Assignment 3

Section1: Multiple choice

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

Ans: Forwarding data packets between networks.

1. What is the purpose of DNS (Domain Name System) in a computer network?

Ans: Converting domain names to IP addresses

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

Ans: Star Topology.

1. Which network protocol is commonly used for securely accessing and transferring files over a network?Ans: HTTPS

Section2: True or False

1. 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: True

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

Ans: False

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

Ans: True

Section3: Short Answers

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

Ans:

|  |  |  |
| --- | --- | --- |
| Feature | Hub | Switch |
| Data Transmission | Broadcasts data to all ports. | Unicasts data to the specific destination port. |
| Intelligence | Not intelligent a layer 1 device. | Intelligent a layer 2 device |
| Collision Domain | All ports are in single domain. | Each port has its own domain. |
| Bandwidth | Shared among all connected devices. | Provides dedicated bandwidth to each port. |
| Mode | Half-Duplex (sends or receives, not both) | Full-Duplex (Sends and receives simultaneously) |
| Cost | Inexpensive | More expensive |

1. Describe the process of troubleshooting network connectivity issues.

Ans: Troubleshooting network connectivity issues involves a systematic, step-by-step process of elimination to identify and resolve the root cause.

* Identify the Problem and scope.
* Check Physical Connections
* Restart network devices
* Use Command-Line Tools
* Check DNS and Firewall Settings
* Contact the ISP

Section 4: Pratical

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

Ans: 1. Access Your Router's Administration Page

The first step is to log in to your router's web interface.

Connect to your network: Connect a computer to your router using an Ethernet cable for the most stable connection. Alternatively, you can connect wirelessly.

Find the IP address: The router's IP address (the default gateway) is typically printed on a sticker on the bottom or back of the router. Common addresses are 192.168.1.1 or 192.168.0.1.

Log in: Open a web browser and type the router's IP address into the address bar. You'll be prompted to enter a username and password. The default credentials are also on the sticker.

2. Change the Default Login Credentials 🔑

This is the most crucial step. Default usernames (like "admin") and passwords ("password" or "admin") are publicly known and a major security risk.

Navigate to the Administration or System Settings section of the router's interface.

Find the option to change the username and password.

Create a strong, unique password that is at least 12 characters long and includes a mix of uppercase and lowercase letters, numbers, and symbols. Write it down and store it securely.

3. Update the Router's Firmware 💻

Firmware is the software that runs your router. Manufacturers release updates to fix security vulnerabilities and improve performance.

In the administration page, look for a section titled Firmware Update, System Tools, or Router Upgrade.

The router may check for and download updates automatically, or you may need to go to the manufacturer's website, download the latest firmware file, and upload it to the router.

4. Configure Wireless Security Settings 🛡️

This section is typically labeled Wireless or Wi-Fi and contains the most important settings for securing your wireless signal.

Change the SSID: The SSID (Service Set Identifier) is the name of your Wi-Fi network. Change the default SSID, which often reveals the router's brand and model, to something unique. Avoid using personal information.

Enable Strong Encryption: This scrambles your data so unauthorized users can't read it.

Set the Security Mode to WPA3-Personal. It's the newest and most secure standard.

If your older devices aren't compatible, use WPA2-Personal (AES). Avoid older, insecure protocols like WEP or WPA.

Create a Strong Wi-Fi Password: This is the password your devices use to connect to the network. Create a unique, long, and complex passphrase.

5. Disable Unnecessary Features 🚫

Many routers have features that can be a security liability if not needed.

Disable WPS: Wi-Fi Protected Setup (WPS) allows devices to connect with a simple button press or an 8-digit PIN. However, the PIN is vulnerable to brute-force attacks. It's a significant security risk, so disable it if you don't use it.

Disable Remote Management: This feature allows you to access your router's settings from outside your network. Unless absolutely necessary, disable this to prevent external attackers from gaining control.

Disable UPnP: Universal Plug and Play (UPnP) can automatically forward ports for devices, which can be exploited by malware to open holes in your firewall. It's best to disable it and manually forward ports only when needed for specific applications.

6. Create a Guest Network

Most modern routers allow you to create a separate network for guests.

Enable the Guest Network feature.

Give it a different name and password from your main network.

This isolates your guests' devices from your primary network, preventing them from accessing your computers, printers, or other shared devices.

Section 5: Essay

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

Ans: Network documentation is a critical practice for any organization, regardless of size, because it provides a comprehensive blueprint of the network infrastructure. It's not just a nice-to-have; it's essential for efficient management, quick troubleshooting, and long-term planning. Without proper documentation, a network can become a black box, making it difficult to onboard new staff, maintain consistency, and recover from disasters. It ensures that critical knowledge is retained within the organization even when key personnel leave.

**1. Network Topology**

This is the visual representation of your network. It should include diagrams of both the **physical** and **logical** layouts.

* **Physical Topology:** A diagram showing the physical location of devices, cables, and connections. This helps in quickly locating a device for maintenance or troubleshooting a physical cable issue.
* **Logical Topology:** A diagram showing how data flows through the network, including information about VLANs, subnets, and routing protocols. This helps in understanding the logical structure and diagnosing communication issues.

**2. IP Addressing Scheme**

This section is a detailed map of all IP addresses and how they're used.

* **IP Address Allocation:** A table or spreadsheet listing all assigned IP addresses, subnets, and the devices or services they are assigned to.
* **DHCP and Static IPs:** Document which devices use DHCP (Dynamic Host Configuration Protocol) to get an IP address automatically and which ones have a static IP address assigned manually. This is crucial for servers, routers, and other critical infrastructure.

**3. Hardware and Software Inventory**

A complete list of all network devices and the software that runs on them.

* **Hardware Inventory:** A list of all routers, switches, firewalls, servers, and other network devices. For each device, document the make, model, serial number, and physical location.
* **Software and Licensing:** A record of all operating systems, applications, and firmware versions used on network devices, along with license keys and support contract information.

**4. Security Policies and Procedures**

Documentation of security measures is vital for protecting the network.

* **Firewall Rules:** A list of all firewall rules, including the purpose and ports for each rule.
* **Security Protocols:** Details on security protocols like VPNs, intrusion detection systems, and access control policies.
* **Access Credentials:** A secure record of administrative passwords and login information for all network devices.

**5. Disaster Recovery and Backup**

This documentation is the blueprint for business continuity in the event of a network outage or disaster.

* **Backup Procedures:** A detailed schedule of what data is backed up, how often, and where the backups are stored.
* **Disaster Recovery Plan:** Step-by-step instructions on how to restore network services from backups and resume normal operations after a major failure.