2024

CNF Wireless Networks Assignment

Njanyana Xaba

223056359

25/08/2024

Table of Content

Scenario 1: 4

1.What is the layout of the office building? [8] 4

2. What frequency bands will be used for the wireless network?[2] 5

3. What type of access points (APs) will be deployed?[2] 5

4. What tools or methods will you use to conduct site surveys? [2] 5

5. How many access points are needed to ensure adequate coverage?[2] 5

6. What security measures will be implemented in the wireless network?[2] 6

7.How will you monitor and maintain the wireless network post-deployment?[2] 6

Scenario 2: 6

1.What is the size of the office space? [3] 6

2. How many devices will be connected to the network? [3] 6

3. What are the specific networking needs of the business? [3] 7

4. What is your budget for setting up and maintaining the wireless Network? [2] 7

5. Are there any physical barriers in the office space that could Affect signal strength? 7

6. What level of scalability do you anticipate needing in the future? [2] 7

7. What type of wireless technology do you want to implement? [2] 7

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

Scenario 3: 8

1. What are the specific security risks associated with providing an open Wi-Fi network? [3] Understanding the potential vulnerabilities is crucial. Common risks include: 8

2. What measures can be implemented to enhance the security of the café's Wi-Fi network? [3] 8

3. How will customer privacy be protected while using the café's Wi-Fi? [3] 8

4. What type of authentication will be used for accessing the Wi-Fi? [3] 9

5. How will the café handle potential legal liabilities associated with providing public internet access? [3] 9

6. What feedback mechanisms will be in place for customers regarding their experience with the Wi-Fi service? [3] 9

Scenario 4: 9

1. What frequency band should be used? [2] 9

2. How will you conduct a site survey to assess signal strength and interference? [2] 10

3. What type of wireless technology (e.g., Wi-Fi 5, Wi-Fi 6) will best suit the environment? [2] 10

4. How many access points (APs) will be required to ensure adequate coverage? [2] 10
5. What channel selection strategy will you implement to minimize interference from neighbouring networks? [2] 10
6. How will you secure the wireless network against unauthorized access? [2] 10
7. What measures will be taken to manage bandwidth effectively among users? [2] 11
8. How will you monitor network performance and troubleshoot issues post-deployment? [2] 11
9. Are there any local regulations or restrictions regarding wireless signal transmission that need to be considered? [2] 11
10. What backup solutions or redundancy plans are in place if the primary network fails? [2] 11
Scenario 5: 11
1. How do you ensure seamless roaming for mobile devices in a wireless network? [5] . 11
2. Explain the concept of multiuser MIMO and how it can enhance the capacity of wireless networks. [5] 12
3. What is 5G and how does it work? [5] 12
4. Explain in detail about IEEE 802.11 Architecture and Protocols. [5]..... 12
5. Compare security issues in Wireless networks with wired network? [5]..... 13

Term 3 Assessment Based on Chapter 6

Scenario 1:

1.What is the layout of the office building? [8]

To find out the layout of the office: we would contact the building management or the people in charge to get the floor plans or the blueprint and a Site Survey needs to be conducted incase blueprints are not available, we would require to assess the client requirement, walk through the building to note the locations of walls, doors, windows. If any existing cabling infrastructure and identify area that would require most coverage and those area that would be more complex to bring the coverage. A thorough site survey will have a look on whether Wi-Fi access points will be used as wireless bridges to create remote wired access to the network and to determine whether certain floors require multiple Aps. Measure the signal coverage and strength from other WLANs, we would perform different test proposed access point locations and wireless access from the farthest corners of your space to avoid an disappointments. The survey will also include a consideration the materials used in objects that aren't always present in the environment and consider how the wireless portions of the LAN will integrate with the wired portions

Having a look at our survey result, we must consider where the building possesses it thick walls, for a better positioning of the radio frequency propagation, due to fact that it can cause an absorption and also reflect on the frequency propagation around the building. Therefore our goal would be to strategically ensure coverage to the whole building by having taken those constraint into consideration, installing different access points would key based around the building but on the facts that we have multiple floors it would not be as efficient, though we could opt for a radio Line of Sight and Fresnel Zone, all the Aps must belong to the same ESS and an ESSID.

Ideas of the network designs

Access Point placements: it essentially advised to place the Aps centrally of each floor to ensure the whole floor is full cover. It guides to stimulate and optimize placement. Centralized wireless management is made possible by a lightweight wireless protocol such as Cisco's LWAPP (Lightweight Access Point Protocol) or Cisco's CAPWAP (Control and Provisioning of Wireless Access Points). A wireless controller can provide:

• Centralized authentication for wireless clients

• Load balancing

• Channel management

• Detection of rogue access points

Bands: since we would be developing for a multiple floor building, we should into consideration of channel planning, a non-overlapping channel to design or planned to reduce the co-channel interference, given it has 24 channels and has a 5GHz that ranges between 5.180 to 5.825. For better performance we could combine channels to create adjacent channels, called channel bonding.

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

Considering the design mentioned above we could use a dual-band APs that operate on both the 2.4 GHz and 5 GHz bands. The 2.4 GHz band has a longer range and better penetration through walls, but the 5 GHz band offers higher speeds and less interference

3. What type of access points (APs) will be deployed?[2]

An ESS will be deployed due to its ability to connect a group of access point to same LAN and share its ESSID, it also moves from one BSS to another without losing connectivity.

4. What tools or methods will you use to conduct site surveys? [2]

We will use the scanning methods surveys surroundings for access point. They are two kinds of Scans: **Active scanning** involves connecting to a network and measuring its performance, like throughput and packet loss. It's also known as a probe while a **Passive scanning** listens for special signal without connecting to the network and understand the radio frequency environment and identify source interference also known as a beacon fame.

5. How many access points are needed to ensure adequate coverage?[2]

That would depend on the:

• Distance

• Type and number of obstacles

• Coverage

• Interference

Because larger WLANs warrant a more systematic approach to access point placement

6. What security measures will be implemented in the wireless network?[2]

The security measure implemented would the: **WPA2** as preference because it's a replacement for **WPA**. It possesses a stronger encryption protocol and most secure communication is made possible by combining a radius server with **WPA/WPA2**, also known as WPA-Enterprise or WPA2-Enterprise. For extra security we could create a separate guest network/ Aps to corporate traffic.

7.How will you monitor and maintain the wireless network postdeployment?[2]

By installing software like: Spectrum analyser and Wireless analyser, both of this software tools would asse the quality of the wireless signal and will evaluate the network availability, optimize WI-FI signal and help identify the security threats.

Scenario 2:

1.What is the size of the office space? [3]

Size of the Office Space:

It is a small office environment; it may be sufficient to use a single access point to provide reliable and efficient network connectivity for all employees. This streamlined approach can simplify setup and management, reduce costs, and ensure consistent wireless coverage throughout the office space.

2. How many devices will be connected to the network? [3]

Number of Devices:

The number of devices that will be connected to the network is a key factor in determining the appropriate network topology. This includes considering:

Current Devices such as computers, printers, and other networked equipment that will be connected initially.

3. What are the specific networking needs of the business? [3]

Specific Networking Needs:

They are primary business applications (e.g., email, web browsing, VoIP) to determine bandwidth requirements and QoS needs.

Different applications have varying sensitivity to network latency and packet loss.

4. What is your budget for setting up and maintaining the wireless Network? [2]

Budget

The available budget dictates the choice of hardware, software, and potential professional services.

Balance cost with desired network performance and features.

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

Physical Barriers:

- Walls, furniture, and equipment can obstruct wireless signals.
- Optimize access point placement to minimize signal attenuation.

6. What level of scalability do you anticipate needing in the future? [2]

Scalability:

- Expected increase in employees
- Projected growth in customers or clients

- Expansion of the business

7. What type of wireless technology do you want to implement? [2]

Wireless Technology:

- Wi-Fi standard (e.g., 802.11ac, 802.11ax) based on coverage, speed, and device compatibility; Considering factors like range, data rate, and power consumption.

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

Redundancy and Reliability:

- Evaluates the business's tolerance for network downtime.
- Implement redundancy measures (e.g., failover, load balancing) if critical operations depend on the network.

Scenario 3:

1. What are the specific security risks associated with providing an open Wi-Fi network? [3] Understanding the potential vulnerabilities is crucial. Common risks include:

- Anyone within the connection range can connect to the Wi-Fi network which could lead to people misusing the Wi-Fi network.
- With open networks, the data transmitted can be easily intercepted by malicious people such as hackers or cyber terrorists which would put both customers and the café at risk.
- Attackers can use the open network to send malware to the connected devices which could put people's personal data at risk.

2. What measures can be implemented to enhance the security of the café's Wi-Fi network? [3]

- To create separate networks such as a guest network where customers can have access to the internet but not the businesses sensitive data.
- Use or implement WPA2 encryption to secure the network.
- Regularly update all network devices and software to protect against unknown vulnerabilities.

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

- By encouraging customers to utilize Virtual Private Networks (VPNs) for additional privacy.
- Having clear privacy policies where the café informs customers or users about data collection and usage policies.

4. What type of authentication will be used for accessing the Wi-Fi? [3]

The café could use either the **Captive Portal System** or the **Voucher System.**

- The **Captive Portal System** redirects connected users to a page which requires them to enter personal details such as an email address or cell phone number and require them to agree to terms and conditions.
- The **Voucher System** is where the café issues a voucher which a customer purchases that allows them to access the internet for a limited amount of time and provides controlled access to the café.

5. How will the café handle potential legal liabilities associated with providing public internet access? [3]

- To clearly outline the acceptable use policies and disclaimers for liabilities.
- Keep track/logs of user activity to help trace any illegal activities back to the source.
- Consult with legal experts to ensure compliance with local laws and regulations regarding public Wi-Fi.

6. What feedback mechanisms will be in place for customers regarding their experience with the Wi-Fi service? [3]

- The café will provide short surveys either online or physical so that users or customers can share their feedback.
- As an alternative the café can also give customers the platform to report issues, give feedback and recommend ways in which our service could be improved.

Scenario 4:

1. What frequency band should be used? [2]

- 5 GHz band because it offers more non-overlapping channels and is less congested compared to the 2.4 GHz band, which is commonly used by various devices and networks.

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

- By Carrying out a comprehensive site survey to identify high-interference and unstable signal including obtaining floor plans of the area, performing a physical walkthrough to identify potential sources of interference and Using Wi-Fi analysers like Netspot to measure signal strength and identify the least congested channels.

3. What type of wireless technology (e.g., Wi-Fi 5, Wi-Fi 6) will best suit the environment? [2]

- Wi-Fi 6 (802.11ax) is the most suitable choice, it has a greater efficiency, lower latency and WiFi 6 offers improved performance, faster data transfer speeds, and better handling of dense environments compared to Wi-Fi 5.

4. How many access points (APs) will be required to ensure adequate coverage? [2]

- 7 Access points more or less, because the number of access points required depends on the size of the area and the desired coverage. In an urban setting, more APs may be needed to ensure adequate coverage due to potential interference from nearby buildings and obstacles. A site survey will help determine the optimal AP locations and the required number of Aps.

5. What channel selection strategy will you implement to minimize interference from neighbouring networks? [2]

- A dynamic channel selection strategy, because it will Continuously monitoring channel conditions and interference levels, also automatically switching to the least congested channel when interference is detected. Some tools will do this automatically such as Cisco CleanAir or Ubiquiti's Auto-Optimize, and lastly make sure to stagger the channels on neighbouring APs, so as not to cause overlap and interference.

6. How will you secure the wireless network against unauthorized access? [2]

- Use WPA3 for extra security. Implement access control mechanisms such as MAC filtering and user authentication. Regularly updating network passwords and firmware to address vulnerabilities.

7. What measures will be taken to manage bandwidth effectively among users? [2]

- Prioritizing important applications (e.g., VoIP or video conferencing) using Quality of Service (QoS) Balance client load balancing across available APs. User access control and non-critical traffic can have a bandwidth throttle applied to ensure that your essential services keep performing smoothly.

8. How will you monitor network performance and troubleshoot issues post-deployment? [2]

- Use monitoring tools like SNMP monitoring, packet capture, and Wi-Fi analysers, because these will help to keep an eye on AP performance and client connections, etc. Trace interference sources when detected This is crucial as it enables you to make the correct adaptations before time and keep your network running at its best.

9. Are there any local regulations or restrictions regarding wireless signal transmission that need to be considered? [2]

- Yes, there are local regulations and restrictions that must be considered which includes Frequency Usage, Power Output Limits, Dynamic Frequency Selection, Licensing Requirements, Health and Safety Standards and International Compliance.

10. What backup solutions or redundancy plans are in place if the primary network fails? [2]

- Redundant APs and network paths. Implement failover for important components and dual band APs as a backup in case of one band experiencing interference. Use mesh networking for failover and also Maintain up-to-date backups of network configurations. Use backup software with built-in redundancy (they should support features like replicating, mirroring), Test backup and restore processes regularly.

Scenario 5:

1. How do you ensure seamless roaming for mobile devices in a wireless network? [5]

- Ensure that your Access Points are placed in such a way that there is 15-20% overlap between them.
- Implement faster WLAN standards, preferably 802.11k for quick and effective handovers, 802.11r for effective AP selection and 802.11r for faster roaming.
- Ensure that you have a good network design to maintain seamless roaming.
- Implement a centralized management system that uses wireless controllers to help manage handoffs.
- Regularly conduct site surveys to ensure that the network is performing the way that you want it to.

2. Explain the concept of multiuser MIMO and how it can enhance the capacity of wireless networks. [5]

- Multiuser MIMO is new technology that allows antennas to service multiple clients simultaneously.
- Mu-MIMO enhances capacity by communicating simultaneously with multiple devices at the same time, improving network performance and increasing throughput.

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

- 5g is the 5th generation of new global wireless cellular technology which offers a higher performance and improved efficiency with a greater speed in the transmissions, a lower latency and therefore greater capacity of remote execution.
- 5g uses high bands of radio frequencies that offer faster speeds and more bandwidth.
- Small cell networks are used to improve its coverage and capacity.
- More data and computing resources are positioned closer to help with its low latency.

4. Explain in detail about IEEE 802.11 Architecture and Protocols. [5]

IEEE 802.11 refers to the set of standards that define communication for wireless LANs which has the following components:

- Service Set Identifier (SSID)

Unique character string identifying access point in beacon from information.

- Basic Service Set (BSS)

Group of stations sharing an access point

- Extended Service Set (ESS)

Group of access points connected to the same LAN.

Protocols:

- Physical Layer Protocol
  -Defines the physical means of transmission of data over the air.
- Medium Access Control Protocol

- Handles access to the wireless medium.

- Authentication and Association Protocol

- Includes several security protocols to protect data transmitted over the wireless network.

5. Compare security issues in Wireless networks with wired network? [5]

Wireless Network	Wired Network

• Data is transmitted over the air using radio waves, making it easier for unauthorized users within range to intercept. • Unauthorized access is a more common issue, as attackers can attempt to connect to the network from any location within the wireless coverage area. • Encryption is critical in wireless networks to protect data from being intercepted. • Wireless networks require strong authentication mechanisms to prevent unauthorized access.	• Data travels through physical cables and that makes it more difficult for unauthorized users to intercept the data without physical access to the network. • Unauthorized access requires physical access to the network, so if physical security is available there are slim chances of accessing the network. • Encryption is often less of a focus in wired networks due to the security measures provided by physical access restrictions. • Authentication typically involves network login credentials, and the risk is lower because physical access to the network is required to attempt unauthorized connections.