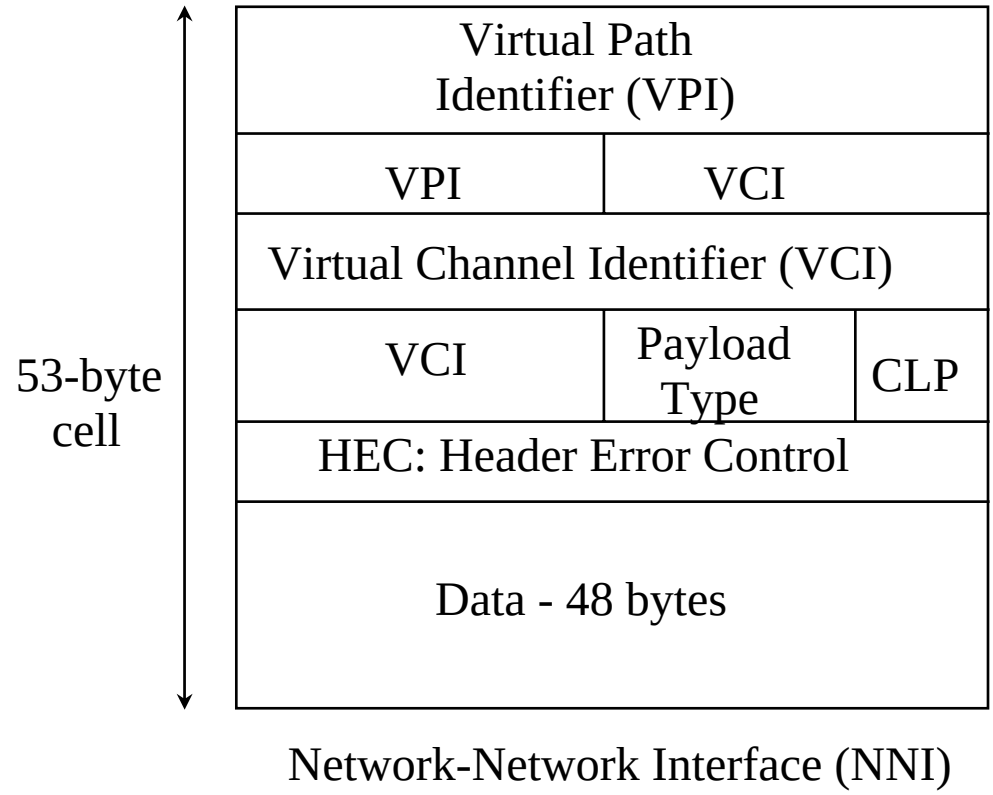
EE4004 Telecommunications Summer 2002 – Answers to Q2(b) and Q3

Q2

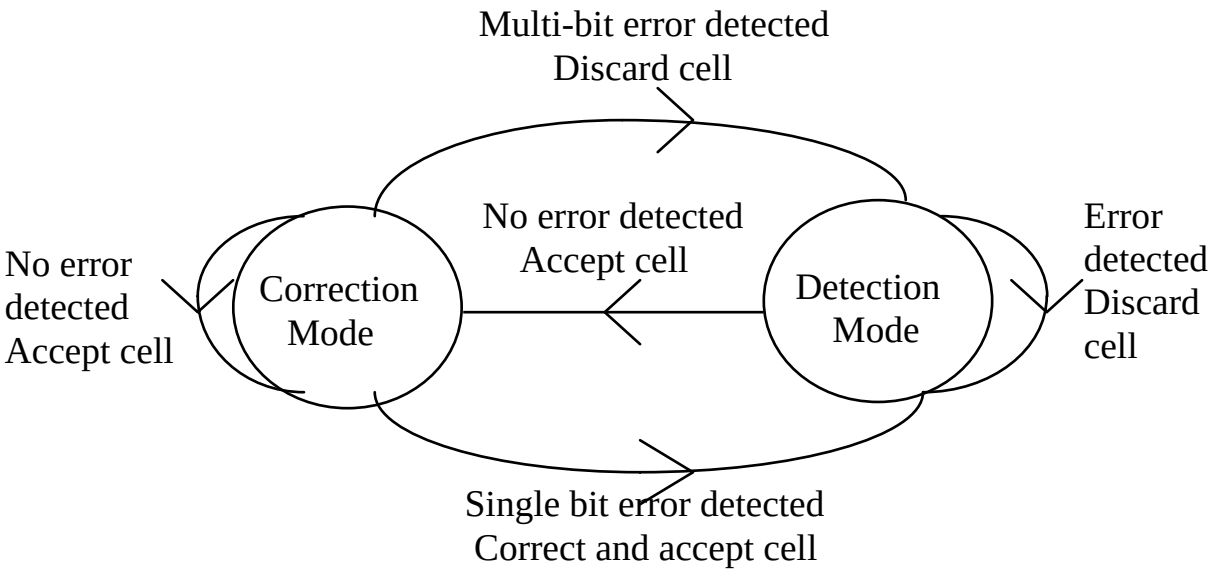
Answer to Q2(b) – 8 marks total, 4 for (i), 4 for (ii)

(i) The following shows the make up of an ATM frame for the network-network interface:



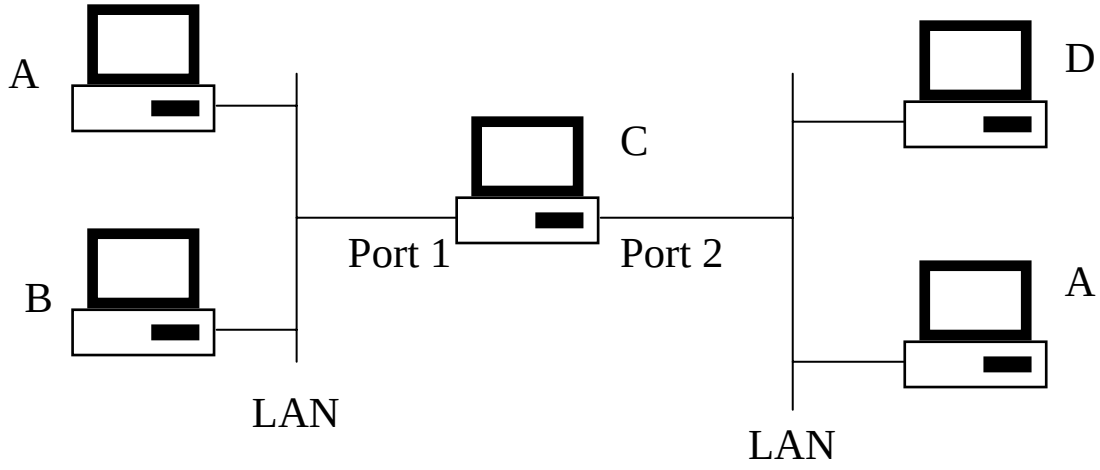
The functions of the various fields are:
Virtual Channel Indicator (VCI) and virtual path Indicator (VPI): These indicate the path in the network through which the packet is routed.
Payload Type: This indicates the type of data in the cell e.g. user data or control data
Cell Loss Priority (CLP): Indicates if a cell may be deleted in cases of congestion.
HEC: Error control bits which are calculated for the 5-byte header only
Data: Data which has been broken up into 48-byte packets.

Answer to Q2(b) continued
(ii) The following is the error handling state diagram used by ATM:

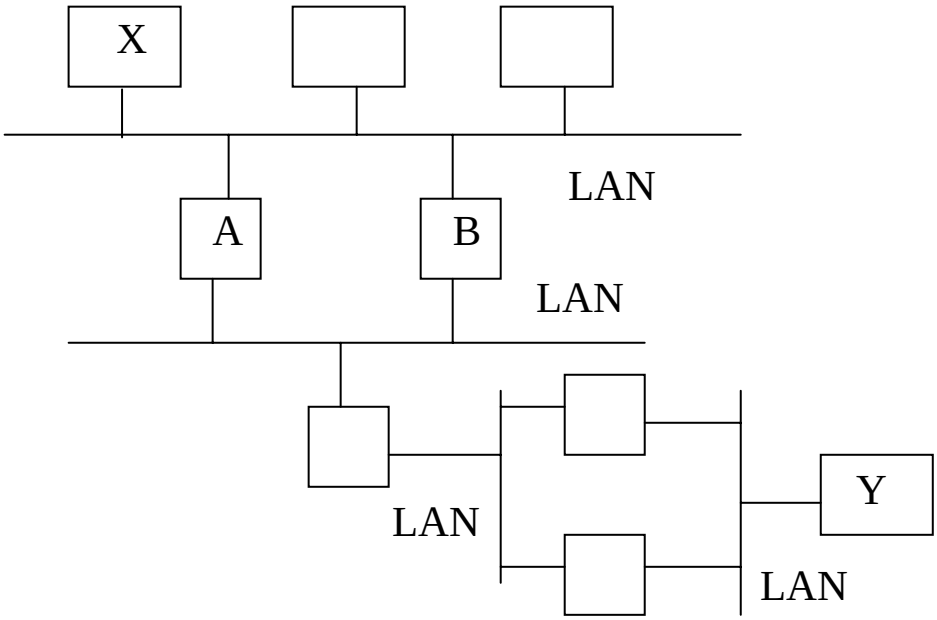


If the decoder has received the previous cells error free then it is in the “correction mode”. In this mode every error-free cell is accepted and the decoder remains in this mode. If a cell with a single-bit error is now received the decoder corrects and accepts the cell but jumps to the “detection mode”. This is the basic handling strategy for single-bit errors. While in the detection mode if the next cell also has an error then this is discarded because this indicates that there may be a burst error condition in which a significant amount of data may be corrupt beyond the scope of the error correcting code. The decoder remains in this “detection” mode until an error-free cell is finally received in which case the cell is accepted and the decoder returns to the “correction mode”. In “correction mode” if a multi-bit error is detected then the cell is discarded and the decoder jumps into the “detection mode” as again this is an indication of a burst error condition.

Answer to Q3 – 16 marks, 8 for section (a), 8 for section (b)
Q3(a)



The diagram illustrates two Local Area Networks (LANs) interconnected by a bridge C. Bridges implement a transparent routing function which ensures that computers on both networks can transmit data to any other computer regardless of which network it is on. This is achieved by the bridge monitoring the source address and the destination address of each data packet sent on both networks.If A sends a message to B then that message is put on to LAN1 and contains A's address and B's address. C reads this message and decides that A and B are on the same LAN and therefore does nothing. However, if A sends a message to D, which it puts on to LAN1, then C will detect that the source (LAN1) is different to the destination (LAN2) and so it will copy the data on to LAN2 so that D will "see" it. To the router a packet on one of its ports is LOCAL if the destination address of the packet is on the same port (LAN). If a bridge detects a non-local packet it copies this packet onto all other ports (LANs) to which it is connected.
The following arrangement illustrates the problem that can occur with loops:



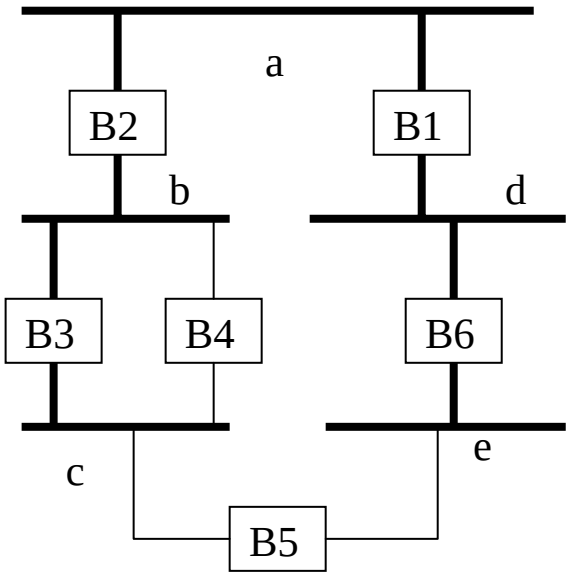
If X sends a message to Y using LAN1, then bridge A detects that Y does not belong to LAN1 and so it re-broadcasts the message on LAN2. B now sees a message on LAN2 but knows that the destination is not on LAN2 and therefore re-transmits the message on LAN1. A detects this and repeats the process causing the data packets to loop forever.

Q3(b) The scanning tree algorithm is as follows:

1. Each bridge sends out a message of the form
   [ID.sender | ID.presumed_root | distance.presumed_root].
2. Each bridge stores the best message that it has received
   so far.
   [S | R | D] is "better" than [S' | R' | D'] if
   R < R', or
   R = R' and D < D', or
   R = R' and D =D' and S < S'
3. When a bridge realizes that it is not the root it stops sending
   messages.
4. When a bridge gets a better message on a port than the ones
   it has sent so far on that port it stops sending messages on that
   port and only relays other messages after adding one to their
   distance.
5. Eventually, only the root (smallest ID) sends messages and the
   other bridges relay them.
6. This process is repeated regularly to cope with updates in the
   network topology.

The quantities mentioned are:
ID.sender = the ID number of the bridge sending a message
ID.presumed_root = the ID of the bridge which the transmitting bridge thinks is the root.
distance.presumed_root = the number of "hops" between the transmitting bridge and the presumed root.

The spanning tree is as follows:



This was obtained using the following steps:

1. Initially all bridges assume they are “the root” so
   B1 sends message [B1:B1:0] B2 sends message [B2:B2:0]
   B3 sends message [B3:B3:0] B4 sends message [B4:B4:0]
   B5 sends message [B5:B5:0] B6 sends message [B6:B6:0]
2. When B2 gets [B1:B1:0] it knows it is not the root and
   stops sending messages claiming to be the root. However, it relays the message [B2:B1:1] onto its lower ports.
3. When B6 gets [B1:B1:0] it stops sending its own messages and relays [B6:B1:1] on its lower port.
4. When B4 gets [B3:B3:0] on both ports it knows that a “better” bridge is attached to both its ports and so it is not on the shortest path.
5. When B3 gets [B2:B2:0] and later it gets [B2:B1:1] it knows it is not the root and only relays messages onto its lower port. It eventually only relays the message [B3:B1:2]
6. B5 eventually receives the messages[B3:B1:2] and [B6:B1:1] indicating that B3 and B6 are both closer to the root than itself and therefore that it is not on the shortest path.