# Generelle protokoller

Indholdsfortegnelse

[FTP (File Transfer Protocol) 1](#_Toc132871550)

[SMTP (Simple Mail Transfer Protocol): 2](#_Toc132871551)

[SSL (Secure Sockets Layer): 2](#_Toc132871552)

[Når SMTP og SSL kombineres: 2](#_Toc132871553)

[TLS (Transport Layer Security) 2](#_Toc132871554)

[TCP (Transmission Control Protocol): 4](#_Toc132871555)

[UDP (User Datagram Protocol): 4](#_Toc132871556)

[HTTPS (Hypertext Transfer Protocol Secure 4](#_Toc132871557)

[DNS 5](#_Toc132871558)

[MX 6](#_Toc132871559)

[DHCP (Dynamic Host Configuration Protocol): 6](#_Toc132871560)

[IP-adresser: 7](#_Toc132871561)

[SMB-protokollen: 7](#_Toc132871562)

[ICMP (Internet Control Message Protocol): 8](#_Toc132871563)

[Web Services: 8](#_Toc132871564)

[SLAAC (Stateless Address Autoconfiguration): 9](#_Toc132871565)

FTP (File Transfer Protocol) er en protokol, der bruges til at overføre filer mellem forskellige enheder over internettet. Her er nogle vigtige punkter om FTP:

* FTP bruger normalt port 21 (TCP) til at etablere en forbindelse mellem to enheder: klienten, der sender filerne, og serveren, der modtager filerne.
* Når en forbindelse er etableret, kan en bruger logge på serveren ved at indtaste et brugernavn og en adgangskode.
* Brugere kan navigere gennem serverens filstruktur og overføre filer ved at trække og slippe filer fra klienten til serveren eller ved at bruge kommandoer, der er specifikke for FTP-protokollen.
* FTP understøtter to forskellige tilstande: ASCII og binær tilstand. ASCII-tilstand bruges til at overføre tekstfiler og binær tilstand bruges til at overføre binære filer, såsom billeder eller programmer.
* Der er flere variationer af FTP-protokollen, såsom SFTP (Secure File Transfer Protocol) og FTPS (FTP over SSL/TLS), der bruger sikkerhedsteknologier til at kryptere data under overførslen og beskytte mod uautoriseret adgang.
* FTP bruges ofte af webudviklere til at uploade filer til en webserver, såsom HTML-filer, billeder og scripts.

Samlet set er FTP en vigtig protokol for at overføre filer mellem enheder over internettet og har en række anvendelser inden for webudvikling og andre industrier.

# SMTP (Simple Mail Transfer Protocol):

* SMTP er en protokol, der bruges til at sende og modtage e-mails over internettet.
* Det fungerer ved at bruge port 25 (TCP) på mailserveren til at kommunikere med andre mailservere og leverer e-mails til modtagerens mailserver.
* SMTP-protokollen kan også bruge andre porte, såsom 587 (TCP) eller 465 (TCP/SSL), afhængigt af konfigurationen.

# SSL (Secure Sockets Layer):

* SSL er en sikkerhedsteknologi, der bruges til at kryptere data, der sendes mellem to enheder på internettet.
* Det fungerer ved at oprette en sikker forbindelse mellem en klient og en server og kryptere alle data, der sendes mellem de to enheder.
* SSL blev erstattet af TLS (Transport Layer Security) og er nu kendt som TLS/SSL.

## Når SMTP og SSL kombineres:

* Ved at bruge SSL med SMTP-protokollen, kan e-mails sendes sikkert og beskyttes mod uautoriseret adgang.
* SMTP over SSL bruger normalt port 465 (TCP/SSL) til at sikre forbindelsen.
* Ved brug af SSL med SMTP, kræves der en gyldig SSL-certifikat på serveren for at sikre, at forbindelsen er autentisk og pålidelig.

TLS (Transport Layer Security) er en krypteringsprotokol, der sikrer sikker kommunikation over internettet. Nogle bulletpoints om TLS inkluderer:

* TLS bruger krypteringsalgoritmer til at beskytte data, der overføres mellem en klient (f.eks. en webbrowser) og en server.
* TLS sikrer, at dataene ikke kan aflyttes eller ændres af uautoriserede parter, mens de overføres.
* TLS bruges i mange internetprotokoller, såsom HTTPS, FTPS, SMTPS og andre.

# TCP (Transmission Control Protocol):

* TCP er en pålidelig og ordnet protokol, der sikrer, at data overføres fra en enhed til en anden uden at miste eller duplikere data.
* TCP opretter en forbindelse mellem senderen og modtageren før overførslen af data og giver også mulighed for at opdele data i mindre pakker for at lette overførslen.
* TCP indeholder også en mekanisme til at håndtere konflikter og fejl under overførslen af data, hvilket sikrer, at dataene ankommer på modtagerens side i samme rækkefølge, som de blev sendt.
* Handshaking: TCP bruger en tre-trins handshaking-proces for at oprette en forbindelse mellem senderen og modtageren. Dette involverer en SYN-besked fra senderen, en SYN-ACK-besked fra modtageren og en ACK-besked fra senderen for at bekræfte, at forbindelsen er oprettet.
* Porte: TCP bruger portnumre til at identificere de applikationer, der er ansvarlige for at sende og modtage data. Der er 65.535 porte, der kan bruges til forskellige applikationer, og standard TCP-porte er normalt tildelt bestemte applikationer.
* CRC: TCP bruger en CRC (Cyclic Redundancy Check) til at sikre, at dataene er blevet overført korrekt, og at der ikke er sket nogen beskadigelse under overførslen.
* Acknowledgement (ACK): TCP sender ACK-pakker tilbage til afsenderen for at bekræfte, at dataene er modtaget korrekt. Hvis afsenderen ikke modtager en ACK-pakke, antages det, at dataene ikke er blevet leveret korrekt, og de sendes igen.

# UDP (User Datagram Protocol):

* UDP er en hurtig og enkel protokol, der ikke har nogen mekanismer til at sikre, at data overføres på en pålidelig og ordnet måde.
* UDP sender data som datagrammer, som er små pakker, der kan sendes uden at oprette en forbindelse først.
* UDP er ideel til applikationer, der kræver hurtig dataoverførsel, og hvor et lille tab af data ikke er afgørende, f.eks. streaming af video eller online spil.

HTTPS (Hypertext Transfer Protocol Secure) er en sikker version af HTTP-protokollen, der bruges til at sende og modtage data over internettet.

* HTTPS bruger krypteringsteknologier, såsom SSL (Secure Sockets Layer) og TLS (Transport Layer Security), til at kryptere data, der overføres mellem en webbrowser og en webserver.
* HTTPS fungerer ved at bruge en certifikatudbyder til at udstede et SSL/TLS-certifikat til webserveren, som bekræfter serverens identitet og sikrer forbindelsen.
* Når en webbrowser opretter forbindelse til en sikker webside via HTTPS, vises der et hængelåsikon i browserens adressefelt for at indikere, at forbindelsen er sikker.
* HTTPS beskytter mod angreb, såsom man-in-the-middle-angreb, hvor en hacker kan fange data, der sendes mellem en browser og en webserver, og mod phishing-angreb, hvor en hacker kan narre brugere til at indtaste deres personlige oplysninger på en falsk webside.
* HTTPS er vigtigt for e-handel, online-bankvirksomhed og andre websider, der indsamler følsomme oplysninger fra brugere.
* HTTPS har også en positiv effekt på SEO, da Google prioriterer websider med HTTPS i deres søgeresultater.

Samlet set er HTTPS en vigtig teknologi, der sikrer, at data, der overføres mellem en browser og en webserver, er krypteret og beskyttet mod uautoriseret adgang.

DNS er et system, der bruges til at oversætte menneskelige, letlæselige domænenavne som "google.com" til maskinlæselige IP-adresser som "172.217.7.174". Det fungerer som en telefonbog for internettet og giver en sammenkobling mellem domænenavne og deres tilsvarende IP-adresser.

Når du indtaster et domænenavn i din webbrowser, sender din computer først en anmodning til en DNS-opløser (også kendt som en DNS-server). Opløseren søger derefter efter IP-adressen, der er forbundet med domænenavnet, ved at sende en række forespørgsler til andre DNS-servere på internettet. Hvis den finder IP-adressen, returnerer den den til din computer, som derefter kan oprette forbindelse til den tilsvarende webserver.

DNS-systemet er hierarkisk med et par rodservere øverst i hierarkiet. Disse rodservere indeholder oplysninger om topdomænerne, såsom ".com", ".org" og ".edu". Hvert topdomæne har sine egne autoritative DNS-servere, som er ansvarlige for at administrere domænenavnsoptegnelserne for det domæne.

Når du registrerer et domænenavn, angiver du normalt IP-adressen på din webserver til den autoritative DNS-server for dit domæne. Disse oplysninger gemmes i DNS-serverens database og bruges til at rute anmodninger til dit domænenavn til din webserver.

A-posten:

* Bruges til at oversætte et domænenavn til en IPv4-adresse.
* Giver en computer mulighed for at finde den korrekte server, der hoster det ønskede website.
* Er en type af DNS-ressourceposter.

AAAA-posten:

* Bruges til at oversætte et domænenavn til en IPv6-adresse.
* Giver en computer mulighed for at finde den korrekte server, der hoster det ønskede website, hvis den har en IPv6-adresse.
* Er også en type af DNS-ressourceposter.

Begge poster er vigtige for at sikre, at internettet fungerer korrekt, og at computere kan kommunikere med hinanden på tværs af netværk.

I alt er DNS et vigtigt system, der gør det muligt for os at bruge letlæselige domænenavne til at få adgang til websteder og andre internetressourcer i stedet for at skulle huske og indtaste de tilknyttede IP-adresser.

MX står for "Mail Exchange" og er en type DNS-post, der angiver, hvilken mailserver der skal modtage e-mails, der sendes til en bestemt domæne-e-mailadresse.

Når du sender en e-mail til en bestemt adresse, for eksempel "[eksempel@minhjemmeside.com](mailto:eksempel@minhjemmeside.com)", bruger din e-mail-klient DNS til at finde ud af, hvor e-mails til denne adresse skal sendes hen. Din e-mail-klient vil først slå op i DNS for at finde "minhjemmeside.com" og derefter se efter MX-posten for at finde den relevante mailserver.

MX-posten indeholder normalt en prioritetsværdi, der angiver, hvilken mailserver der skal prøves først, hvis der er flere mulige mailservere. Hvis den første mailserver ikke er tilgængelig, vil e-mails forsøge at blive leveret til den næste mailserver på listen.

Så kort sagt, MX-posten er en type DNS-post, der er afgørende for at sikre, at e-mails sendt til en bestemt domæne-e-mailadresse, bliver leveret til den korrekte mailserver.

# DHCP (Dynamic Host Configuration Protocol):

* DHCP er en netværksprotokol, der bruges til at tildele IP-adresser og andre netværkskonfigurationer til enheder i et netværk.
* DHCP fungerer ved at have en DHCP-server i netværket, der er ansvarlig for at fordele IP-adresser til enheder, der anmoder om en adresse.
* Når en enhed (f.eks. en computer, smartphone eller printer) opretter forbindelse til netværket, sender den en anmodning om en IP-adresse til DHCP-serveren.
* DHCP-serveren tildeler derefter en ledig IP-adresse til enheden og sender en besked tilbage med de netværkskonfigurationer, der er nødvendige for enheden at kommunikere med andre enheder i netværket.
* DHCP-serveren kan også tildele andre netværkskonfigurationer, såsom undernetmaske, standard gateway og DNS-servere.
* DHCP gør det lettere at administrere og konfigurere netværk, især når der er mange enheder, der skal have en IP-adresse.
* DHCP hjælper også med at undgå IP-adressekonflikter, da DHCP-serveren sikrer, at enheder får tildelt unikke IP-adresser.
* DHCP har to typer af IP-adressetildelingsmetoder: statisk og dynamisk. Statisk tildeling er, når en IP-adresse manuelt tildeles til en enhed, mens dynamisk tildeling er, når DHCP-serveren automatisk tildeler en ledig IP-adresse til en enhed.

Samlet set er DHCP en vigtig protokol, der gør det lettere at administrere og tildele IP-adresser og andre netværkskonfigurationer i et netværk.

# IP-adresser:

* IP-adresser (Internet Protocol addresses) er unikke numeriske identifikatorer, der tildeles enheder (f.eks. computere, smartphones, printere) i et netværk, så de kan kommunikere med hinanden.
* IP-adresser består af fire grupper af tal, der hver især kan have en værdi mellem 0 og 255 (f.eks. 192.168.0.1).
* Der findes to versioner af IP-protokollen: IPv4 og IPv6. IPv4-adresser består af 32 bits og er i gang med at blive udfaset til fordel for IPv6, der består af 128 bits og giver mulighed for et langt større antal unikke adresser.
* Der er to typer af IP-adresser: offentlige og private. Offentlige IP-adresser er tildelt af en internetudbyder og bruges til at identificere en enhed på internettet. Private IP-adresser bruges i et lokalnetværk og er ikke synlige fra internettet.
* En IP-adresse kan også have en subnetmaske, der bruges til at bestemme, hvilke dele af IP-adressen der identificerer netværket, og hvilke dele der identificerer den specifikke enhed i netværket.
* Der findes også en række specialadresser, der har særlige formål, såsom loopback-adressen (127.0.0.1), der bruges til at teste netværksforbindelser på en lokal enhed.
* IP-adresser kan være statiske eller dynamiske. En statisk IP-adresse tildeles manuelt til en enhed og ændres ikke, medmindre den manuelt ændres. En dynamisk IP-adresse tildeles automatisk af en DHCP-server i netværket og kan ændre sig over tid.
* IP-adresser kan også bruges til at identificere geografisk placering, hvilket kan være nyttigt til visse former for netværksanalyse og sikkerhed.

Samlet set er IP-adresser en grundlæggende del af netværkskommunikation og er afgørende for at enheder kan kommunikere med hinanden over internettet og andre netværk.

# SMB-protokollen:

SMB står for Server Message Block og er en netværksprotokol, der bruges til at dele filer, printere og andre ressourcer mellem computere i et netværk.

* SMB er primært brugt i Windows-operativsystemer, men det er også understøttet af andre operativsystemer som Linux og macOS.
* SMB-protokollen fungerer ved, at en klient (en computer) sender en anmodning til en server (en anden computer), der hoster en delt ressource, f.eks. en fil eller en printer.
* Serveren svarer på anmodningen og giver klienten adgang til den ønskede ressource.
* SMB understøtter også forskellige former for sikkerhed og godkendelse, som f.eks. brugernavne og adgangskoder eller digitale certifikater.
* Der er flere versioner af SMB-protokollen, hvoraf de tidligere versioner (f.eks. SMBv1) er kendt for at have sikkerhedsproblemer, og anbefales ikke længere at blive brugt.

# ICMP (Internet Control Message Protocol):

* ICMP er et protokollag i internettet, der bruges til at rapportere om fejl og tilstandsinformation mellem netværksenheder.
* ICMP-pakker indeholder information om netværksforbindelse og -tilstand og bruges til at identificere netværksproblemer, der kræver opmærksomhed og løsning.
* ICMP-pakker sendes normalt af netværksenheder som routere, switch og firewalls.
* Nogle af de mest almindelige ICMP-meddelelser inkluderer "Echo request" og "Echo reply", som bruges til at teste netværksforbindelsen og findes i kommandoerne ping og tracert.
* ICMP bruges også til at rapportere om fejl og advarsler, såsom "Destination Unreachable", "Time Exceeded" og "Packet Too Big", som kan hjælpe med at identificere og rette netværksproblemer.
* Nogle typer af ICMP-meddelelser kan også bruges til at angribe netværkssikkerhed, f.eks. ved at overbelaste en netværksenhed med "Ping of Death" eller "ICMP Flood" angreb.
* ICMP-pakker er normalt ikke krypteret og kan være sårbare over for visse former for netværksangreb og manipulation, f.eks. ICMP-spoofing og ICMP-redirection.
* ICMP er en afgørende del af internettet og spiller en central rolle i netværksfejlfinding og vedligeholdelse.

Samlet set er ICMP en vigtig protokol i internettet, der bruges til at rapportere om fejl og tilstandsinformation mellem netværksenheder.

Web Services: fungerer ved at give forskellige applikationer mulighed for at kommunikere med hinanden over internettet ved hjælp af standardiserede protokoller og teknologier. Her er en grundlæggende trin-for-trin forklaring på, hvordan en typisk Web Service fungerer:

1. En applikation, også kaldet klienten, der ønsker at bruge en bestemt Web Service, opretter en anmodning (request) til Web Service'en.
2. Anmodningen (request) er normalt i form af en XML-baseret besked, der beskriver, hvilken handling (operation) der ønskes udført af Web Service'en, og hvilke data der skal sendes med anmodningen.
3. Web Service'en modtager anmodningen (request) og bruger SOAP-protokollen (Simple Object Access Protocol) til at pakke dataene og sende dem tilbage til klienten.
4. Klienten modtager dataene fra Web Service'en og kan behandle dem og bruge dem i sin egen applikation.

Det er vigtigt at bemærke, at Web Services bruger standardiserede teknologier og protokoller, hvilket betyder, at de kan kommunikere med forskellige applikationer, uanset hvilket programmeringssprog eller operativsystem, de bruger. Derudover giver Web Services også en høj grad af sikkerhed, da de normalt bruger SSL- eller TLS-kryptering til at beskytte dataene, der overføres mellem klienten og Web Service'en. Eksempler på Web Services inkluderer RESTful API'er, SOAP-tjenester og XML-tjenester.

# SLAAC (Stateless Address Autoconfiguration):

* SLAAC er en protokol, der bruges til automatisk at konfigurere IPv6-adresser på et netværk.
* Det er stateless, fordi det ikke kræver yderligere information fra en central server eller netværksadministrator for at fungere.
* SLAAC fungerer ved at bruge MAC-adressen på en enhed til at generere en unik interface-ID, som kombineres med en præfiks, der er opnået fra en routerannoncebesked, for at danne en komplet IPv6-adresse.
* Routerannoncebeskeder sendes periodisk ud af routere på netværket for at informere enhederne om netværkspræfikset og andre konfigurationsoplysninger.
* SLAAC er designet til at være simpelt og nemt at implementere, og det er den foretrukne metode til adressekonfiguration for IPv6.
* Nogle potentielle sikkerhedsproblemer med SLAAC inkluderer muligheden for adresse-spoofing og manglende kontrol over adresse-tildeling af netværksadministratorer.