**Additional protocols**

Innhold

[Dynamic Host Configuration Protocol 1](#_Toc193099214)

[Address Resolution Protocol 1](#_Toc193099215)

[Telnet 1](#_Toc193099216)

[Secure shell 1](#_Toc193099217)

[Post office protocol 1](#_Toc193099218)

[Internet Message Access Protocol 2](#_Toc193099219)

[Simple Mail Transfer Protocol 2](#_Toc193099220)

[Protocols and port numbers 2](#_Toc193099221)

## Dynamic Host Configuration Protocol

**DHCP** is in the management family of network protocols. **DHCP** is an application layer protocol used on a network to configure devices. It works with the router to assign a unique IP address to each device and provides the addresses of the appropriate **DNS server** and default gateway for each device. **DHCP** servers operate on **UDP** port **67** while **DHCP** clients operate on **UDP** port **68.**

## Address Resolution Protocol

**ARP** is mainly a network access layer protocol in the **TCP/IP** model used to translate the IP addresses that are found in data packets into the **MAC address** of the hardware device. Each device on the network performs **ARP** and keeps track of **matching** **IP** and **MAC addresses** in an **ARP cache**. **ARP** does not have a specific port number since it is a layer 2 protocol and port numbers are associated with the layer 7 application layer.

## Telnet

**Telnet** is an application layer protocol that is used to connect with a remote system. **Telnet** sends all information in clear text. It uses command line prompts to control another device similar to secure shell (**SSH**), but telnet is not as secure as **SSH**. **Telnet** can be used to connect to local or remote devices and uses **TCP** port **23**.

## Secure shell

**SSH** or Secure shell protocol is used to create a secure connection with a remote system. This application layer protocol provides an alternative for secure authentication and encrypted communication. **SSH** operates over the **TCP** port **22** and is a replacement for less secure protocols, such as **Telnet**.

## Post office protocol

**POP** is an application layer (layer 4 of the TCP/IP model) protocol used to manage and retrieve email from a mail server. **POP3** is the most commonly used version of **POP**. Many organizations have a dedicated mail server on the network that handles **incoming and outgoing mail** for users on the network. User devices will send requests to the remote **mail server** and download email messages locally. If you have ever refreshed your email application and had new emails populate in your inbox, you are experiencing **POP** and **internet Message Access Protocol (IMAP)** in action. **Unencrypted**, plaintext authentication uses **TCP/UDP** port **110,** and encrypted emails use **Secure Sockets Layer/Transport Layer Security (SSL/TLS**) over **TCP/UDP** port **995**. When using **POP**, mail has to finish downloading on a local device before it can be read. After downloading, the mail may or may not be deleted from the mail server, so it does not guarantee that a user can sync the same email across multiple devices.

## Internet Message Access Protocol

**IMAP** is used for incoming email. It downloads the headers of emails and the message content. The content also remains on the email server, which allows users to access their email from multiple devices. **IMAP** uses **TCP** port **143** for unencrypted email and **TCP** port **993** over the **TLS** protocol. Using IMAP allows users to partially read email before it is finished downloading. Since the mail is kept on the mail server, it allows a user to sync emails across multiple devices.

## Simple Mail Transfer Protocol

**SMTP** is used to transmit and route email from the sender to the recipient’s address. **SMTP** works with **Message Transfer Agent** (**MTA**) software, which searches **DNS servers** to resolve email addresses to IP addresses, to ensure emails reach their intended destination. **SMTP** uses **TCP/UDP** port **25** for unencrypted emails and **TCP/UDP** port **587** using **TLS** for encrypted emails. The **TCP** port **25** is often used by high-volume spam. **SMTP** helps to filter out spam by regulating how many emails a source can send at a time.

## Protocols and port numbers

Port numbers are used by network devices to determine what should be done with the information contained in each data packet once they reach their destination. **Firewalls** can filter out unwanted traffic based on port numbers. For example, an organization may configure a firewall to only allow access to **TCP** port **995** (**POP3**) by IP addresses belonging to the organization.

Et bilde som inneholder tekst, skjermbilde, nummer, Font

KI-generert innhold kan være feil.