COMMUNICATION NETWORKS FOUNDATIONS

CHAPTER 6 ASSIGNMENT

GROUP 30

STEPHANIE TOLA OLUWAFEMI LEWU (230211216)

HLOMLA MAGOPENI (218070349)

ANGEL DINEO MASONGANYE (223008869)

NONDUMISO NKOSINOLWAZI NGOBESE (222703768)

TEBOGO PII (230226442)

OLWETHU TSHINGILANE (

TABLE OF CONTENTS

- Scenario 1
- Scenario 2
- Scenario 3
- Scenario 4
- Scenario 5

SCENARIO 1

1. The office building's layout:

There are six floors.

Wall Thickness and Materials: The structure's steel framing and thick concrete walls are crucial to its security and longevity, but they also have a big effect on the spread of wireless signals. There are large glass windows, however they might be coated with metal, which would further weaken the signal.

Effect on Coverage and Signal Propagation:

Walls Made of Concrete: Signal strength is decreased by the thick concrete walls, especially when the signal passes through several floors or walls.

Steel Framing: Weak signal strength patches and reflections can be produced by the steel framework.

Glass Panes: Glass permits some transmission of the signal, but any metallic covering will further impede the signal.

In order to overcome these obstacles, thoughtful frequency band selection and access point placement are needed to guarantee reliable.

2. Frequency Bands

   2.4 GHz Band and 5 GHz Band

3. Type of Access Points (APs):
   Ceiling-Mounted Aps

4. . Site Surveys:
   Wireless Site Tools: The Wi-fi Analysers

5. . Number of Access Points:
   *Require roughly 3–4 access points per floor, for a total of 18–24 access points across the building, to guarantee sufficient coverage.

6. Security Measures:

WPA3 encryption on the wireless connection. This guarantees that all information sent across the network is safely encrypted, guarding against prying eyes and illegal access.

7. Monitoring and Maintenance After Deployment:

Tool for Network Monitoring: Use SolarWinds Network Performance Monitor to track network performance over time, spot issues, and receive alerts.

SCENARIO 2

Wireless Network Design for Woodstock Web Wizards

Business Name: Woodstock Web Wizards

Location: Woodstock, Cape Town

1.The office space for Woodstock Web Wizards spans approximately 150 square meters. The layout consists of an open-plan area with a few partitioned sections, including private offices and meeting rooms. Given the modest size of the space, the design of the wireless network will focus on ensuring consistent signal strength throughout the entire office.

2.The network currently has 25 devices, but growth is expected to reach 40-50 within two years. The network design must accommodate this increase without compromising performance. Additional APs can be added as needed.

3.Specific networking needs of the business are that the business relies heavily on high-speed internet for tasks such as video conferencing, cloud-based services, and large file transfers. The network must support secure remote access for employees who may need to work from home. In order to meet these demands, the network architecture will incorporate routers and high bandwidth access points that can support several connections concurrently without degrading service quality.

4. About R150 000 will be needed for wireless network setup during the initial phase of implementation. A yearly budget of about R20,000 is also set aside for upgrades and maintenance.

5.Yes there are, office environment's partition walls and electronic devices could impact signal propagation. To address these issues, a site survey will determine optimal AP placement and emphasize the use of the 5 GHz frequency band for stable connections.

6. The company plans to expand operations within two years, potentially increasing connected devices to 0-50. To accommodate this growth, the network will be designed with scalability using modular components, ensuring performance and reliability.

7. Wi-Fi 6 because it offers enhanced performance, capacity, and data rates, enhancing performance in high-bandwidth applications and managing multiple connections, ensuring network efficiency and capacity for business growth.

8**.** The network design prioritizes redundancy and reliability, incorporating dual internet connections from different ISPs for failover, redundant power supplies for routers and switches, and advanced network management tools for proactive maintenance and rapid troubleshooting.

SCENARIO 3

1.

- Man-in-the-Middle attacks allow attackers to manipulate user data without user consent, leading to potential theft.
- Illegal access to wireless networks enables criminals to use the network for illegal activities such cyberattacks.
- Insecure wireless hotspots: cybercriminals have the ability to create phony wireless hotspots that imitate real ones and fool users into connecting to them. The goal of these rogue networks is to steal user information.

2.

- Deploy WPA3 Encryption
- Segment the Network
- Firewall and Intrusion Detection Systems (IDS) Installation.

3.To ensure the data passed over the Wi-Fi network is not accessed by unauthorized hands and information about a client intercepted, WPA2 or WPA3 encryption is used. Utilize a captive portal for Wi-Fi access control and user authentication, requiring users to agree to terms of service and provide basic information, enhancing privacy and accountability

Increase user awareness about secure Wi-Fi practices, such as VPNs and avoiding crucial transactions, to promote privacy and ensure secure online transactions.

4.

- Password-Protected Access
- Email-Based Login,
- User Authentication

5. To ensure a secure Wi-Fi network, create a clear Terms of Service (ToS) contract that customers must approve before using the network. Keep log retention policies to follow legal rules and help law enforcement. Seek legal consultation to ensure compliance with local laws, data protection regulations, and potential network misuse management.

6.The text suggests implementing in-network surveys to gather user feedback on their Wi-Fi experience, identifying issues like slow speeds or connection interruptions. It also suggests a customer support feature on the Wi-Fi landing page for quick problem resolution. The captive portal should feature feedback forms for immediate feedback and problem resolution, enhancing the overall user experience. These strategies aim to improve the Wi-Fi experience.

SCENARIO 4

Wireless Network Setup in a High-Interference Urban Area

Business Name: NS Electro-tech Solutions

Location: City Centre, Cape Town

1. The 5 GHz frequency band is ideal for NS Electro-Tech Solutions due to its reduced interference and larger data rates, making it the optimal choice for urban locations with high population density. Despite its shorter range compared to the 2.4 GHz band, it offers more channels and supports larger data rates.

2. A site inspection will be conducted using programs like Ekahau or NetSpot to measure signal strength and identify interference sources. The signal-to-noise ratio will be measured, and the office space will be mapped for Access Points. A heatmap will be created to optimize coverage and reduce dead zones, identifying strong and weak signals.

3. NS Electro-tech recommends Wi-Fi 6 (802.11ax) for deployment in heavily disturbed environments. This wireless technology is ideal for high-density settings with numerous devices and conflicting signals. It supports BSS Colouring and OFDMA for better efficiency and reliability, making it ideal for densely populated metropolitan regions.

4. NS Electro-tech Solutions office needs 4 to 6 Access Points (APs) for adequate coverage, based on site survey results and office size. AP placement will be guided by heatmap, ensuring robust coverage and reducing overlap and interference.

5. The network uses dynamic channel selection to reduce interference from neighbouring networks. APs analyse the surrounding RF environment and automatically choose the least congested channels in real-time. Avoid nearby

networks and use non-overlapping channels in the 2.4 GHz band or 5 GHz band. This reduces interference and ensures stable network performance.

6.In an urban environment, unauthorized access poses a significant security threat. To address this, data transmissions will be encrypted using WPA3, the latest Wi-Fi encryption standard, and separated from guest traffic using multiple VLANs. A RADIUS server will provide centralized authentication, further preventing unauthorized access. Regular security audits and updates will ensure protection against emerging threats.

7. Efficient bandwidth management ensures consistent network performance during peak consumption hours. Networks apply QoS regulations prioritizing traffic, like VoIP and video conferencing for corporate applications. Load balancing between APs and client isolation prevent excessive bandwidth usage. Bandwidth throttling prevents excessive bandwidth consumption, ensuring fair distribution among users. This approach maintains network efficiency and performance in high-density environments.

8. Continuous monitoring is crucial for network operation post-installation. Tools like Ubiquiti Uni-Fi and Cisco Prime monitor network health, bandwidth utilization, and identify performance issues. Real-time notifications and cloud-based solutions aid in troubleshooting. Regular performance audits evaluate network effectiveness and make necessary adjustments.

9. NS Electro-tech Solutions will comply with ICASA regulations in Cape Town and South Africa for wireless signal transmission, using Dynamic Frequency Selection channels to avoid interference with radar systems and avoid potential fines or disruptions.

10. NS Electro-tech Solutions plans to implement robust redundancy measures, including dual internet connections, failover capability, duplicate power supplies, and offsite backups for network configurations. These measures aim to minimize downtime and ensure uninterrupted operations, ensuring uninterrupted operations even in the event of a network failure.

SCENARIO 5

Wireless Deployment for a retail store with Indoor and Outdoor coverage

Business Name: "Urban Threads Retail"

Location: V&A Waterfront, Cape Town

1. - Use of Multiple Access Points (APs): Multiple APs with overlapping coverage areas will be deployed to allow devices to seamlessly transition between APs without losing connection, with a focus on preventing dead zones near the store entrances where customers gather.

- Fast Roaming Protocols: Implementation of 802.11r (Fast BSS Transition) to enable quick roaming between APs without the need for reauthentication, reducing latency and providing a smoother user experience for mobile devices.

- VLAN Segmentation: a network technique that would ultimately divide the physical network of our retail store's Wi-Fi coverage via multiple, isolated logical networks.

- AP Placement and Signal Strength Optimization: Strategically placing APs to cover indoor and outdoor areas, along with utilizing high-gain antennas in outdoor areas to extend range and maintain strong connections.

- Band Steering: Using band steering to direct dual-band devices to the less congested 5 GHz band, leaving the 2.4 GHz band for legacy devices, thereby optimizing performance.

2.Subsequently, we shall discuss MU-MIMO, its impact on wireless network capacity, and other important aspects, such as:

-MU-MIMO Technology: This increases capacity by using all of the AP's antennas to let many devices to receive their individual data streams at the same time.

- Capacity Enhancement: Enhanced wireless capacity overall, making effective use of available bandwidth to enable simultaneous communication of several devices, particularly in high-density settings like retail stores.

3**.** Firstly the term ‘5G’ stands for the ‘5th generation wireless mobile network’. This means that it is the latest and most reliable global network following the likes of 3G and 4G. For lack of better words, it is a gamer changer in terms of mobile communication. Some of the improved qualities of 5G (compared to the previous generations include:

- Ultra-Reliable Low-Latency Communication (URLLC): good for precise and time efficient communication. Provides reliable low-latency and mission-critical applications.

- Faster speed: can transmit more bits per second (up to 20 Gbps per second). Ideal for streaming and gaming.

- Enhanced Mobile Bandwidth (eMBB): offers speedy mobile bandwidth for better user experience (e.g. 4K video streaming and Virtual Reality)

- Widespread Interconnection: able/built to withstand up to 1 million devices per square kilometres

- Milli meter Waves and Small Cells: By placing small cells across densely populated metropolitan areas, it provides coverage over a minuscule geographic region. High data speeds might be achieved with milli meter waves.

4. Another name for the Institute of Electrical and Electronic Engineers is IEEE. IEEE is a set of standards for WLANs based on these four factors:

- Station (STA): Hardware (such as laptops and cell phones) that is connected to the WLAN.

- One AP and the STAs it is attached to make up the Basic Service Set (BSS).

- Extended Service Set (ESS): A Distribution System (DS) connects several BSSs.

- Access Point (AP): Bridges between STAs and the wired network.

The 802.11 is essentially This is the number assigned to the IEEE Working Group on LANs.

5. A wireless network is a computer network system that uses wireless communication protocols to connect devices, while wired network enables the use of physical cables/wires. Common security issued faced with wired and wireless networks include:

- Viruses and Malware: corrupt software introduced to network via infected devices, visiting malicious sites and downloading infected software downloads.

- Insider threats: malicious individuals with access to network can infect the network

- Weak encryption: specifically in terms of wired networks; weak encryptions can allow for easy access to the leaking of sensitive information to outsiders.

-Phishing and social engineering: malicious people can employ techniques like email and SMS links to fool consumers into disclosing private information or downloading malware.

- Inadequate Monitoring and tracking: It may be challenging to identify and address security events in the absence of adequate monitoring and tracking.