IQRA NATIONAL UNIVERSITY, PESHAWAR, PAKISTAN

NETWORKS MANAGEMENT

Program: MSCS/PhDCS **FINAL-TERM EXAM** **Semester: Spring 2020**

Maximum Marks: 50 **Time Allowed: 6 Hours**

Note : ***Write down the complete statements of Q1 otherwise just answers will lead to zero marks.***

The paper should be submitted in pdf form and plagiarism will be checked; ***2 students with the same plagiarism report and answers will lead to zero marks to both.***

Cc: ***to Vice Chancellor***

Controller of Examination

Head of Department

RAHMAT ULAH
ID: 14437

Q1. Select the correct answer of the given ones. (10)

1) Interactive transmission of data independent of a time sharing system may be best suited to
(a) simplex lines (b) half-duplex lines (c) full-duplex lines (d) biflex lines

Answer: Option (b)

2) The loss in the signal power as of an Electromagnetic signal is called
(a) attenuation (b) propagation (c) scattering (d) interruption

3) Early detection of packet losses improves _____ acknowledgment performance.
(a) odd (b) even (c) positive (d) negative

4) Additional signal introduced in the desired signal in producing hypes is called
(a) fading (b) noise
(c) scattering (d) dispersion

5) Token is a **frame** that rotates around the ring.

6) Ring may have up to **24 bits** (802.5) or **02** (IBM) nodes.

7) FDDI can support a maximum of **500** stations.

8) Error-correcting codes are **not sufficient** enough to handle all errors.

9) ACK is a small **control frame** confirming reception of an earlier frame

10) Electronics are **slower/smaller** as compared to optics

Q2: Distinguish between error correction and error detection. Explain any two error detection techniques with mathematical examples other than given in slides, search from internet. (10)

ANS:

Error Detection:

In computer Networks, error detection refers to the techniques used to detect noise or other impairments introduced into data while it is transmitted from source to destination.

Error detection minimizes the probability of passing incorrect frames to the destination.

Error detection in the link layer is usually more sophisticated and is implemented in hardware.

Error Correction:

It is similar to error detection, except that a receiver not only detects when bit errors have occurred in the frame but also determines exactly where in the frame the errors have occurred and then corrects these errors.

Error Detection Techniques:

Errors in the received frames are detected by means of Parity Check and Cyclic Redundancy Check (CRC). In both cases, few extra bits are sent along with actual data to confirm that bits received at other end are same as they were sent. If the counter-check at receiver' end fails, the bits are considered corrupted.

In the digital world, error correction can be done in two ways:

- **Backward Error Correction** When the receiver detects an error in the data received, it requests back the sender to retransmit the data unit.
- **Forward Error Correction** When the receiver detects some error in the data received, it executes error-correcting code, which helps it to auto-recover and to correct some kinds of errors.

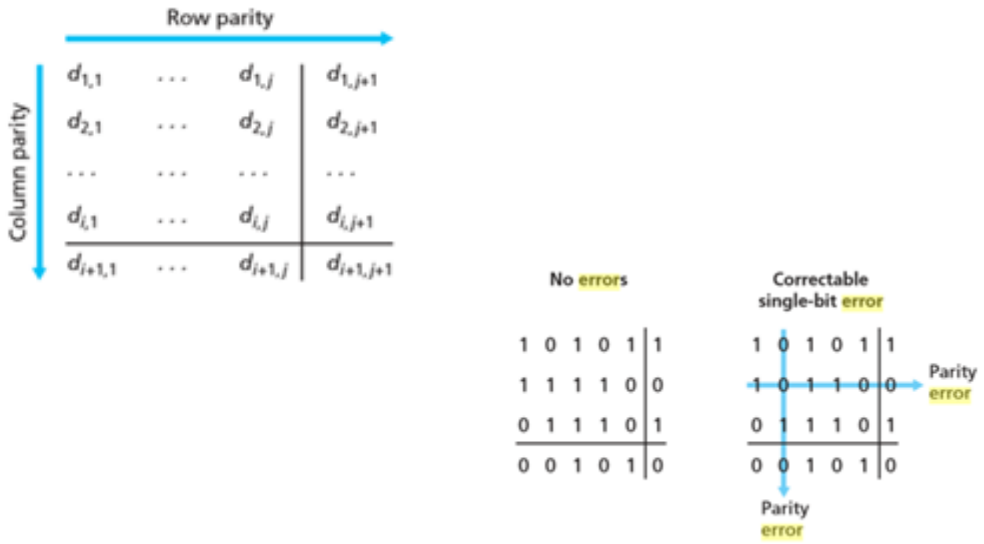
The link-layer hardware in a receiving node can incorrectly decide that a bit in a frame is zero when it was transmitted as a one, and vice versa. Such bit errors are introduced by signal attenuation and electro-magnetic noise. Because there is no need to forward a datagram that has an error, many link-layer protocols provide a mechanism to detect such bit errors. This is done by having the transmitting node include error-detection bits in the frame, and having the receiving node perform an error check.

Techniques:

1. **Parity Checks:**

   It is the simplest form of error detection to use of a single parity bit. Suppose that the information to be sent, D, has d bits. In an even parity scheme, the sender simply includes one additional bit and chooses its value such that the total number of 1s in the d + 1 bits (the original information plus a parity bit) is even. For odd parity schemes, the parity bit value is chosen such that there is an odd number of 1s. The receiver need only count the number of 1s in the received d + 1 bits. If an odd number of 1- valued bits are found with an even parity scheme, the receiver knows that at least one bit error has occurred. More precisely, it knows that some odd number of bit errors have occurred.

In a two-dimensional generalization of the single-bit parity scheme, the d bits in D are divided into i rows and j columns. A parity value is computed for each row and for each column. The resulting i + j + 1 parity bits comprise the link-layer frame's error-detection bits. Suppose now that a single bit error occurs in the original d bits of information. With this two-dimensional parity scheme, the parity of both the column and the row containing the flipped bit will be in error. The receiver can thus not only detect the fact that a single bit error has occurred, but can use the column and row indices of the column and row with parity errors to actually identify the bit that was corrupted and correct that error! Figures for an example is given below.



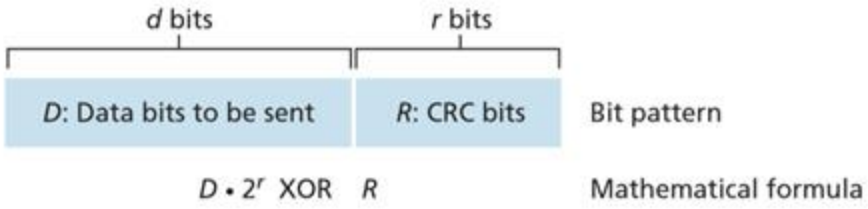
2. Cyclic Redundancy Check :

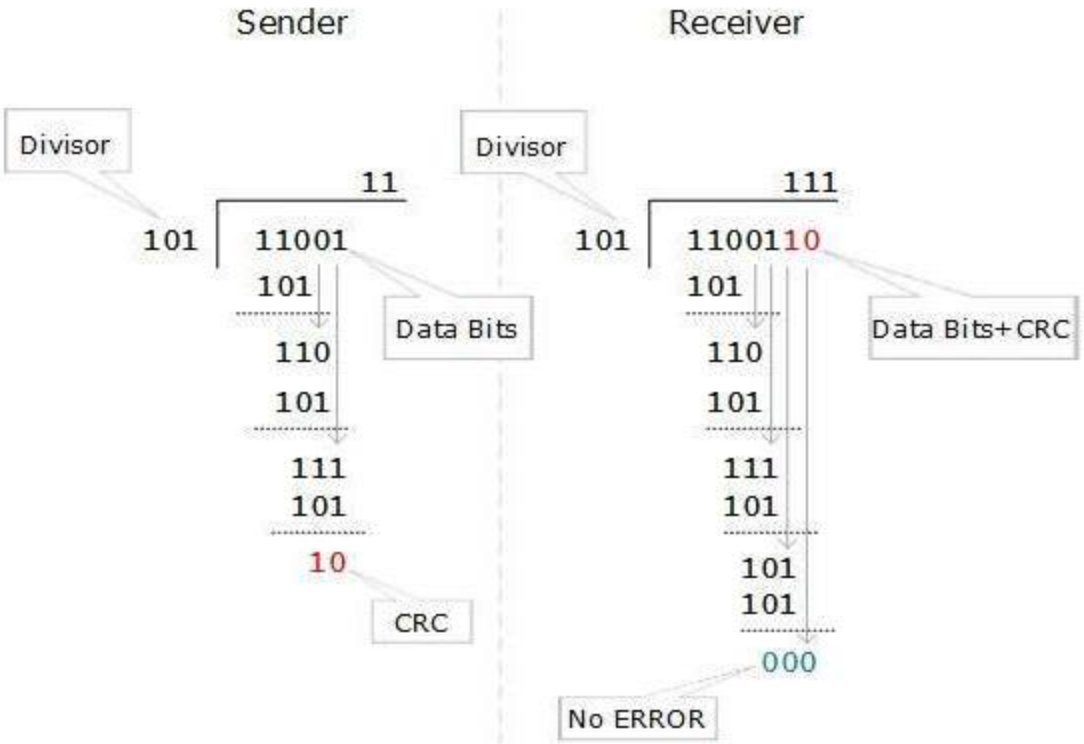
This error-detection technique is used widely in today's computer networks. It is based on cyclic redundancy check (CRC) codes. CRC codes are also known as polynomial codes, since it is possible to view the bit string to be sent as a polyno- mial whose coefficients are the 0 and 1 values in the bit string, with operations on the bit string interpreted as polynomial arithmetic. CRC codes operate as follows.

Consider the d-bit piece of data, D, that the sending node wants to send to the receiving node. The sender and receiver must first agree on an r + 1 bit pattern, known as a generator, which we will denote as G. We will require that the most significant (leftmost) bit of G be a 1. The key idea behind CRC codes is shown in Figure 5.6. For a given piece of data, D, the sender will choose r additional bits, R, and append them to D such that the resulting d + r bit pattern (interpreted as a binary number) is exactly divisible by G (i.e., has no remainder) using modulo-2 arithmetic. The process of error checking with CRCs is thus simple: The receiver divides the d + r received bits by G. If the remainder is nonzero, the receiver knows that an error has occurred; otherwise the data is accepted as being correct.

The following figures can be referred to for Examples:

```
1011 XOR 0101 = 1110
1001 XOR 1101 = 0100
```





****

Q3: What is encoding? Write down different types of encoding. Explain characteristics of AM, FM and PM with mathematical equations. (10)

ANS:

Encoding:

Encoding is the process of putting a sequence of characters (letters, numbers, punctuation, and certain symbols) into a specialized format for efficient transmission or storage.

Different Types of Encoding:

1. **ASCII:**

   The code used by most computers for text files is known as ASCII (American Standard Code for Information Interchange, pronounced ASK-ee).

   ASCII can depict uppercase and lowercase alphabetic characters, numerals, punctuation marks, and common symbols.

   For example the ASCII code for letter A is 065 and B is 066.

2. **Unicode:**

   Unicode is a universal character encoding standard. It defines the way individual characters are represented in text files, web pages, and other types of documents.

   For example the Unicode for letter A is U+0041.

3. **BinHex:**

   BinHex is an encoding system used in converting binary data to text, used by the Macintosh OS to send binary files through email. It has a .hqx extension at the end of its filename. Itencodes an 8-bit binary file, or 8-bit stream representation, into a 7-bit ASCII text format.

4. **Manchester Encoding:**

   Manchester Encoding is a special form of encoding in which the binary digits (bits) represent the transitions between high and low logic states.

Explanation of characteristics of AM, FM and PM with mathematical equations.

Characteristic of AM:

In amplitude modulation, the amplitude (signal strength) of the carrier wave is varied in proportion to that of the message signal being transmitted.

Mathematical Equation:

The message signal *m(t)* is impressed on the implititude of the carrier signal c(t)= $A_c cos(2\pi f_c t)$

Characteristic of FM

The characteristic of frequency modulation is that in this modulation, the frequency of the carrier signal is varied.

Mathematical Equation:

Frequency modulation is that form of angle modulation in which the instantaneous frequency *i* f(t) is varied linearly with the message signal m(t):

$$f_i(t) = f_C + k_f m(t)$$

Characteristic of PM:

The characteristic of phase modulation is the one in which its phase is varied.

Mathematical Equation:

It is a form of angle modulation in which the angle $\theta_i(t)$ is varied **linearly** with the message signal m(t),

$\theta_i(t) = 2\pi f_C t + \phi(t)$

carrier — not a constant

Where $\phi(t) = k_P m(t)$

$$\therefore \theta_i(t) = 2\pi f_C t + k_P m(t)$$

The term $2\pi f_C t$ represents the angle of the carrier ; the constant k_P **represents the phase sensitivity** of the modulator , expressed in radians per volt on the assumption that m(t) is a voltage waveform.

The phase modulated signal s(t) is thus described in the time domain by

$$S(t) = A_C \cos[2\pi f_C t + k_P m(t)]$$

****

Q4: **Compare Ethernet and Token Ring concept of data networking with diagrams. Which one is better in your opinion and why?** (10)

ANS:

Comparison of Ethernet and Token Ring:

In the token ring a token, which a station and special frame, ring passes over a physical ring. After the successful transmission of data frame token are issued.

Whereas Ethernet uses CSMA/CD mechanism. It means that if many stations exist at the same time to talk, all stations will be closed. To resume them, wait for a random time.

Moreover, token ring is a Star shaped topology and handles priority in which some nodes may give priority to the token whereas While Ethernet is a Bus shaped topology and it doesn't employ any priorities.

Finally, Token ring is defined by IEEE 802.5 standard. It contains routing information and is more costly whereas Ethernet is defined by IEEE 802.3 standard. It does not contain routing information and costs less than Token ring.

Diagrams:

Diagram of Token Ring

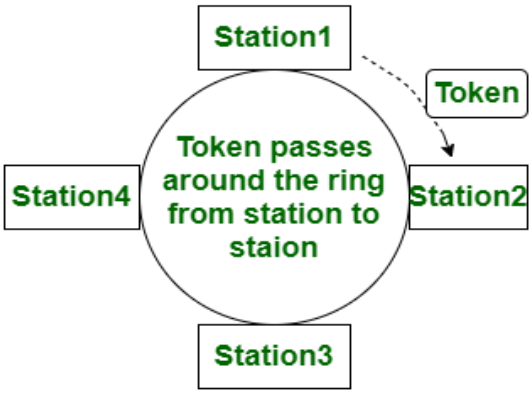
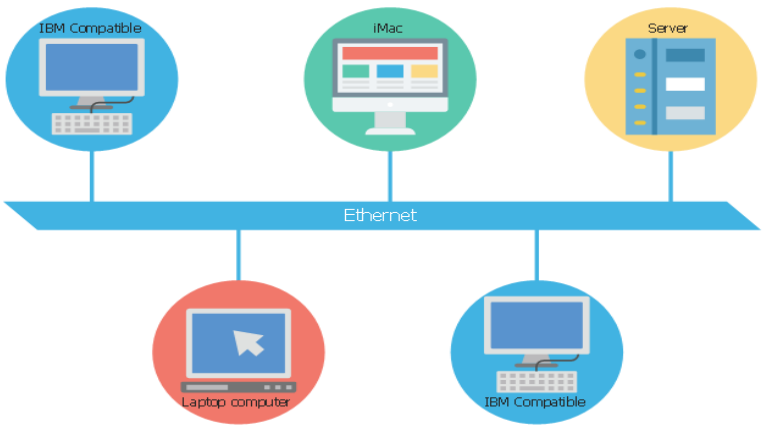


Diagram of Ethernet



Which One Is Better and Why?

In my opinion, Ethernet is better than Token ring. Then main reason why I think so beacasue of the speed of ethernet. Ethernet is several times faster that token ring. Interestingly, the cost of ethernet hardware is also far cheaper than token ring which makes me believe firmly that ehternet is better token ring.

****

Q5. Explain the concept and review of Reliable Transmission with diagram (from a research paper of 2019 or 2020) and its functionality. The name and reference of paper should be given. (10)

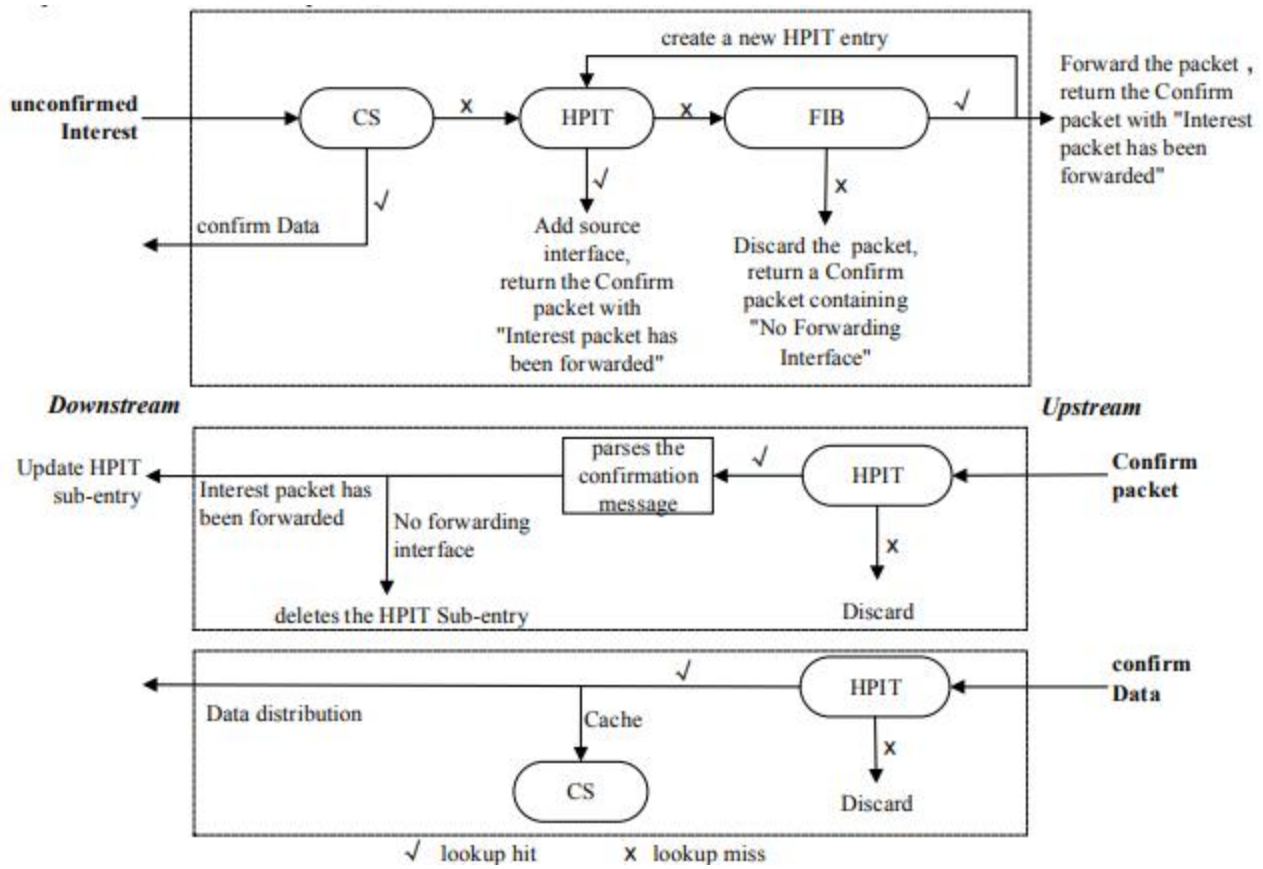
ANS:

The Concept and Review of Reliable Transmission and Its Functionality:

Reliable transmission is that transmission in which the data is ddelivered in same order to receiver's network layer that sender's network layer intended. Reliable transmission has Forward error-correction and Discard frames with bad checksum / CRC. It has mechanism of Acknowledgment such as Control frame, informs peer frame(s) received okay and timeouts to ensure the reliable transmission. It has Automa8c repeat request (ARQ) algorithm which means that the Sender waits for acknowledgement (ACK) before advancing. If no ACK after timeout value is received the frame is resent to ensure reliablaity of transmission.

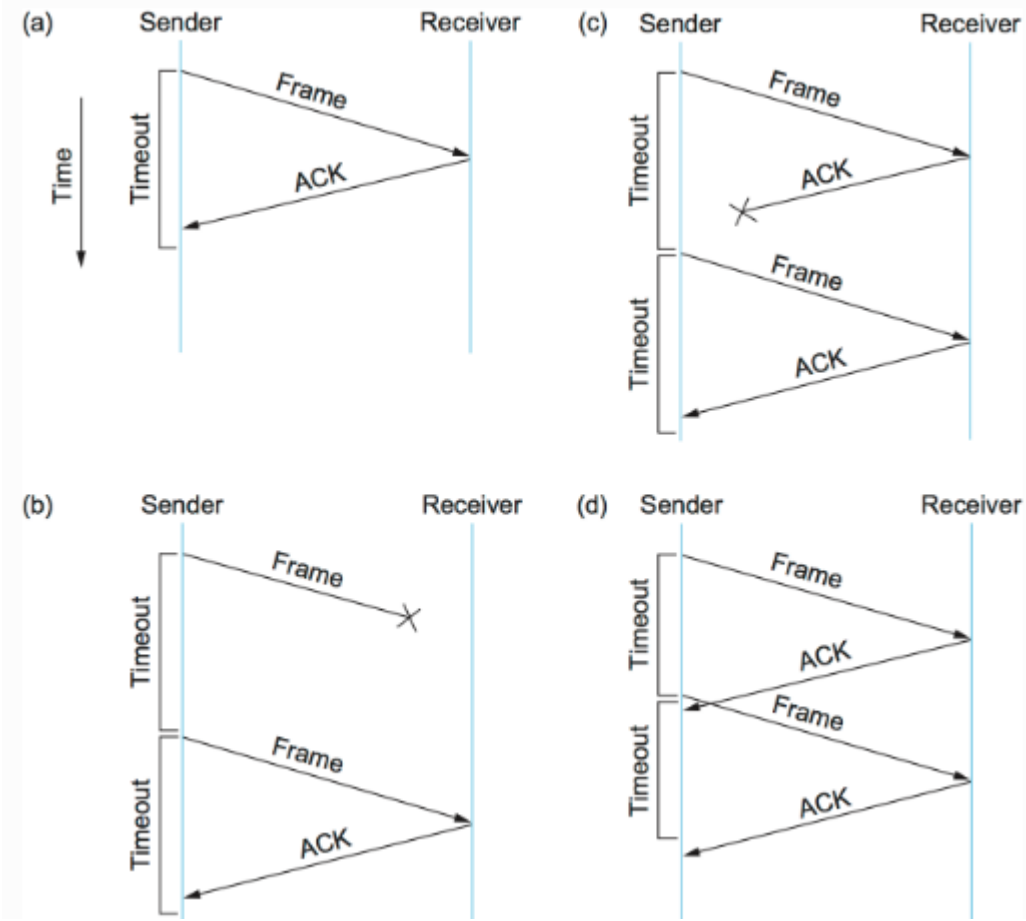
Reference of Paper and Diagram:

Referring to the paper named **"Reliable transmission mechanism of Interest in Named Data Wireless Multi-hop Network"**, published in "**2020 IEEE 4th Information Technology,Networking,Electronic and Automation Control Conference (ITNEC 2020)**", the following diagram is chosen and explained.



After receiving the Confirm packet, the node looks up in HPIT, and discards it if there is no matching HPIT entry; otherwise, parses the confirmation information: if the information is "Interest packet has been forwarded", delays the RTO timer on the matching HPIT sub-entry to wait for the Confirm packet or confirm Data packet; if the information is "No forwarding interface", deletes the matching HPIT subentry. After receiving the confirm Data packet, the node looks up in HPIT, and discards it if there is no matching

HPIT entry; otherwise, caches the Data into CS, and deletes the matching HPIT entry after distributing the Data according to the HPIT entry.



Referring to the diagram above, it can be explained that one way to ensure reliable transmission is the *stop-and-wait* algorithm. The idea of stop-and-wait is straightforward: After transmitting one frame, the sender waits for an acknowledgment before transmitting the next frame. If the acknowledgment does not arrive after a certain period of time, the sender times out and retransmits the original frame.

****