[ASSIGNMENT]

[Wireless Networks]

JUNE 1, 2020

[NAME: FARHAN KHAN]
[ID: 13004]

Question 1:

Answer:

Following are some latest trends in wireless networks:

Mobile edge computing:

While mobile edge computing options were much hyped in the beginning, they are starting to proliferate as suppliers -- both startups and existing -- offer new products and as-a-service offerings. The primary driver for edge computing is the growth of IoT applications with large data sets and low latency requirements. These IoT applications need compute processing and storage near where the information is gathered -- i.e., edge computing -- instead of transporting this information to faraway centralized data centers.

A few of the leading use cases for edge computing include smart grid, oil and gas monitoring, traffic management, remote video processing, and manufacturing monitoring and analytics.

5G dynamic spectrum sharing:

Spectrum limitations have slowed the rollout of 5G services in many countries, including the U.S. and much of Europe. Dynamic spectrum sharing (DSS) is a new technology that enables mobile operators to offer 4G and 5G services over the same band of spectrum. This enables operators to quickly respond to bandwidth demands by allocating spectrum on various services i.e., 4G vs. 5G, on their network. DSS requires software upgrades to both the radio access network (RAN) and 5G.

Open RAN:

The migration to 5G requires operators to deploy large numbers of new base stations for geographic coverage and to deliver high-speed bandwidth with low latency. Three large suppliers -- Ericsson, Huawei and Nokia Networks -- have traditionally dominated the large RAN market, combining for more than $35 billion per year, according to Doyle Research. Proponents of Open RAN hope to break this supplier monopoly by enabling new suppliers and,

ultimately, radically reducing prices. Open RAN is designed to run on lower-cost commodity hardware.

CBRS drives private cellular networks:

CBRS, is another emerging wireless networking trend. CBRS is a repurposed band of unlicensed spectrum recently cleared for commercial use in the U.S. Enterprises can deploy CBRS in select geographic areas -- e.g., mining, large warehouses or manufacturing -- to enable their own private 4G, and soon 5G, networks. This enables enterprises to control the quality of service and ensure the security of the devices and applications. Most organizations will deploy CBRS as the WAN connection to local LAN routers, such as Wi-Fi and Bluetooth, which will connect the individual IoT devices.

Wireless SD-WAN with 5G:

Organizations spend billions per year on traditional wired WAN services to connect their data centers and remote branch offices. The availability of high-speed wireless data services, such as 4G LTE and 5G, provides new competition in the managed business services market. 5G services are as fast or faster than most wired WAN services and can be rapidly provisioned, often in a day.

SD-WAN provides intelligent traffic management across various applications and multiple WAN links. It enables wireless data services to become part of a hybrid WAN services strategy to improve reliability. 4G and 5G offer organizations the option to migrate to wireless-only WAN connectivity, especially for mobile locations e.g., pop-up stores -- and smaller branch offices.

Wi-Fi 6 in the enterprise:

Wi-Fi remains the dominant method of connecting PC, tablets, phones and other devices in the enterprise. Wi-Fi 6, or 802.11ax, is the latest upgraded version of the venerable Wi-Fi standard, which offer improved performance. It increases the number of devices that can simultaneously connect to a single Wi-Fi access point and adds features to improve the battery life of IoT devices, such as Wake on wireless LAN. Wi-Fi 6 is designed to better serve densely populated zones, such as stadiums, hotels and convention centers.

Question 2:

Answer:

⇨ **Issues:**

Some of the main wireless networks issues are following:

Emerging Security Standards and Technologies:

Security is a big concern in wireless networking, especially in m-commerce and e-commerce applications. Mobility of users increases the security concerns in a wireless network. Current wireless networks employ authentication and data encryption techniques on the air interface to provide security to its users.

Wireless LAN Securities:

With the proliferation of inexpensive wireless technology, trying to maintain security has become an interesting challenge for most network administrators. The most serious challenges in securing wireless networks come from two areas:

laptop or other WIFI device can tap into your bandwidth without so much as sending you a thank-you note for the free Internet access. Even more disturbing is that such a hijacker could gain access to your internal network resources through an unsecured WAP.

The Wired Equivalent Privacy (WEP) protocol, previously the standard for wireless encryption, has been "broken" and is only really useful as a means of thwarting casual eavesdropping on a wireless connection, not to prevent the actions of a determined attacker.

Basic Security Issues:

Depending on the size of your network, there are still several measures that you can take to protect your wireless implementation. For a home installation or a network without a server or Active Directory installation.

- ## Challenges:

  Since wireless devices need to be small and wireless networks are bandwidth-limited, some of the key challenges in wireless networks are:

Enhancing Data Rate:

Improving the current data rates to support future high speed applications is essential, especially, if multimedia service is to be provided. Data rate is a function of various factors.

Low Power Design:

The size and battery power limitation of wireless mobile devices place a limit on the range and throughput that can be supported by a wireless LAN. Restricted access in the wired portion of a LAN also affects the throughput.

Improving Performance:

If Windows ever notifies you about a weak signal, it probably means our connection is not as fast or as reliable as it could be. Worse, we might lose our connection entirely in some parts of our home.

Question 3:

Answer:

IEEE 802.11:

802.11 and 802.11x refers to a family of specifications developed by the IEEE for **w**ireless ***LAN*** (WLAN) technology. 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients. The IEEE accepted the specification in 1997.

There are several specifications in the 802.11 family:

- **802.11:** applies to wireless LANs and provides 1 or 2 Mbps transmission in the 2.4 GHz band using either frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS).
- **802.11a:** an extension to 802.11 that applies to wireless LANs and provides up to 54-Mbps in the 5GHz band. 802.11a uses an orthogonal frequency division multiplexing encoding scheme rather than FHSS or DSSS.
- **802.11b:** (also referred to as 802.11 High Rate or Wi-Fi) — an extension to 802.11 that applies to wireless LANS and provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1-Mbps) in the 2.4 GHz band. 802.11b uses only DSSS. 802.11b was a 1999 ratification to the original 802.11 standard, allowing wireless functionality comparable to Ethernet.
- **802.11e:** a wireless draft standard that defines the Quality of Service (QoS) support for LANs, and is an enhancement to the 802.11a and 802.11b wireless LAN (WLAN) specifications. 802.11e adds QoS features and multimedia support to the existing IEEE 802.11b and IEEE 802.11a wireless standards, while maintaining full backward compatibility with these standards.
- **802.11g:** applies to wireless LANs and is used for transmission over short distances at up to 54-Mbps in the 2.4 GHz bands.
- **802.11n:** 802.11n builds upon previous 802.11 standards by adding ***m****ultiple-****i****nput* ***m****ultiple-****o****utput* (MIMO). The additional transmitter and receiver antennas allow for increased data throughput through spatial multiplexing and increased range by exploiting the spatial diversity through coding schemes like Alamouti coding. The real speed would be 100 Mbit/s (even 250 Mbit/s in PHY level), and so up to 4-5 times faster than 802.11g.

- **802.11ac:** 802.11ac builds upon previous 802.11 standards, particularly the 802.11n standard, to deliver data rates of 433Mbps per spatial stream, or 1.3Gbps in a three-antenna (three stream) design. The 802.11ac specification operates only in the 5 GHz frequency range and features support for wider channels (80MHz and 160MHz) and beamforming capabilities by default to help achieve its higher wireless speeds.

- **802.11ac Wave 2:** it is an update for the original 802.11ac spec that uses MU-MIMO technology and other advancements to help increase theoretical maximum wireless speeds for the spec to 6.93 Gbps.

- **802.11ad:** 802.11ad is a wireless specification under development that will operate in the 60GHz frequency band and offer much higher transfer rates than previous 802.11 specs, with a theoretical maximum transfer rate of up to 7Gbps.

- **802.11ah:** 802.11ah is the first Wi-Fi specification to operate in frequency bands below one gigahertz (900 MHz), and it has a range of nearly twice that of other Wi-Fi technologies. It's also able to penetrate walls and other barriers considerably better than previous Wi-Fi standards.

- **802.11r:** 802.11r, also called *Fast **B**asic **S**ervice **S**et* (BSS) Transition, supports Vo-WIFI handoff between access points to enable VoIP roaming on a Wi-Fi network with 802.1X authentication.

- **802.1X:** Not to be confused with 802.11x (which is the term used to describe the family of 802.11 standards) 802.1X is an IEEE standard for port-based Network Access Control that allows network administrators to restricted use of IEEE 802 LAN service access points to secure communication between authenticated and authorized devices.

----------End----------