Assignment: Understanding and Maintenance of Networks

Section 1: Multiple Choice

1. What is the primary function of a router in a computer network?

a) Assigning IP addresses to devices

b) Providing wireless connectivity to devices

c) Forwarding data packets between networks

d) Managing user authentication and access control

Ans – [C]

2. What is the purpose of DNS (Domain Name System) in a computer

network?

a) Encrypting data transmissions for security

b) Assigning IP addresses to devices dynamically

c) Converting domain names to IP addresses

d) Routing data packets between network segments

Ans – [C]

3. What type of network topology uses a centralized hub or switch to connect all devices?

a) Star

b) Bus

c) Ring

d) Mesh

Ans – [D] Mesh

4. Which network protocol is commonly used for securely accessing and transferring files over a network?

a) HTTP

b) FTP

c) SMTP

d) POP3

Ans – [B]

Section 2: True or False

5. A firewall is a hardware or software-based security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

Ans – [Yes]

6. DHCP (Dynamic Host Configuration Protocol) assigns static IP addresses to network devices automatically.

Ans – [No]

7. VLANs (Virtual Local Area Networks) enable network segmentation by dividing a single physical network into multiple logical networks.

Ans – [Yes]

Section 3: Short Answer

8. Explain the difference between a hub and a switch in a computer network.

Ans –

|  |  |
| --- | --- |
| Hub | Switch |
| * It basically works on layer 1   {PHYSICAL LAYER}.   * It does not recognize the Mac Address. * It is a less expensive device. * It is a Broadcast Device. * It also works Slower in performing operations then Switch | * It basically works on layer 2   {PRESENTATION LAYER}.   * It recongnize the Mac Address. * It is Expensive device then Hub. * It is Unicast Device. * It Works Faster then Hub and performes operations quicker then Hub. |

9. Describe the process of troubleshooting network connectivity issues.

Ans –

* Check the physical connections: Ensure the cables are in place and your router turned on.
* Verify the device's settings: Double-check the network settings of your device to see if there is an IP address conflict.
* Restart devices: Power cycle both the router and your device. Sometimes, this simple procedure is exactly what you needed for this to work.
* Check outages: Confirm with your ISP whether or not the service is shut off because of an outage.
* Run diagnostics: Utilize your computer's built-in network diagnostic tools to troubleshoot issues.
* Check firewall settings: Ensure the firewall rules are not restricting access to your network.
* Drivers and firmware updates: Make sure your network drivers and firmware within your router have been upgraded.
* Ping and trace: The Ping and Traceroute commands will attempt to trace the source of the problem with your connection.
* Logs: Go through the logs both on your router and device in search of any error messages or alerts.

Section 4: Practical Application

10. Demonstrate how to configure a wireless router's security settings to enhance network security.

Ans –

* Change the default logins. Normally, these can be accessed through a web browser. Change the username and password to prevent unauthorized access.
* Update the firmware of your router with fresh firmware. Check for updates and install them on your router. You will ensure you are having the latest patch on security.
* Encrypt your Wi-Fi network with WPA3, if available. If not, use WPA2-PSK (AES).
* WPS: Wi-Fi Protected Setup Disable WPS as it is known to be a security weakness.
* Set strong Wi-Fi network password: Your password should not be ordinary but very strong. Avoid easily guessed information, such as your name or even your children's name.
* Set the router's built-in firewall: An enabled router firewall will block unwanted traffic.
* Disable remote access: Disable remote access to the router settings so that it does not allow external access.
* Guest network creation: You can easily create a guest network for visitors without compromising your main network.
* UPnP[Universal Plug & Play] disabling: can open ports that might be exploited by attackers, so it's safer to disable it. Always monitor device connected to: Keep reviewing the list of all devices connected to your network and delete any unknown entries.

Section 5: Essay

11. Discuss the importance of network documentation and provide examples of information that should be documented.

Ans –

* Many reasons why the network should be documented include:
* Troubleshooting: More efficient repair and troubleshooting when the details are there.
* Maintenance: Smooth upgrades and routine servicing through a clear understanding of where the network stands now.
* Security: Recognition of potential security vulnerabilities and eliminating these based on complete documentation.
* Compliance: In this regard, the documentation ensures that the industry standards and legal obligations are met.
* Knowledge transfer: Bringing new team members or even third-party vendors up to speed. The kind of information to document:
* Network Topology: Diagrams depicting the physical relationship between devices.
* IP Addressing Scheme: All assigned IP addresses, static and dynamic.
* Hardware Inventory: Details of all hardware utilized in your network, including model, serial number, and location.
* Configuration settings for routers, switches, firewalls, etc.
* Security policies: Established security protocols and all firewall rules, encryption schemes.
* ISP information: Contact details and account numbers with internet service providers.
* Backup procedures: It is the procedure for backing up and restoring the network configurations.
* Change logs: In this category, all those networks infrastructures that have been changed including this one.
* User access controls: Here, a user list is along with their permission, which have been given to access the network.