Cape Peninsula University of Technology

Course:	COMMUNICATIONS NETWORKS FOUNDATIONS 1
Course code:	CNF150S/151S/152S
Lecturer/s:	Rebecca Dzidzai Bure, Tabisa Ncubukezi, Zukile Ndyalivana, Israel Christian Tchouya'a Ngoko, Nomawethu Tungela
Term 3 assessment:	Based on Chapter 6
Total:	100 marks
Weight:	30%
Due Date:	**Sunday, 25 August 2024**

Name and surname	**Student number**	**Contribution**
Mogamat Yaseen Kannemeyer	**240453182**	Scenario 1
Malik Muhammed	**230388175**	Scenario 2
Siyalezo Mbuyisa	**221789812**	Scenario 3
Hlanganani Mkhwanazi	**221814701**	Scenario 4
Katlego Malaka	**230443370**	Scenario 5
Mbongeleni Sibaya	**N/A**	NO CONTRIBUTION

Scenario: Imagine you are tasked with designing a wireless network for a large office building. The building has multiple floors, thick concrete walls, and various electronic devices that could interfere with the signal. Understanding RF propagation is crucial for your design.

When tasked with designing a wireless network for a large office building, especially one with multiple floors and thick concrete walls, it is essential to consider various factors that affect RF (Radio Frequency) propagation. Below are several questions that can guide the design process:

Done by: MOGAMAT YASEEN KANNEMEYER, **Student Number:** 240453182

1. **What is the layout of the office building?**

Given the building's construction, the thick concrete walls present significant obstacles to RF propagation, causing signal attenuation as the wireless signal weakens when moving away from the transmission source. Additionally, electronic devices like printers, microwaves, and security systems, predominantly located in areas such as the staff kitchen and IT room, pose a risk of interference, which could degrade the Signal-to-Noise Ratio (SNR).

- **Wireless Network Design:**
  a) Line of Sight (LOS) Considerations:

Wireless signals primarily travel in a straight line from the transmitter to the receiver. However, thick walls and obstacles can cause the signal to fade, potentially leading to dropped connections or slow data transmission.

b) Multipath Signal Propagation:

In this environment, wireless signals may follow multiple paths to their destination. While this increases the likelihood of the signal reaching its intended receiver, it can also cause signal delay and potential data errors due to multipath interference.

c) Correcting Signal Issues:

To address signal attenuation and interference, a combination of Infrastructure and Mesh Topologies should be utilized. The infrastructure topology allows for centralized management through strategically placed Wireless Access Points (WAPs) on each floor, ensuring optimal coverage and integration with the existing wired network.

Mesh topology adds reliability by creating redundant paths, enhancing coverage in areas where signals are weaker.

2. **What frequency bands will be used for the wireless network?**

Using both 2.4 GHz and 5 GHz bands will optimize wireless network performance throughout the large office building. The 2.4 GHz band will provide coverage through thick concrete walls and reach obstructed areas, making it suitable for long-range devices like IoT sensors and basic peripherals. Meanwhile, the 5 GHz band will support high-speed data transfer and bandwidth-intensive applications, such as video conferencing and file transfers, in high-density areas. Integrating these bands with dual-band access points and effective network management ensures robust coverage and high performance, leveraging the strengths of both frequencies for efficient connectivity throughout the building.

3. **What type of access points (APs) will be deployed?**

Dual-band access points that support both 2.4 GHz and 5 GHz frequencies should be used for coverage and performance. APs like the Ubiquiti UniFi AP AC Pro and Cisco Catalyst 9100 Series are suitable for business environments. High-power and outdoor-rated APs, such as the Aruba Networks AP-377 and Ruckus ZoneFlex T300, can enhance signal strength and penetration. Mesh access points, like the Meraki MR36 and EnGenius EWS357AP, will extend coverage and improve reliability by creating redundant paths. Managed access points with centralized control will facilitate efficient network management, including channel management and load balancing. Additionally, APs with CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) support will minimize collision risks and enhance throughput. This approach will effectively address challenges posed by thick walls and RF interference

4. **What tools or methods will you use to conduct site surveys?**

To conduct site surveys for designing a wireless network in a large office building with multiple floors and thick concrete walls, we will use the following tools and methods:

- **Spectrum Analyzer**: This tool assesses the quality of the wireless signal, identifies interference, and measures signal strength. It helps in evaluating the effects of attenuation, signal loss, and noise.
- **Wireless Analyzer (Wi-Fi Analyzer)**: This tool evaluates Wi-Fi network availability, optimizes Wi-Fi signal settings, and identifies security threats. It measures signal strength, ensures proper association and reassociation between APs, captures and interprets traffic, and assesses data transmission errors.

By using these tools, we can accurately identify access points, measure signal strength, analyze channel characteristics, and optimize network performance to address RF propagation challenges in the building.

5. **How many access points are needed to ensure adequate coverage?**

To determine the number of access points (APs) required for adequate coverage in a large office building with multiple floors and thick concrete walls, we start by Estimate the coverage area per AP, which is typically around 30-46 meters indoors for dual-band models like the Ubiquiti UniFi AP AC Pro. Divide the total floor area by this coverage estimate to calculate the number of APs needed per floor, adding extra APs to account for coverage reduction due to thick walls and floors then we adjust for potential RF interference and ensure comprehensive coverage. For a large office building with multiple floors and thick concrete walls, an estimated total of **around 40 access points** may be needed.

6. **What security measures will be implemented in the wireless network?**

In designing the wireless network for a large office building with multiple floors, thick concrete walls, and potential RF interference, security will be addressed by the following. WPA2/WPA3 encryption will be implemented, with WPA2-Enterprise and a RADIUS server providing maximum security. Strong authentication methods will ensure only authorized devices gain access, while MAC address filtering will block unauthorized devices. A separate guest network, protected by a captive portal, will isolate guest traffic from the main network. Managed access points with centralized control will streamline network management and monitoring. To safeguard against common attacks like war driving and evil twins, security protocols will be regularly updated, and vulnerability assessments will be conducted.

7. **How will you monitor and maintain the wireless network post-deployment?**

Post-deployment, the wireless network will be monitored and maintained by utilizing centralized management tools like Cisco Meraki Dashboard or Ubiquiti UniFi Controller for real-time performance insights and access point management. Key metrics such as signal strength, bandwidth usage, and throughput will be continuously tracked to identify and address weak coverage or interference. Firmware updates will be applied regularly to ensure security and performance improvements. Periodic security audits will be conducted to identify vulnerabilities and ensure compliance with security protocols. User feedback will be collected to address connectivity issues and improve the user experience, while a responsive support system will quickly resolve any problems based on network monitoring data.

Scenario: When consulting a small business looking to set up a wireless network, it is crucial to consider various factors that will influence the choice of network topology.

Done by: MALIK MUHAMMED, **Student Number:** 230388175

1. **What is the size of the office space?**

- **Small (less than 100 square meters):**

Single access point (AP) may suffice

- **Medium (100-500 square meters):**

Multiple APs required for adequate coverage

- **Large (over 500 square meters):**

More APs and potential need for wireless controllers

2. **How many devices will be connected to the network?**

- **Fewer than 10 devices:**

Basic network infrastructure sufficient

- **10-50 devices:**

Mid-range network infrastructure with redundancy

- **Over 50 devices:**

Advanced network infrastructure with high-capacity APs

3. **What are the specific networking needs of the business?**

- **Basic internet access:**

Simple network topology

- **High-bandwidth applications (e.g., video conferencing):**

Advanced network topology with Quality of Service (QoS)

- **Secure data transfer:**

Network topology with robust security features (e.g., firewalls, encryption)

4. **What is your budget for setting up and maintaining the wireless network?**

- **Limited budget (<R10,000):**

Basic network setup with minimal features

- **Moderate budget (R10,000-R50,000):**

Mid-range network setup with standard features

- **Extensive budget (>R50,000):**

Advanced network setup with premium features and support

5. **Are there any physical barriers in the office space that could affect signal strength?**

- **Walls, floors, and ceilings:**

Potential signal degradation; strategic AP placement necessary

- **Glass, wood, or plaster:**

Minimal signal impact; standard AP placement sufficient

6. **What level of scalability do you anticipate needing in the future?**

- **Low scalability needs:**

Basic network infrastructure sufficient

- **Medium scalability needs:**

Mid-range network infrastructure with redundancy

- **High scalability needs:**

Advanced network infrastructure with high-capacity APs and wireless controllers

7. **What type of wireless technology do you want to implement?**

- **Wi-Fi 5 (802.11ac):**

Suitable for most small businesses

- **Wi-Fi 6 (802.11ax):**

Ideal for high-density environments or futureproofing

8. **How important is redundancy and reliability in your network setup?**

- **Basic redundancy:**

Single AP and switch sufficient

- **Advanced redundancy:**

Multiple APs, switches, and redundant links for high uptime

Scenario: A local café wants to provide Wi-Fi access for customers but is concerned about security risks associated with open networks.

When considering the scenario where a local café wants to provide Wi-Fi access while addressing security risks associated with open networks, several questions can be formulated to guide the café's decision-making process. Below are detailed questions that can help assess the situation comprehensively.

Done by: SIYALEZO MBUYISA, **Student Number**: 221789812

1. **What are the specific security risks associated with providing an open Wi-Fi network?**

Common risks include unauthorized access, malware, and data theft.

2. **What measures can be implemented to enhance the security of the café's Wi-Fi network?**

I would implement WPA2-PSK encryption, a guest network, and a captive portal to ensure secure authentication and encryption.

3. **How will customer privacy be protected while using the café's Wi-Fi?**

I would implement a privacy policy and ensure that customer data is not stored or shared.

4. **What type of authentication will be used for accessing the Wi-Fi?**

I would use a captive portal with a simple authentication mechanism (e.g., username/password).

5. **How will the café handle potential legal liabilities associated with providing public internet access?**

The café would need to have a terms of service agreement and ensure compliance with local laws and regulations.

6. **What feedback mechanisms will be in place for customers regarding their experience with the Wi-Fi service?**

I would implement a feedback system (e.g., surveys, comment cards) to ensure customer satisfaction.

Scenario: You're setting up a wireless network in an urban area where many competing signals exist from nearby businesses and residential buildings.

Done by: HLANGANANI MKHWANAZI, **Student Number:** 221814701

1. **What frequency band should be used?**

Since many competing signals exist, operating in the 5 GHz band would be preferable. This band offers more channels and typically experiences less interference than the 2.4 GHz band, making it more suitable for crowded environments.

2. **How will you conduct a site survey to assess signal strength and interference?**

A site survey can be conducted using specialized tools like Wi-Fi analyzers (e.g., Ekahau or NetSpot). These tools will help map the signal strength and identify interference sources by measuring the Received Signal Strength Indicator (RSSI) and signal-to-noise ratio (SNR) across the area.

3. **What type of wireless technology (e.g., Wi-Fi 5, Wi-Fi 6) will best suit the environment?**

Wi-Fi 6 (802.11ax) is recommended as it provides better performance in dense environments through features like MU-MIMO (Multi-User Multiple Input Multiple Output), improved speed, and increased capacity, making it ideal for busy urban settings.

4. **How many access points (APs) will be required to ensure adequate coverage?**

The number of APs required will depend on the specific layout and dimensions of the area but generally, conducting a preliminary coverage assessment through the site survey will provide insights. A starting estimate might range from 3 to 5 APs for moderate-sized urban areas, but this should be confirmed with detailed planning.

5. **What channel selection strategy will you implement to minimize interference from neighboring networks?**

Implementing automatic channel selection (where possible) using dual-band capability allows APs to choose the least congested channels in the 5 GHz band. Manually selecting non-overlapping channels such as 36, 40, 44, 48, 149, 153, 157, or 161 can also help minimize interference.

6. **How will you secure the wireless network against unauthorized access?**

Utilize WPA3 security protocols for robust encryption. Incorporate MAC address filtering, network segmentation, and strong, unique passwords for access points. Regularly updating passwords and firmware will also bolster security.

7. **What measures will be taken to manage bandwidth effectively among users?**

Implementing Quality of Service (QoS) policies will help prioritize traffic, ensuring that bandwidth is allocated fairly among users. Traffic shaping and bandwidth limits can be imposed on less critical applications to ensure that high-priority applications (such as VoIP) receive adequate resources.

8. **How will you monitor network performance and troubleshoot issues post-deployment?**

Continuous monitoring can be achieved using network management software. Solutions like Cisco’s DNA Center or other cloud-managed services can provide insights on performance metrics, user experience, and alerts for troubleshooting.

9. **Are there any local regulations or restrictions regarding wireless signal transmission that need to be considered?**

It's essential to consult the FCC regulations (or pertinent local governing bodies) concerning allowable frequencies and power output. Ensure compliance with local zoning laws that might affect wireless infrastructure deployment.

10. **What backup solutions or redundancy plans are in place if the primary network fails?**

Implementing redundant internet connections (e.g., using separate ISPs) along with hot standby configurations for access points and backup power supplies (like UPS) will ensure service continuity in the event of a primary network failure.

Scenario: A retail store wants reliable Wi-Fi coverage throughout its premises including outdoor areas where customers often gather near entrances.

Done by: KATLEGO MALAKA**, Student Number**: 230443370

1. **How do you ensure seamless roaming for mobile devices in a wireless network?**

- **Multiple Access Points:** to ensure that as a user moves, their device can connect to the nearest AP with the strongest signal.
- **Wi-Fi Band Management**: To lessen interference and boost efficiency, make use of both the 2.4 GHz and 5 GHz bands. Higher speeds and fewer interference are provided by the 5 GHz range, which is advantageous in densely populated locations.
- **Advanced roaming protocols**: Use protocols like 802.11k, 802.11r, and 802.11v. These let devices travel more efficiently by enabling them to decide when to switch APs and to do so more rapidly. Faster handovers are made possible by these standards, which also give client devices information about network conditions.
- **Network Management and Monitoring:** To keep an eye on the wireless network's performance, use network management tools. This enables real-time modifications to maximize coverage and performance, such as adjusting AP power levels or channels.

Distribute client connections among APs equally by using Load balancing techniques. This keeps any one AP from being overwhelmed, which might impair roaming capabilities and cause performance to suffer.

2. **Explain the concept of multiuser MIMO and how it can enhance the capacity of wireless networks**

Using the same frequency band, MU-MIMO uses spatial multiplexing to provide various data streams to numerous devices simultaneously. By taking use of the spatial variety offered by the several antennas at the transmitter and reception ends, this is accomplished.

- **Enhanced Capacity:** MU-MIMO, as opposed to conventional single-user MIMO systems, greatly expands the network capacity by providing simultaneous service

to many users. When several devices are linked to the same AP in crowded areas, this is very helpful.

- **Greater Utilization of Available Spectrum:** MU-MIMO increases spectral efficiency by permitting multiple users to reuse frequencies, which results in a better use of the available spectrum.
- **Improved User Experience:** Due to MU-MIMO's simultaneous transmission capabilities, users even in crowded places enjoy quicker data rates and lower latency.
- **Energy Efficiency:** MU-MIMO systems can function more effectively and consume less power by directing energy toward certain users rather than disseminating signals generally.

3. What is 5G and how does it work?

- **Enhanced Speed and Capacity:** 5G uses higher frequency bands, including millimeter waves, to provide substantially faster speeds than previous generations (up to 10 Gbps under ideal circumstances). Faster downloads, more fluid streaming, and enhanced overall performance are all made possible by this increased speed.
- **Network Slicing**: Network slicing, introduced by 5G, enables the development of virtual networks customized to requirements or services.
- **Enhanced Connectivity and Capacity:** Compared to 4G, 5G can support many more concurrent connections per square kilometer. Supporting the increasing number of Internet of Things (IoT) devices and guaranteeing dependable service even in highly populated regions need this.
- **Low Latency:** The time it takes for data to move from its source to its destination is known as latency, and 5G dramatically lowers it. As opposed to about 30 milliseconds in 4G, latency in 5G can be as low as 1 millisecond. Applications like driverless cars and remote surgery that demand real-time reactions depend on this low latency.
- **Edge Computing:** Edge computing capabilities are integrated into 5G networks, which move computational resources closer to the end users. This lowers latency and facilitates real-time applications such as autonomous driving and virtual reality (VR)

4. **Explain in detail about IEEE 802.11 Architecture and Protocols**

Architecture:

- **Stations (STAs):** Devices that connect to the wireless network, such as laptops, smartphones, and tablets.
- **Access Points (APs):** Devices that provide wireless connectivity to the network and act as a bridge between the wired network and wireless devices.
- **Service Set Identifier (SSID):** A unique identifier (name) for a wireless network that allows devices to identify and connect to the appropriate network.

Protocols:

- **802.11i:** This protocol uses WPA2 (Wi-Fi Protected Access II), which has more robust encryption techniques than earlier standards, to provide increased security.
- **802.11r:** This protocol makes it easier for access points to handoff quickly, which is essential for smooth roaming.
- **802.11k/v:** These protocols help with improved roaming decisions and network performance, as well as network administration and optimization.

5. **Compare security issues in Wireless networks with wired networks**

- **Vulnerability to Eavesdropping:** Wireless transmissions are more vulnerable to eavesdropping and illegal access than connected connections because they are easier to intercept.
- **Authentication Difficulties:** Shared keys, which are frequently used by wireless networks for authentication, might be exploited if improperly maintained. Wired networks, on the other hand, usually employ physical security measures that are more difficult to get around.

Attackers could install rogue access points (APs) that imitate authentic ones to fool users into joining and disclosing personal information.

- **Risks to Data Integrity:** Signal deterioration and interference are increasingly common in wireless networks, which can compromise data integrity. These

hazards are decreased by wired networks, which maintain a more solid connection.