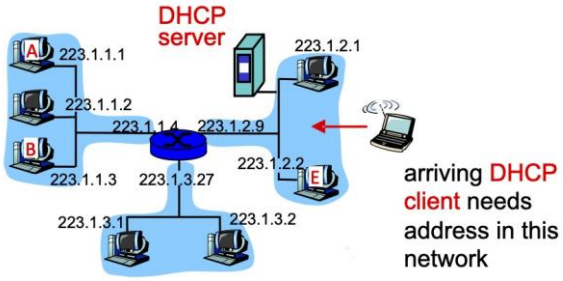
IK2218 Protocols and Principles of the Internet EP2120 Internetworking

Homework 4

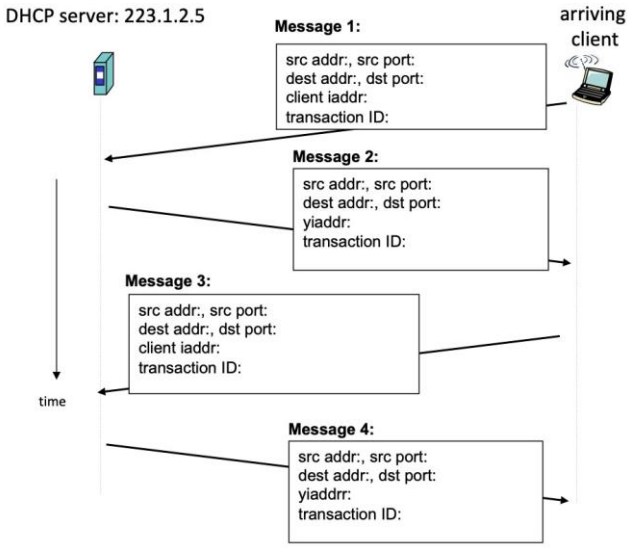
Solutions due: 19:00, October 16, 2023
Review due: 19:00, October 18, 2023

1. DHCP (15 p)

Consider the following scenario, where a DHCP client arrives and requests an IP address from the DCHP server.



In the simplest case, four DHCP messages will be exchanged according to the figure below. Name these four DHCP messages (message type) and fill in the missing fields in each message. You can assume that the subnet to which the DHCP client arrives is a /24 network and that all addresses below 223.1.2.10 are occupied. Based on that, you can let the DHCP server hand out a suitable IP address. You also have to select reasonable transaction IDs.



Ans:

1. **Message1:- DHCP discovery**
   Source address: 0.0.0.0
   Source Port: 68
   Destination address: 255.255.255.255
   Destination port: 67
   Client IP address: 0.0.0.0
   Transaction ID: 655

2. **Message2:-DHCP offer**
   Source address: 223.1.2.5
   Source Port: 67
   Destination address: 255.255.255.255
   Destination port: 68

Your IP address: 223.1.2.4
Transaction ID: 655
Lifetime: 3600 secs

3. **Message3:- DHCP request**
   Source address: 0.0.0.0
   Source Port: 68
   Destination address: 255.255.255.255
   Destination port: 67
   Transaction ID: 655
   Lifetime: 3600 secs

4. **Message4:- DHCP ACK**
   Source address: 223.1.2.5
   Source Port: 67
   Destination address: 255.255.255.255
   Destination port: 68
   Your address: 223.1.2.4
   Transaction ID: 655
   Lifetime: 3600 secs

   The DHCP client successfully obtains an IP address (223.1.2.5) from the DHCP server after these four steps, and the transaction ID is same for all these steps .Both the client and server agree on the lease terms and the assigned IP address.

2. IPv6 Autoconfiguration (10 p)

In IPv6 stateless autoconfiguration, the client can create an IP address based on the client's MAC address, instead of requesting the IP address from a DHCP server. Discuss advantages and problems with using an IPv6 address generated from the MAC address, and explain how IPv6 privacy extensions address the problems.

Ans:

IPv6 stateless autoconfiguration allows client to make IP addreses based on MAC address. Although it has some advantages and drawbacks.

Advantages:

- To solve the problems with using an IPv6 address generated from the MAC address, IPv6 privacy extensions were proposed.
- It is simple to generate an IPv6 address from the MAC address and does not require for any further configuration or the involvement of a DHCP server. This makes network installation and maintenance easier.
- In order to identify and track devices within a network, the IPv6 address is automatically made from the MAC address.

Problems:

- The most common problem that MAC-based IPv6 addresses face is with user privacy. These addresses are unique and static, which makes it easier to track the movements and activities of the device in the network.
- The device and its IP address are inseparably linked via MAC-based IPv6 addresses. This is a challenge since a device may want to modify its IP address for security reasons.
- These IPv6 addresses based on MAC are generally predictable making them exploitable to perform attacks on the network.

The IPv6 privacy extensions were introduced to prevent the problems that were caused with the usage of MAC-based Ipv6 addresses.

- These extensions involved creating random and temporary interface identifiers which prevent the devices from getting tracked down easily.
- The IPv6 privacy extension allowed periodic change of addresses which improved privacy by making the device link to different addresses over time.
- Devices using IPv6 can also produce a consistent IPv6 address over time. For services like server applications, where persistence is necessary, this stable address can be used.

3. Firewalls (25 p)

Firewalls can be placed in a number of different places, providing different protection. Give at least three examples of places where deploying firewalls is motivated, and explain the motivation for placing them there.

Ans:

Firewalls can be placed in a number of different places, providing different protection based on the requirements of the network and security goals. The three examples where they are motivated are:

1) **Network Perimeter:**
   Having a firewall in the network perimeter is usually a general way to protect a company/organization's network from external threats like malware, cyberattacks and unauthorized access from the internet. And the motivation for using firewalls at network perimeter includes:
   - Firewall at the network perimeter functions as a filter for incoming traffic that allows only authorized traffic to get into the network and blocks any other malicious or unauthorized access.
   - It can also be very crucial in preventing DDOS attacks by blocking excess traffic from a single source.
   - Also, the firewalls can provide security in application layers.
2) **Internal Network Segments:**
   Placing firewalls between the segments in the internal architecture of an organization's network can help in identifying and fixing the major security breaches & threats, and protect sensitive data. And the reasons for motivation include:

- Based on trust levels, the firewalls can segment the organization's network into different zones (ex: separating high-security zone from lower ones).
- Strict access control rules are enforced by firewalls in the segments making it more secure and only authorizing the trusted users to communicate.
- Firewalls can also control the traffic flow in less secure segments that can prevent untrusted access to private data.

3) Host-based firewalls:

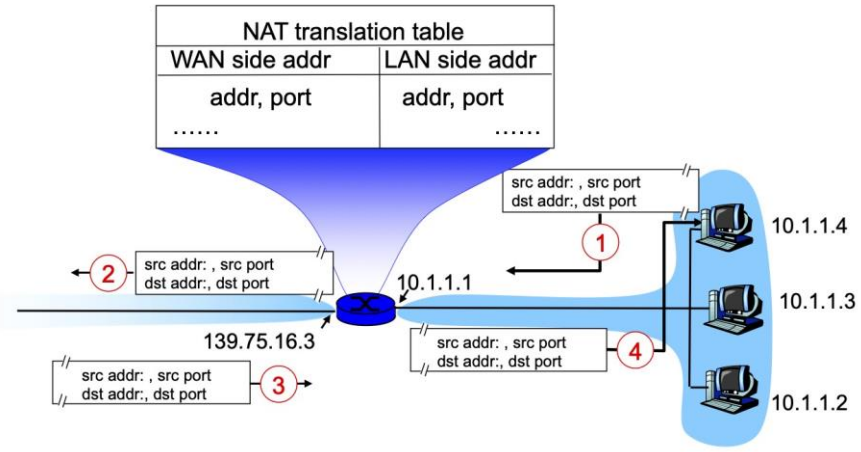
The firewalls deployed on separate individual devices/servers are called host-based and the main reason for using them is to protect devices from local network-based threats. And the motivation for using them include:

- The firewalls protect devices from malware by blocking communication with malicious IP addresses or websites and also the infections on the host's device.
- They enhance the application layer security as they can control the applications that are allowed to communicate over the network.
- Also, they have control over which users/processes can start or receive network connections.

4. NAT (25 p)

Consider the figure below. Assume that host 10.1.1.4 on a private network (10.1.1.0/24) sends an HTTP request through its NAT box to a web server on address 130.237.20.12 and that this web server answers with an HTTP response back to the host. Fill in

source address, source port, destination address, and destination port in the IP packets 1-4 in the figure. Also, fill in the NAT table as it will look when the four packets have been exchanged.



- **PACKET 1:**
  Source address: 10.1.1.4
  Source port: 3345
  Dest address: 130.237.20.12
  Dest port: 80

- **PACKET 2:** Nat router changes datagram source address from 10.1.1.4 to
  Source address:139.75.16.3
  Source port: 5001
  Dest address: 130.237.20.12
  Dest port: 80

- **PACKET 3:** Reply arrives
  Source address: 130.237.20.12
  Source port: 80
  Dest address: 139.75.16.3
  Dest port: 5001

- **PACKET 4:** Nat router changes datagram destination address from 139.75.16.3 to
  Source address: 130.237.20.12
  Source port: 80
  Dest address: 10.1.1.4
  Dest port: 3345

- **NAT translation table:**

WAN side address	LAN side address
139.75.16.3, 5001	10.1.1.4, 3345

5. Software-Defined Networking (25 p)

(a) Describe the traditional model of a router, partitioned into a control plane and data plane. Your answer should cover properties of control plane and data plane and examples of functions in the control plane and data plane respectively.

(b) Explain the idea of generalized forwardingand software-defined networking (SDN). What does it mean that the SDN control plane is (15 p)

logically centralized? In what way is SDN forwarding more general than traditional IP forwarding? What is the OpenFlow protocol?

(a)Ans:

The traditional model of router is partitioned into two parts known as control plane and data plane. These planes differ by how the routers work and mage the traffic in the network.

1) **Control plane:**

The main responsibility of the control plane is to make decisions on how the data traffic is sent/forwarded in the network. It handles the routing protocols, and routing tables and decides the most efficient path for the data from source to destination. Its functionalities mainly lies in decision & selection of routes, topology & management of the network. It basically establishes a connection for communication with other routers and devices to exchange routing information and other network details.

Example functions:

- Routing protocols such as RIP and OSPF, which are used to exchange routing information.
- The plane maintains the routing tables that contain data about the network paths available.
- Also, it handles network events such as link failures and automatically makes the routing decisions based on the current network state.

2) **Data Plane:**

The data plane is mainly responsible for the transmission of data packets in the network and that's the reason it is also known as the packet forwarding plane. The decisions made by the control plane enables the data plane to forward packets from the source address to the destination. Therefore, the data plane doesn't itself make the routing decision but only is responsible for high-speed packet forwarding. It also makes sure that the packet transfer has less latency, ensuring efficient processing and maximum throughput.

Example functions:

- As said earlier packet forwarding is the main function of data plane which involves finding and redirecting packets to correct destination address according to the routing table.
- Also the plane has this functionality to check the packet header to make forwarding decisions, this process is known as packet switching.
- Qos(Quality of service) enforcement where data plane gives priority to some specific traffic types.
- To manage which packets are permitted or refused, access control and filtering techniques like firewall rules and Access Control Lists (ACLs) are used.

(b)

- **Generalized Forwarding:** We could say that generalized forwarding is an extension of traditional IP forwarding that allows more flexible and adaptable handling of network traffic. It involves separating the actual data forwarding process (data plane) from the decision-making process (control plane) in network devices, increasing the programmability and flexibility of the network infrastructure. The forwarding decisions are made based on different factors not just IP addresses but also application awareness, patterns of the traffic, and policies. This type of forwarding can adjust to any changing network states that prioritize particular types of traffic and makes resource utilization more efficient.

- **Software-defined networking (SDN):** The idea of general forwarding is embodied in the networking architecture known as SDN. The data plane is separated from the control plane in SDN and the software based controllers are responsible for the decision making and the network intelligence. Networks become more agile and responsive to changing requirements by using SDN, which enables network administrators to design and configure network behavior via software. In order to guarantee connectivity across various network devices and vendors, SDN is implemented utilizing open, standardized protocols and interfaces.

- The control plane in SDN is logically centralized, meaning that the decision-making authority lies in a central controller or a set of controllers. It allows an overall view of the whole network which helps the controller to have a good understanding of the topology and traffic of the network. Other than control plane the data plane may still be distributed throughout the network and the controller connects with these devices to convey the forwarding details.

- SDN forwarding is more general than traditional forwarding as it can make forwarding decisions based on a variety of factors, not only IP addresses but can take into account the network traffic, the quality of service (QoS) specifications, network policies, and current network conditions. In traditional IP forwarding, a packet's next hop is essentially determined by the destination IP address.

- The SDN controller and network devices (such switches and routers) in the data plane can communicate with one another using the open-source OpenFlow protocol. It gives the controller a means of directing how packets and flows should be handled by network devices.