CSE421

Lab-02

Homework Questions on

HTTP, ARP, TCP, Email and DNS

ID: 19301261

1. What is the main difference between ARP and DNS requests?

ANS: ARP (Address Resolution Protocol) and DNS (Domain Name System) are both protocols used in computer networks, but they serve different purposes. The main difference between ARP and DNS requests is the type of information they request and the layer of the networking stack they operate on. ARP is used to map a known IP address to a MAC (Media Access Control) address, which is a unique identifier assigned to every network interface on a device. This mapping is necessary for communication to occur on a local network segment. ARP operates on the data link layer (Layer 2) of the networking stack, and its requests are broadcast to all devices on the local network. DNS, on the other hand, is used to map a human-readable domain name to an IP address. DNS operates on the application layer (Layer 7) of the networking stack and its requests are sent to DNS servers, which are responsible for resolving domain names to IP addresses.

In summary, ARP is used for mapping IP addresses to MAC addresses on the local network segment, while DNS is used for mapping domain names to IP addresses on the internet.

2. By checking which section of a TCP packet one can identify if it is a TCP packet for opening the connection or closing the connection? Explain how?

ANS: In a TCP (Transmission Control Protocol) packet, the flags in the TCP header section are used to identify the type of packet and its purpose. Specifically, the TCP flags that indicate the opening or closing of a connection are the SYN (synchronize) and FIN (finish) flags. When a TCP packet is used to initiate a connection, it is called a SYN packet. This packet has the SYN flag set to 1 in the TCP header section. The SYN packet is sent by the client to the server to request the opening of a connection. The SYN packet contains a

sequence number that is randomly generated by the client to establish a unique connection. On the other hand, when a TCP connection is being closed, it is done by exchanging FIN packets between the two endpoints of the connection. The FIN packet has the FIN flag set to 1 in the TCP header section. When the client wants to close the connection, it sends a FIN packet to the server, and the server acknowledges the request by sending its own FIN packet back to the client. This exchange of FIN packets is known as the TCP 4-way handshake and is used to close the connection gracefully.

To summarize, to identify whether a TCP packet is for opening or closing a connection, you need to examine the TCP header section of the packet and look for the SYN or FIN flag. If the SYN flag is set, the packet is a SYN packet used for initiating a connection, and if the FIN flag is set, the packet is a FIN packet used for closing a connection.

3. How can you resolve an ARP IP Address to an Ethernet MAC address?

ANS: To resolve an ARP (Address Resolution Protocol) IP address to an Ethernet MAC (Media Access Control) address, you can use the ARP protocol itself. Here are the steps involved in resolving an ARP IP address to an Ethernet MAC address:

- The sender device checks its ARP cache to see if it already has the ARP mapping for the IP address it wants to resolve. If it does, the sender device can use the MAC address from the cache for communication.
- If the sender device does not have the ARP mapping in its cache, it sends a broadcast ARP request on the local network segment asking the device with the IP address to respond with its MAC address.
- The ARP request contains the sender device's MAC address, IP address, and the target IP address that the sender device wants to communicate with.
- The device with the IP address in the ARP request checks to see if the IP address matches its own IP address. If it does, the device responds to the ARP request with its MAC address.
- The sender device receives the ARP response and updates its ARP cache with the MAC address of the target device.

By following these steps, the sender device can resolve an ARP IP address to an Ethernet MAC address, which is necessary for communication to occur on a local network segment

4. How does a router help the communication and interchange of information between a pc from a network with a web server from a different network?

ANS: A router is a networking device that connects multiple networks together and helps to facilitate the communication and interchange of information between devices on different

networks. In the scenario you described, a router would be used to connect a PC on one network with a web server on a different network. Here's how a router helps with this communication:

- The PC on the local network sends a request to the web server, which is located on a different network. The request includes the IP address of the web server.
- The router on the local network receives the request from the PC and looks up the destination IP address in its routing table. The routing table is a set of rules that tells the router how to forward packets to different networks.
- If the router does not have a specific route to the destination network, it forwards the packet to the default gateway, which is usually the next hop router in the path to the destination network.
- The packet is then forwarded through a series of routers until it reaches the web server's network.
- When the packet arrives at the web server's network, the router on that network forwards the packet to the web server using its MAC address.
- The web server receives the packet, processes the request, and sends a response back to the PC using the same process.

In summary, the router helps to route packets between different networks by forwarding them to their destination network based on the destination IP address. This allows devices on different networks to communicate and interchange information with each other.

5. Suppose, you want to access facebook.com and your PC does not know its local DNS server. Which protocol between ARP and DNS will be executed first and why?

ANS: When a PC wants to access a website, such as facebook.com, it needs to know the IP address of the web server that hosts the website. The IP address is used to establish a network connection between the PC and the web server. To resolve the domain name (e.g. facebook.com) to its corresponding IP address, the PC will typically use the DNS (Domain Name System) protocol. In our case, the PC does not know the IP address of the DNS server that it needs to query for the IP address of facebook.com. Therefore, the PC will first need to discover the MAC address of the local default gateway/router using the ARP (Address Resolution Protocol) protocol, before it can use the DNS protocol to resolve the IP address of facebook.com. Here's how the process would typically work:

- The PC sends an ARP broadcast message on its local network segment, asking for the MAC address of the local default gateway/router.
- The default gateway/router responds with its MAC address, allowing the PC to send traffic to the router.

- The PC then sends a DNS query to the default gateway/router, asking for the IP address of facebook.com.
- The default gateway/router forwards the DNS query to a DNS server on the internet that is responsible for resolving the domain name facebook.com.
- The DNS server responds to the DNS query with the IP address of the web server that hosts facebook.com.
- The PC then uses the IP address to establish a network connection with the web server and access the website.

In summary, in the scenario you described, the ARP protocol will be executed first to discover the MAC address of the local default gateway/router, which is necessary for the PC to communicate with other devices on the network. Once the default gateway/router has been discovered, the DNS protocol can be used to resolve the IP address of the web server that hosts facebook.com.

6. For the same scenario mentioned above, what will be the destination/target IP address?

ANS: In the same case, the PC is trying to access the website facebook.com and needs to obtain the IP address of the web server that hosts the website. To do this, the PC sends a DNS query to a DNS server that is responsible for resolving the domain name facebook.com. The destination/target IP address for the DNS query will depend on the configuration of the local network and the DNS server being used. In general, the destination/target IP address for the DNS query will be the IP address of the local DNS server or the IP address of the default gateway/router if the DNS server is located on a different network.

In summary, the destination/target IP address for the DNS query will depend on the network configuration and the location of the DNS server being used. It could be the IP address of the local DNS server or the default gateway/router, depending on the network topology.

7. After establishing a connection with the local DNS server PC1 now knows the IP and MAC addresses of PC2. Suppose PC1 [IP Address: 192.168.2.1, MAC Address: 0010.1191.A946] is sending an ARP packet to PC2 [IP Address: 192.168.2.2, MAC Address: 0110.1290.AD23]. What will be written in the target MAC address before the packet reaches PC2.

ANS: When PC1 sends an ARP packet to PC2 to resolve its IP address to its MAC address, it will set the destination/target MAC address in the Ethernet header of the packet to the MAC address of PC2 [0110.1290.AD23]. This is because PC1 needs to send the ARP packet directly to PC2 to request its MAC address, and the destination MAC address must be set to the MAC address of PC2 for the packet to be delivered to it. The source MAC address in the

Ethernet header of the ARP packet will be set to the MAC address of PC1 [0010.1191.A946], indicating that the packet was sent by PC1. Once the ARP packet is received by PC2, it will respond with an ARP reply containing its MAC address, which PC1 can then use to communicate with PC2 over the network.

8. How can you tell the difference between an ARP request packet and an ARP reply packet as the Ethernet type field on both packets is identical?

ANS: In an Ethernet frame, the Ethernet type field is used to identify the type of protocol data that is encapsulated in the frame. For ARP packets, the Ethernet type field is set to 0x0806, which indicates that the protocol data is an ARP packet. To distinguish between an ARP request packet and an ARP reply packet, we need to examine the opcode field in the ARP packet header. The opcode field specifies whether the packet is an ARP request or an ARP reply. In an ARP request packet, the opcode field is set to 1. This indicates that the packet is a request for the MAC address that corresponds to a specific IP address. In an ARP reply packet, the opcode field is set to 2. This indicates that the packet is a response to an ARP request and contains the MAC address that corresponds to the IP address specified in the original request. So, to tell the difference between an ARP request packet and an ARP reply packet, we need to examine the opcode field in the ARP packet header. If the opcode field is set to 1, it's an ARP request. If the opcode field is set to 2, it's an ARP reply.

9. What is HTTP response and in which layer of OSI model does HTTP work?

ANS: HTTP (Hypertext Transfer Protocol) is a protocol used for transferring data over the World Wide Web. When a client (e.g., web browser) sends an HTTP request to a server (e.g., web server), the server responds with an HTTP response. An HTTP response is a message sent by a server to a client in response to an HTTP request. The response contains the requested resource (e.g., a web page) and metadata about the resource (e.g., status code, content type, etc.). The content of the response is typically in the form of HTML, CSS, JavaScript, images, or other types of data. HTTP is an application layer protocol, which means it operates at the top layer of the OSI (Open Systems Interconnection) model. The OSI model has seven layers, with each layer responsible for a specific aspect of network communication. The application layer (layer 7) is the top layer of the OSI model and is responsible for providing services to applications that communicate over a network. HTTP works at the application layer of the OSI model and uses underlying transport layer protocols such as TCP (Transmission Control Protocol) or UDP (User Datagram Protocol) to establish a connection and transfer data between a client and server.

10. If the flag section of the TCP packet contains 00010000, what type of TCP packet will that be?

ANS: The TCP header consists of several fields, including the flag section, which is a 9-bit field used to control the behavior of TCP connections. The flag section is also called the Control Bits field or the Flags field. The 9 bits of the flag section are divided into several 1-bit flags, with each bit representing a different flag. The flags are used to perform various operations, such as establishing a connection, closing a connection, and acknowledging data. In the flag section of the TCP packet, the 5th bit (counting from the rightmost bit) represents the "ACK" flag, which is set to 1 if the packet is an acknowledgment packet. If the flag section of the TCP packet contains 00010000, it means that the ACK flag is set to 1 and all the other flags are set to 0. Therefore, this is an ACK packet. An ACK packet is a type of TCP packet that is used to acknowledge the receipt of data. When a device receives a TCP packet, it sends an ACK packet back to the sender to confirm that the packet has been received. This helps to ensure that data is transmitted reliably over the network.

11. How many TCP packets does the Client PC send to the server in the process of an HTTP request?

ANS: The number of TCP packets that a client sends to a server in an HTTP request can vary depending on several factors, such as the size of the request and the network conditions. However, in general, an HTTP request involves the following process:

- The client initiates a TCP connection with the server by sending a SYN packet.
- The server responds to the client's SYN packet with a SYN-ACK packet to establish the connection.
- The client sends an ACK packet to the server to confirm the connection.
- The client sends an HTTP request packet to the server.
- The server responds to the client's request with one or more HTTP response packets.

So, in the process of an HTTP request, the client sends at least 3 TCP packets to the server: a SYN packet to initiate the connection, an ACK packet to confirm the connection, and an HTTP request packet to send the request. However, the server's response may require multiple TCP packets to transmit the complete HTTP response back to the client, depending on the size of the response and other network factors.

12. Why does email need both SMTP and POP3 protocols? And how do they work together?

ANS: Email uses both the SMTP (Simple Mail Transfer Protocol) and POP3 (Post Office Protocol version 3) protocols for different stages of the email delivery process.

SMTP is used for sending email messages from the sender's email client to the recipient's email server. When a user composes and sends an email message, the SMTP protocol is

used to transmit the message from the user's email client to the recipient's email server over the internet. SMTP is responsible for delivering the message from the sender to the recipient's mail server, where it is stored until the recipient is ready to retrieve it. POP3, on the other hand, is used for retrieving email messages from a mail server. When the recipient is ready to access their email, they use an email client to connect to their email server using the POP3 protocol. The POP3 protocol allows the email client to retrieve the stored email messages from the recipient's email server and download them to the client's local device for viewing. So, SMTP and POP3 work together to provide end-to-end email communication. When a user sends an email, SMTP is used to send the email message from the sender's email client to the recipient's email server. When the recipient wants to read their email, POP3 is used to retrieve the email messages from the recipient's email server and download them to the recipient's email client for viewing. It's worth noting that there are other email protocols as well, such as IMAP (Internet Message Access Protocol), which also allow users to retrieve email messages from a mail server. IMAP provides more advanced features than POP3, such as the ability to keep messages stored on the server and access them from multiple devices. However, the basic SMTP and POP3 protocols are still widely used for email communication.

13. In a TCP packet coming back from the server, the sequence number is written as 1 and the acknowledgement is written as 1. What do you understand from this scenario? Explain.

ANS: If a TCP packet coming back from the server has a sequence number of 1 and an acknowledgement of 1, it means that the server is acknowledging the receipt of the first byte of data sent by the client. In the TCP protocol, both the client and server keep track of the sequence numbers and acknowledgement numbers for the data they send and receive. When the client sends data to the server, it assigns a sequence number to the first byte of data it sends. The server acknowledges the receipt of the data by sending an acknowledgement packet back to the client with an acknowledgement number that indicates the next expected sequence number that the server is waiting to receive. In our case, the client has sent a packet with a sequence number of 1, indicating that it is the first byte of data being sent. The server has received this packet and is acknowledging it by sending back a packet with an acknowledgement number of 1. This means that the server is expecting the next sequence number to be 2, indicating that it is ready to receive the next byte of data from the client. Overall, this sequence and acknowledgement number exchange between the client and server helps to ensure that data is transmitted reliably between the two endpoints, with each side keeping track of what data has been sent and received.

14. Why is it necessary to map an IP address to a MAC address? Why can't the Ip address be used to represent the MAC address?

ANS: It is necessary to map an IP address to a MAC address because these addresses serve different functions in the network communication process. An IP address is a logical address that identifies a device on an IP network. IP addresses are used for routing and addressing packets of data as they are transmitted over the network. In contrast, a MAC address is a unique identifier assigned to a network interface controller (NIC) of a device. The MAC address is used by the Data Link Layer of the OSI model to identify a specific device on a network. IP addresses and MAC addresses are not interchangeable because they serve different purposes in the network communication process. The IP address is used to identify the destination of the data and is necessary for routing the data across different networks. The MAC address is used to identify the specific device that the data is being sent to on the local network. When a device on a network wants to send data to another device, it needs to know the MAC address of the destination device in order to create an Ethernet frame that can be transmitted over the local network. This is why the Address Resolution Protocol (ARP) is used to map IP addresses to MAC addresses.

In summary, IP addresses and MAC addresses are both important for network communication, but they serve different functions. Mapping an IP address to a MAC address enables a device to create an Ethernet frame that can be transmitted over the local network to the correct destination device.

15. In an outbound PDU packet, what does source port: 1025 and destination port: 80 means?

ANS: In an outbound PDU (Protocol Data Unit) packet, the source port number and destination port number are both 16-bit fields that are used to identify the endpoints of the communication. In the case of a packet with source port number 1025 and destination port number 80, it means that the packet was sent from a process on the local device that is using port number 1025 as its source port, and it is being sent to a process on the remote device that is listening on port number 80 as its destination port. Port number 80 is the standard port used for HTTP (Hypertext Transfer Protocol) traffic, which is used for communicating with web servers. When a device wants to retrieve a web page from a web server, it will send an HTTP request to the web server's IP address, with destination port number 80. The web server will then respond with an HTTP response, which will be sent back to the device's IP address, with source port number 80. In the case of a source port number of 1025, this is a non-standard port that is often used by client applications as their source port number. Client applications will typically choose a random port number between 1024 and 65535 as their source port number, in order to avoid conflicts with other applications using well-known port numbers.

In summary, in an outbound PDU packet, a source port number of 1025 and destination port number of 80 indicates that the packet is being sent from a client application on the local device to a web server on a remote device, using the HTTP protocol.

16. How does your laptop know it's local DNS server?

ANS: When a laptop or any device connects to a network, it needs to obtain an IP address and other network configuration information in order to communicate with other devices on the network. One of the pieces of information that a device typically obtains during this process is the IP address of its local DNS server. This information is usually provided through DHCP (Dynamic Host Configuration Protocol), which is a protocol used to automatically assign IP addresses and other network settings to devices on a network. When a laptop or other device connects to a network using DHCP, it sends a request to the DHCP server on the network to obtain an IP address and other network settings. The DHCP server responds with a lease that includes the device's IP address, subnet mask, default gateway, and DNS server IP address. The laptop then uses this DNS server to resolve domain names to IP addresses. In some cases, the laptop may be configured to use a specific DNS server rather than obtaining one automatically through DHCP. This can be done by manually configuring the DNS server settings in the network adapter settings on the laptop.