Data Communication & Networks
Sessional Assignment

Name: Babar kamal
ID: 5507

Question 1 (a):
Answer: Internet Draft is a series of working documents published by the Internet Engineering Task Force. Typically, they are drafts for RFCs, but may be other works in progress not intended for publication as RFCs. During the development of a specification, draft versions of the document are made available for informal review and comment by placing them in the IETF Internet drafts directory. This makes an evolving working document readily available to a wide audience, facilitating the process of review and revision.

Question 1 (b):
Answer:

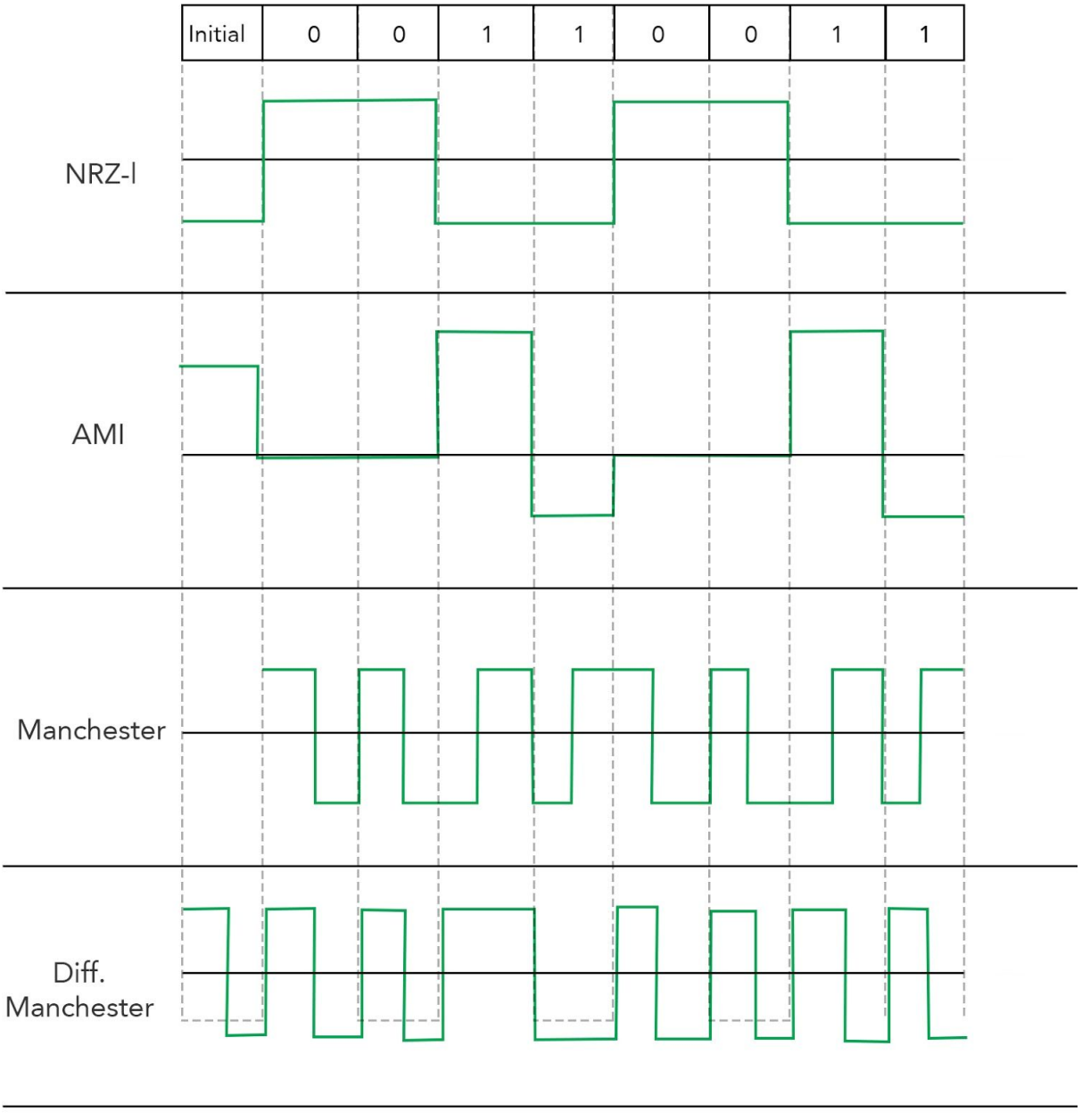
1. **Proposed Standard:**
    - The entry-level maturity for the standards track is Proposed Standard. A specific action by the IESG is required to move a specification onto the standards track at the Proposed Standard level.
    - A Proposed Standard specification is generally stable, has resolved known design choices, is believed to be well-understood, has received significant community review, and appears to enjoy enough community interest to be considered valuable.
    - Further experience might result in a change or even retraction of the specification before it advances.
    - Usually, neither implementation nor operational experience is required for the designation of a specification as a Proposed Standard. However, such experience is highly desirable, and will usually represent a strong argument in favour of a Proposed Standard designation.

2. **Draft Standard:**
    - A specification from which at least two independent and interoperable implementations from different code bases have been developed, and for which sufficient successful operational experience has been obtained, may be elevated to the Draft Standard level.
    - A Draft Standard must be well-understood and known to be quite stable, both in its semantics and as a basis for developing an implementation.
    - A Draft Standard is normally considered to be a final specification, and changes are likely to be made only to solve specific problems encountered.
    - In most circumstances, it is reasonable for vendors to deploy implementations of Draft Standards into a disruption sensitive environment.

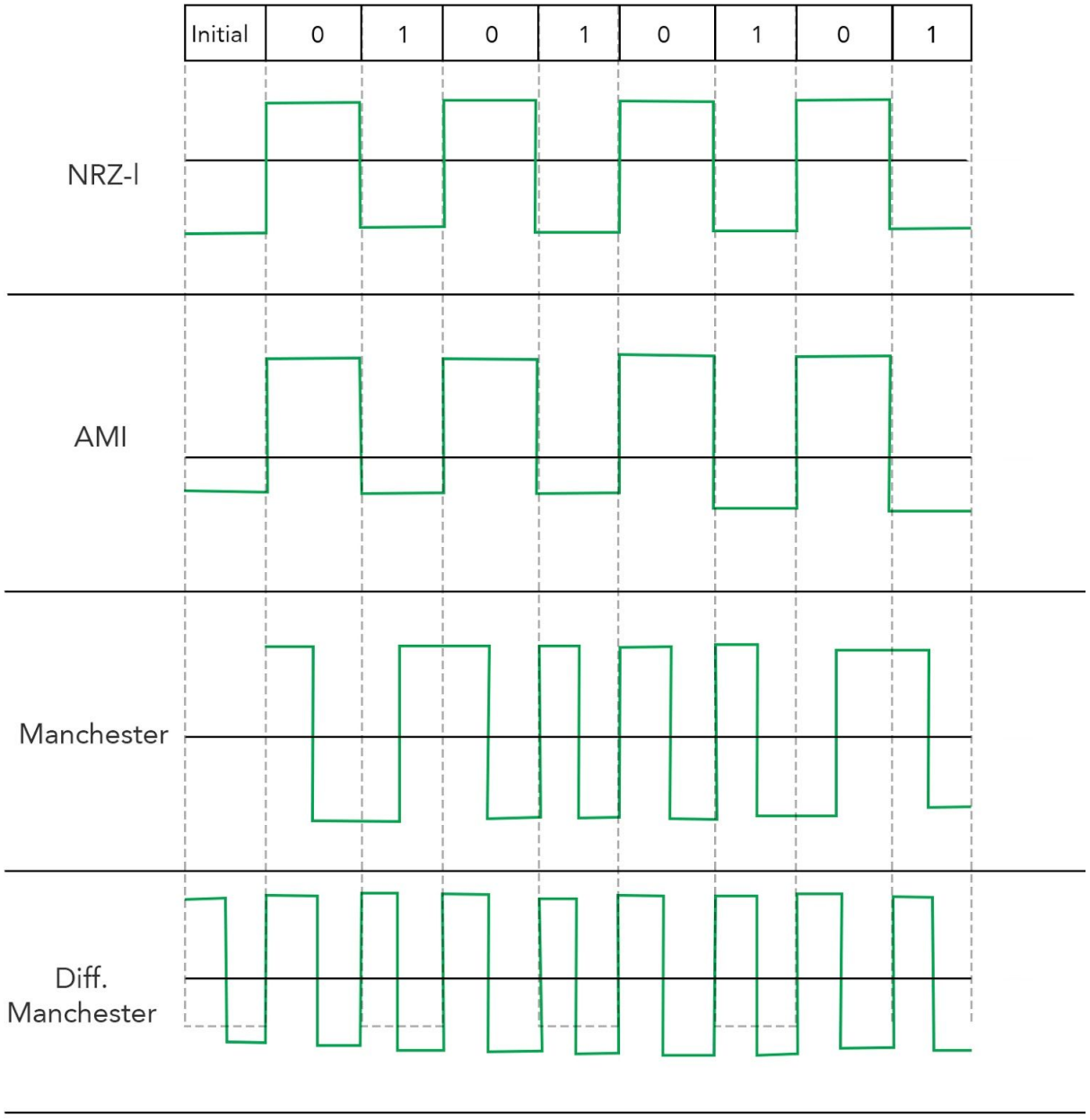
3. **Standard:**
    - A specification for which significant implementation and successful operational experience has been obtained may be elevated to the Internet Standard level.
    - An Internet Standard is characterized by a high degree of technical maturity and by a generally held belief that the specified protocol or service provides significant benefit to the Internet community.
    - All specifications unconditionally accepted.
    - Has cleared requirements of both Proposed and Draft and beyond.

Question 2:

Answer: **i. 00110011**



Ii. 01010101



Question 3:

Answer:

ISSUES AND CHALLENGES IN THE PRESENT WIRELESS NETWORKS

There are a number of issues and challenges that exist in wireless networks, some of them are as follows:

1: Physical Object Interference / Design

The reliability of your WLAN is heavily dependent on not only the architecture of your hardware and software but also the design and placement of the crucial pieces of your network. So if you're getting spotty signal in certain parts of your WLAN, make sure that your access points and routers are positioned optimally.

Walls, ceilings, and other large objects can inhibit the reach of your wireless signal. Even things like metal filing cabinets can affect your WLAN's performance. Therefore, moving your hardware to the right place can be just as important as sourcing the right hardware.

2: RF Interference

802.11 technology has made the overall performance and reliability of WLAN networks much more suitable for daily enterprise use. Despite this, an invisible culprit often puts a fork in the road regarding signal strength: radio frequency (RF) interference.

RF interference can be caused by any device that emits electromagnetic signals. Examples of devices that emit these signals are:

- Mobile phones
- AM/FM radios
- Televisions
- Microwave ovens
- MRI machines
- Wi-Fi routers
-

3: Incorrect Antenna Configuration

If your WLAN router has antennas, the positioning of them can make a huge difference when it comes to the strength and reliability of your wireless signal within your network. Some wireless AP manufacturers will suggest a preferred way to position your antennas, but we typically have encountered the following types of configurations during wireless audits:

- Upright – all antennas are pointed upright, perpendicular to the router
- 45 degrees – all antennas are angled at 45 degrees to the router
- Flat – all antennas are positioned on the same plane as the router (0 degrees)
- Perpendicular – antenna position is mixed, with some upright and some flat, overall making the antennas perpendicular to each other.

4: Hardware Architecture & Firmware

Hardware issues are another major contributing factor to poor Wi-Fi performance on large WLANs. More specifically, the two most common hardware issues we see affecting WLAN performance are either having not enough or too many access points, or having outdated firmware.

Deciding on the number of access points your network needs can be tricky. This design issue can be challenging for even the most seasoned WLAN architects. Also, power configuration and channel selection can make the architectural decision-making process more complex. There is no straightforward answer to this issue and the type, number, and configuration of your WLAN's routers, controllers, and access points will depend on your network. From a business perspective, choosing the right mix can also contribute to budgetary issues which can affect the bottom line. Overall, doing your due diligence and

investing the appropriate amount of time into the architecture of your WLAN's hardware is a crucial step that should not be overlooked.
In addition to power configuration and channel selection, firmware updates can have a major effect on your WLAN performance. Security updates and bug fixes are addressed in firmware updates, and sometimes a coordinate update plan is all that is needed to fix wireless signal and performance issues.
5: WLAN Security & Protection from Internal/External Threats
Sometimes, firmware updates can address security issues. However, many security issues need more than just a hardware update to fix, especially when it comes to protecting your network's integrity and sensitive data.
Common wireless issues that we've seen include, but are not limited to:

- Rogue APs or ad-hoc networks – Setting up a rogue AP in the proximity of an existing WLAN with the attempt to fool devices into accessing this AP instead of the correct one.
- Denial of service – Network attack where large amounts of traffic at a specific target, or through purposely interfering with a WLAN networks connectivity (e.g. through RF interference)
- Configuration problems – Usually an internal issue with hardware/software is not configured with the proper security protocols
- Passive capturing – When an attacker gets within range of a WLAN and attempts to 'listen' or capture user data of people on that network.

ISSUES AND CHALLENGES IN THE FUTURE

Using New Spectrum Wisely
We have outgrown the radio spectrum we use for wireless communication. Fortunately, in 2020 we will see growth in the use of new frequency bands. We're going to see high frequencies, from about 30 to about 60 GHz, called "millimeter wave" rolled out for mobile data communications (5G) and as an extension of Wi-Fi (802.11ay).

Maximizing Performance
Wireless today is very fast, but performance falls off considerably in complex or crowded environments. If a sporting arena wanted to provide every person in every seat with their own customized augmented-reality experience, we couldn't do it efficiently today. (However, there are creative proposals, such as putting a wireless access point under every attendee's seat, which is both cost-prohibitive and would lead to interference issues.)

Networks that Know Themselves
In a few years, literally billions of new wireless devices will come online. How should each wireless network treat each new device as it connects? Some devices will need lots of bandwidth. Some will require ultra-low latency. Some will be battery-power-limited. Some may be malicious.

Radios as Software

There are fascinating engineering challenges ahead in the field of software-defined radios (SDRs) and cognitive radio. Rather than having to engineer all the advancements I discussed above into new radio hardware, and worry about them quickly becoming outdated, we may be able to add capabilities to our wireless systems through software updates – just like we update our smartphones today. As new spectrum or encoding methods become available, we could update existing devices in place.

Network as Sensor

We can use wireless networks for more than just data transfer. Network devices are constantly painting their environments with radio waves; how those waves are reflected back provides useful information about the environment.

Today, we can use various techniques to geolocate devices indoors, where GPS doesn't work: We collect data based on received signal strength, time-of-flight, and angle-of-arrival to estimate the location of various devices relative to indoor APs. Improving the accuracy, frequency, and scale of estimating indoor locations can open up many applications, like autonomous indoor robots.