PRAKTISK IT

“If you cannot do great things, do small things in a great way”

Innholdsfortegnelse

Statisk elektrisitet

Statisk elektrisitet oppstår når en gjenstand blir oppladet. Det vil si at elektroner fjernes eller tilføres slik at gjenstanden ikke lenger er elektrisk nøytral. Det blir da en spenning mellom den oppladede gjenstanden og jord (jord regnes som elektrisk nøytral), og det oppstår et elektrisk felt omkring den ladede gjenstanden.
Når gjenstanden kommer i nærheten av andre gjenstander eller personer som ikke har den samme positive eller negative ladningen, får vi en elektrostatisk utladning (ESD). Denne kan ha mange tusen volt og kan lage synlige gnister som lett kan antenne brennbare materialer.

Hvorfor statisk elektrisitet er skadelig for elektronikk

Moderne elektronikk består av mange mikrobrikker hvor det går elektriske ledere som er tynnere enn hårstrå. Hvis disse blir utsatt for elektrostatisk utladning kan lederne få skader, brenne av eller gnister kan hoppe mellom ledere. Resultatet kan dermed være at elektronikken blir ødelagt eller ustabil. Det er derfor viktig å unngå elektrostatiske utladninger hvis vi skal arbeide inne i datamaskiner.

Hvordan unngå/motvirke statisk elektrisitet og skader på elektronikk

Valg av klær

De fleste klær kan bygge statisk elektrisitet når de gnisses mot hud eller andre klær. Spesielt klær av polyester og ull har lett for å bygge opp en statisk ladning. Lav luftfuktighet kan også bidra til at klær lettere bygger ladning. Tøymyknere kan hjelpe med å gjøre klær mindre statiske.
Unngå helst å ha på mange lag med klær (for eksempel ytterjakke) når du arbeider med elektronikk. Pels og falsk pels bør spesielt unngås.

Unngå gnissing

Statisk elektrisitet bygges opp på grunn av gnissing mellom materialer. Ved å unngå gnissing kan du unngå oppbygging av statisk elektrisitet. Dette kan gjøres ved å holde seg mest mulig i ro mens du arbeider med elektronikk. Ikke dra beina over gulvet eller snu på stolen du sitter på.

Bruk av antistatiske armbånd og matter

I bedrifter som arbeider med elektronikk er det et vanlig tiltak å bruke antistatiske armbånd eller matter for å unngå oppbygging av statisk elektrisitet. Armbåndet eller matten lager kontakt mellom personen som arbeider med elektronikken og et jordingspunkt. Dette gjør at ladning som genereres, for eksempel med klesplagg som gnisser mot hverandre, blir ledet bort til jord fortløpende og at datautstyret har den samme ladningen som du selv har.

Manuell utladning

Hvis du ikke har tilgang til antistatiske armbånd, kan du manuelt utlade deg mot et jordet metallobjekt. Dette kan for eksempel være en vannkran. Du kan også utlade deg mot datamaskinens kabinett. På den måten har du samme ladning som enheten og dermed ingen fare for utladning.

Disse tiltakene er bedre enn ingenting, men definitivt dårligere enn bruk av antistatiske armbånd og matter, fordi du hele tiden må fokusere på det.

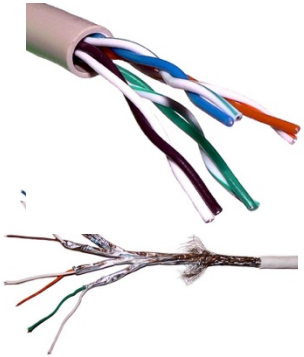
Antistatiske poser

Antistatiske poser brukes under lagring og transport av utstyr som er sensitivt for elektrostatisk utladninger. Posen er elektrisk ledende slik at statisk elektrisitet ikke får bygget seg opp i enkeltkomponenter ved gnisninger og fordeler eventuell elektrostatisk ladning utover når en tar i posen. Dermed reduseres faren for skade på utstyret i posen.

Oppgaver

- Hvordan oppstår statisk elektrisitet
- Hvorfor er statisk elektrisitet farlig for elektroniske komponenter?
- Hvordan kan vi unngå /motvirke/beskytte utstyr mot statisk elektrisitet

Nettverkskabel og RJ45 plugg



Når vi sier nettverkskabel, mener vi som oftest en kabel med åtte tynne kobberledere. Lederne er buntet sammen parvis og tvinnet sammen (Twisted Pair eller TP). Derav navnet tvinnet parkabel eller bare TP-kabel. Slike kabler brukes mye i datanettverk og er for det meste enkle å arbeide med.

Link til wiki

Støy og kabelskjerming

Kobberledere som bærer elektriske signaler, stråler ut elektromagnetisk støy. Denne støyen kan forstyrre signalene som går i de andre lederne i kabelen (crosstalk). Kobberlederne kan også påvirkes av ekstern støy. Slike forstyrrelser kan gjøre at innholdet i datapakkene som sendes over kabelen, får feil i seg. Datapakkene må da sendes på nytt, og det skaper forsinkelser og vi får redusert overføringskapasitet. Når trådparene tvinnes, slik som i en "Twisted Pair"-kabel, elimineres mye av denne støyen. Hvert par i kabelen har forskjellig revolvering (antall tvinninger per centimeter med kabel). Det er viktig å beholde mest mulig av denne revolveringen når vi arbeider på enden av kabelen, for eksempel når vi setter på plugg eller den termineres i nettverksuttak eller patchepanel.

De fleste nettverkskablene har ingen ekstra skjerming. I områder med mye ekstern elektromagnetisk støy, eller i en TP-kabel som skal ha høy hastighet (10Gbit), finnes det nettverkskabelversjoner der hvert par med ledere eller hele kabelen er beskyttet med metallfolie eller flettet skjerming. Listen under viser de vanligste typene skjerming av TP-kabel.

Navn	Skjerming av hele kabelen	Skjerming av enkeltpar
U/UTP (vanlig TP-kabel)	Ingen	Ingen
U/FTP	Ingen	Folie
F/UTP	Folie	Ingen
F/FTP	Folie	Folie
S/UTP	Flettet skjerming*	Ingen
S/FTP	Flettet skjerming*	Folie

*Flettet skjerming gir kabelen mer fleksibilitet og lett jording. Beskyttelsen mot elektromagnetisk støy kan være dårligere enn for folieskjermet kabel.

Kabeltyper og hastighet

TP-kabel var en videreutvikling av telefonkabler og har forandret seg mye i løpet av de siste tiårene. For å holde orden på hvilke kabler som tåler hvilken hastighet og lengde, er det laget et kategorisystem. Kabler må følge spesifikasjonene til den kategorien kabelen er klassifisert innen.

For nye installasjoner er Cat 6 og Cat 6a de mest vanlige. Disse kablene gir god kapasitet for de fleste brukstilfeller og har en akseptabel pris. For høyere hastigheter, nettverksryggrad og lengre avstander brukes fiber.

Kategori	Båndbredde	Hastighet	Makslengde kabel	Pluggtype
Cat 5*	100 MHz	100 Mbit	100 m	8P8C (RJ45)
Cat 5e	100 MHz	1 Gbit	100 m	8P8C (RJ45)
Cat 6	250 MHz	10 Gbit**	100 m	8P8C (RJ45)
Cat 6a	500 MHz	10 Gbit	100 m	8P8C (RJ45)
Cat 7a	1 GHz	10 Gbit	100 m (skjermet)	GG45, TERA
Cat 8	2 GHz	40 Gbit	30 m (skjermet)	8P8C (RJ45)

For ned graving eller ute bruk er det egne varianter av disse kablene som har en mer slitesterk og UV-bestandig ytterisolasjon.

POE (Power Over Ethernet)

En fordel med bruk av TP-kabel er at kabelen i tillegg til datasignal også kan levere mindre mengder strøm til utstyr. For eksempel IP-telefon, kameraer, aksesspunkt og alarmklokker.

POE kan gjøres passivt, hvor fire av åtte ledere dedikeres til strøm og en injektor fører inn strøm på de riktige lederne. Passiv POE har svakheten at den kan skade nettverkskort og svitsjporter hvis POE-strøm sendes mot enheter som ikke er laget for det. Hastigheten blir også begrenset, siden fire av lederne tas opp til å levere strøm.

I dag er aktiv POE mer vanlig. Her fordeles strøm på alle ledere. På mottakersiden filtreres strømmen bort fra datasignalet. Aktiv POE kommer i flere standarder. Til felles har de at POE-strøm kun leveres etter en håndhilsning, hvor spenning og strømmengde avtales mellom avsender og mottaker. Dette gjør at utstyr som ikke støtter POE trygt kan bruke en aktiv POE-port på en svitsj.

Patchepanel

Patchepaneler brukes som et sentralt samlingspunkt for kabling i større bygg der det er mange nettverkspunkter over større områder. Alle kabler som går ut til disse punktene kobles til på baksiden av et patchepanel og termineres med kroneverktøy.

Vi benytter så patchekabel til å koble sammen patchepanelet og svitsjen. Dette gir oss fleksibilitet slik at vi kan rokere om på det kablede nettet, og det gjør det enklere å bytte ut eksisterende utstyr.

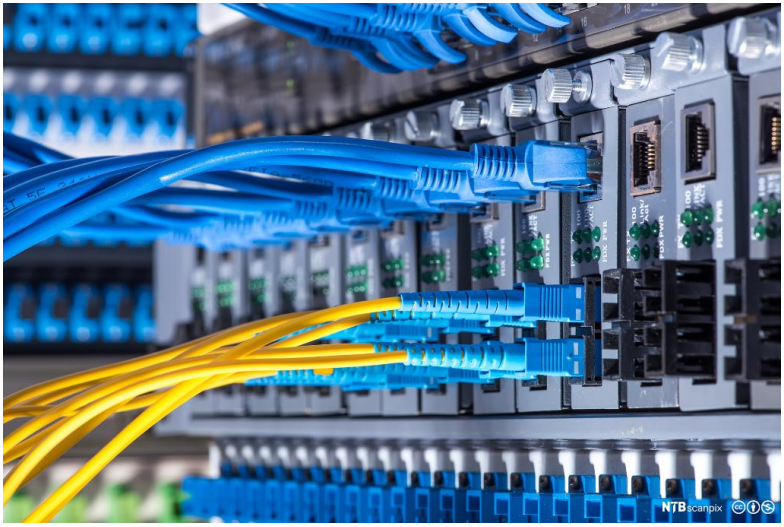
Kabelgater

Kabelgater bruker vi når vi skal trekke én eller flere kabler over samme distanse. Grunnen til at vi benytter kabelgater, er at vi da får en strukturert og ryddig måte å distribuere kablet nett ut i lokalene på. Kabelgater finnes i mange typer og størrelser, helt fra tynne, små kabelgater for få kabler, til store, tunge løsninger med plass til mangfoldige kabler.
Kabelgater er ikke mye brukt i private hjem, men er vanlig hos bedrifter og på kontorer.
Kabelgater har den fordelen at vi også kan trekke andre typer kabler i dem, ikke bare nettverkskabler. Audio/video-kabling og strøm er eksempler på dette.

Koblingsboks

Koblingsbokser er noe vi ser overalt. Bokser brukes både i private hjem og hos bedrifter og på kontorer. Disse boksene brukes til både data og tele, og vi kan kombinere dem med enkelte typer kabelgater. Koblingsboksene finnes i forskjellige kvaliteter, og det stilles krav til både merking og boks- type for godkjente installasjoner.

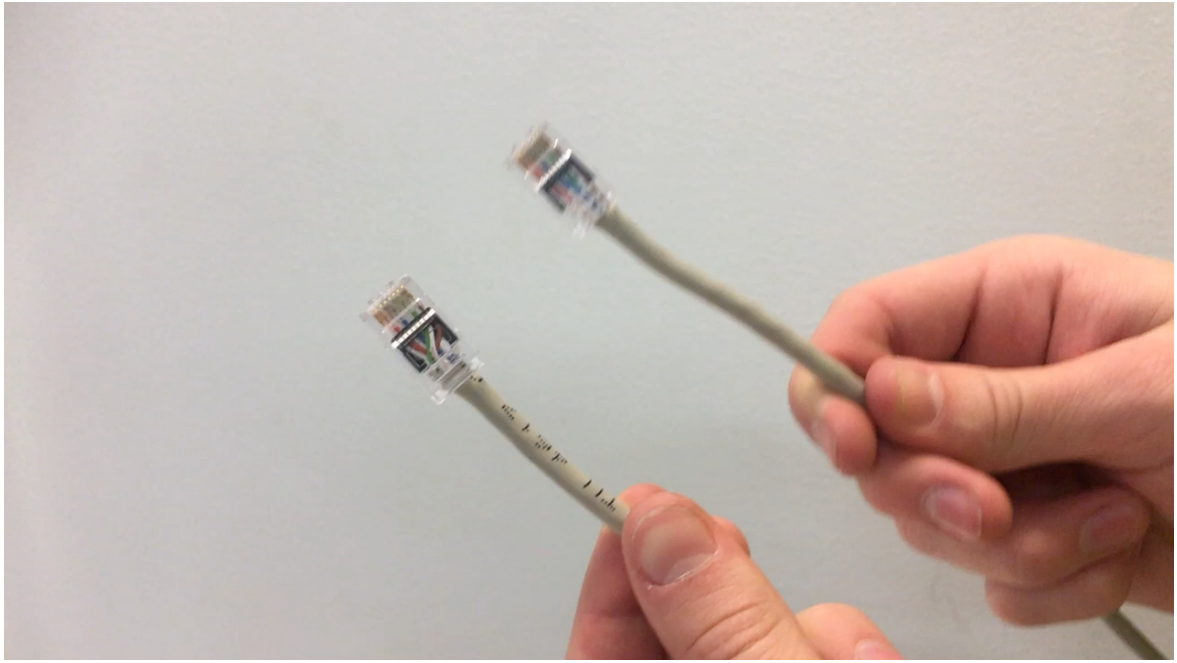
Fiberoptiske kabler



For tilkoblinger over lengre distanser bruker vi fiberoptiske kabler. Det spesielle med denne typen kabel er at den har en kjerne av plast eller rent glass som kan lede lyssignaler. Den innerste delen av glass kaller vi for kjerne, og på utsiden av kjernen er det en kappe som sørger for at kjernen fungerer som en bølgeleder. Det ytterste laget er laget av plast og har en beskyttende funksjon.
Siden fiberoptiske kabler overfører lyssignaler, kan kabelen i teorien overføre med lysets hastighet. I praksis vil hastigheten på fiberkabelen avhenge av ulike faktorer, som for eksempel renheten av glasset i kjernen. For å kunne oversette trafikk fra en fiberkobling til en TP-kabel må man ha en fiberkonverter som oversetter lyssignaler til elektriske signaler.

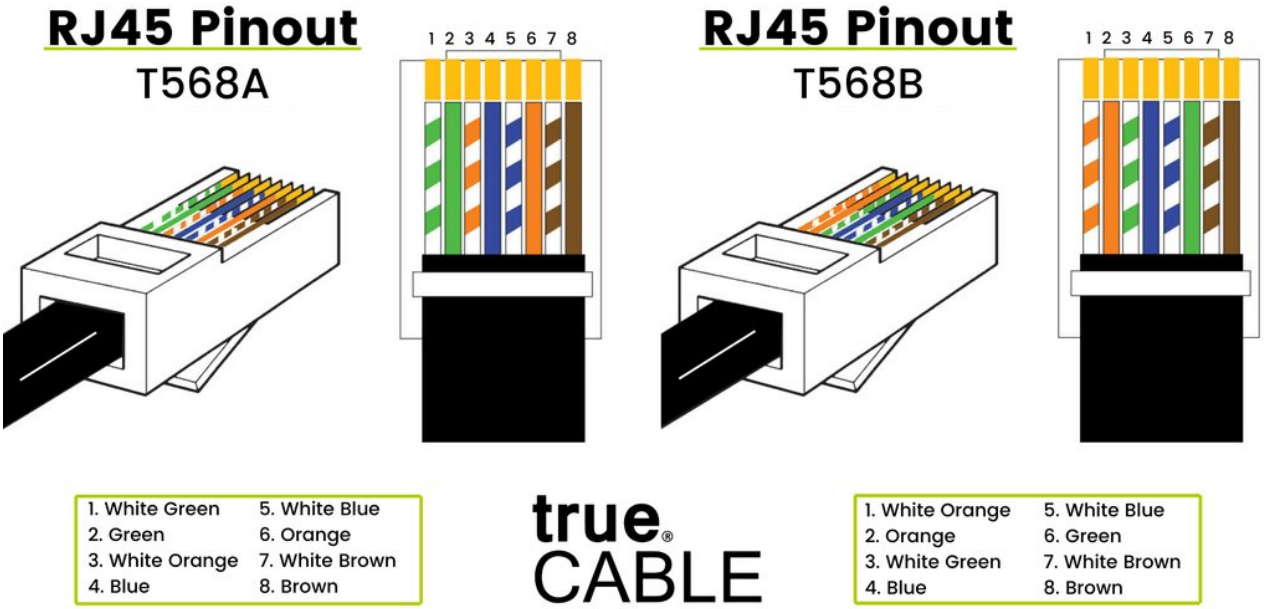
Terminering av RJ45-plugg

Her lærer du hvordan du terminerer en nettverkskabel med 8-pin-plugg (RJ-45).



Patchekabel – montering

Nå skal nettverkskabelen termineres i en 8-pin 8P8C-plugg (RJ-45). Her er det viktig at du har rett fargekode i rett rekkefølge. Lær deg hvordan den termineres og prøv selv.



Memorer fargekodene i riktig rekkefølge, og legg merke til at par 2 (grønn) splittes i pluggen. Her leser vi, og legger ledninger, fra venstre mot høyre. Montører som ikke kan dette skikkelig, risikerer å måtte feilsøke på nye installasjoner, noe som er uheldig for alle parter. Vi bruker T568B-standarden for terminering av nettverkskabel.

Hvis du har nettverkspluggen med kontaktpunktene og hullet hvor kabelen skal inn i pluggen, mot deg, så starter du fra venstre med hvit-oransje-lederen.
Når det lages en ethernetkabel, skal aldri mer enn cirka 2 cm av kabeltvinningen tas opp. Dette er for å unngå støy ("crosstalk"). Ethernetkabler bør aldri bøyes eller deformeres mye, det vil si aldri mer enn tilsvarende kurven på en CD-plate. De skal heller ikke legges i nærheten av støykilder som høyspentledninger, lysstoffrør eller lignende som kan føre til støy.

Krysset kabel

Instruksjonen over viser hvordan en vanlig nettverkskabel lages. Det finnes også en annen variant, som vi kaller en krysset kabel. Disse ble tidligere brukt mellom svitsjer, eller hvis datamaskiner ble koblet direkte til hverandre. I dag har det meste av utstyr støtte for Auto MDI-X-standarden, som internt tar seg av eventuell kryssing. Det er derfor vanligvis ikke nødvendig å bruke kryssede nettverkskabler i nettverk.

Oppgaver

- Hva er en nettverkskabel og hvilke egenskaper bør denne ha?
- Hvorfor er en nettverkskabel sine ledere flettet (Twisted)?
- Hvorfor er skjerming viktig?
- Nevn noe av utstyret som benyttes med nettverkskabler under montering og strukturering av nettverket
- Fortell hva du vet om fiberoptiske kabler
- Hvorfor har man utarbeidet standard for RJ45 kabler? Og hva sier denne standarden?

Praktisk arbeide

- Lage egne Nettverkskabler RJ45, og kontrollere disse.
- Feilsøke i enkelt nett på kabelfeil
- Enkel øvelse med fiberoptisk kabel

Feilsøking på nettverk og maskinvare

Det å feilsøke nettverk krever noe erfaring og en del grunnleggende kunnskap om hvordan datakommunikasjon fungerer. En god grunnregel er at vi tar for oss feilsøking i flere steg, slik at det er lettere å eliminere feilkilder.

Feilsøking er en prosess for å eliminere bort mulige årsaker og man kan sette dette opp i en generell eller individuell rekkefølge, eksempelvis slik:

Femfingerregelen (NDLA)

Strøm og medieoverføring:

- Sjekk at alle enheter og komponenter har strøm.
- Sjekk at alle strømkabler er koblet til
- Sjekk at nettverkskabler fungerer. Nettverkskabler kan vi teste ved hjelp av en nettverkstester som gir raskt svar på om det er brudd på kabelen.

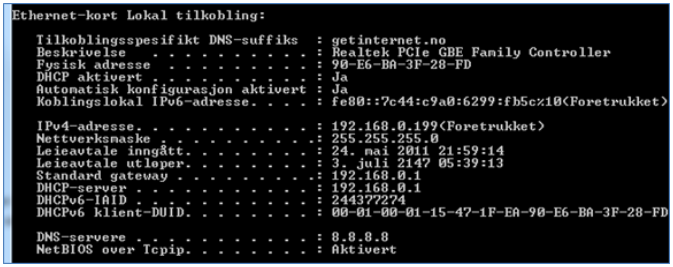
Sjekk nettverkskort:
Sjekk om det er lys på nettverkskontakten. Dette kan du se på både nettverkskortet og på svitsjen/ruteren.
Sjekke veggkontakter om det finnes kabelgater som nettverkskabler ligger i.

Sjekk IP-adresser og nettverksinnstillinger:
Her er "ipconfig" og "ping" gode hjelpemidler. Vi kan kontrollere om vi har kontakt med andre enheter i nettverket og eventuelt Internett.

Sjekk innstillinger på ruteren og andre enheter som kan ha påvirkning på nettverket.
Kontroller maskinvare og komponenter
Sjekk at alle komponenter står montert i maskinen slik de skal.
Se til at det ikke er løse deler og komponenter som kan forårsake feil.

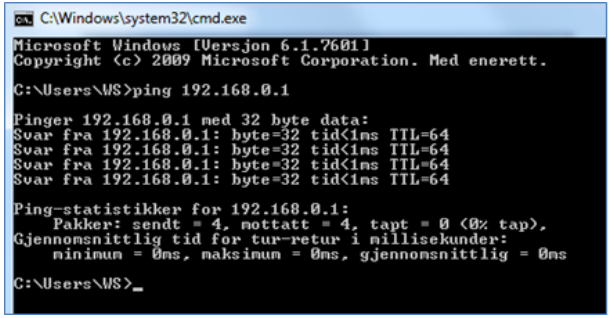
Sjekk applikasjoner og programvare:
Sjekk drivere og at programvare er oppdatert. Kontroller at applikasjoner og programvare har lisenser, og at de starter slik de er ment å fungere.

IPconfig



"Ipconfig" er et verktøy som blir mye brukt for å fastsette statusen på nettverkstilkoblinger. "Ipconfig" kan si deg mye om nettverkskonfigurasjonen på maskinen. Det gir deg status over alle nettverkstilkoblinger på datamaskinen og kan gi informasjon om IP-adresse, "Gateway", DHCP, DNS med mer. "Ipconfig" kjøres i CMD/CLI-vinduet på maskinen. Skriv CMD i "Søk/kjør"-feltet, og CMD-vinduet vil komme opp. Deretter skriver du «ipconfig /all», og du får oversikt over alle nettverksenheter på maskinen.

Ping



Ping er en kommando som kan hjelpe deg å fastslå om du har kontakt med andre enheter. Dette kan være enheter lokalt på nettverket eller på Internett. Se bilet, pinget ruteren med kommando «ping 192.168.0.1»

Mer om kommandoer og Ipconfig

ISP

ISP står for Internet Service Provider. På norsk kaller vi dette for internettleverandør. Det er internettleverandøren som har ansvaret for at du får tilgang til internett. Det hender også at ISP har problemer med internettleveransen. Da oppstår som regel problemet mellom Digital Subscriber Line Access Multiplexer (DSLAM) og din veggkontakt. DSLAM er en komponent som er montert i sentralen til internettleverandøren vi bruker. Her kan vi ikke gjøre annet enn å feilmelde problemene til ISP-en det gjelder.

Oppgaver

- Hva sier Femfingerregelen?
- Hva står ISP for
- Hva er en DSLAM

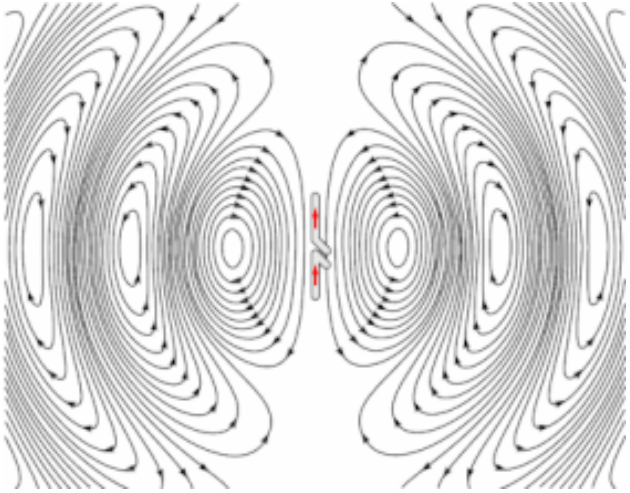
Praksis oppgaver

Kople sammen 2 PCer som et LAN og sett statisk IP adresse på dem, 192.168.1.10 og 192.168.1.20

- Ping hverandre og legg ved bilde av skjerm i oppgave innleveringen.
- Ta en ipconfig/all på maskinen din, legg ved bilde

Radiolinker, trådløse løsninger

Retningsantenner (Directional antennas) og radioutstyr kan gi lang rekkevidde. Men på de åpne frekvensene (2,4 GHz og 5 GHz) er det mange kilder til forstyrrelser og begrensinger på sendestyrke. Dette gjør at det kan være utfordrende å sette opp radiolinker.
Ofte er antenne og sender bygd sammen i en enhet som bare trenger en nettverkskabel med strøm og nettverk for å fungere. En slik radiolink-sender kan som oftest konfigureres ved hjelp av Web-GUI mot utstyrets IP-adresse.
Bruk riktig utstyr til riktig jobb



Wi-Fi-forsterkere er nyttige enheter som kan brukes for å utvide et eksisterende trådløst nettverk. Men de bruker rundstrålende antenner (Omnidirectional antennas) og har dermed kort rekkevidde. De kan være nyttige inne i et hus, men ved lengre avstander bør vi bruke bedre og mer tilpasset utstyr. Utstyr til radiolinker koster fra litt under tusenlappen per sender og antenne opp til mange titalls tusen, avhengig av rekkevidde og overføringskapasitet. Men for de fleste kan utstyr til noen få tusen kroner dekke behovet.

Andres erfaringer kan være gull verd

Med mindre du har erfaring med utstyret fra før, kan det være utfordrende å finne riktig utstyr når du skal sette opp en radiolink. En mulig løsning er å bruke nettbaserte simuleringsverktøy. Da kan du legge inn plasseringen til radiolinken i et kart og «teste» forskjellig utstyr. En annen kilde til informasjon er tester som andre har gjort og publisert på for eksempel YouTube. Kanskje noen har prøvd å sette opp det utstyret du har tenkt å bruke, på en lignende måte tidligere? Da kan deres erfaringer komme godt med.
Konfigurer utstyret før du monterer det opp ute!

For at en radiolink skal fungere, må du konfigurere de trådløse enhetene. Den ene enheten skal fungere som aksesspunkt og den andre som klient. Hvis du monterer utstyret før du konfigurerer, må du enten ha en person ved hver enhet eller selv forflytte deg mellom enhetene og konfigurere inntil linken fungerer. Dette tar fort mye tid. Og hvis du er uheldig, må du kanskje fysisk tilbakestille utstyret til fabrikkinnstillinger.

Bruk faste IP-adresser

Å bruke dynamiske IP-adresser er ofte veldig praktiske, men du bør ikke bruke det på infrastruktur som radiolinker. Hvis du bruker faste IP-adresser, er det nemlig lettere å konfigurere utstyret. Og hvis radiolinken slutter å fungere, vil utstyret som ikke er på den siden av nettverket som har DHCP-server, fortsatt ha en IP-adresse. Datamaskinen som brukes til konfigurering, kan også ha fast IP-adresse mens konfigureringen pågår.

Radiolinker er infrastruktur og ikke for sluttbrukere

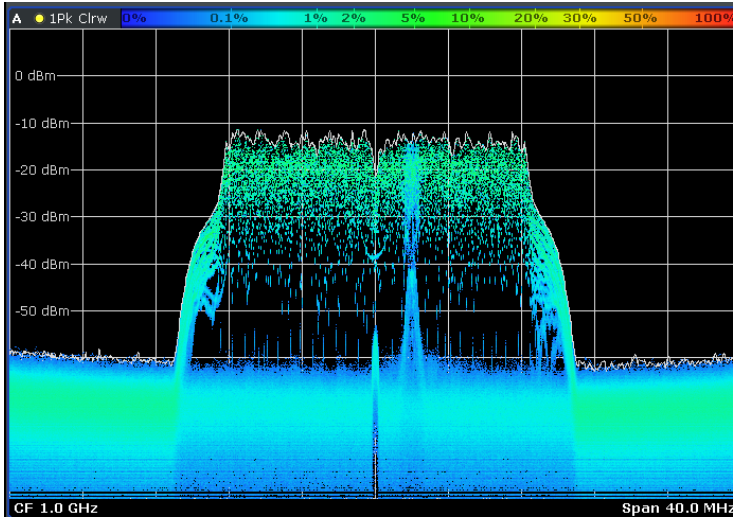
Det er som oftest ingenting som hindrer en vanlig mobiltelefon eller datamaskin i å koble seg til aksesspunktet i en radiolink. Men dette fraråder vi, siden kapasiteten da må deles mellom flere enheter. Dette kan gi dårligere hastighet og mer pakketap. Vi bør derfor tenke på radiolinker som infrastruktur som vanlige brukere ikke skal koble seg til (trådløst).

Bruk skjult SSID

Et aksesspunkt med retningsantenne og synlig SSID vil være søkbart og synlig for enheter på lang avstand. Men selv om andre enheter kan se nettverket, vil de ikke kunne koble seg til (selv om de har WPA2-nøkkel). De rundstrålende antennene i telefoner og bærbare datamaskiner er rett og slett for dårlige til at de kan nå tilbake til aksesspunktet. Det kan også være forvirrende for brukerne. Derfor er det mye mer praktisk å bruke skjult SSID på aksesspunktet. Ulempen er at du må legge inn mer av aksesspunkt-informasjonen manuelt i senderen.

Valg av frekvens

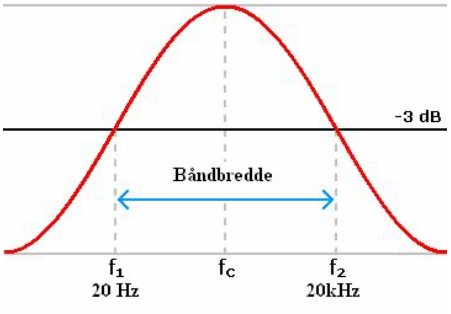
De åpne Wi-Fi frekvensene brukes av mange, noe som medfører forstyrrelser. Det er derfor viktig å bruke en best mulig frekvens. De fleste typer radiolink-utstyr har mulighet for å skanne frekvensområdene. Det kan gi et godt inntrykk av hvilke frekvenser som er minst brukt. Ulempen er at situasjonen kan forandre seg.



Det kan derfor også være lurt å la aksesspunktet selv regulere frekvensen.
Kalibrere retningen på antennene
Retningsantenner er mest effektive hvis de peker rett på hverandre. Å justere antennene både horisontalt og vertikalt slik at de peker mest mulig direkte på hverandre, vil derfor gi best mulig signal. De fleste leverandører av radiolink-utstyr tilbyr verktøy for retningskalibrering i webgrensesnittet til radioutstyret.

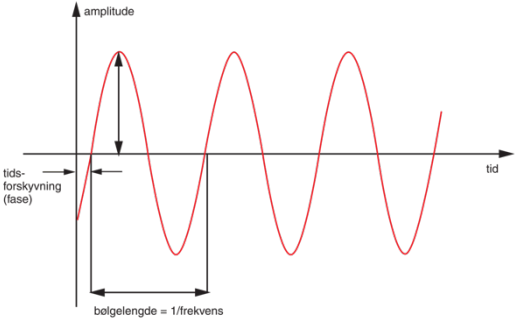
Valg av båndbredde

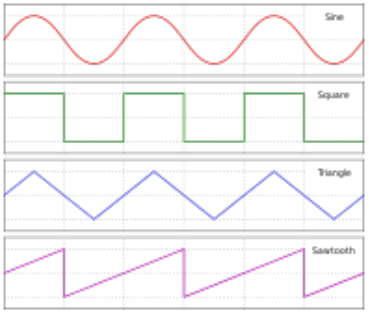
I de åpne frekvensområdene er det en øvre grense for sendestyrke. Bruker vi gode retningsantenner, fokuseres sendestyrken i én retning. Dette hjelper mye, men spesielt på lange radiolinker kan signalet bli for svakt. Da kan vi i stedet redusere antall frekvenser det sendes på, for eksempel fra 20 MHz ned til 10 eller 5 MHz.
Dette gir mer sendestyrke på noen få frekvenser. Ulempen er at mengden data som kan sendes per sekund, går ned.
Men dette er bedre enn økt forsinkelse på grunn av en svak radiolink med mye pakketap.



Frekvens

Båndbredde

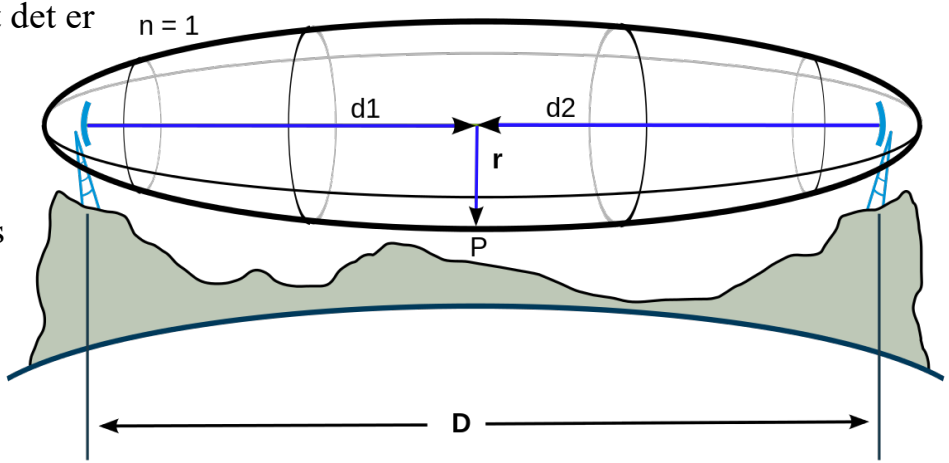




Unngå hindringer i Fresnelsone

Hovedregelen er at radiolinker trenger klar siktelinje mellom aksesspunkt og klientantenne. I tillegg bør et område under og over være fritt for hindringer. Derfor er radiolink-antenner ofte plassert høyt i terrenget.

Økt sendestyrke betyr ikke bedre signal
Sendestyrke gjør det mulig å nå langt med radiosignalet, men det kan også gi forstyrrelser og andre problemer. Det er derfor lurt å justere sendestyrken på aksesspunktet og klienten slik at det er tilpasset behovet. Mindre sendestyrke (spesielt på korte avstander) vil ofte gi bedre **kvalitet** på signalet enn full sendestyrke. Dette må kalibreres for hver enkelt radiolink.

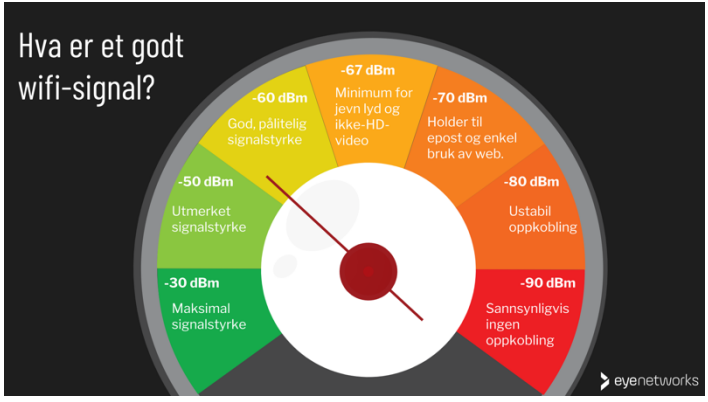


Augustin- Jean Fresnel

Radiolinker kan bli ustabile under bestemte værforhold

Radiolinker, spesielt de som skal dekke lengre avstander, kan bli negativt påvirket av regn, tåke, snø og lyn.
Det er derfor lurt å kalibrere utstyret med gode marginer (sendestyrke og båndbredde).

Det er også lurt å sjekke linken jevnlig for å se om den er stabil også under krevende værforhold.



Gode Wi-Fi signaler og bruk av heatmapper

Lag oppsett med redundans

Radiolinker er som oftest en sentral del av nettverks-infrastrukturen. Det innebærer at hvis radiolinken slutter å fungere, vil nettverket bli splittet opp i deler, og tjenester som internett-tilgang kan bli utilgjengelige for mange brukere. Redundans innebærer at hvis det oppstår feil, har vi løsninger i bakhånd for å redusere eller hindre nedetid. Den enkleste og billigste løsningen er å ha en reserveantenne du kan sette opp hvis den ene radiosenderen skulle slutte å fungere. En annen mulighet er å sette opp parallelle radiolinker, slik at hvis én faller ut, tar den andre over. Det finnes også radioutstyr som fungerer på flere frekvensområder samtidig. Eksempel: En radiolink bruker 30 GHz og kan overføre med en hastighet på flere Gbit. Hvis denne 30 GHz-linken slutter å fungere (for eksempel ved uvær), tar en annen radiolink i 5 GHz-båndet over. Men denne kan bare overføre med en hastighet på 200 Mbit. Som tross alt er bedre enn ingenting.

Redundans er en duplisering av kritiske komponenter eller funksjoner i et system, for å øke stabiliteten, påliteligheten og driftssikkerheten i systemet. Slutter den ene komponenten eller funksjonen å fungere, har du andre komponenter og funksjoner som fungerer som back-up.

Forstyrrelser av radiosignaler

Radiosignaler påvirkes av omgivelsene de går gjennom. Dette er spesielt merkbart inne i bygninger og tuneller, men selv i tilfeller med fri siktlinje utendørs kan radiosignaler bli forstyrret.

Materialer som absorberer radiosignaler

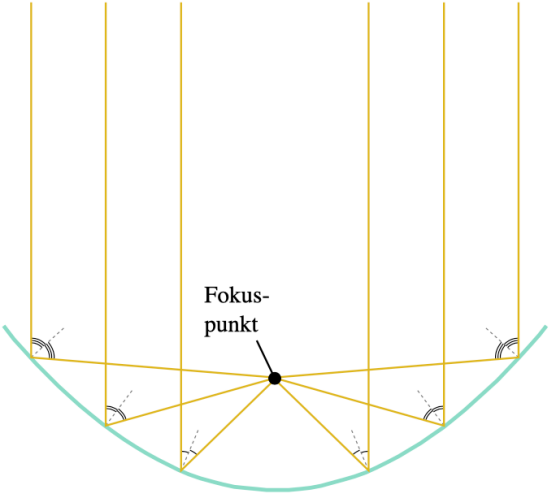
Strømledende metaller som jern, aluminium og kobber kan i stor grad absorbere radiosignaler. Vann er også effektivt. Det er derfor upraktisk å plassere radiosendere/-mottakere som aksesspunkter i nærheten av akvarier eller store metallflater.

Radiobølger som blir absorbert, vil omdannes til varme i materialet de treffer. Du kan sammenligne dette med sollys som treffer en mørk overflate.

Mange materialer (også de som ikke er strømledende) kan absorbere radiosignaler. Tykkelsen på materialet og frekvensen på radiosignalet påvirker absorberingsgraden.

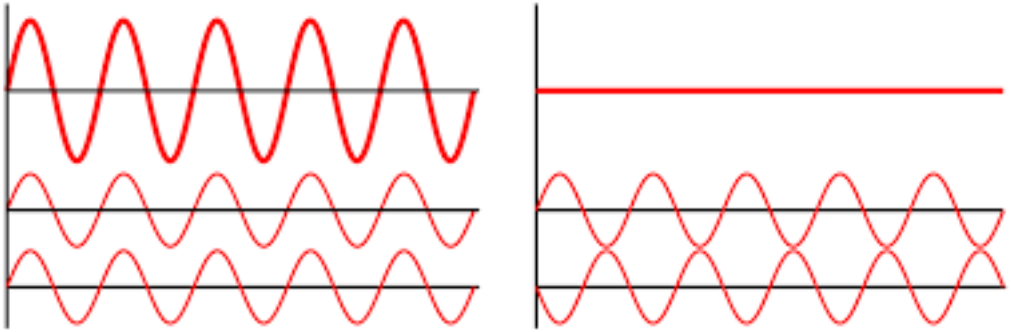
Materialer som reflekterer radiosignaler

Radiosignaler som kommer inn med en vinkel mot strømledende metaller, vil i stor grad bli reflektert av metallet i en ny retning. Dette skjer for eksempel på en parabolantenne, hvor signalet som kommer inn, blir reflektert av reflektoren. Reflektoren samler signalet inn mot mottakeren (som er plassert ved fokuspunktet).
Et annet eksempel er radarsignaler som treffer en båt eller et fly: Det er refleksjonen av signalet som kommer tilbake, som gjør det mulig å måle avstanden og retningen til fartøyet.
Mange forskjellige materialer (også ikke-strømledende) kan reflektere radiosignaler.



Interferens

Signaler med samme frekvens som er i fase, vil ha en konstruktiv interferens, hvor signalet blir sterkere. Er signalene ute av fase, blir det en destruktiv interferens, og signalet utlignes og blir borte.



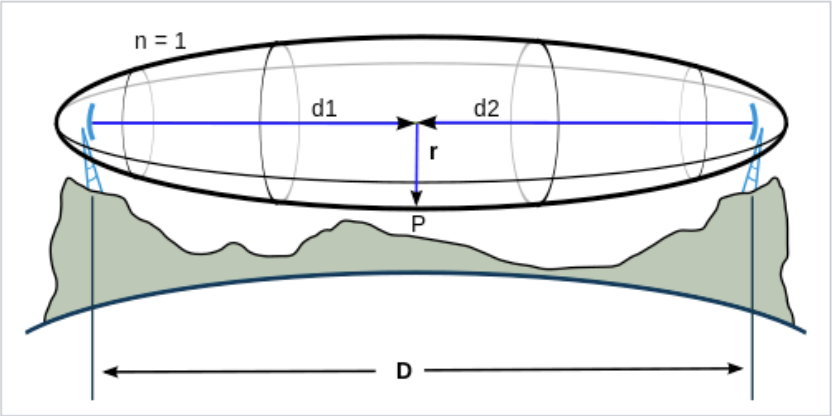
Radiobølger på samme frekvens vil påvirke hverandre. Hvis to signaler er i fase (synkronisert med samme topp-punkt og bunnpunkt i kurvene sine, som i eksempelbildet), vil de forsterke hverandre. Dette kalles **konstruktiv interferens** og er en av teknikkene som brukes ved nye antenner som bruker beamforming for å sende signalet med ekstra styrke i en bestemt retning.

Hvis signalene har motsatt fase (hvor topp-punktet på den ene bølgen samsvarer med bunnpunktet på den andre, som i eksempelet), vil de utligne hverandre, og signalet går tapt. Et signal som er delvis ute av fase, vil kunne bli forstyrret slik at informasjonen som overføres, ikke er mulig å avlese.

Vi har et begrenset antall frekvenser vi kan sende radiosignaler på, og spesielt i de åpne områdene for trådløse nettverk (Wi-Fi) bruker mange de samme frekvensene. For enheter som er i samme nettverk, vil aksesspunktet styre hvem som får sende signaler når det er noe som hindrer at to sender signaler samtidig. Forskjellige nettverk vil ikke ha noen slik hindring.
Dette gjør at vi lett kan få datapakketap på grunn av **destruktiv interferens** hvis forskjellige nettverk som er i nærheten av hverandre, bruker samme frekvens.
Derfor er det viktig å forsøke å bruke frekvenser som færrest mulig andre i nærheten bruker.

Nødvendig frisikt for radiolink (fresnelsone)

Fresnelsonen er et område under og over direktelinjen mellom en sender og en mottaker (lys eller radiosignal) hvor deler av signalet naturlig vil reflektere, men fremdeles vil kunne nå mottakeren.
Klar siktlinje mellom avsender- og mottakerantenne er veldig fordelaktig når vi setter opp radiolinker.



Fresnelsone: *D* er avstanden mellom kjelda og mottakaren; *r* er radien til den første frenselsonen (n=1) ved punktet P. P er d1 unna kjelda og d2 unna mottakaren.

I tillegg til siktlinjen er det lurt at et område over og
under siktlinjen også er fri for hindringer. Dette kalles fresnelsonen og er et område hvor radiosignalene naturlig vil spre seg ut og reflektere inn mot mottakeren igjen.
Om vi plasserer radiolinkantennene så høyt at det ikke er hindringer i fresnelsonen, vil mer av signalet komme fram. Dette vil gi en mer stabil radiolink, som kan være raskere eller bruke mindre sendestyrke.
Det finnes egne kalkulatorer vi kan bruke til å regne ut hvor mange meter under og over siktlinjen som helst bør være fri.

Oppgave

Sett dere sammen i gruppe. Gruppene skal hver for seg lage en presentasjon av:

Gruppe 1 Hva er et aksesspunkt og hvordan fungerer dette

Gruppe 2 GSM nett i Norge

Gruppe 3 Nettvett (nettvett.no)

Gruppe 4 Fresnelsone og Redundans

Feilsøkingsmetodikk

Feilsøking er en systematisk fremgangsmåte for å arbeide seg frem til en eller flere feil/feilkilder. Systematisk feilsøking og problemløsing kan normalt oppsummeres i følgende punkter:

1. Kartlegge omstendighetene rundt feilen
2. Reprodusere feilen
3. Lokalisere og begrense feilkildene
4. Innhente nødvendig informasjon
5. Bestemme mulige løsninger
6. Teste ut mulige løsninger
7. Dokumentere feilen og løsningen

1. Kartlegge omstendighetene rundt feilen

Det første du må gjøre, er å kartlegge omstendighetene rundt feilen. Dette gjøres ved å spørre brukeren om feilen. Under følger en liste over de mest aktuelle spørsmålene. Merk at alle spørsmålene ikke nødvendigvis er like relevante for alle typer problemer, og at rekkefølgen det er naturlig å stille spørsmålene i, vil variere.

Hva består problemet i?

Be brukeren om å beskrive hva feilen består i. Dette hjelper deg til å fastslå hva det er brukeren forsøker å gjøre. Hvis det er snakk om et brukerproblem, kan du ofte allerede her fastslå hva som er problemet, og løse det. Men hvis feilen er relatert til maskin eller programvare, er det at brukeren ikke klarer å få gjort det han eller hun ønsker, bare et symptom på den faktiske feilen.

Når oppstod feilen?

Det hender at brukere har hatt et problem i lengre tid, men ikke brydd seg om å melde fra. De har funnet en annen måte å få gjort tingene på, eller feilen har ikke vært så stor at det har skapt vesentlige problemer i jobben deres.

Hvem brukte datamaskinen da feilen oppstod eller ble oppdaget?

Hvis det er flere som bruker samme maskin, eller du er usikker på om du snakker med den som oppdaget feilen, er det greit å få fastslått hvem som var brukeren.

Har denne feilen oppstått tidligere?

Mange feil kan være sporadiske. Det vil si at de bare opptrer av og til eller i bestemte situasjoner. Det kan også tenkes at det er en svakhet i systemet som ikke har vært utbedret skikkelig tidligere. Hvis feilen har vært fikset tidligere, er det naturlig å spørre hvem som da løste den, slik at du eventuelt kan ta kontakt med vedkommende for å få vite hva som ble gjort. Hvis bedriften har en rutine for registrering og dokumentasjon av brukerstøtte, bør det også finnes et dokument som redegjør for hva som er gjort tidligere.

Er det andre som har brukt maskinen nylig?

Hvis andre har brukt maskinen, kan de ha endret konfigurasjoner, installert programvare, koblet til maskinvare midlertidig eller gjort noe annet som har ført til at maskinoppsettet er endret.

Er det andre som har eller har hatt det samme problemet?

Hvis andre har brukt den samme maskinen, er det naturlig å undersøke om de har opplevd det samme problemet. Det kan også tenkes at det er andre som har eller har hatt det samme problemet på sine maskiner.

Er det blitt installert noen nye program eller oppgraderinger på maskinen nylig?
Er det blitt installert eller skiftet noe deler i maskinen nylig?

Det er viktig å fastslå om det er gjort program- eller maskinendringer i forkant av at feilen oppstod. Enhver slik endring er en mulig feilkilde og et godt utgangspunkt for videre feilsøking.

Er det blitt kjørt noen oppryddingsprogram eller lignende nylig?

For eksempel diskdefragmentering, program som rydder opp i *registry*, eller lignende.

Har brukeren slettet noen filer eller manuelt ryddet på maskinen nylig?

Det kan tenkes at brukeren ved et uhell har slettet eller flyttet kritiske filer eller mapper.

Har noen andre forsøkt å rette feilen?

Hvis feilen har vært forsøkt rettet, for eksempel av brukeren eller andre, kan det opprinnelige maskinoppsettet være endret. Dette er det viktig å være oppmerksom på når du starter feilsøkingen, da tidligere forsøk på å rette en feil kan ha medført at maskinen ikke lenger har den samme konfigurasjonen som da den sist fungerte som den skulle.

Hva tror brukeren er årsaken til feilen?

Av og til har brukeren selv en oppfatning om hva som har forårsaket en feil, eller hva som er årsaken til et problem. Brukere med mye IT-kunnskap vet ofte også hva som er feilen, men mangler det nødvendige utstyret eller rettighetene til å kunne fikse den selv.
Spørsmålene over vil ofte være nok til at du kan fastslå hva som er galt, og rette feilen. Hvis ikke har du i hvert fall kartlagt omstendighetene rundt feilen og kan ta fatt på selve feilsøkingen.

2. Reprodusere feilen

Når du har kartlagt omstendighetene rundt en feil, er det neste steget å forsøke å reprodusere den. Det er ikke alltid det er behov for å reprodusere en feil. Vi skiller mellom permanente, konsekvente og sporadiske feil.

Permanent feil

En permanent feil er en feil som opptrer hele tida. At en maskin ikke får kontakt med nettet, en svart skjerm eller at maskinen ikke starter, er eksempler på permanente feil.

Konsekvent feil

En konsekvent feil er en feil som alltid oppstår som resultat av en bestemt handling eller en serie handlinger. Når et program henger seg hver gang man forsøker å bruke en bestemt funksjon, er det snakk om en konsekvent feil.

Sporadiske feil

Sporadiske feil er feil som opptrer av og til, men ikke som følge av en bestemt handling eller i en bestemt situasjon. Typisk vil det at program plutselig avsluttes uten noe forvarsel, eller at maskinen slår seg av tilfeldig, være eksempler på sporadiske feil.
Det er særlig når det gjelder sporadiske feil, at du bør forsøke å finne en måte å reprodusere feilen på. Som hovedregel er det enklere å feilsøke permanente feil enn konsekvente og

enklere å feilsøke konsekvente feil enn sporadiske. Hvis du kan reprodusere en sporadisk feil, slik at den opptrer konsekvent, vil det som regel gjøre den videre feilsøkingen enklere. For å reprodusere en feil bør du la brukeren forklare hva vedkommende gjorde da feilen oppstod, og gjenta dette steg for steg. Forsøk å få med alle detaljer – som hvilke andre program som kjørte samtidig, om det var startet noen eksterne jobber (for eksempel søk i en database), utskriftsjobber eller annet som kan ha hatt betydning.

3. Lokalisere og begrense feilkildene

Når du har et klart bilde av hva problemet består i, og i hvilke sammenhenger det opptrer, er neste steg å begrense de mulige feilkildene. Noen ganger er årsaken opplagt, men i mange tilfeller er det flere mulige årsaker til en feil. En svart skjerm kan for eksempel skyldes feil med skjermen, feil på strømforsyningen til skjermen, feil på kabelen mellom skjermen og maskinen, feil på skjermkortet, dårlig kontakt mellom skjermkortet og hovedkortet, feil driver for skjermkortet, feil innstilling av skjermen (lysstyrke og kontrast), feil konfigurasjon av skjermoppløsningen i operativsystemet eller feil konfigurasjon av multiskjermfunksjonen i operativsystemet.

Når du starter denne delen av feilsøkingen, bør du derfor begynne så bredt som mulig og forsøke å eliminere de faktorene som ikke kan være årsak til feilen.
Det er naturlig å begynne med å forsøke å avgjøre om feilen skyldes maskinvare eller programvare. Deretter jobber du deg systematisk videre til du har begrenset feilkildene så mye som mulig.

Hensikten med å begrense feilkildene er å begrense de mulige løsningene du trenger å innhente informasjon om og teste ut. Hvis du kan isolere problemet til en bestemt enhet (nettverkskort, skriver, skjerm og så videre) eller et bestemt program, forenkler det arbeidet med å innhente informasjon om mulige løsninger.

4. Innhente nødvendig informasjon

Før du fortsetter feilsøkingen, bør du undersøke om det allerede finnes informasjon om det problemet du forsøker å løse. Mange feil er kjent og løsningene dokumentert av produsenten. Hvis du har klart å isolere problemet til en bestemt enhet eller et bestemt program, er det naturlig enten å ta kontakt med leverandørens supporttjeneste eller forsøke å finne informasjon om det aktuelle problemet i håndboka eller på leverandørens nettsider

5. Bestemme mulige løsninger

Når du har begrenset de mulige feilkildene og innhentet den informasjonen som er tilgjengelig om utstyret og den aktuelle feilen, kan du avgjøre hvilke mulige løsninger som bør testes ut. Hvis feilen er svært komplisert, kan det være nødvendig først å systematisere mulighetene ved å skrive dem opp og ordne dem i den rekkefølgen de bør forsøkes, slik at du prøver de mest sannsynlige løsningene først. Det kan også være nødvendig å prøve ut ulike løsninger i en bestemt rekkefølge.

6. Teste ut mulige løsninger

Når det er klart hvilke muligheter du bør forsøke, må disse testes ut. I en feilsøkingsprosess er det viktig at du arbeider deg gjennom de ulike alternative løsningene i tur og orden og aldri gjør mer enn én endring av gangen. Hvis mulig bør du også reversere én endring før du forsøker den neste, slik at du alltid starter fra det samme utgangspunktet.
Hvis du gjør flere endringer samtidig, mister du lett oversikten over hva som eventuelt løser feilen, og det blir vanskeligere å fastslå hva som faktisk var årsaken. En endring du gjør i forbindelse med feilsøking, kan av og til også forårsake nye problemer eller feil, og med flere samtidige endringer kan det være vanskelig å si hva som skapte det nye problemet.

7. Dokumentere feilen og løsningen

Siste ledd i feilsøkingsprosessen er å dokumentere feilen og løsningen på problemet. Det gjelder også de gangene du ikke finner en løsning. Noen ganger vil den raskeste og rimeligste løsningen være å skifte ut en maskin eller reinstallere programvaren. I så fall bør feilen og de løsningene du har forsøkt, dokumenteres, slik at du har et grunnlag å arbeide ut fra hvis problemet oppstår igjen.
Også i de tilfellene der feilen løses, må du selvsagt dokumentere hva som var årsaken til feilen, og hvordan den ble løst. Slik dokumentasjon er vesentlig både med tanke på framtidig feilsøking og når man skal føre statistikk over antall og typer feil.

Hentet fra NDLA

Gruppeoppgave

a) Hele gruppen, lage et skjema som tar for seg prosessen feilsøking og feilsøkingsmetodikk.
Her bør man dele opp i flere prosesser, mens noe av informasjonen skal gå igjen på alle skjemaene, eksempelvis personopplysninger, utstyrstype/Model osv. Sett opp eksempler i et flytskjema.

b) Hvorfor er det viktig med god dokumentasjon av feil og løsninger, og hvordan kan dette lagres for raskt å kunne hentes opp ved liknende feil?

Wordpress læringsstier og Step by Step opplæring

a) Oppsett av Wordpress med Virtual Box og Ubuntu Server
b) Oppsett av Wordpress på Virtual Ubuntu Server kjørt fra Hyper-V (Windows 2019)
c) Installasjon av Ubuntu Server og Wordpress på fysisk maskin
d) Wordpress

1. Oppsett av virtuell maskin med Virtual Box
2. Ubuntu Server 20.04-installasjon
3. Fjernstyre Linuxmaskin med SSH
4. Oppdatere Linux med APT
5. Tekstbaserte kommandoer i Linux
6. Navigere tekst basert i Linux
7. Installere (L)AMP på Ubuntu 20.04
8. Installasjon av Wordpress
9. Virtualisering i Windows Server 2019
10. Installasjon av Hyper-V
11. Opprett virtuell maskin i Hyper-V
12. Klargjøre maskin til å brukes som server
13. Lage oppstartsmedium

Eksempel

Oppgave

Utfør installasjonen i henhold til versjon X, oppsett av WordPress på en Ubuntu server.

Vi skal her benytte en Rasp Berry enhet versjon 4 for å installere og drifte Webserveren og Wordpress.

a) 1 Install and setup SSH (Secure Shell) and Wireless Connectivity
b) Sette opp Ubuntu og Wordpress

A1 **A2** **B1** **B2**

Kompetansemål

- Kjerneelementet teknologi og metode handler om forståelse for hvordan ulike teknologier og bransjefaglige metoder er bygd opp, hvordan de virker, og hvilke muligheter de gir. Kjerneelementet handler også om å utvikle praktiske ferdigheter knyttet til bruk av teknologi og metode. Dette omfatter forståelse for valg, bruk og utvikling av teknologi og metode.
- beskrive, utforske og konfigurere datanettverk med egne subnett
- kjenne til og anvende bransjefaglige metoder og relevant utstyr i produksjon

Sjekkpunkter, hva har jeg lært?

_____ Hva statisk elektrisitet er og hvordan man kan unngå og sikre seg mot dette
_____ Hva Nettverkskabel er, de ulike modellene og hastighet
_____ Hva POE, Power Over Ethernet er og hvordan dette fungerer
_____ Kjenner til utstyr som benyttes i forbindelse med oppsett av nettverk
_____ Hva Fiberoptiske kabler er og testet denne i praksis
_____ Hvordan man terminerer en RJ 45 kabel og tester denne
_____ Fargekoder på RJ 45 i henhold til standarder
_____ Femfingerregelen for feilsøking
_____ Kunne bruke Ping og ipconfig til kontroll i nettverk og sender/mottakere
_____ Ulike Radiolinker og faste IP adresser
_____ Frekvens, valg av frekvens, båndbredde og hva Fresnelsone er
_____ Hva som kan skape forstyrrelser i radiosignalene
_____ Hva Redundans er og hvorfor dette benyttes
_____ Hva er konstruktiv og destruktiv interferens
_____ Nettvett og GSM nett i Norge
_____ Feilsøkingsmetodikk og kunne sette opp dokumentasjonsunderlag for dette i flere trinn
_____ Sette opp en maskin og eller server for å bruke Wordpress på den