and the same AS-PATH length), the route with the closest NEXT-HOProuter is selected. Here, closest means the router for which the cost of the least-cost path, determined by the intra-AS algorithm, is the smallest. As discussed in Section 4.5.3, this process is called hot-potato routing

6. Discuss about the different techniques used to control the flooding in broadcasting? (10)

Answer:

The key to avoiding a broadcast storm is for a node to judiciously choose when to flood a packet and (e.g., if it has already received and flooded an earlier copy of a packet) when not to flood a packet.

In practice, this can be done by the following two ways.

<u>Sequence number</u>: 4

- In sequence-number-controlled flooding, a source node puts its address (or other unique identifier) as well as a broadcast sequence number into a broadcast packet, then sends the packet to all of its neighbors.

- Each node maintains a list of the source address and sequence number of each broadcast packet it has already received, duplicated, and forwarded.

- When a node receives a broadcast packet, it first checks whether the packet is in this list. If so, the packet is dropped; if not, the packet is duplicated and forwarded to all the node's neighbors (except the node from which the packet has just been received).

- The Gnutella protocol, uses sequence-number-controlled flooding to broadcast queries in its overlay network

<u>Reverse Path Forwarding (RPF):</u> 6

- A second approach to controlled flooding is known as reverse path forwarding (RPF) , also sometimes referred to as reverse path broadcast (RPB).

- The idea behind RPF is simple, yet elegant. When a router receives a broadcast packet with a given source address, it transmits the packet on all of its outgoing links (except the one on which it was received) only if the packet arrived on the link that is on its own shortest unicast path back to the source.

- Otherwise, the router simply discards the incoming packet without forwarding it on any of its outgoing links.

- Such a packet can be dropped because the router knows it either will receive or has already received a copy of this packet on the link that is on its own shortest path back to the sender.

- Note that RPF does not use unicast routing to actually deliver a packet to a destination, nor does it require that a router know the complete shortest path from itself to the source.

- RPF need only know the next neighbor on its unicast shortest path to the sender; it uses this neighbor's identity only to determine whether or not to flood a received broadcast packet.

- Following figure illustrates RPF. Suppose that the links drawn with thick lines represent the least-cost paths from the receivers to the source (A). Node A initially broadcasts a source-A packet to nodes C and B. Node B will forward the source-A packet it has received from A (since A is on its least-cost path to A) to both C and D. B will ignore (drop, without forwarding) any source-A packets it receives from any other nodes (for example, from routers C or D). Let us now consider node C, which will receive a source-A packet directly from A as well as from B. Since B is not on C's own shortest path back to A, C will ignore any source-A packets it receives from B. On the other hand, when C receives a source-A packet directly from A, it will forward the packet to nodes B, E, and F.

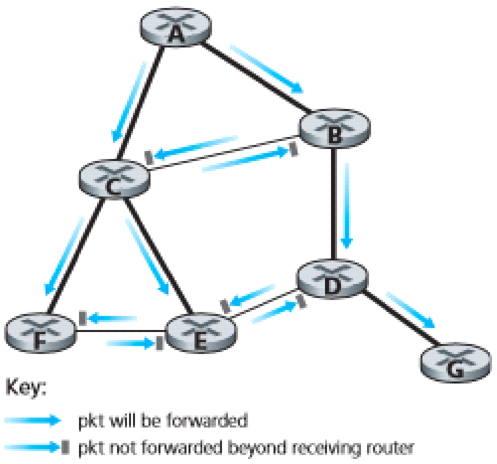
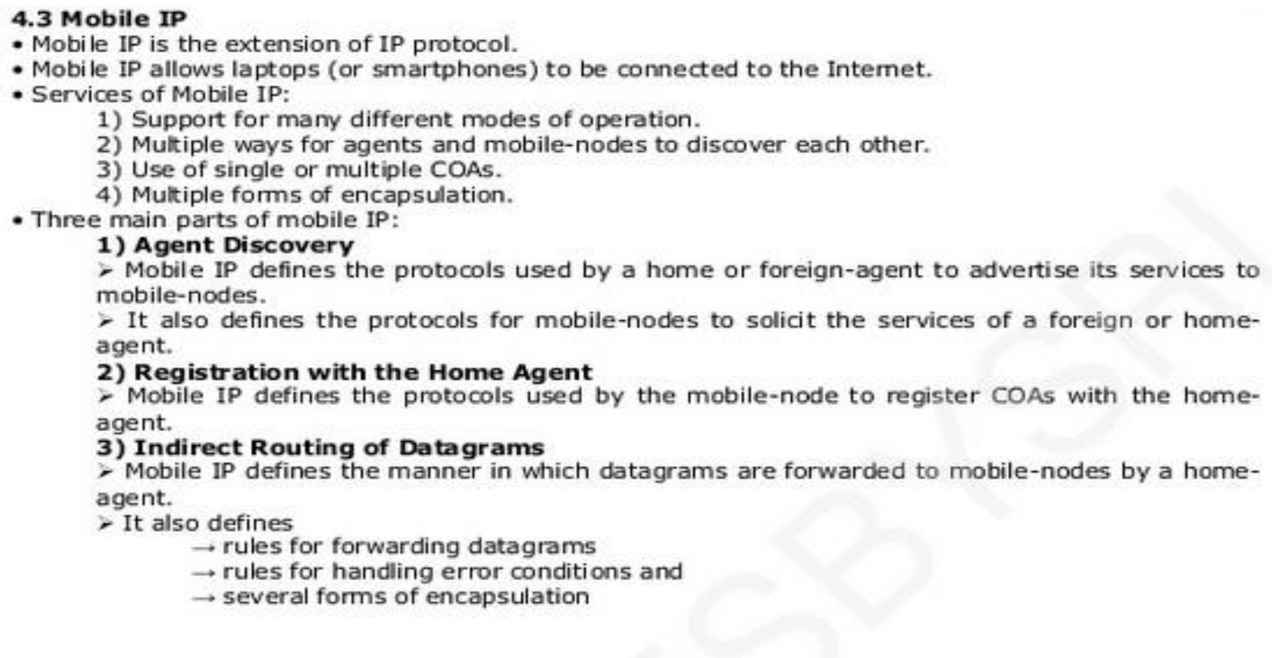


Fig: Reverse Path Forwarding

IAT-II Question paper with solution of 15CS52 Computer networks Nov-2017-Shyamasree Ghosh

7. Explain the concept of Mobile IP 10

Introduction 1



4.3 Mobile IP

- Mobile IP is the extension of IP protocol.
- Mobile IP allows laptops (or smartphones) to be connected to the Internet.
- Services of Mobile IP:
  1) Support for many different modes of operation.
  2) Multiple ways for agents and mobile-nodes to discover each other.
  3) Use of single or multiple COAs.
  4) Multiple forms of encapsulation.
- Three main parts of mobile IP:

  1) Agent Discovery

  ➢ Mobile IP defines the protocols used by a home or foreign-agent to advertise its services to mobile-nodes.

  ➢ It also defines the protocols for mobile-nodes to solicit the services of a foreign or home-agent.

  2) Registration with the Home Agent

  ➢ Mobile IP defines the protocols used by the mobile-node to register COAs with the home-agent.

  3) Indirect Routing of Datagrams

  ➢ Mobile IP defines the manner in which datagrams are forwarded to mobile-nodes by a home-agent.

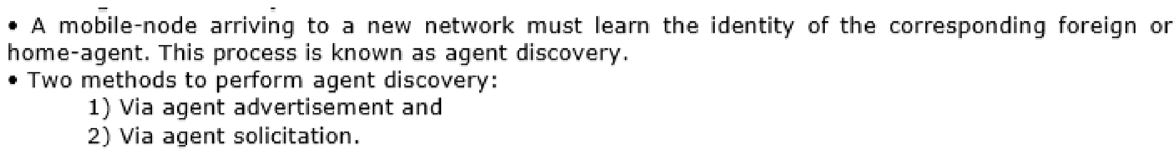
  ➢ It also defines

  → rules for forwarding datagrams

  → rules for handling error conditions and

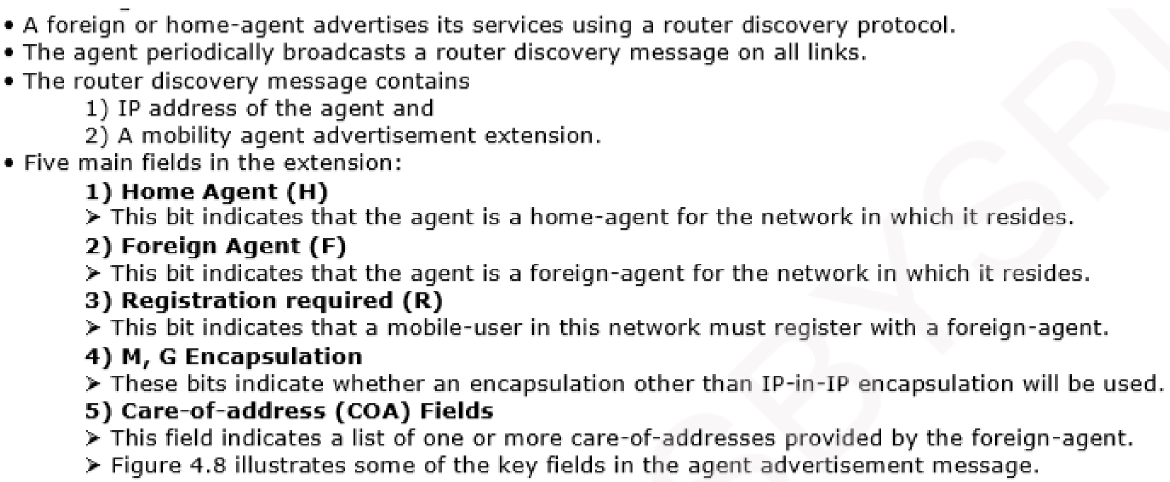
  → several forms of encapsulation

Agent Discovery: 3



- A mobile-node arriving to a new network must learn the identity of the corresponding foreign or home-agent. This process is known as agent discovery.
- Two methods to perform agent discovery:
  1) Via agent advertisement and
  2) Via agent solicitation.

- **Agent Advertisement:**



- A foreign or home-agent advertises its services using a router discovery protocol.
- The agent periodically broadcasts a router discovery message on all links.
- The router discovery message contains
  1) IP address of the agent and
  2) A mobility agent advertisement extension.
- Five main fields in the extension:

  1) Home Agent (H)

  ➢ This bit indicates that the agent is a home-agent for the network in which it resides.

  2) Foreign Agent (F)

  ➢ This bit indicates that the agent is a foreign-agent for the network in which it resides.

  3) Registration required (R)

  ➢ This bit indicates that a mobile-user in this network must register with a foreign-agent.

  4) M, G Encapsulation

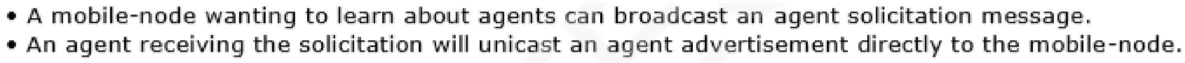
  ➢ These bits indicate whether an encapsulation other than IP-in-IP encapsulation will be used.

  5) Care-of-address (COA) Fields

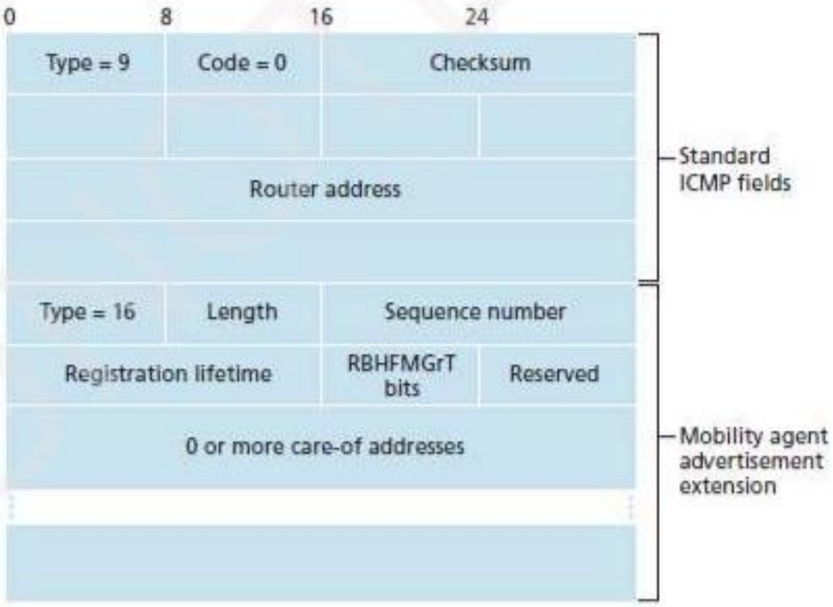
  ➢ This field indicates a list of one or more care-of-addresses provided by the foreign-agent.

  ➢ Figure 4.8 illustrates some of the key fields in the agent advertisement message.

- **Agent Solicitation**



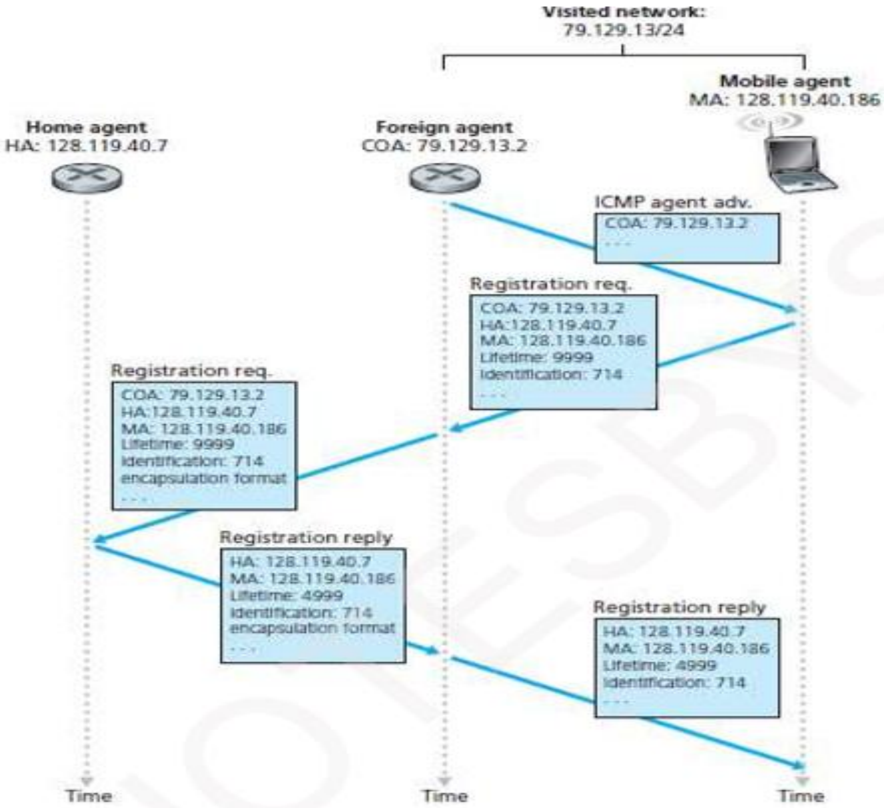
- A mobile-node wanting to learn about agents can broadcast an agent solicitation message.
- An agent receiving the solicitation will unicast an agent advertisement directly to the mobile-node.



: ICMP router discovery message with mobility agent advertisement extension

Registration with Home Agent **3**

- Address must be registered with the home-agent. This can be done in 2 ways:
  1) Via the foreign-agent who then registers the COA with the home-agent.
  2) By the mobile IP node itself.



- Four steps are involved. Figure 4.9 illustrates the 4 steps.

1) When a mobile receives a foreign-agent advertisement, the mobile sends a registration-request to the foreign-agent.

➢ The registration-request contains

i) COA advertised by the foreign-agent
ii) address of the home-agent (HA)
iii) permanent-address of the mobile (MA)
iv) registration identification and
v) requested lifetime of the registration.

➢ The requested registration lifetime indicates number of seconds the registration is valid.

➢ If registration is not renewed within the specified lifetime, the registration will become invalid.

2) When the foreign-agent receives the registration-request, the foreign-agent records the mobile's permanent IP address.

➢ The foreign-agent then sends a registration-request to the home-agent.

3) When home-agent receives the registration-request, the home-agent checks for correctness.

➢ The home-agent binds the mobile's permanent IP address with the COA.

➢ The home-agent sends a registration-reply.

4) The foreign-agent receives and forwards the registration-reply to the mobile-node.

Indirect Routing **3**

4.2.2.1 Indirect Routing to a Mobile Node

- Four steps are involved. Figure 4.5 illustrates the 4 steps.

Step 1

➢ The correspondent

→ addresses the datagram to the mobile-node's permanent-address and
→ routes the datagram to the mobile-node's home-network.

Step 2

➢ Home-agent encapsulates the correspondent's original datagram within a larger datagram.

➢ This larger datagram is addressed & delivered to the mobile-node's COA.

Step 3

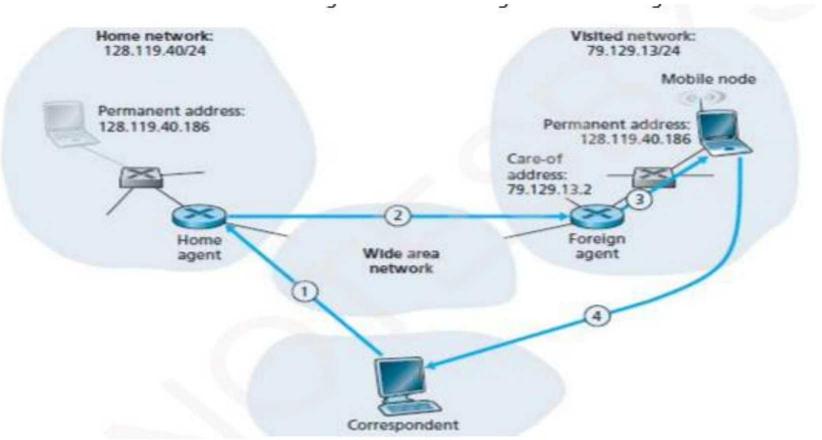
➢ The foreign-agent receives and decapsulates the datagram.

➢ The foreign-agent forwards the original datagram to the mobile-node.

Step 4

➢ The mobile-node directly routes the datagram to the correspondent.

➢ There is no need to route the datagram back through the home-agent.



IAT-II Question paper with solution of 15CS52 Computer networks Nov-2017-Shyamasree Ghosh

8. What are cellular networks? explain the working of 2G and 3G cellular networks with their architecture

Wireless Network: **2**

A cellular network or mobile network is a communication network where the last link is wireless. The network is distributed over land areas called cells, each served by at least one fixed-location transceiver, but more normally three cell sites or base transceiver stations. These base stations provide the cell with the network coverage which can be used for transmission of voice, data and others. A cell typically uses a different set of frequencies from neighboring cells, to avoid interference and provide guaranteed service quality within each cell.

Architecture of 2G Wireless Network **4**

- The region covered by cellular-network is divided into no. of geographic coverage-areas called cells.
- Each cell contains a BTS (Base Transceiver Station) (Figure 4.1).
- BTS is responsible for delivering the signals to/from the mobile-stations in the cell.
- The coverage-area of a cell depends on following factors:
  1) The transmitting power of the BTS.
  2) The transmitting power of the user devices.
  3) Obstructing buildings in the cell.
  4) The height of base-station antennas.
- The 2G systems use combined FDM/TDM for the air-interface.
- In combined FDM/TDM systems,
  1) The channel is divided into a number of frequency sub-bands.
  2) Within each sub-band, time is partitioned into frames and slots.

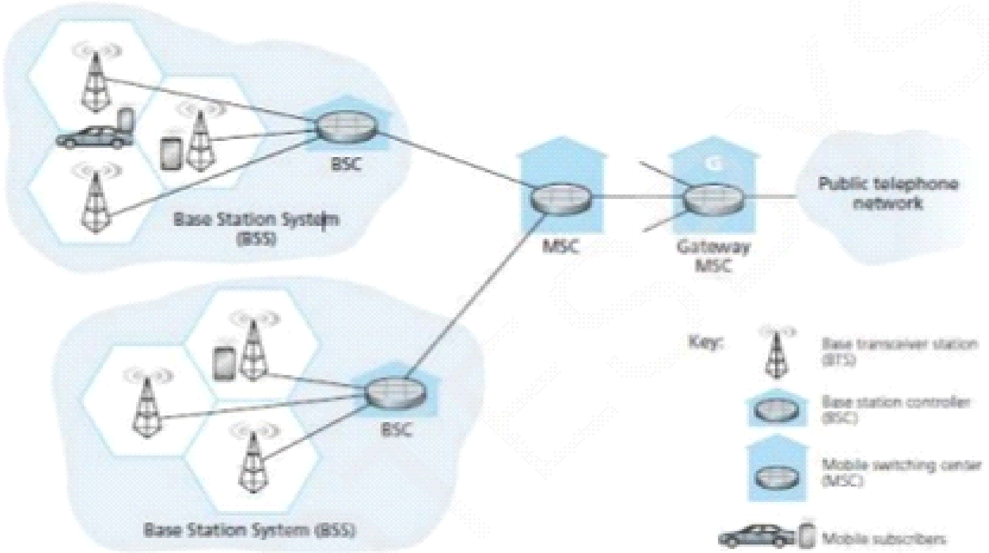
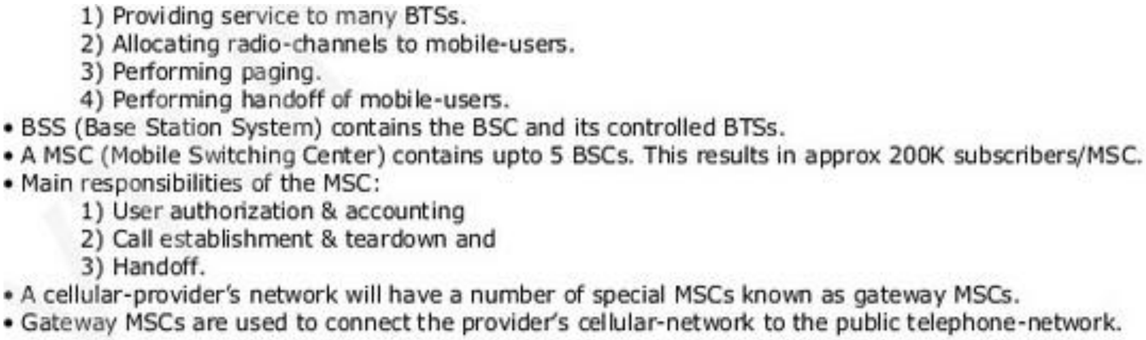


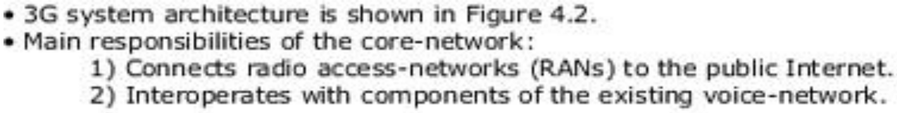
Figure 4.1: Components of the GSM 2G cellular network architecture

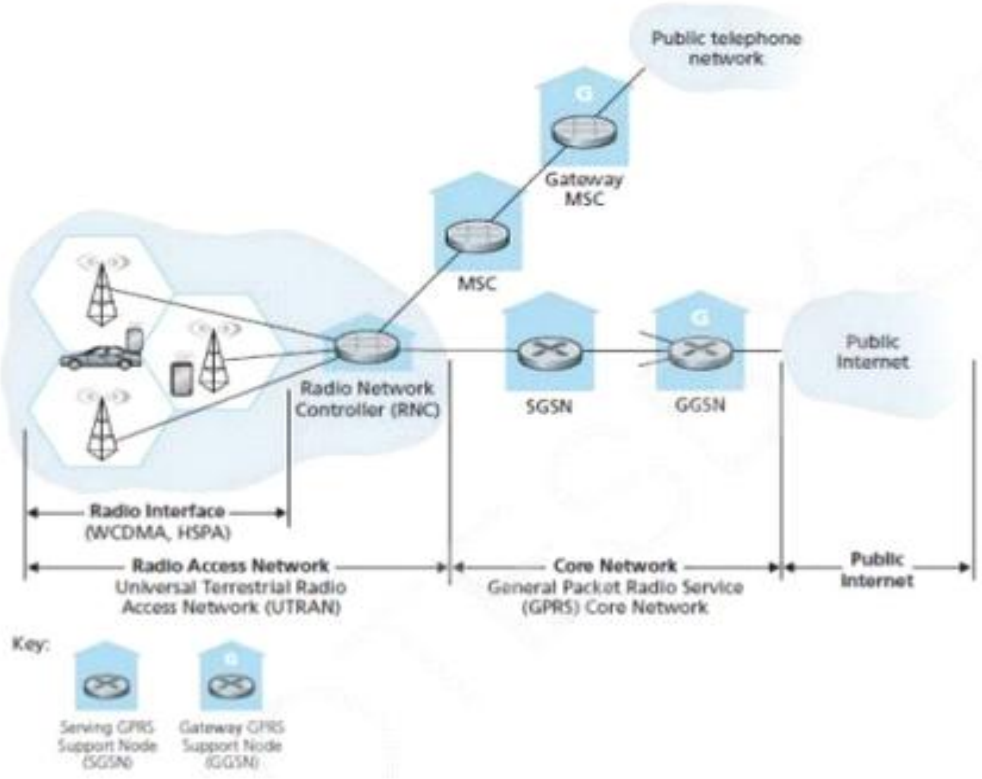
- The GSM network contains many BSCs (Base Station Controllers).
- Main responsibilities of the BSC:

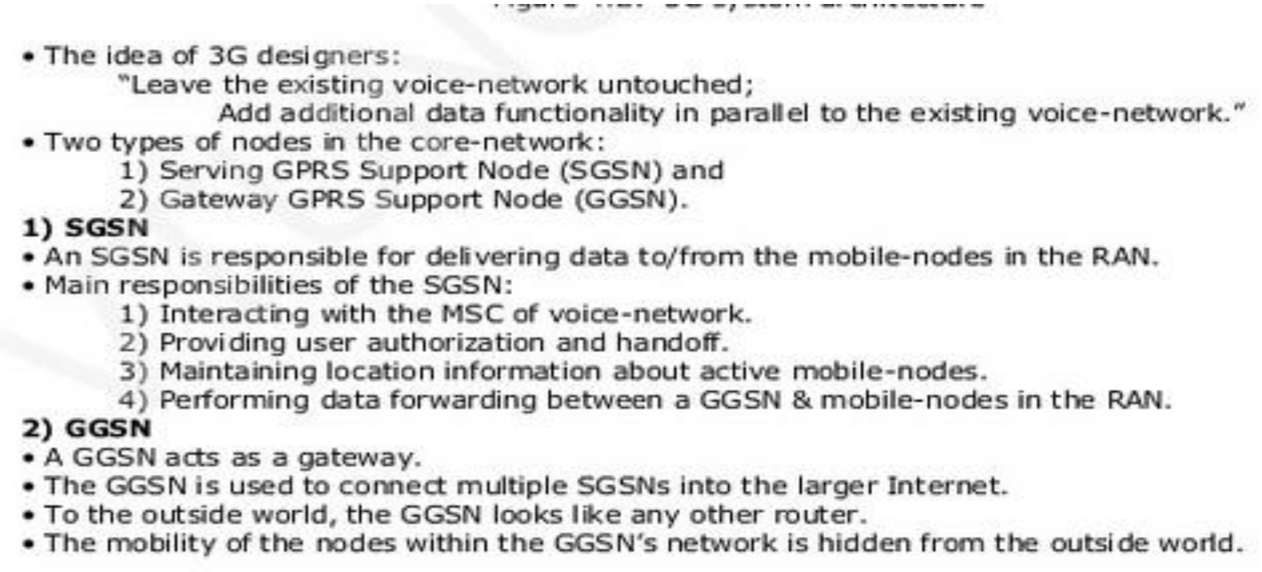

1) Providing service to many BTSs.
2) Allocating radio-channels to mobile-users.
3) Performing paging.
4) Performing handoff of mobile-users.

- BSS (Base Station System) contains the BSC and its controlled BTSs.
- A MSC (Mobile Switching Center) contains upto 5 BSCs. This results in approx 200K subscribers/MSC.
- Main responsibilities of the MSC:
  1) User authorization & accounting
  2) Call establishment & teardown and
  3) Handoff.
- A cellular-provider's network will have a number of special MSCs known as gateway MSCs.
- Gateway MSCs are used to connect the provider's cellular-network to the public telephone-network.

Architecture of 3G Wireless Network **4**


- 3G system architecture is shown in Figure 4.2.
- Main responsibilities of the core-network:
  1) Connects radio access-networks (RANs) to the public Internet.
  2) Interoperates with components of the existing voice-network.


Public telephone network
G
Gateway MSC
MSC
Radio Network Controller (RNC)
SGSN
G
GGSN
Public Internet
Radio Interface (WCDMA, HSPA)
Radio Access Network
Universal Terrestrial Radio Access Network (UTRAN)
Core Network
General Packet Radio Service (GPRS) Core Network
Public Internet
Key:
G
Serving GPRS Support Node (SGSN)
Gateway GPRS Support Node (GGSN)



- The idea of 3G designers:

  "Leave the existing voice-network untouched;
  Add additional data functionality in parallel to the existing voice-network."
- Two types of nodes in the core-network:
  1) Serving GPRS Support Node (SGSN) and
  2) Gateway GPRS Support Node (GGSN).

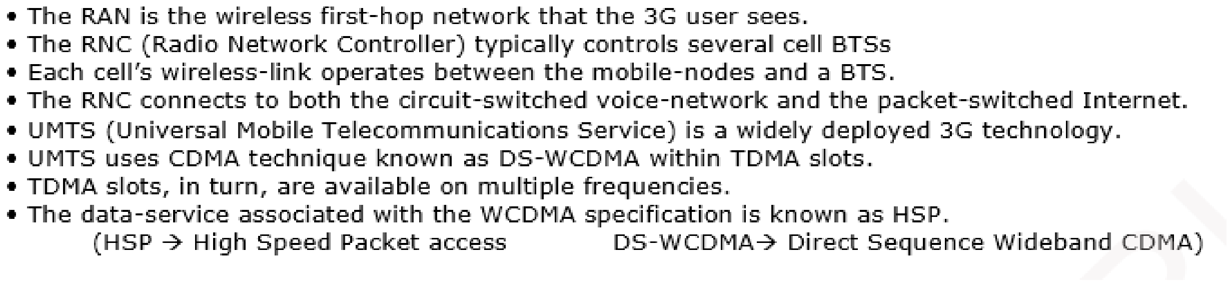
1) SGSN

- An SGSN is responsible for delivering data to/from the mobile-nodes in the RAN.
- Main responsibilities of the SGSN:
  1) Interacting with the MSC of voice-network.
  2) Providing user authorization and handoff.
  3) Maintaining location information about active mobile-nodes.
  4) Performing data forwarding between a GGSN & mobile-nodes in the RAN.

2) GGSN

- A GGSN acts as a gateway.
- The GGSN is used to connect multiple SGSNs into the larger Internet.
- To the outside world, the GGSN looks like any other router.
- The mobility of the nodes within the GGSN's network is hidden from the outside world.

Radio Access Network: The Wireless Edge



- The RAN is the wireless first-hop network that the 3G user sees.
- The RNC (Radio Network Controller) typically controls several cell BTSs
- Each cell's wireless-link operates between the mobile-nodes and a BTS.
- The RNC connects to both the circuit-switched voice-network and the packet-switched Internet.
- UMTS (Universal Mobile Telecommunications Service) is a widely deployed 3G technology.
- UMTS uses CDMA technique known as DS-WCDMA within TDMA slots.
- TDMA slots, in turn, are available on multiple frequencies.
- The data-service associated with the WCDMA specification is known as HSP.

  (HSP → High Speed Packet access   DS-WCDMA→ Direct Sequence Wideband CDMA)