

Assignment module :- 5 Network fundamental and building Networks

Section :1 multiple choice

1 what is the primary function of router in computer network?

Answer:- (c) forwarding data packets between networks

2 what is the purpose of DHCP in compilation network?

Answers:- (A) Assigning static IP address to devices

3 which network device operates at layer 2 of the OSI model and forwards data packets based on MAC address?

Answer:- (B) switch

4 which network topology connects all device in a linear fashion with each device connected to central cable or backbone?

Answer:- (B) bus

Section 2 TRUE or false

5 A VLAN allows network administration logically segment a single physical network into multiple virtual network. Each with it's own broadcast domain

Answer:- TRUE

6 TCP is a connectionless protocol that provides reliable, ordered and error-checked delivery of Data packets over a network

Answer:- false

7 A firewall is a hardware or software-

based security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules

Answer:- TRUE

8 describe the steps involved in settings up a wireless network for a small office or home office environment

Answer:- Setting up a wireless network for a small office or home office involves several steps to ensure proper connectivity, security, and performance. Here's a detailed guide:

1. Plan Your Network

Assess Needs: Determine the number of

devices and the coverage area required.

Choose Equipment: Select a wireless router or a combination of a modem and router, and additional access points if necessary for larger spaces.

Select Internet Provider: Choose a reliable ISP (Internet Service Provider) based on your location and bandwidth requirements.

2. Set Up the Router

Connect the Router to Modem: Use an Ethernet cable to connect the modem to the router's WAN (Internet) port.

Power Up: Plug in the router and turn it on. Wait for the indicator lights to show a stable connection.

3. Access the Router Configuration Interface

Connect to Router: Use a computer or smartphone to connect to the router's default wireless network or via an Ethernet cable.

Open Configuration Page: Open a web browser and enter the router's IP address (usually something like 192.168.1.1 or 192.168.0.1).

Login: Enter the default username and password (found in the router manual or on the device itself).

4. Configure the Network

Change Default Credentials: Change the router's admin username and password to secure the device.

Set SSID (Network Name): Customize your wireless network name for easier identification.

Select Wi-Fi Standards: Choose an appropriate wireless standard (e.g., Wi-Fi 5 or Wi-Fi 6).

Set Security Protocol: Use WPA3 (or at least WPA2) encryption for secure connections. Avoid outdated protocols like WEP.

Set Password: Create a strong password for the Wi-Fi network.

5. Optimize Network Settings

Choose a Channel: Set the router to automatically select the least congested channel or manually choose based on analysis (e.g., 2.4 GHz for range, 5 GHz for speed).

Enable QoS (Quality of Service): Prioritize bandwidth for critical devices like work computers or VoIP systems.

Set Guest Network: Configure a separate guest network if needed to isolate visitors from the main network.

6. Test and Adjust Coverage

Place the Router: Position the router centrally in the office or home to maximize coverage. Avoid placing it near walls, metal objects, or other electronics.

Test Signal Strength: Use a smartphone or app to test Wi-Fi coverage.

Add Range Extenders: If signal strength is weak in certain areas, install Wi-Fi extenders or additional access points.

7. Secure the Network

Enable Firewall: Most modern routers include a built-in firewall that should be enabled.

Disable WPS (if not needed): Turn off Wi-Fi Protected Setup to prevent unauthorized access.

Update Firmware: Ensure the router's firmware is up-to-date to protect against

vulnerabilities.

8. Connect Devices

Join the Network: Connect devices to the Wi-Fi network using the SSID and password.

Test Connectivity: Verify that all devices can access the internet and communicate with each other as needed.

9. Regular Maintenance

Monitor Network: Periodically check the router's settings and connected devices.

Update Security: Regularly change passwords and update firmware.

Backup Settings: Save the router configuration to restore quickly in case of issues.

Following these steps will provide a reliable and secure wireless network for your small office or home office environment.

Section 4 practical

9 done in lab

Section 5

10 discuss the importance of network documentation in the context of building and managing networks

Answer:-The Importance of Network Documentation in Building and Managing Networks

Network documentation is an essential aspect of designing, implementing, and managing networks. It involves creating detailed records of a network's structure, devices, configurations, and processes. Proper documentation provides a clear roadmap for network administrators, ensuring the network remains secure,

efficient, and scalable. In this essay, we will explore the key reasons why network documentation is vital in building and managing networks, including its role in troubleshooting, scalability, compliance, and disaster recovery.

Facilitating Troubleshooting and Maintenance

One of the primary benefits of network documentation is its ability to simplify troubleshooting and maintenance. When issues arise, detailed network documentation provides administrators with quick access to information about the network's topology, IP addressing schemes, hardware configurations, and

software versions. This reduces downtime and allows for more efficient problem resolution. Without documentation, network administrators would need to spend significant time investigating the network's layout, leading to delays and potential disruptions in business operations.

For instance, if a router fails, network documentation can identify its exact location, the configuration settings, and how it connects to other devices. This enables technicians to replace or reconfigure the device with minimal effort.

Enabling Scalability and Future Planning

As organizations grow, their networks must expand to accommodate additional devices, users, and applications. Network documentation ensures that this growth occurs smoothly by providing a comprehensive overview of the existing infrastructure. Detailed records of current configurations allow administrators to identify potential bottlenecks and plan upgrades without disrupting the network.

Moreover, documentation aids in preventing redundant purchases or incompatible upgrades. For example, knowing the specifications of existing network switches or access points helps ensure new devices are compatible with the current setup, saving both time and resources.

Ensuring Compliance and Security

Many industries are subject to regulations that require secure and well-documented network practices. Network documentation plays a critical role in demonstrating compliance with standards such as GDPR, HIPAA, or ISO 27001. Auditors often require detailed information about how data flows through the network, which devices handle sensitive information, and what security measures are in place.

Additionally, documentation enhances security by tracking changes to configurations and access permissions. Maintaining a record of who made changes, when they were made, and why

they occurred helps identify vulnerabilities and mitigate risks. It also supports the implementation of robust policies such as role-based access control (RBAC) and network segmentation.

Supporting Disaster Recovery and Business Continuity

Network documentation is invaluable in disaster recovery scenarios. Whether a network is affected by hardware failure, cyberattacks, or natural disasters, comprehensive documentation enables administrators to restore services quickly. A detailed record of network configurations, IP assignments, and software versions allows for efficient

rebuilding of the network.

For example, if an organization experiences a ransomware attack that compromises its systems, having a backup of the network configuration can accelerate the recovery process by reinstating pre-attack settings. Without proper documentation, recovery efforts may be chaotic, leading to prolonged downtime and loss of revenue.

Streamlining Collaboration and Knowledge Transfer

In many organizations, network management involves multiple teams or personnel. Documentation ensures

consistency by providing a central source of truth about the network. This is especially important when onboarding new employees or transitioning responsibilities.

For example, when a new network administrator joins the team, documentation reduces the learning curve by offering a comprehensive understanding of the network's design, policies, and history. It also fosters collaboration among teams by eliminating guesswork and promoting standardized procedures.

Conclusion

Network documentation is a cornerstone

of effective network management. It simplifies troubleshooting, enables scalability, ensures compliance, supports disaster recovery, and facilitates collaboration. Despite its importance, documentation is often overlooked due to time constraints or resource limitations. However, investing in thorough and up-to-date network documentation pays dividends in the form of improved efficiency, enhanced security, and long-term cost savings.

In an increasingly connected world, where networks underpin critical business operations, proper documentation is not just a best practice—it is a necessity. Organizations that prioritize network documentation are better equipped to manage their networks, adapt to change, and respond to challenges with confidence.

