A star topology is ideal for small offices because it connects all devices to a central hub, making it easier to manage and troubleshoot. If one connection fails, it does not affect the entire network.

Using DHCP allows automatic assignment of IP addresses to devices, reducing the administrative burden and minimizing the risk of address conflicts in a dynamic environment.

WPA3 offers the highest level of security with stronger encryption and protection against brute-force attacks compared to older protocols like WEP, WPA, and WPA2.

WPA3 encryption provides the highest level of security available for Wi-Fi networks, protecting sensitive data more effectively than older standards like WEP or WPA2

Monitoring bandwidth utilization helps identify periods of high usage and potential congestion, allowing for proactive management and optimization of network resources.

The ping tool helps verify connectivity between devices on the network by sending ICMP echo requests and measuring response times

The first step in troubleshooting connectivity issues should be to ensure all physical connections and cables are securely connected, as loose or damaged cables are a common cause of intermittent connectivity problems.

Implementing VLANs helps segment the network into logical groups, improving manageability, performance, and security. This strategy allows the network to scale efficiently as the company grows.

Placing the router centrally on the first floor can help ensure even distribution of Wi-Fi signals throughout both floors, minimizing dead zones caused by thick walls.

Using different channels for each WAP helps avoid interference, and strategic placement ensures seamless coverage throughout the office, reducing dead zones and signal overlap

Placing the repeater midway ensures it receives a strong enough signal from the router to effectively extend the coverage to areas with weak signal.

Quality of Service (QoS) allows you to prioritize certain types of traffic, ensuring that important applications like video conferencing get the necessary bandwidth, even when the network is under heavy use.

Physical obstructions and interference are common causes of connectivity issues. Identifying and mitigating these factors can often resolve the problem without needing hardware changes

Creating a separate guest network isolates guest traffic from the main network, enhancing security by preventing unauthorized access to sensitive internal resources and data.

Cat 6 cables support higher data transfer rates and provide better performance and future scalability compared to Cat 5 and Cat 5e. Coaxial cables are not typically used for modern Ethernet networks.

The maximum recommended length for Cat 6 cables to maintain optimal performance is 100 meters, including both horizontal cabling and patch cables.

Using cable trays and Velcro straps helps organize cables neatly, making maintenance easier and reducing the risk of damage or performance issues caused by tightly bundled or unsecured cables.

A cable tester checks the continuity, signal strength, and performance of network cables, ensuring they function correctly and meet the required specifications.

Testing the network cable with a cable tester helps determine if the issue lies with the physical cable, which is a common cause of network connection problems.

Plenum-rated cables are designed to meet fire safety standards and reduce the risk of toxic fumes in case of a fire. They are required when running cables through spaces used for air circulation, such as drop ceilings.

Correctly arranging the wires according to the T568B standard ensures that the cable functions properly and meets Ethernet specifications

**Router** - a networking device that forwards data packets between computer

Ipconfig - command is used to check the current network configuration on a Windows machine

Ping – a command used to test the reachability of its web server from a remote location

telnet – A tool use to test the connection

Traceroute – a tool used to determine the path packets take to reach a specific IP address

DHCP - protocol is used to automatically assign IP addresses to devices on a network

Nslookup -A command used to command can verify if DNS resolution is working.

Netstat command is used to display network connections, routing tables, and interface statistics

* to verify if a specific port on a server is open and listening

Firewall - network device can be configured to achieve blocking of access to specified user.

Wireshark – a tool used to monitor real-time network traffic and diagnose network issues

Route add - command can be used to add a static route on a Windows machine

Iperf – used to test the speed and performance of the network.

Repeater – a device used to extend Wi-Fi coverage in a large office, home or in an area.

Wi-fi Repeater / Extender – used to improve coverage without needing to run new cables

**essential steps to secure a wireless network**

* Changing default router passwords.
* Enabling network encryption (WPA3 is recommended).
* Disabling SSID broadcasting.
* Implementing MAC address filtering.
* Keeping firmware up to date. Implementing WPA3 is considered a best practice because it provides stronger encryption than previous standards (like WPA2), protecting against offline dictionary attacks and improving security on open networks through individualized data encryption.\*\*

**intermittent connectivity issues**, steps to follow

A: Steps include:

1. Checking physical connections and ensuring cables are securely connected.
2. Reviewing network device logs for error messages or unusual activity.
3. Using network monitoring tools to check for patterns or spikes in traffic that may indicate a specific cause.
4. Running diagnostic tests on network hardware (switches, routers) to identify potential faults.
5. Verifying that firmware and drivers are up to date.
6. Isolating segments of the network to identify if the issue is localized. Resolving the problem may involve replacing faulty hardware, reconfiguring network settings, or addressing external factors like interference in a wireless network.\*\*

A star topology is ideal for small offices because it connects all devices to a central hub, making it easier to manage and troubleshoot. If one connection fails, it does not affect the entire network.

Using DHCP allows automatic assignment of IP addresses to devices, reducing the administrative burden and minimizing the risk of address conflicts in a dynamic environment.

WPA3 offers the highest level of security with stronger encryption and protection against brute-force attacks compared to older protocols like WEP, WPA, and WPA2.

WPA3 encryption provides the highest level of security available for Wi-Fi networks, protecting sensitive data more effectively than older standards like WEP or WPA2

Monitoring bandwidth utilization helps identify periods of high usage and potential congestion, allowing for proactive management and optimization of network resources.

The ping tool helps verify connectivity between devices on the network by sending ICMP echo requests and measuring response times

The first step in troubleshooting connectivity issues should be to ensure all physical connections and cables are securely connected, as loose or damaged cables are a common cause of intermittent connectivity problems.

Implementing VLANs helps segment the network into logical groups, improving manageability, performance, and security. This strategy allows the network to scale efficiently as the company grows.

Placing the router centrally on the first floor can help ensure even distribution of Wi-Fi signals throughout both floors, minimizing dead zones caused by thick walls.

Using different channels for each WAP helps avoid interference, and strategic placement ensures seamless coverage throughout the office, reducing dead zones and signal overlap

Placing the repeater midway ensures it receives a strong enough signal from the router to effectively extend the coverage to areas with weak signal.

Quality of Service (QoS) allows you to prioritize certain types of traffic, ensuring that important applications like video conferencing get the necessary bandwidth, even when the network is under heavy use.

Physical obstructions and interference are common causes of connectivity issues. Identifying and mitigating these factors can often resolve the problem without needing hardware changes

Creating a separate guest network isolates guest traffic from the main network, enhancing security by preventing unauthorized access to sensitive internal resources and data.

Cat 6 cables support higher data transfer rates and provide better performance and future scalability compared to Cat 5 and Cat 5e. Coaxial cables are not typically used for modern Ethernet networks.

The maximum recommended length for Cat 6 cables to maintain optimal performance is 100 meters, including both horizontal cabling and patch cables.

Using cable trays and Velcro straps helps organize cables neatly, making maintenance easier and reducing the risk of damage or performance issues caused by tightly bundled or unsecured cables.

A cable tester checks the continuity, signal strength, and performance of network cables, ensuring they function correctly and meet the required specifications.

Testing the network cable with a cable tester helps determine if the issue lies with the physical cable, which is a common cause of network connection problems.

Plenum-rated cables are designed to meet fire safety standards and reduce the risk of toxic fumes in case of a fire. They are required when running cables through spaces used for air circulation, such as drop ceilings.

Correctly arranging the wires according to the T568B standard ensures that the cable functions properly and meets Ethernet specifications

**Router** - a networking device that forwards data packets between computer

Ipconfig - command is used to check the current network configuration on a Windows machine

Ping – a command used to test the reachability of its web server from a remote location

telnet – A tool use to test the connection

Traceroute – a tool used to determine the path packets take to reach a specific IP address

DHCP - protocol is used to automatically assign IP addresses to devices on a network

Nslookup -A command used to command can verify if DNS resolution is working.

Netstat command is used to display network connections, routing tables, and interface statistics

* to verify if a specific port on a server is open and listening

Firewall - network device can be configured to achieve blocking of access to specified user.

Wireshark – a tool used to monitor real-time network traffic and diagnose network issues

Route add - command can be used to add a static route on a Windows machine

Iperf – used to test the speed and performance of the network.

Repeater – a device used to extend Wi-Fi coverage in a large office, home or in an area.

Wi-fi Repeater / Extender – used to improve coverage without needing to run new cables

**essential steps to secure a wireless network**

* Changing default router passwords.
* Enabling network encryption (WPA3 is recommended).
* Disabling SSID broadcasting.
* Implementing MAC address filtering.
* Keeping firmware up to date. Implementing WPA3 is considered a best practice because it provides stronger encryption than previous standards (like WPA2), protecting against offline dictionary attacks and improving security on open networks through individualized data encryption.\*\*

**intermittent connectivity issues**, steps to follow

A: Steps include:

1. Checking physical connections and ensuring cables are securely connected.
2. Reviewing network device logs for error messages or unusual activity.
3. Using network monitoring tools to check for patterns or spikes in traffic that may indicate a specific cause.
4. Running diagnostic tests on network hardware (switches, routers) to identify potential faults.
5. Verifying that firmware and drivers are up to date.
6. Isolating segments of the network to identify if the issue is localized. Resolving the problem may involve replacing faulty hardware, reconfiguring network settings, or addressing external factors like interference in a wireless network.\*\*