         What is a Host?

A host (also known as "network host") is a computer or other device that communicates with other hosts on a network. Hosts on a network include clients and servers -- that send or receive data, services or applications.

         What are Network Devices? Study different types of network devices.

**Network devices**, or networking hardware, are physical devices that are required for communication and interaction between hardware on a computer network.

* **Hub**.

A network hub is a node that broadcasts data to every computer or Ethernet-based device connected to it. A hub is less sophisticated than a switch, the latter of which can isolate data transmissions to specific devices. Network hubs are best suited for small, simple local area network (LAN) environments

* **Switch**.

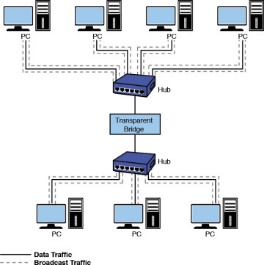
Switches are key building blocks for any network. They connect multiple devices, such as computers, wireless access points, printers, and servers; on the same network within a building or campus. A switch enables connected devices to share information and talk to each other.

* **Router**.

A router is a switching device for networks, which is able to route network packets, based on their addresses, to other networks or devices. Among other things, they are used for Internet access, for coupling networks or for connecting branch offices to a central office via VPN (Virtual Private Network).

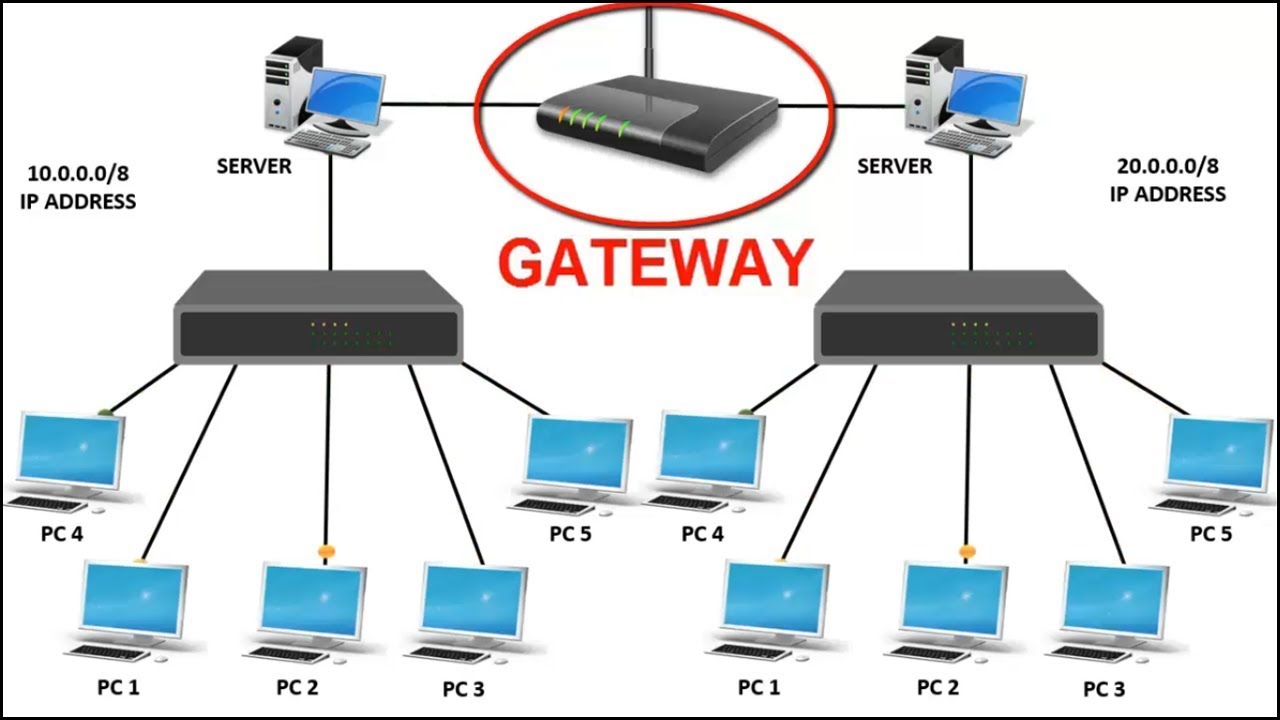
* **Bridge**.

A bridge can be used in computer networks to interconnect two LANs together and separate network segments. This makes it possible to isolate or segment the network data traffic.



* **Gateway**.

A gateway is a hardware device that acts as a "gate" between two networks. It may be a router, firewall, server, or another device that enables traffic to flow in and out of the network. For example, a proxy server may only allow local computers to access a list of authorized websites.



* **Modem**.

A **modem** or **broadband** **modem** is a hardware device that connects a computer or router to a broadband network. For example, a cable modem and DSL modem are two examples of these types of Modems. Similarly, when an analog signal is received, the modem converts it back ("demodulates" it) to a digital signal.

* **Repeater**.

Repeater is a network device that retransmits a received signal with more power and to an extended geographical or topological network boundary than what would be capable with the original signal. Repeaters are also known as signal boosters.

Access Point.

         What is sequence number in a TCP packer?

The sequence number is a counter used to keep track of every byte sent outward by a host. If a TCP packet contains 1400 bytes of data, then the sequence number will be increased by 1400 after the packet is transmitted. ... This number is a counter to keep track of every byte that has been received

         What is a port?

A port is a virtual point where network connections start and end. Ports are software-based and managed by a computer's operating system. Each port is associated with a specific process or service.

         Study different common ports.

|  |  |
| --- | --- |
| Port Number | Usage |
| 20 | File Transfer Protocol (FTP) Data Transfer |
| 21 | File Transfer Protocol (FTP) Command Control |
| 22 | Secure Shell (SSH) |
| 23 | Telnet - Remote login service, unencrypted text messages |
| 25 | Simple Mail Transfer Protocol (SMTP) E-mail Routing |
| 53 | Domain Name System (DNS) service |
| 80 | Hypertext Transfer Protocol (HTTP) used in World Wide Web |
| 110 | Post Office Protocol (POP3) used by e-mail clients to retrieve e-mail from a server |
| 119 | Network News Transfer Protocol (NNTP) |
| 123 | Network Time Protocol (NTP) |
| 143 | Internet Message Access Protocol (IMAP) Management of Digital Mail |
| 161 | Simple Network Management Protocol (SNMP) |
| 194 | Internet Relay Chat (IRC) |
| 443 | HTTP Secure (HTTPS) HTTP over TLS/SSL |

         Difference between telnet and SSH.

Telnet transfers the data in simple plain text. On other hand SSH uses Encrypted format to send data and also uses a secure channel. No authentication or privileges are provided for user's authentication. As SSH is more secure so it uses public key encryption for authentication.

         Study about network Layer 2 and Layer 3 attacks.

* ARP (Address resolution Protocol) Poisoning:

The attack works as follows: The attacker must have access to the network. They scan the network to determine the IP addresses of at least two devices⁠—let's say these are a workstation and a router. The attacker uses a spoofing tool, such as Arpspoof or Driftnet, to send out forged ARP responses.

* DHCP spoofing:

DHCP spoofing occurs when an attacker attempts to respond to DHCP requests and trying to list itself (spoof) as the default gateway or DNS server, hence, initiating a man in the middle attack

Whereas

* IP Spoofing:

In IP spoofing, a hacker uses tools to modify the source address in the packet header to make the receiving computer system think the packet is from a trusted source, such as another computer on a legitimate network, and accept it. Because this occurs at the network level, there are no external signs of tampering.

* ICMP attack:

An ICMP request requires some server resources to process each request and to send a response. ... The attacker sends many ICMP echo request packets to the targeted server using multiple devices. The targeted server then sends an ICMP echo reply packet to each requesting device's IP address as a response.

* DoS attack with fake IPs:

A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users.

In a DoS attack, hackers use spoofed IP addresses to overwhelm computer servers with packets of data, shutting them down.