**Module 5 and 6 Assignment**

**Module 5**

1. C**apture and analyze ARP packets using Wireshark. Inspect the ARP request and reply frames, and discuss the role of the sender's IP and MAC address in these packets.**

**ARP Request:**

A screenshot of a computer

AI-generated content may be incorrect.

**ARP Reply:**

**A screenshot of a computer

AI-generated content may be incorrect.**

1. **Using Packet Tracer, simulate an ARP spoofing attack. Analyze the behavior of devices on the network when they receive a malicious ARP response.**

A diagram of a network

AI-generated content may be incorrect.

A close-up of a computer address

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

1. **Manually configure static IPs on the client devices (like Pc or your mobile phone) and verify connectivity using ping.**

NETWORK TOPOLOGY:

A screenshot of a computer

AI-generated content may be incorrect.

PING:

PC0:

A computer screen with a black background

AI-generated content may be incorrect.

PC1:

A computer screen with a black background

AI-generated content may be incorrect.

1. **Use Wireshark to capture DHCP Discover, Offer, Request, and Acknowledge messages and explain the process.**

A screenshot of a computer

AI-generated content may be incorrect.

DHCP - Discover:

A screenshot of a computer

AI-generated content may be incorrect.

DHCP – Offer:

A screenshot of a computer

AI-generated content may be incorrect.

DHCP – Request:

**A screenshot of a computer

AI-generated content may be incorrect.**

**DHCP – Acknowledge:**

**A screenshot of a computer

AI-generated content may be incorrect.**

**5. Given an IP address range of 192.168.1.0/24, divide the network into 4 subnets.**

**Task: Manually calculate the new subnet mask and the range of valid IP addresses fo each subnet.**

**Assign IP addresses from these subnets to devices in Cisco Packet Tracer and verify connectivity using ping between them.**

**Subnet 1:** Starting with the original network address, 192.168.1.0/26.

The IP range is 192.168.1.1 to 192.168.1.62.

The broadcast address is 192.168.1.63.

**Subnet 2:** Adding 64, the next network address is 192.168.1.64/26.

The IP range is 192.168.1.65 to 192.168.1.126.

The broadcast address is 192.168.1.127.

**Subnet 3:** Adding another 64, the network address is 192.168.1.128/26.

The IP range is 192.168.1.129 to 192.168.1.190.

The broadcast address is 192.168.1.191.

**Subnet 4:** Adding 64 again, the network address is 192.168.1.192/26.

The IP range is 192.168.1.193 to 192.168.1.254.

The broadcast address is 192.168.1.255.

A computer screen shot of a black screen

AI-generated content may be incorrect.

6. **You are given three IP addresses: 10.1.1.1, 172.16.5.10, and 192.168.1.5.**

**Task: Identify the class of each IP address (Class A, B, or C). What is the default subnet mask for each class?**

**Provide the range of IP addresses for each class.**

|  |  |  |  |
| --- | --- | --- | --- |
| **IP Address** | **Class** | **Default Subnet Mask** | **Class Range** |
| 10.1.1.1 | Class A | 255.0.0.0 | 1.0.0.0 – 126.255.255.255 |
| 172.16.5.10 | Class B | 255.255.0.0 | 128.0.0.0 – 191.255.255.255 |
| 192.168.1.5 | Class C | 255.255.255.0 | 192.0.0.0 – 223.255.255.255 |

**Module 6**

1. **Capture and analyze ARP packets using Wireshark. Inspect the ARP request and reply frames when your device attempts to find the router's MAC address.**

**ARP Request:**

**A screenshot of a computer

AI-generated content may be incorrect.**

**ARP Reply:**

**A screenshot of a computer

AI-generated content may be incorrect.**

**IMPORTANCE OF ARP IN PACKET FORWARDING:**

**MAC Address Resolution:**

* ARP is essential for mapping IP addresses to MAC addresses, enabling packet delivery within a local network.

**Facilitating Communication:**

* Without ARP, devices wouldn’t know the MAC address of the next-hop gateway (router), preventing network communication.

**Efficient Packet Forwarding:**

* Once resolved, MAC addresses are cached, reducing unnecessary ARP requests and improving efficiency.

**Security Considerations:**

* ARP spoofing/poisoning attacks can compromise network security. Tools like Gratuitous ARP and Dynamic ARP Inspection (DAI) help mitigate risks.

1. **Manually configure static routes on a router to direct packets to different subnets.**

**NETWORK TOPOLOGY:**

**A diagram of a computer network

AI-generated content may be incorrect.**

**Iproute – Router 1**

**A screenshot of a computer program

AI-generated content may be incorrect.**

**Iproute – Router 2**

**A computer screen shot of a computer program

AI-generated content may be incorrect.**

**Testing Connectivity:**

**A screenshot of a computer

AI-generated content may be incorrect.**

**Tracert:**

**A screen shot of a computer

AI-generated content may be incorrect.**

**3. Given a network address of 10.0.0.0/24, divide it into 4 equal subnets.**

Network: 10.0.0.0/24

Subnet mask: 255.255.255.0

Total number of IPs: 256

Subnet 1:

* Network address: 10.0.0.0/26
* Broadcast address: 10.0.0.63

Subnet 2:

* Network address: 10.0.0.64/26
* Broadcast address: 10.0.0.127

Subnet 3:

* Network address: 10.0.0.128/26
* Broadcast address: 10.0.0.191

Subnet 4:

* Network address: 10.0.0.192/26
* Broadcast address: 10.0.0.255

**A screenshot of a computer screen

AI-generated content may be incorrect.**

**4. You are given three IP addresses: 192.168.10.5, 172.20.15.1, and 8.8.8.8.**

**Identify the class of each IP address.**

**Determine if it is private or public.**

**Explain how NAT would handle a private IP when accessing the internet.**

* 192.168.10.5 → Class C, Private - Falls within 192.168.0.0 - 192.168.255.255.
* 172.20.15.1 → Class B, Private - Falls within 172.16.0.0 - 172.31.255.255.
* 8.8.8.8 → Class A, Public - Not in any private IP range, belongs to Google DNS

NAT in handling Private IP when accessing the internet:

* When a private IP like 192.168.10.5 or 172.20.15.1 tries to access the internet, NAT translates it into a public IP assigned by the ISP.
* The router maintains a NAT table to track which private IP is mapped to which public IP.
* When the response comes back from the internet, NAT translates it back to the original private IP.
* This allows devices with private IPs to communicate with the internet while keeping internal network addresses hidden.

**5. In Cisco Packet Tracer, configure NAT on a router to allow internal devices (192.168.1.x) to access the internet.**

**Test connectivity by pinging an external public IP.**

**Capture the traffic in Wireshark and analyze the source IP before and after NAT translation.**

**NETWORK TOPOLOGY:**

**A diagram of a computer network

AI-generated content may be incorrect.**

**NAT Configuration:**

**A screenshot of a computer

AI-generated content may be incorrect.**

**A screenshot of a computer screen

AI-generated content may be incorrect.**

**Pinging 8.8.8.8 from 192.168.1.10:**

**A screen shot of a computer

AI-generated content may be incorrect.**

**A screenshot of a computer

AI-generated content may be incorrect.**

**Source IP before and after NAT translation:**

**Before the NAT translation, the Source IP is 192.168.1.10**

**A black and white rectangular object with text

AI-generated content may be incorrect.**

**After the NAT translation, the Source IP has become 200.100.50.1**

**A white rectangular object with black text

AI-generated content may be incorrect.**