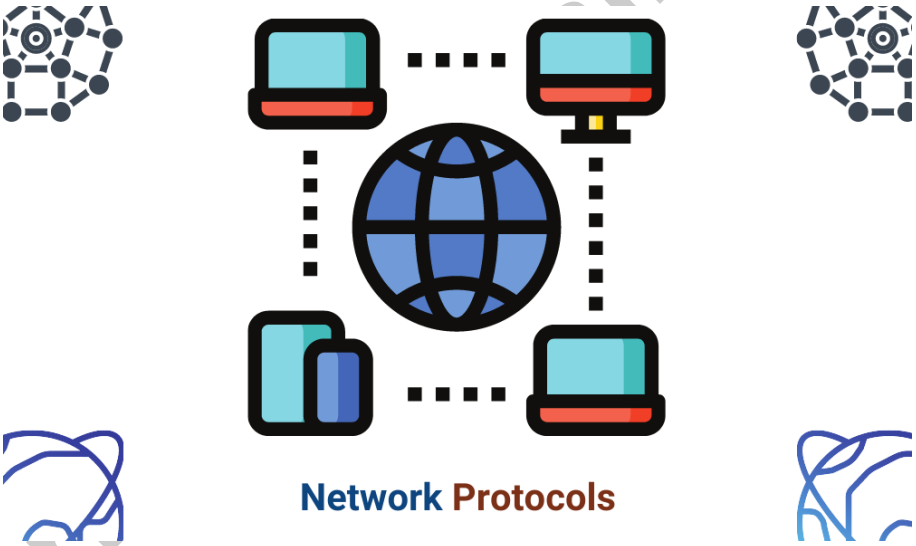
17th Oct 2023

Network Protocol

- In networking, a protocol is a set of rules and conventions for formatting and processing data.



- SSH Protocol - Used For Login on Linux Servers (DevOps)
    - SSH Port - 22
- RDP Protocol - Used For Login on Windows Servers (AWS)
    - RDP Port - 3389
- HTTP Protocol - Used For Viewing Web Pages on internet (Java)
    - HTTP Port - 80

What are the different port numbers?

There are 65,535 possible port numbers, although not all are in common use. Some of the most commonly used ports, along with their associated networking protocol, are:

- **Ports 20 and 21**: File Transfer Protocol (FTP). FTP is for transferring files between a client and a server.
- **Port 22**: Secure Shell (SSH). SSH is one of many tunneling protocols that create secure network connections.
- **Port 25**: Simple Mail Transfer Protocol (SMTP). SMTP is used for email.
- **Port 53**: Domain Name System (DNS). DNS is an essential process for the modern Internet; it matches human-readable domain names to machine-readable IP addresses, enabling users to load websites and applications without memorizing a long list of IP addresses.
- **Port 80**: Hypertext Transfer Protocol (HTTP). HTTP is the protocol that makes the World Wide Web possible.
- **Port 443**: HTTP Secure (HTTPS). HTTPS is the secure and encrypted version of HTTP. All HTTPS web traffic goes to port 443. Network services that use HTTPS for encryption, such as DNS over HTTPS, also connect at this port.
- **Port 3389**: Remote Desktop Protocol (RDP). RDP enables users to remotely connect to their desktop computers from another device.

Firewall

- A firewall can be defined as a special type of network security device or a software program that monitors and filters incoming and outgoing network traffic based on a defined set of security rules (protocols & ports).

- The primary purpose of a firewall is to allow non-threatening traffic and prevent malicious or unwanted data traffic for protecting the computer from viruses and attacks.