Ports

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. Ports allow computers to easily differentiate between different kinds of traffic: emails go to a different port than webpages, for instance, even though both reach a computer over the same Internet connection.

They are different types of ports in networking.

1.Port 20

These Ports are used for FTP (file transfer protocol) connection. FTP uses two TCP connections for communication. Port 20 transfer only the data.

2.Port 21

FTP is a standard network protocol used for transferring files from one host to another over a TCP-based network, such as the internet.

Port 21 is used for pass control information.

3.Port 22

Secure Shell (SSH), secure logins, file transfers (scp, sftp) and port forwarding.Port 22 is the designated port for SSH, allowing devices to establish secure connections for remote administration and file transfer. It's important to note that port 22 must be open and accessible on the network for SSH connections to be established.

4.Port 23

Port 23 is typically used by the Telnet protocol. Telnet commonly provides remote access to a variety of communications systems. Telnet is also often used for remote maintenance of many networking communications devices including routers and switches.

5.Port 25

Port 25 is the default SMTP port that is used to enable communication between the sending and receiving servers when delivering an email message to a recipient. Despite its pedigree, many ISPs (Internet Service Providers) and email providers have started to block incoming connections on port 25 as a security measure.

6.Port 53

The standard port for DNS is port 53. DNS client applications use the DNS protocol to query and request information from DNS servers, and the server returns the results to the client using the same port. Port 53 is used for both TCP and UDP communication.

7.Port 67/68

The DHCP employs a connectionless service model, using the User Datagram Protocol (UDP). It is implemented with two UDP port numbers for its operations which are the same as for the bootstrap protocol (BOOTP). The server listens on UDP port number 67, and the client listens on UDP port number 68.

8.Port 80

The number that identifies Internet packets as Web transactions (HTTP transactions). All port numbers reside in the header of the packets, and requests that are marked port 80 are processed by the Web server (see TCP/IP port). Port 80 requests may activate any number of different server-side processes before a Web page or some other file is returned to the user.

9.Port 123

Network Time Protocol (NTP) is an internet protocol used to synchronize with computer clock time sources in a network. It belongs to and is one of the oldest parts of the TCP/IP suite. The term NTP applies to both the protocol and the client-server programs that run on computers.

10.Port 161,162

SNMP uses both port 161 and port 162 for sending commands and messages. SNMP managers communicate with SNMP agents through designated SNMP ports. SNMP message transfers happen via the User Datagram Protocol (UDP).

11.Port 389

Port 389 has historically been used for unencrypted connections into an LDAP server. Port 636 is used for legacy SSL connections. Port 389 is used for TLS connections; TLS establishes a non encrypted connection on port 389 that it 'upgrades' to an encrypted TLS connection as the initial connection proceeds.

12.Port 443

Port 443 is the standard port for HTTPS, the secure version of HTTP. HTTPS is used by websites and other online services to protect your data from being intercepted by eavesdroppers. Imagine port 443 as a secure tunnel between your web browser and a website.