Network Layer Protocols

Overview

Internet Control Message Protocol can be a network layer protocol used by network devices to diagnose network communication problems. ICMP is used primarily to determine whether data arrives at its intended destination in time. The ICMP protocol is generally used in network devices such as routers. ICMP is essential for error testing and reporting, but it can also be used for distributed denial of service (DDoS) attacks. It is a protocol by which devices in the network often communicate with data transmission problems. In this definition of ICMP, the first method used by ICMP is to determine whether the data arrives at the destination at the correct time. This makes ICMP an essential aspect of the error reporting process and testing to assess data transmission status over the network. However, it can also run distributed denial of service (DDoS) attacks. The way ICMP works in network communication is similar to communication between a carpenter who builds a house and a home improvement store. Assuming that all the components arrive in the correct order, the store will deliver utility poles, floors, roofing materials, insulation materials, etc.

ARP

Address Resolution Protocol (ARP) can be a protocol or program that connects changing Internet Protocol (IP) addresses to hard and fast physical machine addresses, also known as media access control addresses (MAC). The IP and MAC addresses have different lengths and need to be converted so that the system can recognize each other. The most widely used IP today is IP version 4 (IPv4). The length of the IP address is 32 bits. However, the size of the MAC address is 48 bits. ARP converts the address from 32 bits to 48 bits and vice versa. There is a network model called the Open Systems Interconnection (OSI) model. The OSI model was first developed in the late 1970s, and the usage layer provides the IT team with a visualization of what is happening in a particular network system. This will help determine which layer affects the applications, devices, or software installed on the network and which IT or engineering professional is responsible for managing that layer. The MAC address is also called the information link layer, which establishes and terminates a connection between two physically connected devices for data transmission. The IP address is further mentioned because the network layer is responsible for forwarding knowledge packets through different routers. ARP works between these layers. Devices that are in a local area network (LAN) are programmed to communicate using link-layer addresses. The switch is not configured for a specific IP, allowing the destination to decide to match the IP within the equivalent broadcast domain. Tools that are not connected to the network will not have an IP address. In this case, the network must resort to the use of MAC addresses for communication. If a tool wants to talk to another device on the same LAN, it must know the MAC address of the other device's NIC. This allows communication between 2 end devices to be unicast.

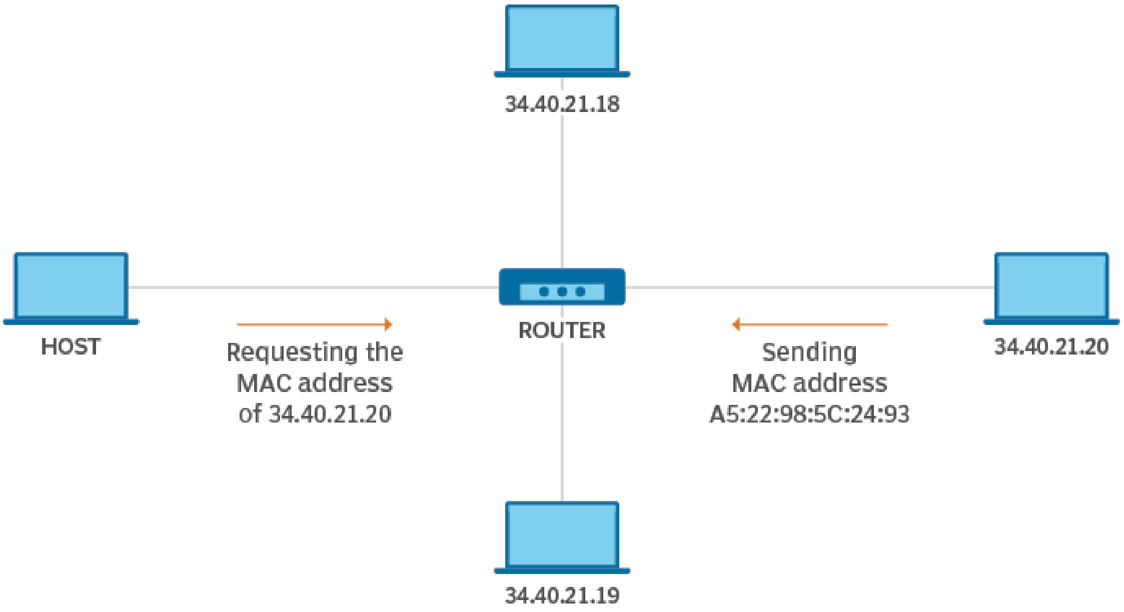
34.40.21.18
HOST
Requesting the MAC address of 34.40.21.20
ROUTER
Sending MAC address A5:22:98:5C:24:93
34.40.21.20
34.40.21.19

Figure 1: ARP

RARP

RARP is used on older diskless workstations. These old hosts do not have disks and, therefore, cannot store IP addresses. They have a hard-coded MAC address. When the workstation starts, it transmits RARP requests using its MAC address. In the host equivalent network, we have a RARP server that logs RARP requests. The server has a table that contains a combination of MAC and IP addresses. When it receives a RARP request, it checks its table to find the IP address that matches the MAC address in the RARP request packet. Then, the RARP server responds to the host with a RARP reply. When the host receives the RARP response, it knows its IP address.

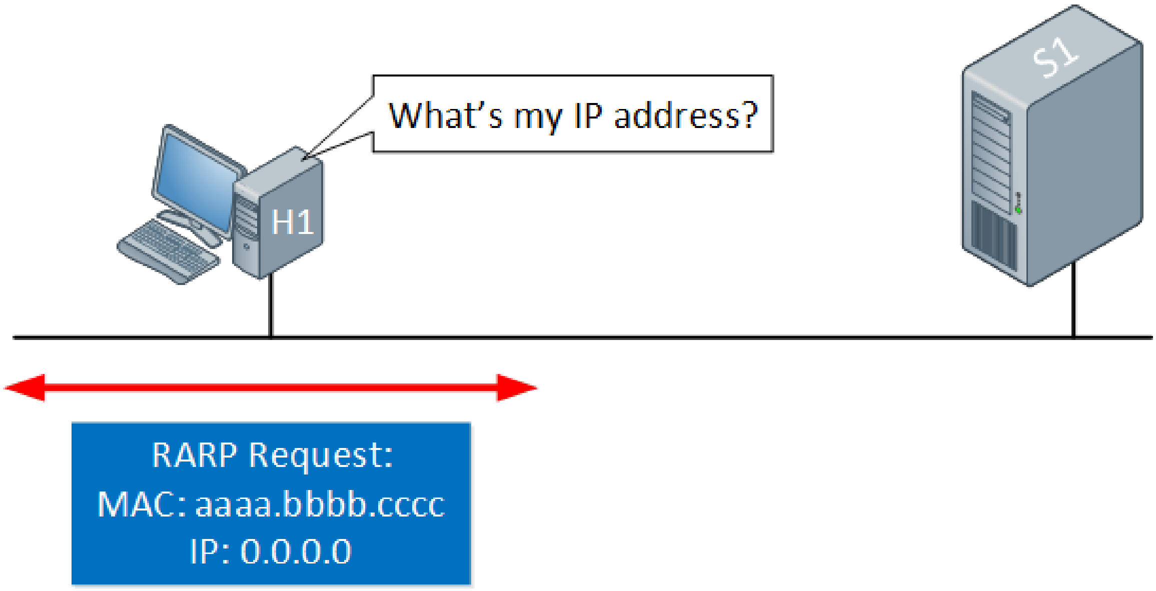

Figure 2: RARP

BOOTP

Bootstrap Protocol (BOOTP) provides a dynamic method of associating workstations with servers. It also provides a process for assigning workstation Internet Protocol (IP) addresses and initial program load (IPL) sources. BOOTP can be TCP/IP protocol. It allows the client to look up its IP address and thus the uploaded file's name from the webserver. The customer uses BOOTP to find this information without the customer's user intervention. The BOOTP server listens on the well-known port 67 of the BOOTP server, also used by the Dynamic Host Configuration Protocol (DHCP). Therefore, BOOTP and DHCP cannot run simultaneously on equivalent systems. (DHCP is the preferred method to support BOOTP clients.) When the server receives a request from the client, it sets an IP address for the client and returns a response to it. This response contains the IP address of the client and thus the name of the uploaded file. The client then initiates a Trivial File Transfer Protocol (TFTP) request to the server to get the uploaded file. The

The bootstrap protocol is used during the startup process to determine the network connection during the initial startup of the computer. Initially, the protocol used a floppy disk, but it was quickly integrated into the motherboard's hardware and network adapter, so no drivers were required.

BOOTP can be a broadcast protocol because it must send dubbing messages to all available hosts on the network to request responses or resources. BOOTP is used during the boot process when the PC is initially started, hence the name. BOOTP initially required the use of a floppy disk to determine the initial network connection. Still, this method was quickly integrated into the BIOS of the network interface card and motherboard to allow direct network boot.

BOOTP is designed for diskless systems because they need a protocol to communicate with the server to obtain the network address and information about which operating system to use. The computer then downloads the operating system through a standard file transfer protocol.

DHCP

Dynamic Host Configuration Protocol (DHCP) can be a network management protocol that does not automatically configure devices on the IP network, allowing them to use network services such as DNS, NTP, and any communication protocol that support UDP or TCP. The DHCP server dynamically assigns IP addresses and other network configuration parameters to each device on the network to communicate with other networks. DHCP is an improvement on the old protocol called BOOTP. The first reason for the need for DHCP is to simplify the management of IP addresses on the network. No two hosts can have the same IP address. If you configure them manually, errors are likely to occur. Manual IP address assignment is often confusing in small networks, especially for mobile devices that do not permanently require IP addresses. In addition, most users are not technically capable of locating and assigning IP address information on the computer. Automating this process makes the lives of users and network administrators easier. The following are the components of DHCP:

- **DHCP Server** A network device runs the DCHP service, containing the IP address and related configuration information. This is usually the most typical server or router, but it could also be anything that acts like a number, such as an SDWAN device.
- **DHCP Client** - An endpoint that receives configuration information from a DHCP server. This will be a computer, mobile device, IoT endpoint, or any device that needs to be connected to the network. Most configurations receive DHCP information by default.
- **IP Address Pool** - The range of addresses available to DHCP clients. The addresses are generally distributed from smallest to largest.
- **Subnet:** An IP network is generally divided into segments called subnets. Subnets help maintain the manageability of the network.
- **Lease:** The length of time that the DHCP client retains the IP address information. When the lease expires, the customer must renew it.

- **DHCP Relay:** The router or host listens for messages from the client broadcast on its network and then forwards them to the configured server. The server then sends the responses to the relay agent, passing them on to the client. This will not centralize the DHCP servers instead of having one server on each subnet.