Sessional Assignment- Spring 2020

Name: **Muhammad Idrees Khan**
ID: **6659**
Data Communication & Networks

Question 1: Go to www.ietf.org/rfc.html and look up RFC 2026 and read it. Answer these questions:

(a) What is an Internet Draft?

Answer: Internet draft (I-D) is a short-lived document, often published by IETF working groups and also released by others. It contains preliminary technical specifications, results of network research or other technical information. Internet projects are generally work-in-progress documents that will be published as a request for comment (RFC), which potentially leads to the Internet standard. Before becoming an RFC, I-D functions as an evolving working document, easily accessible to a wide audience, facilitating the review and revision process.

Drafts are archived for six months after their publication. Although some end up becoming RFCs and follow the general RFC format. Internet Drafts should not be considered authorized sources. They do not have an official status and can be modified or deleted at any time; therefore, they should not be cited or cited in any official document.

(b) What are the differences between a Proposed Standard, Draft Standard, and Standard?

Answer:

➔**Proposed Standard:**

IETF and IESG documents typically go through different levels of maturity and revision to a standard level. One of the first levels is the "proposed standard". This is the entry level for a number of IETF and IESG standards.

The proposed standard is generally stable, it solves the well-known and necessary design options, received significant improvements from the community, while it was at the level of RFC and Internet-Draft, it is considered well understood and understandable and seems to be interested in the community enough to be considered valuable.

It is advisable to implement the proposed standard in order to gain experience and verify, test and refine specifications and how it works. However, since the content of the proposed standards can be changed if problems are found or better solutions are found, it is not recommended to use these standards in an interrupt-sensitive environment.

Since the proposed standard goes a long way and must be verified by the implementation before proceeding to the next step, therefore, it should not have any known technical flaws with respect to the requirements. However, the IESG may waive this requirement to allow the specification to go into the state of the proposed standard when it is considered useful and necessary (and timely), even with a known technical omission.

In general, neither implementation nor operational experience is required to define a specification as a proposed Standard. However, this experience is highly desirable and, as a rule, constitutes a good basis for the proposed standard designation.

➔**Draft Standard:**

This is the next level document after changing the proposed standard to a standard after full implementation and verification. The specification, on the basis of which at least two independent and compatible implementations of various code bases have been developed and for which sufficiently successful work experience has been gained, can be brought to the level of “Draft Standard”. The requirement of at least two independent and compatible implementations applies to all variants and functions of the specification. In cases where one or more parameters or functions have not been demonstrated in at least two compatible implementations, the specification can go to the standard draft level only if these parameters or functions are removed.

A standard project should be well understood and known as fairly stable both in terms of its semantics and as the basis for the development of an implementation. The draft standard is usually considered the final specification, and changes are likely to be made only to address specific problems.

In most cases, it is advisable for vendors to implement Draft Standards implementations in an interrupt-sensitive environment.

➔**Internet Standard:**

This is a last-level document that can only be achieved after successful implementations, checks, tests, and operations of a specification. Formally an Internet Standard or Standard is a specification for which significant implementation and successful operational experience has been obtained may be elevated to this level. It is characterized by a high degree of technical maturity and the general belief that the specified protocol or service offers significant benefits to the Internet community.

Standards are fully acceptable for execution in an interrupt-sensitive environment, as they are thoroughly tested with various implementations of all their features.

Question 2: Draw the graph of the NRZ-L, Manchester, Differential Manchester, and AMI schemes of the following data streams:

- 00110011

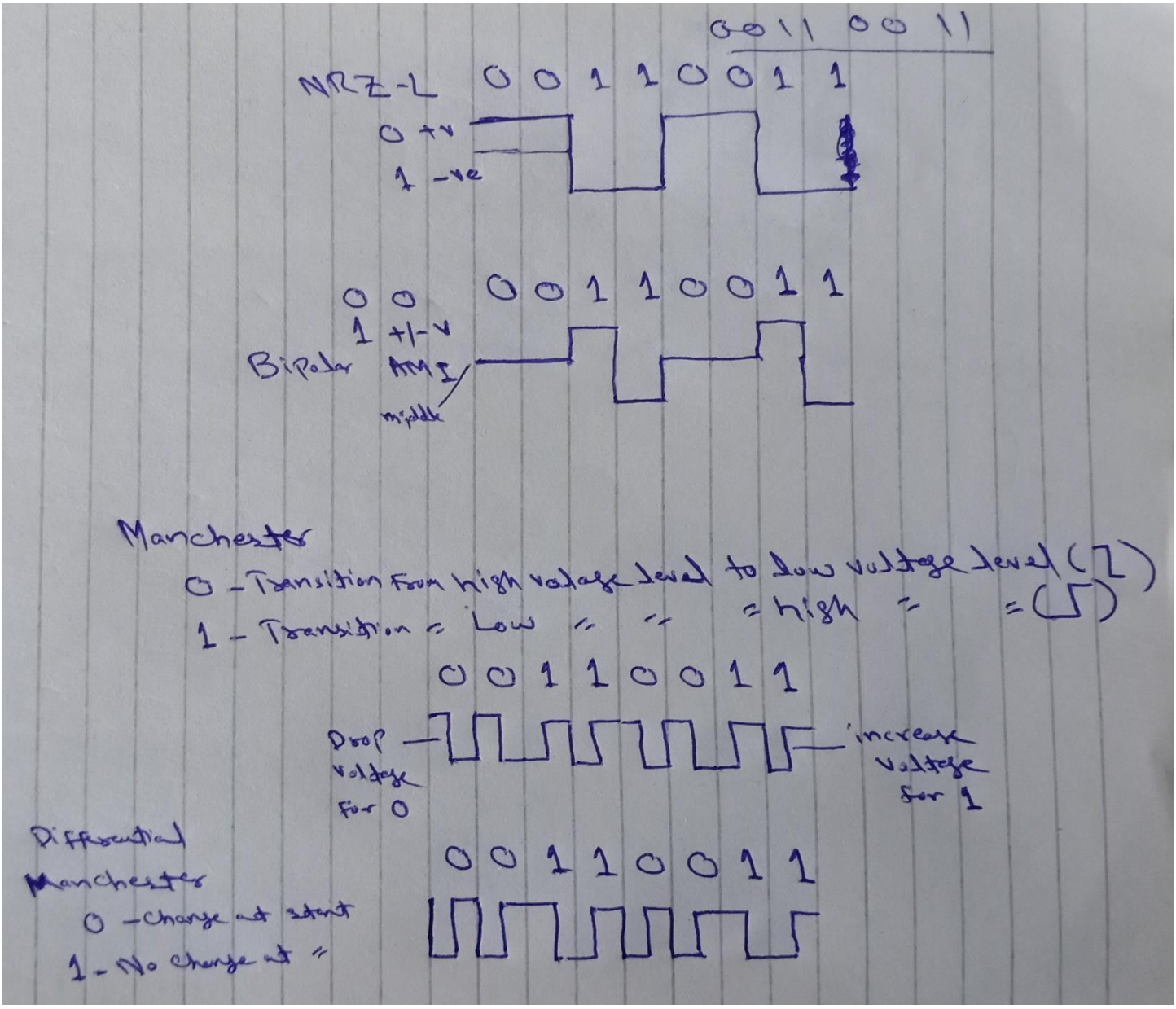


Figure 1 - NRZ-L, Manchester, Differential Manchester, and AMI Encoding of **00110011**

- 01010101

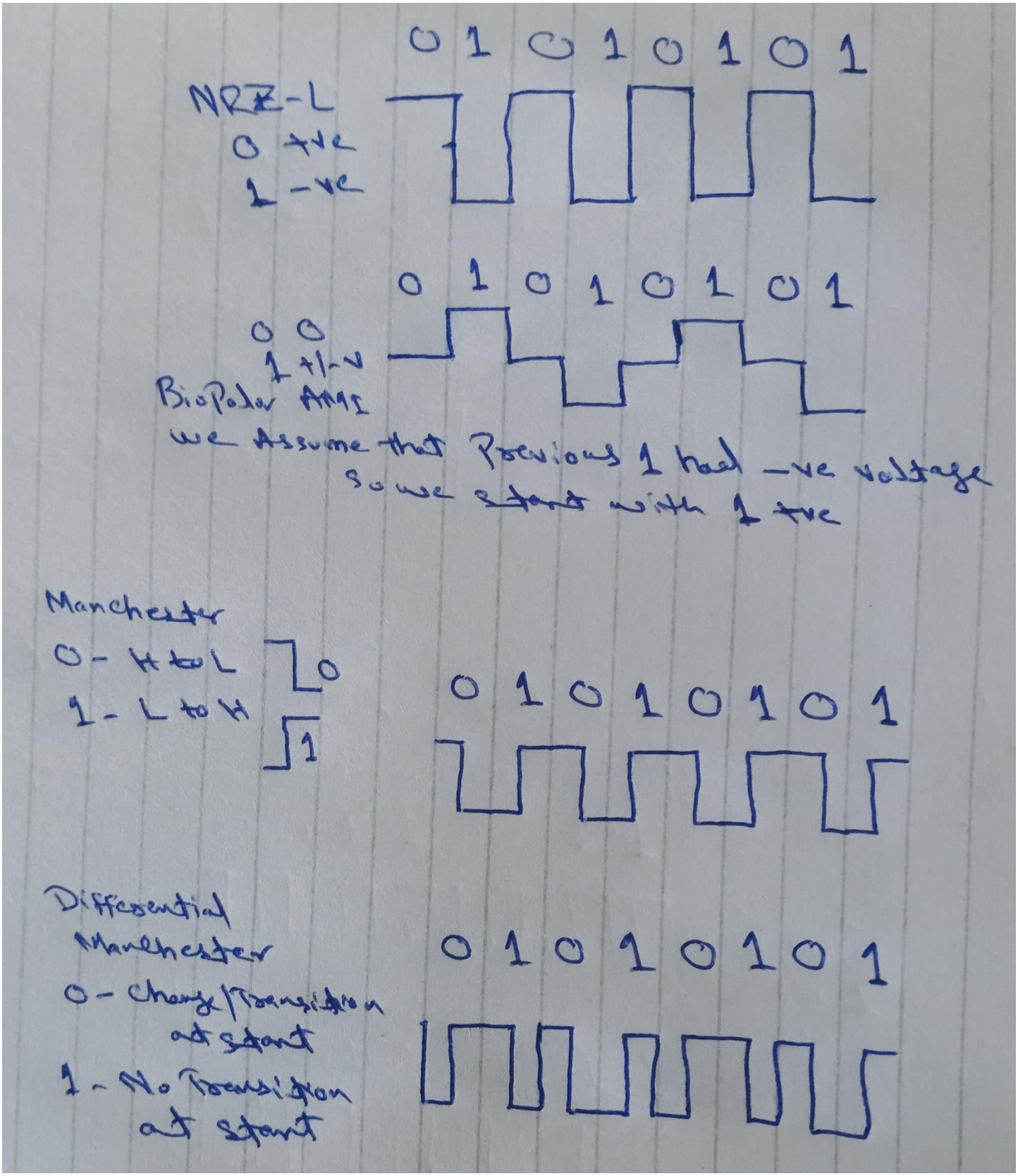


Figure 2 - NRZ-L, Manchester, Differential Manchester, and AMI Encoding of 01010101

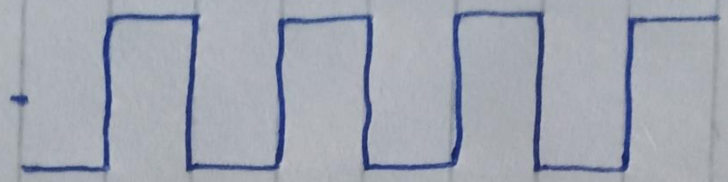
- 10101010

NRZ-L

0 +ve

1 -ve

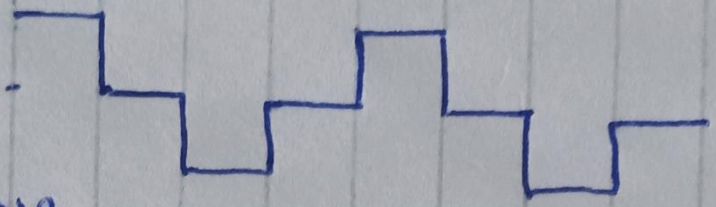
1 0 1 0 1 0 1 0



Bipolar AMI

0 0v

1 +/-v

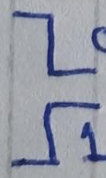


we assume that Previous 1 had -ve voltage transition

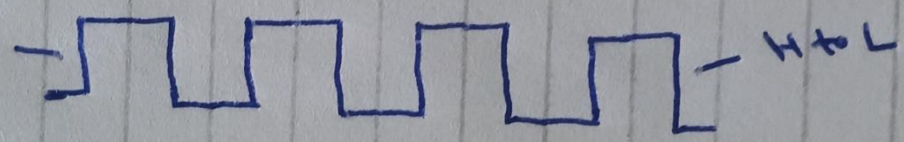
Manchester

0 - H to L

1 - L to H



1 0 1 0 1 0 1 0



Differential Manchester

0 - change at start

1 - No change at start

1 0 1 0 1 0 1 0

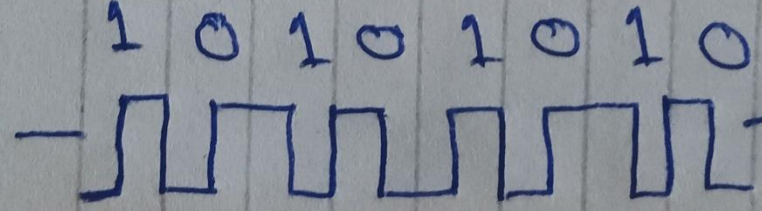


Figure 3 - NRZ-L, Manchester, Differential Manchester, and AMI Encoding of 10101010

Question 3: You are working as a Network Specialist in ABC organization. You are asked to do research on the **current and future Wireless Networks issues and challenges**?

Answer: Despite the advantages offered by wireless networks, such as portability, flexibility, increased productivity, roaming services, cheap installation costs and more, there are some problems that cause great concern. Today, the challenges of the wireless network are increasing due to the growing demand for higher data rates, the need for advanced and roaming services and the huge spread of services all over the world. As a result, this has created serious problems in the security and operation of wireless systems and applications in wireless environments.

Here I am presenting some of the issues and of current wireless networks and future challenges. The list is not exhaustive, I have focused on most prominent issues and challenges.

➔Issues in Current Wireless Networking Technologies:

Here are some of the pressing issues of current wireless networks:

Robustness

Robustness is the primary concern of today's wireless networks. Robustness is the ability to handle unstable network changes. An unstable network can experience interruptions and loss of important information when launching applications in real time. Some military and real-time applications, such as air systems, disposal operations, and disaster operations, require real-time information exchange. If the network cannot tolerate interruptions due to an adverse environment, the real-time application may lose control of the destination.

Reliability

Reliability in the network is the ability to provide the right information in the right place. An unstable network detects unreliable data delivery. Packets may be dropped or corrupted due to network instability. This is caused by a hostile environment. Intermittent interference can result in packet loss. A hostile attack may try to eliminate or modify packets that are transmitted over the network. Reliability issues also include delivering information to the right place. This path to the destination must be trusted. Interference instability can damage the packet header and forward the packet to the wrong destination. Attackers could create a trusted node and redirect the packet to the wrong destination.

Security

Security issues are a major concern in wireless networks with hostile attacks by attackers. An attacker can log into the network and try to steal, publish or modify network information. This forged assembly leads to a problem of information trust. Attackers can fill the network by sending a large number of packets, which will cause problems with network congestion and availability. An interference signal may interrupt network communications, causing reliability and availability problems. Similarly, insecure networks lead to privacy and confidentially loss which is one of the most essential functions of wireless networks.

➔Future Challenges of Wireless Networks:

Here are some of the pressing future challenges of Wireless networks that needs to be tackled

Maximizing Performance

Wireless networks are very fast today, but performance is significantly reduced in complex or busy environments. If the sports hall wanted to offer each person in each place their own individual experience of augmented reality, today we would not be able to do it effectively.

New wireless standards will help. Wi-Fi 6, for example, offers significant advantages over previous generations of Wi-Fi in terms of predictability and aggregate bandwidth, which elegantly adapts to the increase in the number of devices.

But it is still difficult to develop radio systems that can take full advantage of these new protocols. For example, on Wi-Fi 6, access points and devices can use different methods to optimize spectrum usage. The challenge is to make them choose and perform a better optimization together. For example, a wireless access point must determine in real time for all devices in its coverage which set of packets (for one or more receivers) is best suited for the subsequent transmission - how to code and plan it - while the wireless environment is changing rapidly along with traffic requirements.

In addition, each access point probably exists in an environment with other access points. Simply put, it is difficult to ensure that all access points and devices optimize the use of their spectrum, in order to maximize the quality of experience (QoE) of each application used, continuously, in real time and with low complexity. (for a budget). One of the technical problems is that it is not the average or median performance that counts, but the tail of the probability density function: we want the queue to be as short as possible, because even a final package of 10,000 can degrade the application. performance.

Networks that Know Themselves

In a few years, billions of new wireless devices will appear on the network. How should each wireless network be connected to each new device when connected? Network administrators find it surprisingly difficult to find out what's on their networks. Not all devices identify themselves. Malicious devices can lie about what they are. In addition, as more traffic is encrypted (as it should be for security), authentication becomes even more difficult. There are serious research challenges and opportunities to increase security by simply telling networks which devices are present.

The increasing complexity will also make it difficult to determine whether the network is working as expected or if there is a problem. Ideally, due to the speed and scalability of the reaction, the network itself should be able to determine this, which is impossible with modern wireless networks.

Security Challenges

Security research often solves the problem of congestion, reliability and accessibility caused by hostile attacks. The research focuses on protecting information from theft, denial or alteration by attackers. Some researchers are interested in protecting the path. In addition, the security research attempted to detect cyber criminals on networks based on their abnormal behavior, such as dropped or packet changes. In an adverse environment, packets are regularly discarded and damaged on the host. Detection mechanisms can consider this behavior as a threat and false detection can occur. **The challenge is to develop an accurate detection mechanism that takes into account not only the loss of packages due to inappropriate behavior, but also downloading the package from an aggressive environment**.

User Identification and Localization

One of the significant problems is that the network must be able to locate a specific user among millions of mobile terminals and send a call to that user, who can move at speeds of up to 160 kilometers per hour. The resources of the final network must be distributed in a fair and efficient manner to meet the changing needs of users and their position. Today, a huge infrastructure for wired networks has been developed: a telephone system, the Internet and a fiber optic cable, which should also be used to connect wireless systems to the global network. **However, as wireless systems with mobile users are unlikely to compete with wired systems in terms of speed and reliability of data transfer, the development of protocols to provide interfaces between wireless and wired networks with completely performance characteristics remains challenge.**