Week 4 Assignment

[Author Name]

[Institutional Affiliation(s)]

Week 4 Assignment

**Response 1**

ARP is communication-based. Its purpose is to assign the IP address of any system to its MAC address. It operates between data link layer and Network layer of OSI model by providing physical address to frames that are to be sent. To initiate a communication first client will send a request (a broadcast message) to get the destination’s physical address. After that, if the server will respond with a unicast ARP message containing MAC address to device 1. The Mac address will be placed in the cache and will be used to address frames.

DHCP servers automatically assign a unique IP address to the host, from the range of different IP address as well as other network configurations. This protocol is used on UDP/IP networks.  First, a client will broadcast a message to the server. In case client and server do not use the same subnet, then the DHCP relay agent can be used. If a client remains at the same network then server will grant request. After receiving the leased IP address from the server, it also reserves an IP address especially, for the client by sending a DHCP offer message. The client will respond to the server’s DHCP offer message by sending the DHCP request message. A sever will acknowledge the message and allocate an IP address to the client (Lim & Goedman, 1999).

ICMP provides diagnostic feedback or information regarding any errors. It is neither a transport layer protocol nor used by any end-user. However, it is used by network administrators to troubleshoot internet connections.

SNMP is responsible for collecting and organizing information regarding managed devices that are on the IP network. It is also responsible for modifying information that will, in turn, change the behavior of the device. Devices such as modems, routers, and switches use the SNMP protocol.

DNS is also known as the phonebook of the system. Every device has a unique IP address that is used to locate the device. DNS servers eliminate the need to memorize the IP address as it automatically converts the hostname to the IP address that can be used by the computer to find the requested material (Ariyapperuma & Mitchell, 2007).

**Response 2**

  **Bastion host**: A specialized computer that is designed specifically to withstand any attacks. In the firewall architecture, bastion host is the only node that is exposed outside and is prone to attacks. It filters incoming traffic while also preventing malicious data from entering the network.

**Dual-homed firewall**: It refers to the Ethernet device having more than one network phase or one of the firewall architecture used for implementing security to prevent any attack. The routing function must be disabled to implement a dual-homed host. It is the front line defense of the network from potential threats and attacks (Cheswick, & Rubin, 2003).

**Screened host**: It is typically more flexible than the dual-homed gateway. It combines a packet-filtering router with an application gateway that is located on the protected subset side of the router.

**Screened subnet**: The use of one or more than one screening routers as a firewall to define three subnets that are external router used for separating the external network from the perimeter network. The internal router that is used to separate the internal network from the perimeter network. It is essential for secure usage of the World Wide Web, electronic payment, etc.

**Response 3**

 The four main tunneling protocols used in the VPN (Simpson, 1995) are as follows:

**PPTP**: Point to point tunneling protocol was developed by Microsoft, and is one of the oldest protocols that are still in use. It uses TCP connection creating, maintaining and terminations the tunnel. It operates at layer 2 of the OSI model and can be created by using two steps.

**L2TP**: Layer two tunneling protocol is used with the internet protocol security to create a secure tunneling protocol as compared to PPTP. It provides double encapsulation due to which it is relatively slow. It uses fixed ports due to which are difficult to bypass the firewall.

**IPsec**: internet protocol security is used to secure communication across the IP network by authenticating the communication session. It provides authentication by encrypting each data packet during the session.

**SSH**: the secure shell is a network protocol that is used for operating network services on the insecure network. It ensures the security of the data tunnel encryption process. The SSH client data is transferred from local ports through the encrypted tunnel.

**References**

Ariyapperuma, S., & Mitchell, C. J. (2007, April). Security vulnerabilities in DNS and DNSSEC. In *The Second International Conference on Availability, Reliability and Security (ARES'07)* (pp. 335-342). IEEE.

Cheswick, W. R., Bellovin, S. M., & Rubin, A. D. (2003). *Firewalls and Internet security: repelling the wily hacker*. Addison-Wesley Longman Publishing Co., Inc..

Simpson, W. (1995). IP in IP tunneling.