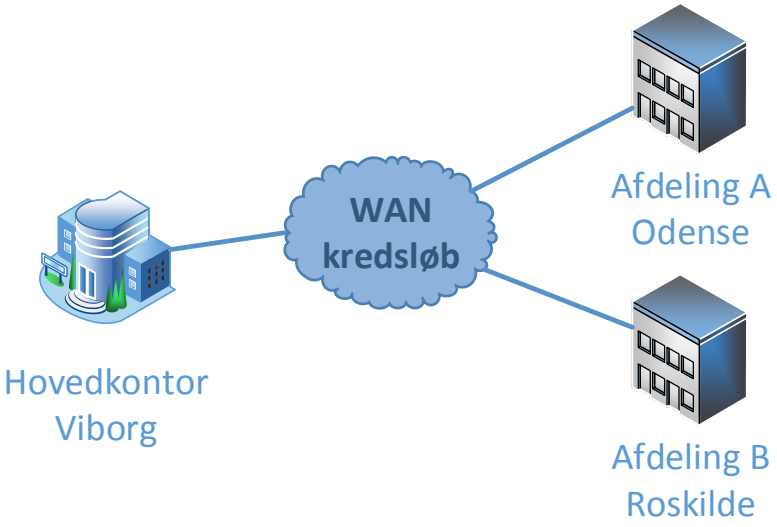
Netværk, WAN teknik

WAN og sikkerhed



©2018 Henrik Thomsen

Indhold

Introduktion til WAN netværk 4
Sikkerhed 5
WAN teknologier 5
Anvendte WAN topologier 6
Punkt-til-punkt topologi 6
Matrix topologi 6
Fuld matrix 6
Delvis matrix 7
Træ topologi 8
Bus topologi 8
Halv duplex 9
Netværks sky 9
Fuld duplex 9
Blandet topologi 10
Forudsætninger 10
IP adresseplaner 10
IP adresseplan eksempel 12
Overordnet IP adresseplan 12
Underinddelt afdelings IP adresseplan 12
Detaljeret subnet IP adresseplan 13
Brug af IP adresseplaner 14
IP adresseplaner – og fremtiden 14
Sammenlægning af netværk 14
Introduktion til VPN 15
VPN tunnel 15
Site-to-site VPN tunnel 15
Site-to-site VPN tunnel princip 16
Konfiguration af hosts 16
Konfiguration af gateways 17
Indre og ydre pakker 18

Overførsel af trafik gennem tunnelen 18
Kryptering i VPN tunnel 18
Klient VPN tunnel 19
Konfiguration af VPN server og VPN klienter 20
Konfiguration af VPN server 20
Konfiguration af VPN klienter 21
Opkobling af VPN klient 21
Sikkerhed 22
VPN tunneling protokoller 23
Hash værdi 23
Hash funktioner 24
Anvendelse af hash værdier 25
Overførsel af filer 25
Downloads af ISO filer til CD og DVD 25
Kontrol af passwords 26
Overførsel af password via netværket 26
Hash værdi med nonce 28
Eksempel opfanget med Wireshark 29
Kryptering med nøgler 29
Cæsar krypterings algoritme 30
Symmetriske nøgler 30
Udveksling af nøgler 30
Asymmetriske nøgler 30
Offentlig nøgle kryptering 31
Anvendelse af asymmetriske nøgler 32
Identitet 32
Diffie-Hellman nøgle udveksling 32
Anvendelse 33
Ulemper 34

Introduktion til WAN netværk

WAN – eller Wide Area Network – er et netværk der strækker sig over store geografiske områder. Generelt inddeles netværkstyper efter deres geografiske udstrækning. Se tabel herunder for eksempler.

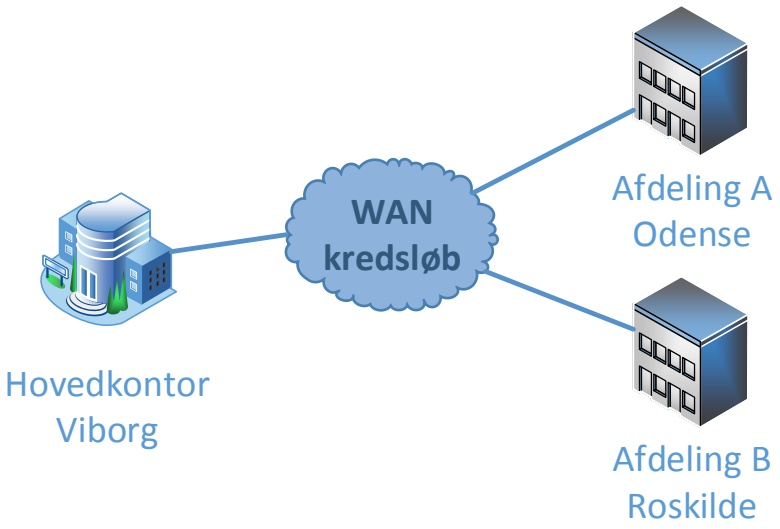
Forkortelse	Betydning	Typisk udstrækning	Eksempler på teknologier
PAN	Personal Area Network	< 10 meter	Bluetooth, IrDa
LAN	Local Area Network	< 1 kilometer	Ethernet
MAN	Metropolitan Area Network	< 10 kilometer	Ethernet, metro ethernet
WAN	Wide Area Network	> 10 kilometer	MPLS, VPLS

Internettet er verdens største WAN netværk der med global udstrækning og flere milliarder tilslutninger har ændret verden og den måde vi tænker og arbejder på.

Normalt tænker de fleste på private lukkede netværk når der omtales WAN netværk – også benævnt WAN kredsløb.

Virksomheder, organisationer og offentlige institutioner er de største forbrugere af WAN kredsløb, da de ønsker at koble geografisk adskilte afdelinger sammen i et stort samlet privat lukket netværk.

WAN kredsløb kan enten lejes hos en WAN udbyder eller være ejet af organisationen selv.

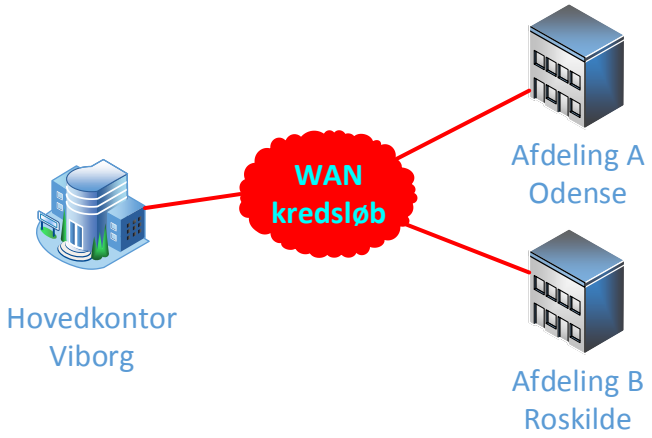


Figur 1 - Eksempel på virksomheds WAN kredsløb

Sikkerhed

De fleste brugere af WAN kredsløb overvejer sikkerhed meget nøje. En bank vil for eksempel sikre fysisk adgang til netværk og netværksenheder i deres egne bygninger. Serverrum og rackskabe er aflåste for at forhindre ikke autoriseret adgang. Der er installeret tyverialarm og andre sikkerhedsforanstaltninger for at sikre bygningen.

Hvis banken anvender WAN kredsløb, vil dataene være uden for bankens kontrol i det øjeblik de forlader bygningen – typisk i et fiberoptisk kabel der er tilsluttet udbyderen af WAN kredsløbet. Banken vil derfor sikre dataene i WAN kredsløbet ved at kryptere dem før de forlader bygningen.



WAN teknologier

Der findes mange WAN teknologier der hver har deres fordele og ulemper. Her i Danmark hvor vi – i modsætning til for eksempel Australien – bor meget tæt sammen og har en geografi der gør det nemt at trække fiberoptiske kabler mellem byer og landsdele, anvender teknologier der giver adgang til høje hastigheder relativt billigt i hele landet. Der er mange udbydere i Danmark nogle der dækker geografisk regionalt andre nationalt og enkelte internationalt i samarbejde med udbydere i andre lande.

Forkortelse	Betydning	Typiske båndbredder	Eksempler på udbydere
MPLS	Multi Protocol Label Switching	10 Mbps til 1 Gbps	TDC, Telia, Telenor…
VPLS	Virtual Private LAN Service	10 Mbps til 10 Gbps	Global Connect…
Site-to-site VPN	VPN via internettet	10 til 100 Mbps	Alle Internet udbydere
Frame Relay	Ældre teknologi	64 Kb til 8 Mbps	Lukket i Danmark

Figur 3 - Eksempler på WAN udbydere i Danmark

De enkelte WAN teknologier bliver gennemgået detaljeret senere i forløbet.

Anvendte WAN topologier

WAN topologier beskriver den måde kredsløbet er opbygget.

Punkt-til-punkt topologi

Engelsk: Point-to-point topologi

En punkt-til-punkt topologi har kun to tilslutninger. Der er ikke nødvendigt med adressering, da det altid er den samme samtalepartner i den anden ende.

Figur 4 - Eksempel på Punkt-til-punkt

Eksempler på punkt-til-punkt forbindelser er VPN gennem Internettet og dedikeret fiberkabel.

Matrix topologi

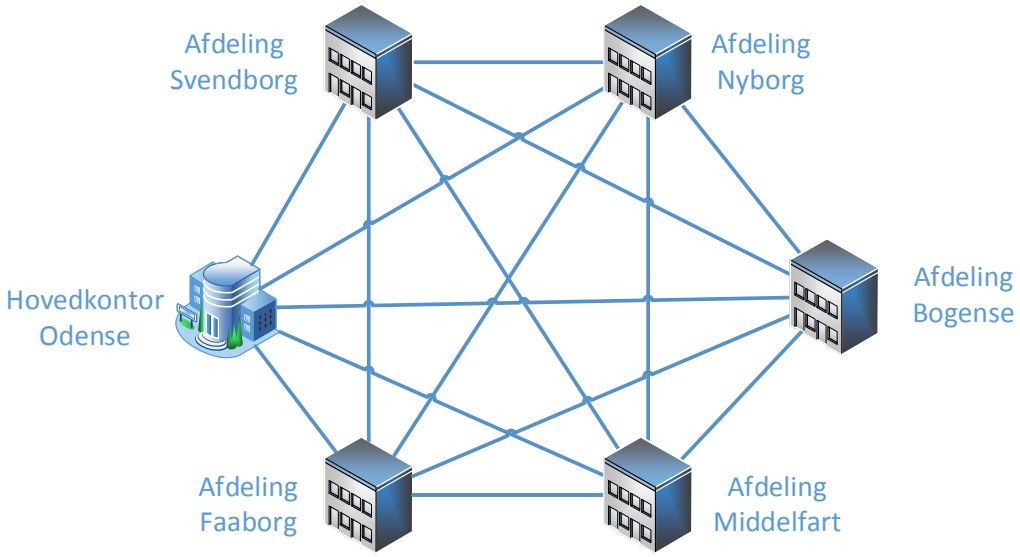
Engelsk: Mesh topologi

En matrix topologi består af punkt-til-punkt forbindelser mellem lokationer der skal kommunikere med hinanden.

Fuld matrix

Engelsk: Full mesh topologi

En fuld matrix består af punkt-til-punkt forbindelser mellem alle lokationer.



Figur 5 - Eksempel på fuld matrix topologi (Engelsk: full mesh)

En matrix med tilslutninger mellem alle lokationer skalerer ikke så godt og bliver meget ofte meget dyr og uoverskuelig. Hvis der i Figur 5 anvendes dedikeret fiberkabel mellem hver lokation vil WAN løsningen blive meget dyr. Fordelen er dog at et enkelt nedbrud på et kabel ikke lukker hele netværket ned.

Antallet af forbindelser i en fuld matrix beregnes som:

$$\boldsymbol{Antal\ point-to-point\ forbindelser} = \frac{n \times (n-1)}{\mathbf{2}}$$

I eksemplet i Figur 5 er der seks lokationer og derfor

$$\frac{\mathbf{6} \times (\mathbf{6}-1)}{\mathbf{2}} = \mathbf{15}\ \boldsymbol{forbindelser}$$

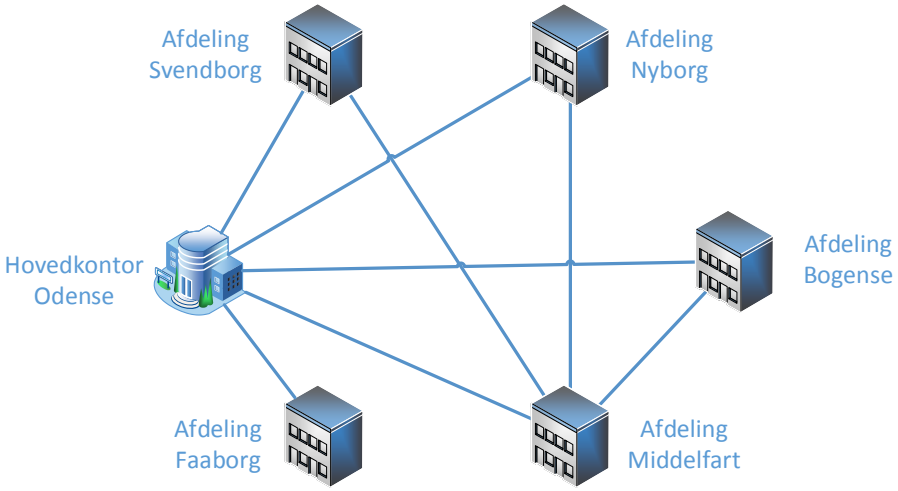
Hvis der for eksempel er 100 lokationer er antallet af punkt-til-punkt forbindelser:

$$\frac{\mathbf{100} \times (\mathbf{100}-1)}{\mathbf{2}} = \mathbf{4950}\ \boldsymbol{forbindelser}$$

Delvis matrix

Engelsk: Partial mesh topologi

En delvis matrix består af en række punkt-til-punkt forbindelser hvor WAN designeren har vurderet at der er brug for stor båndbredde eller/og redundans (backup forbindelser).

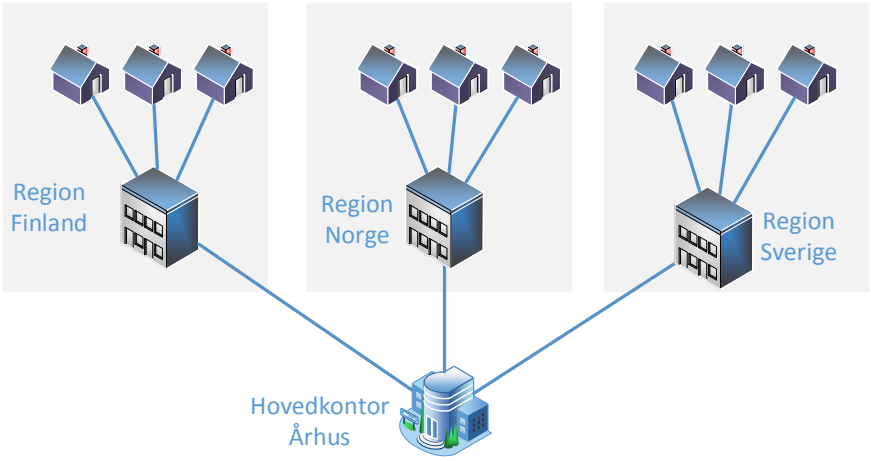


Figur 6 - Delvis matrix (Engelsk: Partial mesh)

Træ topologi

Engelsk: Tree topologi

Træ topologi består af punkt-til-punkt forbindelse. I en trætopologi prøver designeren af WAN kredsløbet at optimere netværket med hensyn til geografiske forhold, økonomi og krav til båndbredde mellem tilsluttede lokationer.

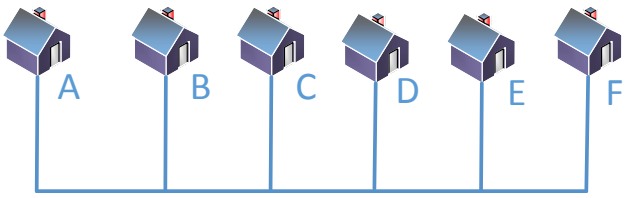


I eksemplet har designeren taget hensyn til de regionale centre har deres egne data-centre som de små filialer i hvert enkelt land anvender.

Bus topologi

Engelsk: Bus topologi

I en bustopologi er alle lokationer forbundet til det samme medium. Da der er mere end to deltagere er det nødvendigt med adressering for at kommunikere med en anden specifik lokation. Trådløse netværk er et eksempel på bus topologi netværk.



I eksemplet i Figur 8 kan alle lokationer kommunikere ved at anvende adressering. Alle andre lokationer kan lytte med da kommunikationen modtags af alle tilsluttet bussen. Ulempen med bus topologien er at der kun er en der kan sende af gangen. De andre må vente på at bussen er ledig, såfremt de ønsker at sende, en anden ulempe er at alle tilsluttede til bussen anvender samme båndbredde.

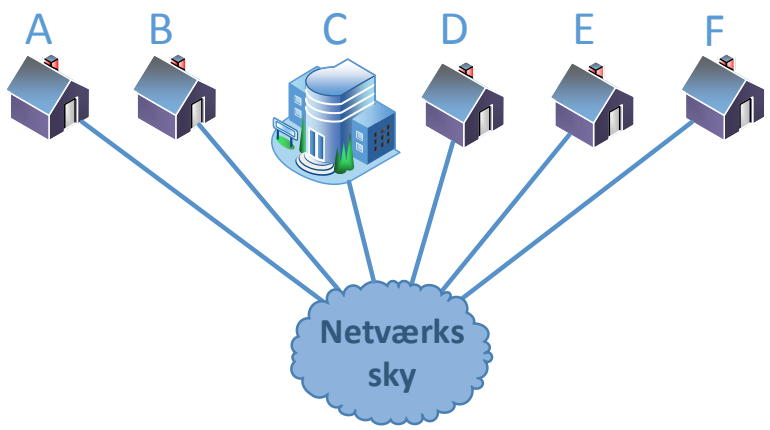
Halv duplex

En bus topologi er halv duplex – det vil sige at der kun kan kommunikeres i en retning af gangen. De enkelte lokationer kan enten modtage eller sende – ikke begge dele samtidigt.

Netværks sky

Engelsk: Network cloud

En netværkssky er en intelligent bus topologi, hvor skyen kun videresender kommunikation til den tiltænkte modtager. Hver lokation kan anvende sin egen båndbredde, ofte vil hovedkontoret have større båndbredde end afdelinger og filialer.



Figur 9 - Eksempel på netværkssky (Engelsk network cloud)

Nogle af fordelene ved en netværkssky er at der kan kommunikeres direkte mellem de enkelte lokationer. Alle kan kommunikere med hinanden samtidigt og at der kan vælges en passende båndbredde til hver enkelt lokation.

Eksempler på netværksskyer er MPLS der anvender IP adresser til adressering og VPLS der anvender MAC adresser til adressering.

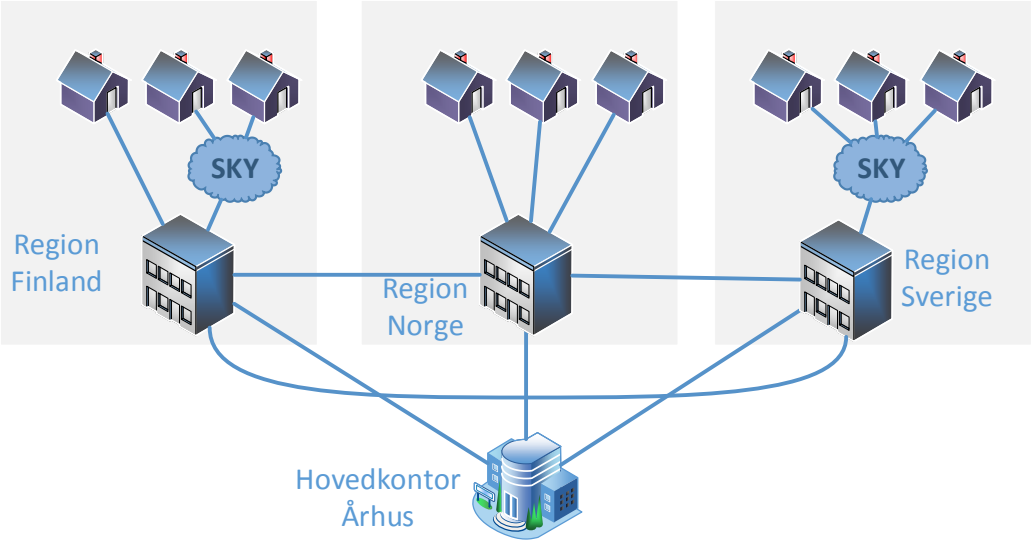
Den største netværks sky er Internettet med milliarder af tilslutninger.

Fuld duplex

En netværks sky er normalt fuld duplex – det vil sige der kan kommunikeres i begge retninger samtidig.

Blandet topologi

Ofte vil man i større organisationer benytte flere typer af topologier, for at tilpasse geografiske, økonomiske og udbudte WAN tjenester bedst muligt.



Figur 10 - Eksempel på blandet topologi

I eksemplet i Figur 10 anvendes en fuld matrix mellem regionale centre og hovedkontoret samtidigt med at der benyttes punkt-til-punkt og sky baserede løsninger til filialerne.

Forudsætninger

- Kendskab til forudgående afsnit i WAN teknik ikke nødvendigt
- Kendskab til IP version 4 – IPv4 – adresser – LINK TIL IPv4 ADRESSER
- Grundlæggende kendskab til NAT – LINK TIL NAT
- Grundlæggende kendskab til IPv4 subnetting – LINK TIL IPv4SUBNETTING

IP adresseplaner

De fleste virksomheder og offentlige institutioner anvender IPv4[1] sammen med NAT[2] i opbygningen af deres interne netværk. Når man anvender NAT anbefales det at anvende private IP adresser – de såkaldte RFC 1918[3] adresser. De private IP adresser er ulovlige på Internettet og anvendes kun internt i privat netværk.

Privat netværk	IP adresseområde
10.0.0.0/8	10.0.0.0 til 10.255.255.255
172.16.0.0/12	172.16.0.0 til 172.31.255.255
192.168.0.0/16	192.168.0.0 til 192.168.255.255

[1] IPv4 er IP version 4 som anvender 32 bits IP adresser for eksempel 192.168.1.10
[2] NAT eller Network Address Translation er behandlet separat i et senere afsnit
[3] Se http://tools.ietf.org/html/rfc1918

Figur 11 - RFC 1918 private IP adresser

Når man designer et større netværk prøver man at lave et system for tildeling af IP adresser på en logisk og overskuelig måde. Dette kaldes for en IP adresseplan. IP adresseplanen vil ofte være udført efter geografiske hensyn således at man ud fra IP adressen kan se hvor hosten[4] med den adresse fysisk er.

[4] En host er en enhed med en IP adresse. For eksempel en computer.

IP adresseplan eksempel

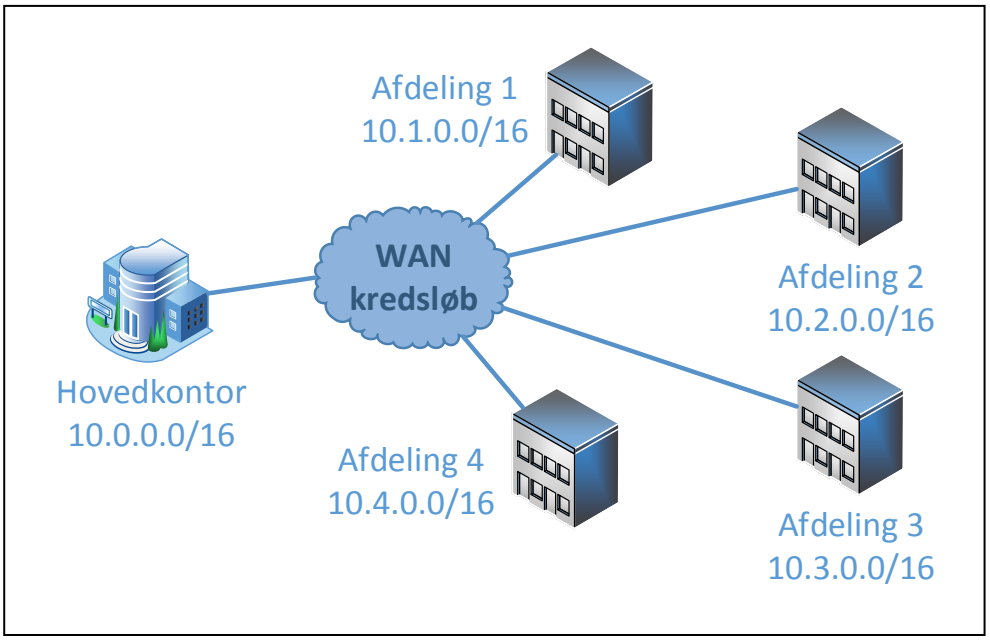
En virksomhed har et hovedkontor og fire afdelinger.

Overordnet IP adresseplan

Løsningen tager udgangspunkt i overblik. Hver afdeling tildeles deres eget logiske netværk i en overordnet IP adresseplan.

Lokation	Tildelt netværk	IP adresseområde	Antal IP adresser
Hovedkontor	10.0.0.0/16	10.0.0.0 til 10.0.255.255	65.534
Afdeling 1	10.1.0.0/16	10.1.0.0 til 10.1.255.255	65.534
Afdeling 2	10.2.0.0/16	10.2.0.0 til 10.2.255.255	65.534
Afdeling 3	10.3.0.0/16	10.3.0.0 til 10.3.255.255	65.534
Afdeling 4	10.4.0.0/16	10.4.0.0 til 10.4.255.255	65.534

Figur 12 – Eksempel på overordnet IP adresseplan



Figur 13 - Topologi tegning med overordnet IP adresseplan

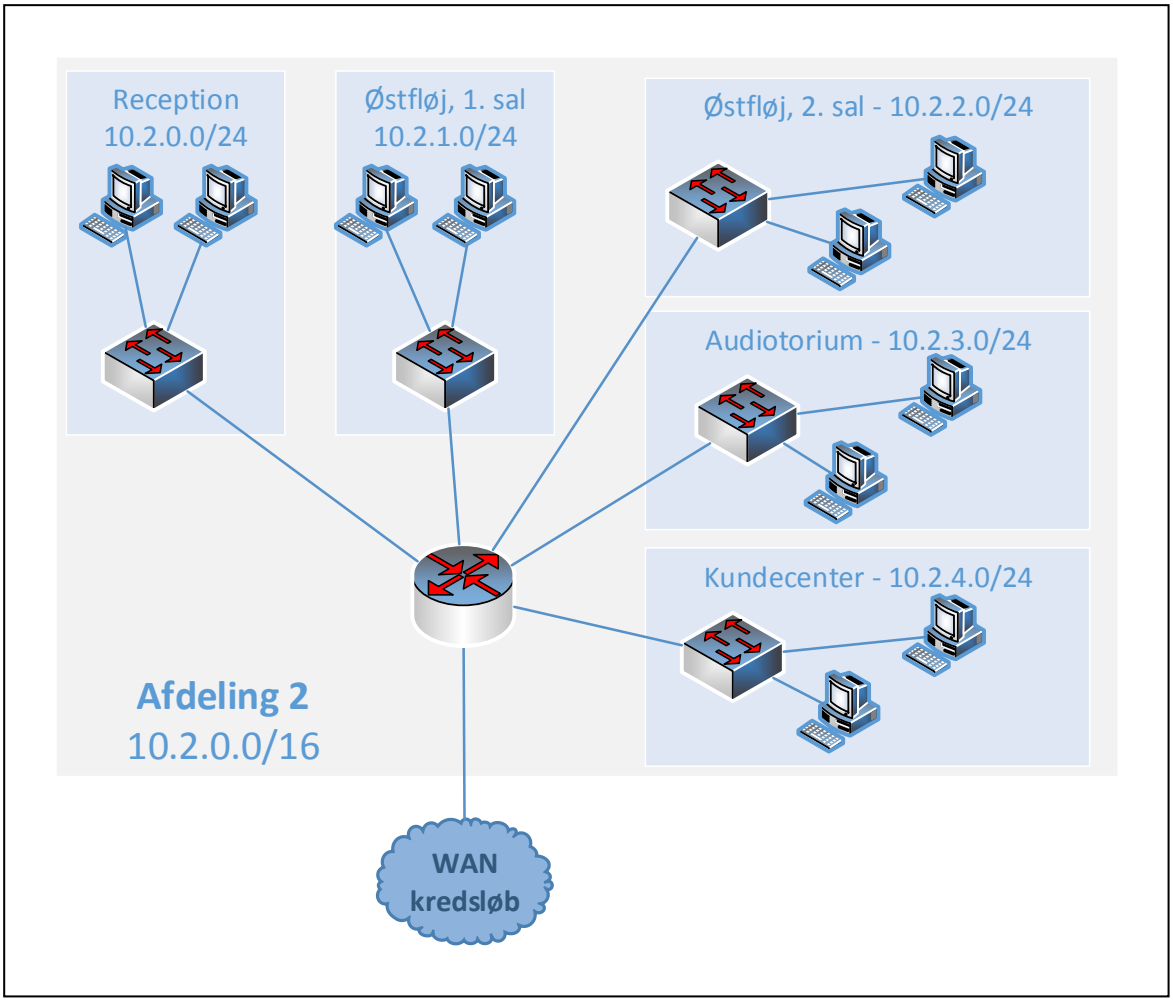
Underinddelt afdelings IP adresseplan

I hver lokation inddeles afdelingens logiske netværk i en række undernet – engelsk subnet. De fysiske forhold, antal medarbejdere og andre faktorer er medbestemmende for udformningen af afdelings planer.

Lokation	Tildelt subnet	IP adresseområde	Antal IP adresser
Reception	10.2.0.0/24	10.2.0.0 til 10.2.0.255	254
Østfløj, 1. sal	10.2.1.0/24	10.2.1.0 til 10.2.1.255	254
Østfløj, 2. sal	10.2.2.0/24	10.2.2.0 til 10.2.2.255	254
auditorium	10.2.3.0/24	10.2.3.0 til 10.2.3.255	254
Kundecenter	10.2.4.0/24	10.2.4.0 til 10.2.4.255	254
....			

Figur 14 – Eksempel på afdeling 2 subnet IP adressesplan eksempel

Figur 15 –



Eksempel på netværks diagram i afdeling 2

Detaljeret subnet IP adresseplan

I hvert subnet tildeles hosts IP adresser ud fra deres funktion.

- Hvor X er afdeling fra den overordnede adresseplan
- Hvor Y er subnet tildelt i den underinddelte adresseplan

IP adresse	Funktion	Antal IP adresser
10.X.Y.[1-19]	Netværksudstyr	19
10.X.Y.[20-39]	Servere og andet udstyr	20
10.X.Y.[40-99]	Ledig	60
10.X.Y.[100-199]	DHCP tildelte adresser	100
10.X.Y.[200-239]	ledig	40
10.X.Y.240.[240-254]	Printere	15

Figur 16 – Eksempel på inddeling af de enkelte subnet

Med den viste IP adresseplan vil man kunne konkludere at IP adressen 10.4.3.251 er en printer i afdeling 4 i kundecenteret.

Brug af IP adresseplaner

I større netværk er det nødvendigt at dokumentere sin adresseplan og hvilke IP adresser man har tildelt til servere, netværksudstyr printere og andet udstyr. I nogle organisationer anvendes et regneark og i andre et IP adresse management program også kaldet et IPAM program.

I en større organisation er det vigtigt at alle medarbejdere i IT afdelingen samt eksterne samarbejdspartnere har overblik over netværket, så det er nemt at installere nye enheder og fejlfinde på netværket. Der skal være dokumentation over netværket som er tilgængelig for alle, helst i en database som løbende bliver opdateret. Netværks dokumentation som ikke løbende bliver opdateret kan være meget forvirrende i en fejlfindingssituation og være skyld i at netværksnedbrud tager uforholdsmæssigt lang tid at udbedre, idet der skal bruges tid på at få overblik over netværket først.

IP adresseplaner – og fremtiden

Det kan være svært at udarbejde IP adresseplaner idet det er nødvendigt at allokere IP adresser nok til fremtidige begivenheder. I eksemplet i Figur 17 er der tildelt et /11[5] netværk til hovedkontoret og et /13 netværk til hver afdeling, således det er muligt at udvide de enkelte afdelinger i fremtiden. Samtidigt er der mange ledige IP adresseområder som kan anvendes hvis der oprettes flere afdelinger.

Lokation	Tildelt netværk	IP adresseområde	Antal IP adresser
Hovedkontor	10.[0-31].0.0/11	10.0.0.0 til 10.31.255.255	2.097.150
Afdeling 1	10.[64-67].0.0/13	10.64.0.0 til 10.67.255.255	524.286
Afdeling 2	10.[68-71].0.0/13	10.68.0.0 til 10.71.255.255	524.286
Afdeling 3	10.[72-75].0.0/13	10.72.0.0 til 10.75.255.255	524.286
Afdeling 4	10.[76-79].0.0/13	10.76.0.0 til 10.79.255.255	524.286

Figur 17 - Tildeling af IP adresser med anvendelse af subnetting[5]

- Subnet mask ved /11 = 11111111.11100000.00000000.0000000 = 255.224.0.0
- Subnet mask ved /13 = 11111111.11111000.00000000.0000000 = 255.248.0.0

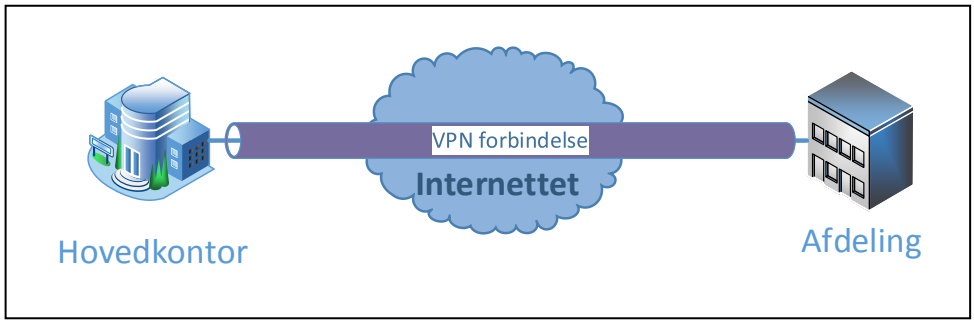
Sammenlægning af netværk

Når to virksomheder fusionerer og deres netværk skal kobles sammen vil det ofte være et stort problem at begge virksomheder har valgt at bruge de samme private netværks IP adresser. Det gør det besværligt og til en stor opgave at lave de to netværk om til et stort. Det kan være nødvendigt at lave en helt ny IP adresseplan for det nye netværk og skifte IP adresser overalt.

[5] For yderligere information om subnetting se netværk grundlæggende afsnit IP subnetting

Introduktion til VPN

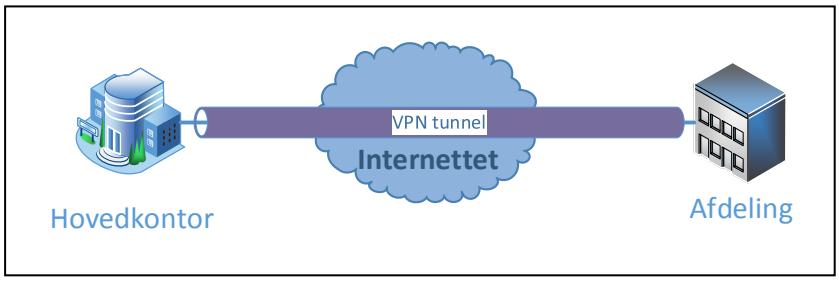
Et VPN – eller Virtual Private Network – er en netværksforbindelse som anvendes af organisationer som ønsker en privat WAN-løsning i et eksisterende delt netværk. Internettet er et eksempel på et eksisterende delt netværk, hvor det er muligt at lave en VPN forbindelse mellem to lokationer.



Figur 18 – illustration af en VPN WAN forbindelse gennem Internettet

VPN tunnel

En VPN tunnel er indpakning af data pakker i en tunneling protokol der har ansvaret for transport af data gennem det delte netværk. Tunnelen vist i Figur 19 er et *site-to-site* VPN tunnel der er oprettet gennem Internettet. Formålet med dette er at anvende Internettet som en WAN forbindelse – i dette tilfælde mellem hovedkontor og en afdeling. Fordelen ved at anvende Internettet til at sammenkoble geografisk adskilte lokationer med et VPN er primært økonomi, da det er billigere at bruge Internettet end at leje en dedikeret WAN forbindelse som for eksempel MPLS[6] eller VPLS[7]

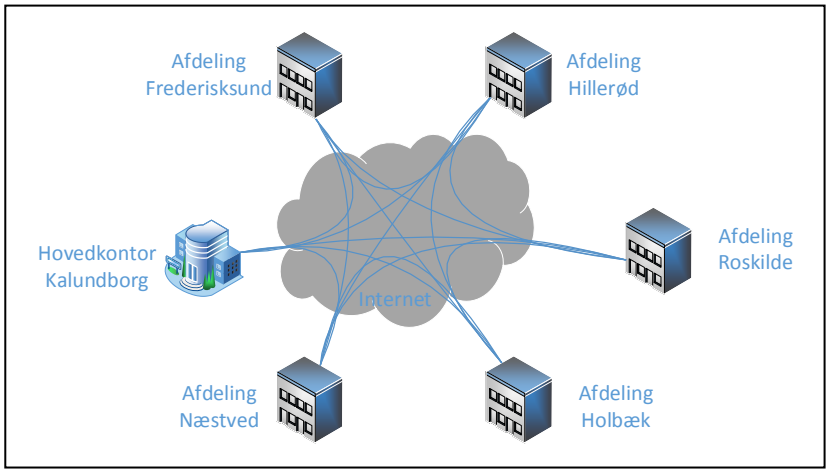


Figur 19 - VPN tunnel overordnet princip

Site-to-site VPN tunnel

Site-to-site VPN tunneler er punkt-til-punkt forbindelser mellem to lokationer. Hvis der er mere end to lokationer er det nødvendigt at lave en delvis eller fuld matrix – partial eller full mesh. I Figur 20 er der vist et eksempel på en fuld matrix af site-to-site VPN tunneler gennem Internettet. Hver lokation benytter den sammen Internetforbindelse til alle VPN tunneler.

[6] MPLS – Multi Protocol Label Switching – er en WAN tjeneste der kan lejes fra WAN udbydere
[7] VPLS – Virtual Private LAN Service – er en WAN tjeneste der kan lejes fra WAN udbydere

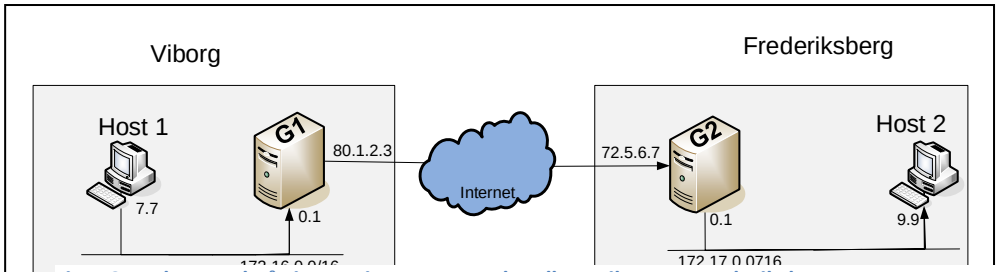


Figur 20 - Eksempel på fuld matrix af site-to-site VPN tunneler

Site-to-site VPN tunnel princip

En tunnel er opbygget ved at anvende en tunneling protokol. I eksemplet vist i Figur 21 ønsker en virksomhed at koble to lokationer sammen på den billigst mulige måde. Virksomhedens mål er at kunne sende trafik mellem netværket 172.16.0.0/16 i Viborg og netværket 172.17.0.0/16 på Frederiksberg.

Virksomheden anskaffer Internet forbindelser i begge lokationer – eller bruger dem de har – til at lave tunnelen igennem. I begge lokationer anvender virksomheden en gateway – G1 og G2 – med tunneling protokol software installeret. Begge gateways bliver tildelt offentlige IP adresser af Internetudbyderen, når de tilsluttes til Internettet. I eksemplet 80.1.2.3 i Viborg og 72.5.6.7 på Frederiksberg.



Figur 21 - Eksempel på site-to-site VPN tunnel mellem Viborg og Frederiksberg

Konfiguration af hosts

Hosts skal konfigureres til at sende trafik til den anden ende af tunnelen til den lokale gateway. Se eksempel i Figur 22.

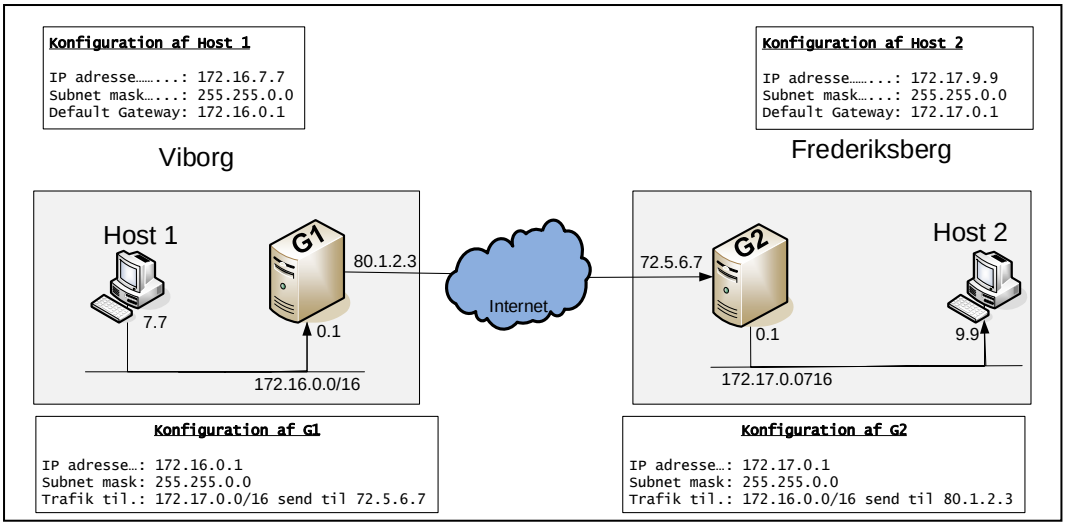
- Host 1 i Viborg konfigureres til at anvende G1 – 172.16.0.1 – som default gateway. Host 1 vil derfor sende alle pakker der ikke er lokale på 172.16.0.0/16 til G1, herunder trafik til Frederiksberg 172.17.0.0/16.

- Host 2 på Frederiksberg konfigureres til at anvende G2 – 172.17.0.1 – som default gateway. Host 2 vil derfor sende alle pakker der ikke er lokale på 172.17.0.0/16 til G2, herunder trafik til Viborg 172.16.0.0/16.

Konfiguration af gateways

For at tunnelen kan oprettes skal begge gateways konfigureres.

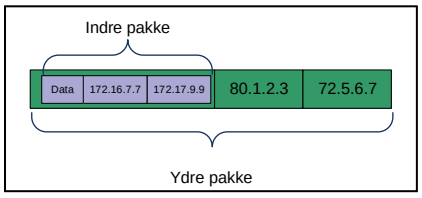
- Gateway G1 skal konfigureres til at videresende trafik til Frederiksberg 172.17.0.0/16 til G2's offentlige IP adresse 72.5.6.7
    - Trafik til andre IP adresser end 172.16.0.0/16 og 172.17.0.0/16 sendes til Internettet
- Gateway G2 skal konfigureres til at videresende trafik til Viborg 172.16.0.0/16 til G1's offentlige IP adresse 80.1.2.3
    - Trafik til andre IP adresser end 172.16.0.0/16 og 172.17.0.0/16 sendes til Internettet



Figur 22 - Tegning med delvis konfiguration af hosts og gateways

Indre og ydre pakker

Når en pakke transporteres i en anden pakke kaldes den transporterede pakke den indre pakke og den pakke der transporterer den ydre pakke. Se Figur 23.

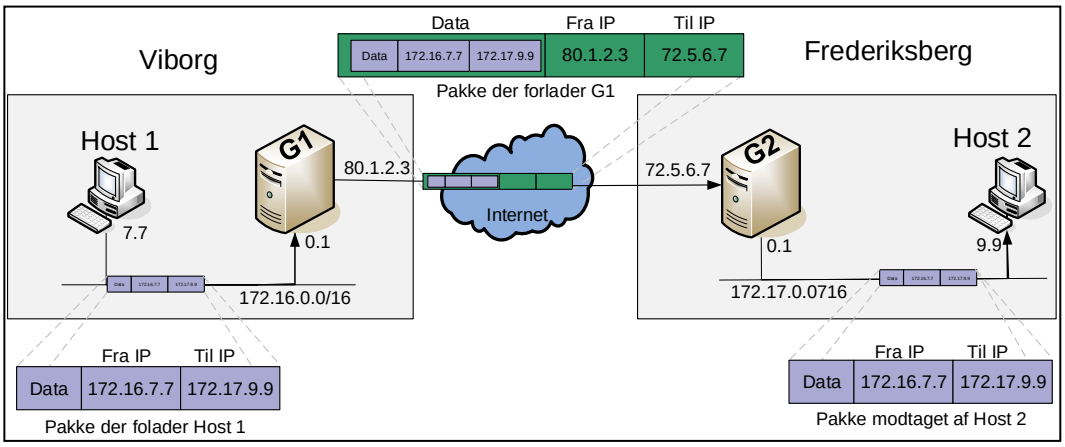


Figur 23 - Indre og ydre pakke

Overførsel af trafik gennem tunnelen

Transporten af data gennem tunnelen foregår ved at tunneling softwaren på gatewayen pakker den originale IP pakke ind i en ny IP pakke, som vist i Figur 24.

De private IP netværk 172.16.0.0/16 og 172.17.0.0/16 er ulovlige på Internettet, hvor kun offentlige IP adresser videresendes.



Figur 24 - Eksempel på transport af pakke gennem tunnel

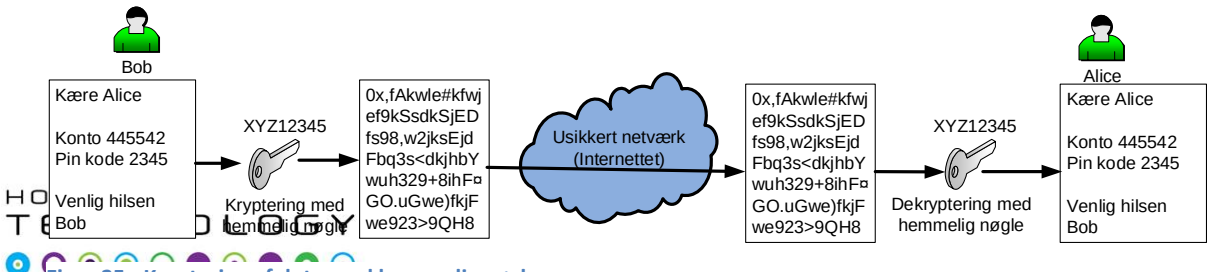
1. Host 1 ønsker at sende en IP pakke til 172.17.9.9 på Frederiksberg og sender den til G1
2. G1 ser IP pakken skal til 172.17.0.0/16 netværket og pakker den originale pakke ind i en ny IP pakke med offentlige til og fra adresser – fra 80.1.2.3 til 72.5.6.7
3. Internettet router pakken fra Viborg til G2 på Frederiksberg. (72.5.6.7)
4. G2 pakker den indre pakke ud og videresender den til modtageren 172.17.9.9

Pakken har passeret tunnelen mellem G1 og G2 uændret – tilsyneladende gennem en tunnel fra G1 i Viborg til G2 på Frederiksberg.

Kryptering i VPN tunnel

For at øge sikkerheden vil man ofte vælge at kryptere dataene i tunnelen mellem de to gateways. Dette kræver at der er installeret og konfigureret krypteringssoftware på begge gateways.

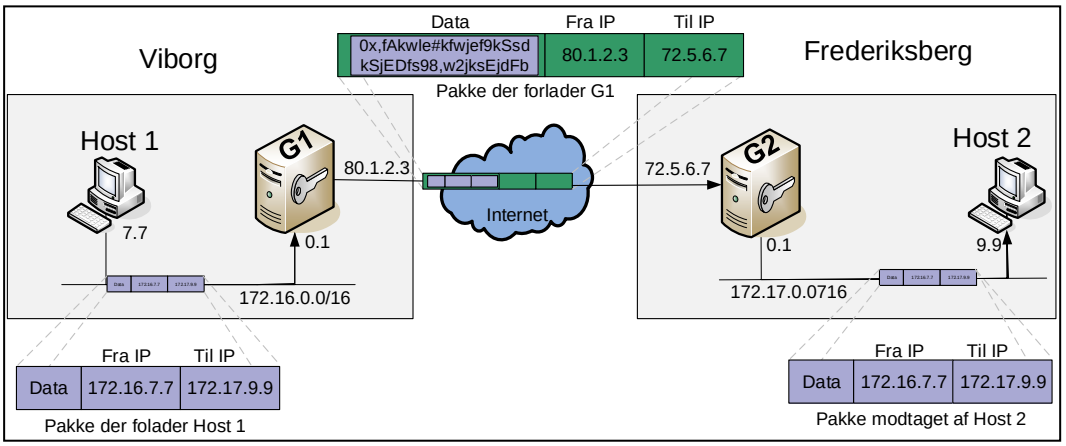
Det grundlæggende princip i kryptering er vist i Figur 25 hvor Bob krypterer den hemmelige meddelelse med krypteringsnøglen *XYZ12345* og sender den igennem Internettet til Alice. Alice dekrypterer Bobs meddelelse da hun også kender den hemmelige nøgle *XYZ12345*.



Figur 25 - Kryptering af data med hemmelig nøgle

Med anvendelse af kryptering i en site-to-site VPN krypteres hele den indre pakke. Fordelen ved at kryptere hele den indre pakke er at eventuelle personer der prøver at samle informationer om kommunikationen mellem Viborg og Frederiksberg ikke kan se

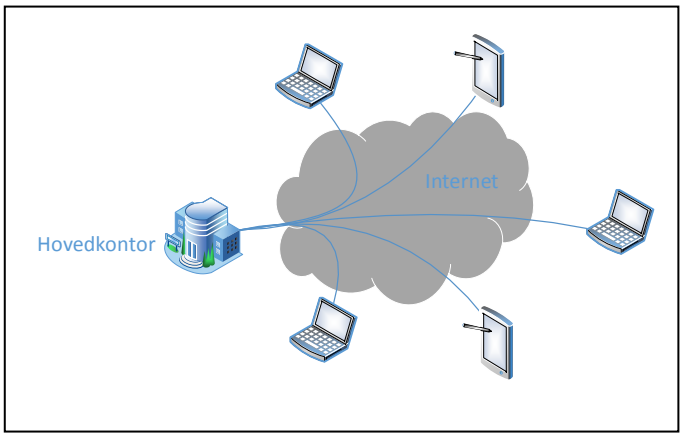
1. Dataene i den indre pakke er krypteret. (Data er skjult)
2. IP adressen på afsenderen i Viborg er krypteret. (Identitet på afsender skjult)
3. IP adressen på modtageren på Frederiksberg er krypteret. (Identitet på modtager skjult)



Figur 26 - Den indre pakke er krypteret med den hemmelige nøgle

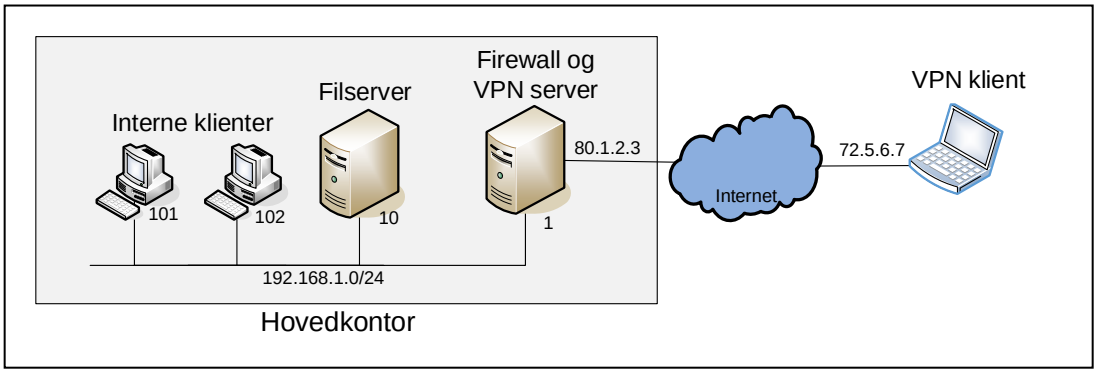
Klient VPN tunnel

Klient VPN benyttes ofte af organisationer som ønsker medarbejdere der ikke fysisk er i organisationen, kan lave en forbindelse til organisationens netværk via Internettet. Se eksempel i Figur 27. Klient VPN tunnel opkoblinger benyttes ofte som hjemmearbejdspladser eller til rejsende medarbejdere, således de kan koble op på det interne netværk i organisationen.



Figur 27 - Klient VPN opkoblinger via Internettet

Det grundlæggende scenarie i en klient VPN opkobling er en klient tilkoblet Internettet – se Figur 28 – som ønsker adgang til organisationens interne ressourcer, i dette tilfælde den interne filserver med IP adressen 192.168.1.10.



Figur 28 - Klient tilsluttet Internettet før opkobling af VPN forbindelse

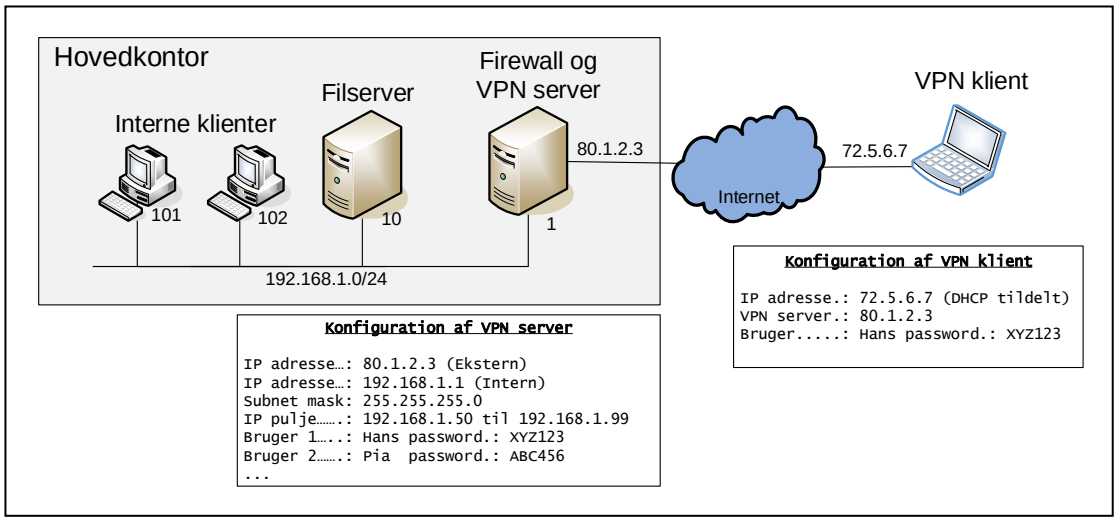
Konfiguration af VPN server og VPN klienter

VPN serveren og VPN klienterne skal konfigureres

Konfiguration af VPN server

En VPN server kan være direkte tilsluttet Internettet som i eksemplet i Figur 28 eller være beskyttet bag en firewall. VPN serveren skal være tilgængelig fra Internettet for at VPN klienterne kan koble op. Hvis VPN serveren er beskyttet bag en firewall er det nødvendigt at konfigurere firewallen til at tillade trafik fra VPN klienterne til VPN serveren.

En VPN server bliver typisk konfigureret med en pulje af IP adresser som den kan tildele VPN klienter når de kobler op. I eksemplet i Figur 29 er puljen fra 192.168.1.50 til og med 192.168.1.99. Herudover har VPN serveren typisk en database over brugere og deres passwords.



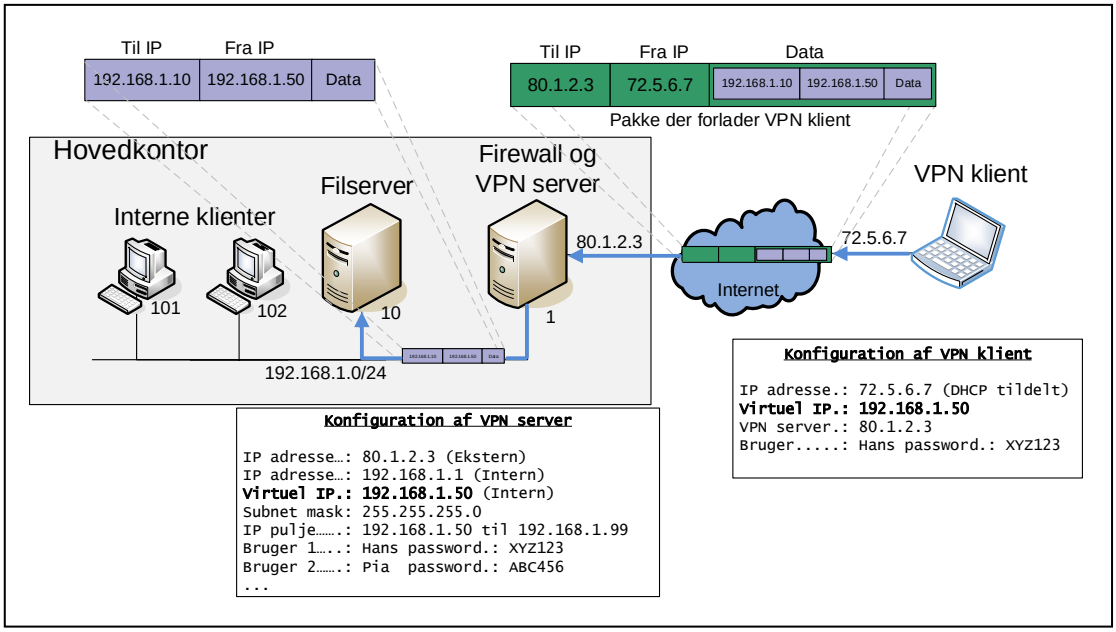
Figur 29 - Konfiguration af VPN server og VPN klienter

Konfiguration af VPN klienter

VPN klienterne er typisk konfigureret med IP adressen eller host navnet på VPN serveren. Host navnet kunne for eksempel være VPN.DOMÆNE.DK som VPN klienten via DNS kunne resolve – omsætte – til en IP adresse. Herudover kan VPN klienten være konfigureret med et brugernavn og et password.

Opkobling af VPN klient

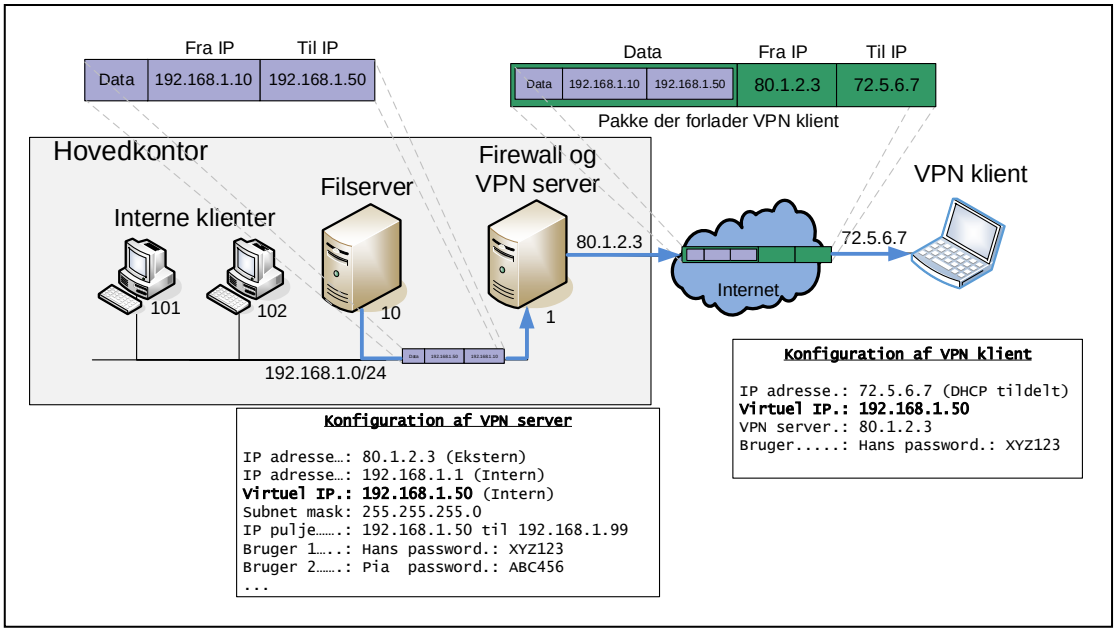
Når VPN klienten kobler op til VPN serveren vil VPN serveren tildele VPN klienten en IP adresse fra IP puljen. I eksempel i Figur 30 bliver klienten tildelt IP adressen 192.168.1.50 som den bruger som en virtuel IP adresse. En virtuel IP adresse har ikke sit eget fysiske netværkskort. Ved at anvende den virtuelle IP adresse er VPN klienten tilsyneladende koblet til netværket 192.168.1.0/24. VPN klienten har samme funktionalitet som de interne klienter i hovedkontoret.



Figur 30 - Pakke fra VPN klient til filserver igennem tunnelen

VPN serveren har samtidigt med at den tildelte IP adressen 192.168.1.50 til VPN klienten oprettet en virtuel IP adresse på sit interne netværkskort som i eksemplet har to IP adresser – 192.168.1.1 og 192.168.1.50. Filserveren som i Figur 30 får en pakke fra VPN klienten ser filserveren som afsender af pakken fra IP adresse 192.168.1.50.

Når filserveren returner pakker til afsenderen vil den sende pakken til 192.168.1.50, som er VPN serveren internt. VPN serveren vil herefter – som vist i Figur 31 – videresende pakken i tunnelen til VPN klienten.



Figur 31 - Pakke fra filserver til VPN klient

Sikkerhed

Oftest vil en VPN server/klient løsning blive kombineret med kryptering efter samme princip som i afsnittet Kryptering i VPN tunnel.

VPN tunneling protokoller

Der findes adskillige VPN tunneling protokoller, hver med deres fordele og ulemper.

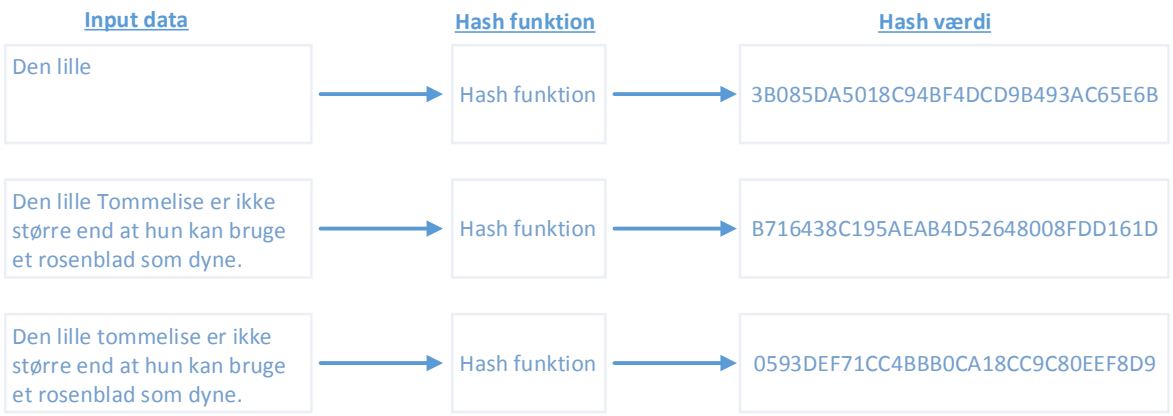
Protokol	Betydning	Kan kryptere data
L2TP	Layer 2 Tunneling Protocol	Nej
PPTP	Point-to-Point Tunneling Protocol	Nej/ja
GRE	Generic Routing Encapsulation	Nej
IPSec	Internet Protocol Security	Ja
SSL/TLS	Secure Sockets Layer/Tranport	Ja

Hash værdi

En hash værdi er et digitalt fingeraftryk af en vilkårlig datamængde og anvendes i flere sammenhænge til øget datasikkerhed. En hash værdi kaldes på engelsk for en *message digest* og dannes ved at sende data gennem en hash funktion. Hash funktionen er en algoritme som omfatter avanceret matematik og anvendes til at generere en unik hash værdi for et givet sæt af data.

I eksemplet i Figur 32 kan det ses at hash værdien har en konstant længde uanset størrelsen på input dataene. En hash værdi vises oftest som et hexadecimalt tal.

En hash funktion er en envejs funktion – det vil sige man kan generere hash værdien hvis man kender input-data, men der er ikke muligt at finde input-data hvis man kender hash værdien.



Figur 32 - Eksempel på generering af hash værdier. Bemærk ændring ved at ændre T'et fra stort til småt i Tommelise

En lille ændring af input dataene giver en stor ændring af hash værdien, for at gøre det svært at gætte input dataene. I Figur 32 er T'et i Tommelise ændret til småt i det sidste eksempel hvilket genererer en helt anden hash værdi. En given hash funktion vil altid generere den samme hash værdi med de samme input data.

Hash funktioner

Der findes adskillige hash funktioner hvor den største forskel er sikkerhed og størrelse af hash værdien.

Hash funktion	Fra	Hash værdi størrelse	Sikkerheds status
MD4	1990	128 bit	Alvorligt truet
MD5	1992	128 bit	Truet
SHA-0	1993	160 bit	Truet
SHA-1	1995	160 bit	Snart truet
SHA-2	2002	224, 256, 384 eller 512 bit	OK
SHA-3	2012	224, 256, 384 eller 512 bit	OK – stadig i udvikling

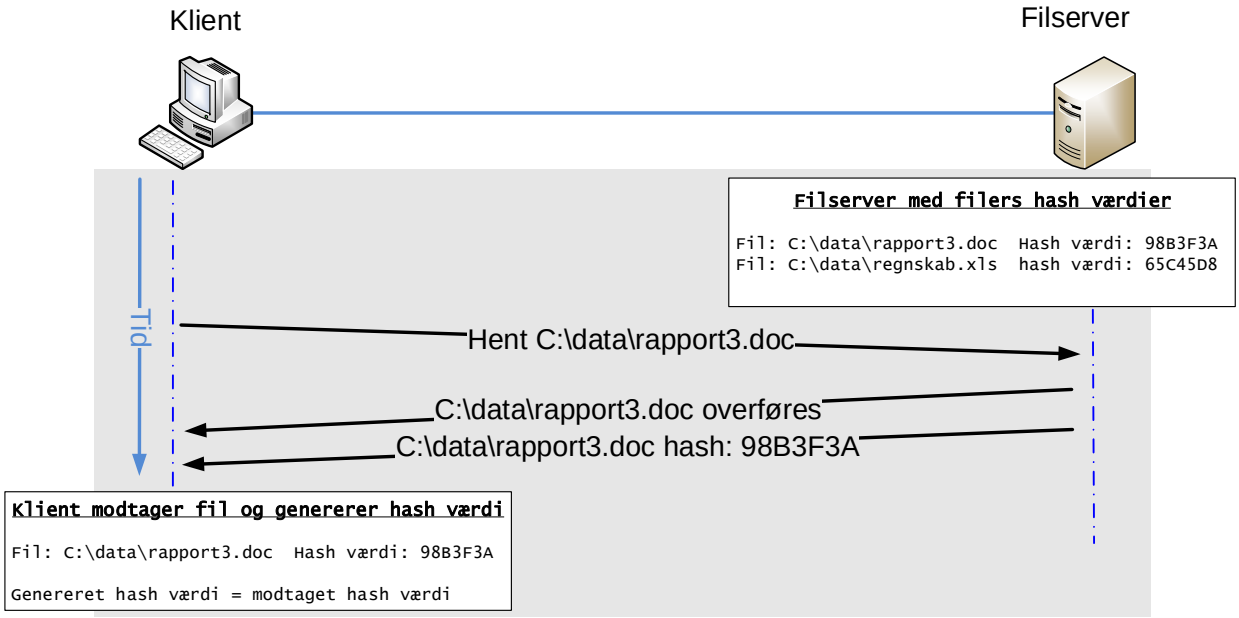
Figur 33 - Forskellige hash funktioner og deres sikkerheds status. Informationer fra NIST 2013

Anvendelse af hash værdier

Hash værdier anvendes i mange sammenhænge til at sikre at dataoverførsel er sket uden fejl og til at sikre at passwords ikke kan aflyttes.

Overførsel af filer

Ved overførsel af filer mellem to computere kan en hash anvendes til at sikre at den modtagne fil er en eksakt kopi af den afsendte. I eksemplet i Figur 34 henter klienten filen C:\data\rapport3.doc og får samtidig hash værdien som er udregnet af filserveren. Klienten genererer selv en hash værdi af den modtagne fil og sammenligner denne med den modtagne hash værdi. Er de ens er filoverførslen lykkedes uden fejl.



Figur 34 - Filoverførsel mellem filserver og klient lykkedes

Downloads af ISO filer til CD og DVD

Når man downloader ISO filer er det vigtigt at checke det er den rigtige version man har hentet og ikke en version som er ændret af en ondsindet person. I eksemplet i Figur 35 er det muligt at undersøge at den hentede fil er en skakt kopi af Microsofts egen udgivelse ved selv at finde hash værdien af ISO filen.

Windows 7 Home Premium (x64) - DVD (English)
File Name: en_windows_7_home_premium_x64_dvd_x15-65733.iso
Languages: English
SHA1: 336779ea6b65f63e11a609b4d021439c47ab315b

Windows 7 Professional (x64) - DVD (English)
File Name: en_windows_7_professional_x64_dvd_x15-65805.iso
Languages: English
SHA1: 50127304441a793ee51b3f501289f6599a559e9f

Windows 7 Ultimate (x64) - DVD (English)
File Name: en_windows_7_ultimate_x64_dvd_x15-65922.iso
Languages: English
SHA1: 326327cc2ff9f05379f5058c41be6bc5e004baa7

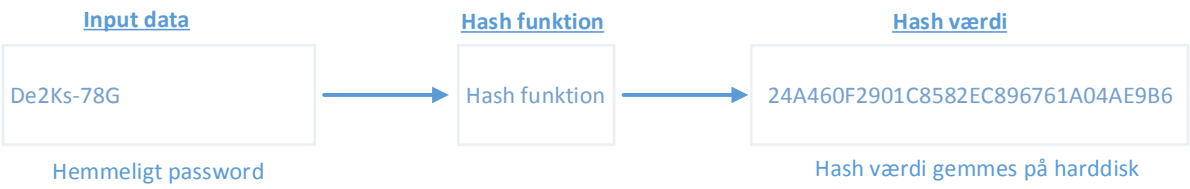
Figur 35 - SHA-1 hash værdier hentet fra Microsofts hjemmeside

Kontrol af passwords

Generelt er det en dårlig ide at servere gemmer bruger-passwords i klar tekst. Hvis harddisken bliver stjålet eller hackere får adgang til serveren er det muligt for crackeren at logge ind som andre og derved begå identitets tyveri.

I stedet for at gemme passwordet som klar tekst gemmes hash værdien af passwordet som vist i Figur 36. Det er kun muligt at logge ind på serveren hvis man kender input-data der genererer præcis den samme hash værdi som gemt på harddisken. Brugeren har bevist sin identitet hvis det indtastede password genererer den samme hash værdi som er gemt på harddisken.

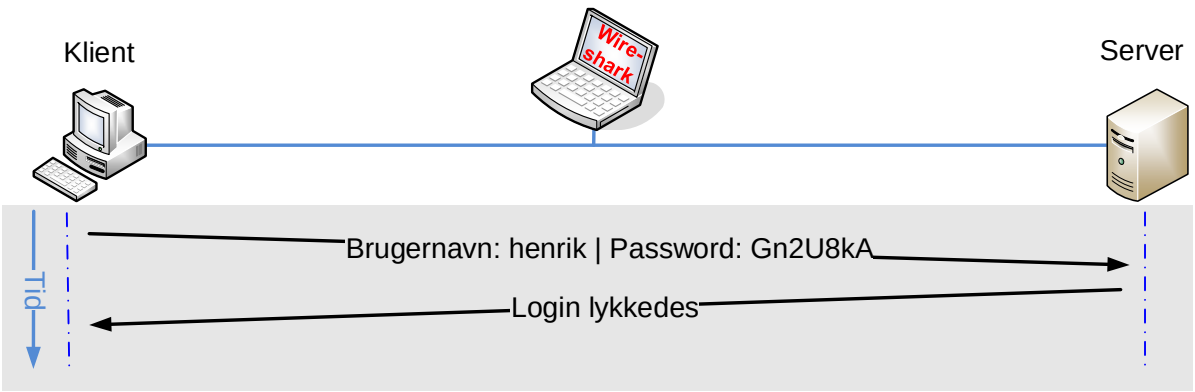
En Cracker kan derfor ikke bruge hash værdien til noget, da hash værdien ikke repræsenterer passwordet, men kun er et fingeraftryk heraf. Da hash værdien altid har samme størrelse kan hackeren ikke gætte på længden af det hemmelige password.



Figur 36 - Hash værdi fra password gemmes på harddisken

Overførsel af password via netværket

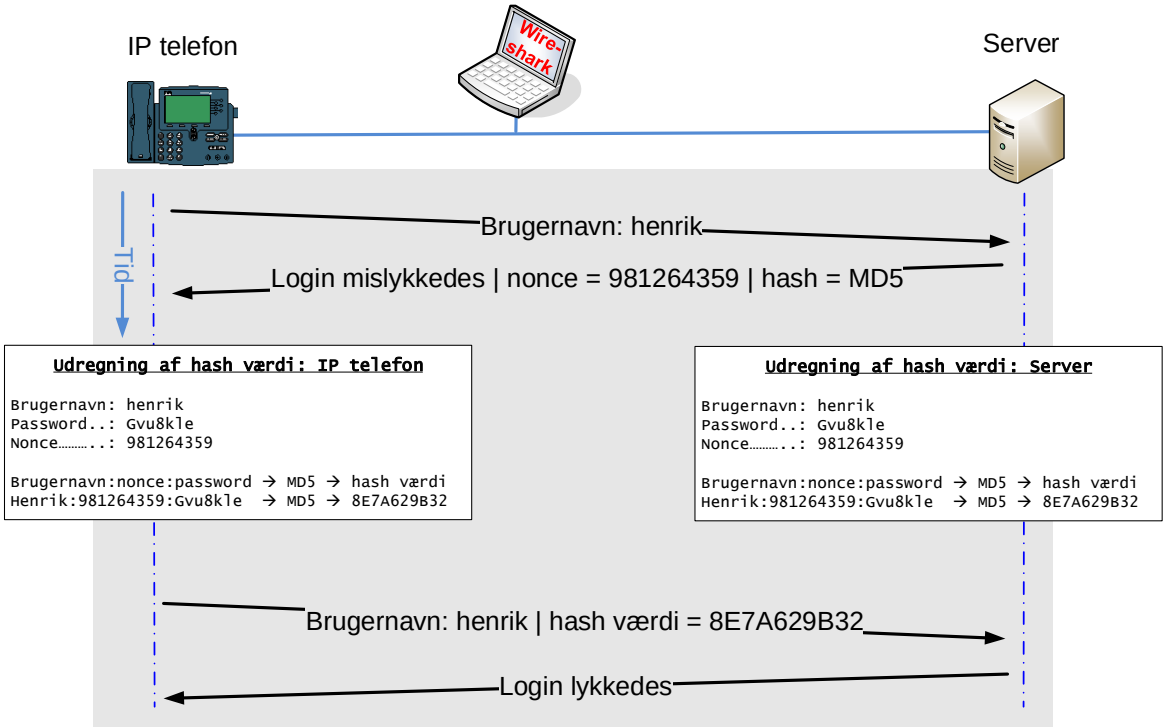
Hvis et password eller en hash værdi overføres via netværket uden kryptering er det muligt at aflytte kommunikationen og opsnappe brugernavn og password. I eksemplet i Figur 37 sender klienten en pakke til serveren som indeholder brugernavn og password i klar tekst, som opfanges af Wireshark.



Figur 37 - Klient logger ind med brugernavn og password i klartekst

Hash værdi med nonce

En nonce er et tilfældigt tal som serveren genererer til klienten. I eksemplet i Figur 38 prøver IP telefonen først at logge ind med brugernavn uden password. Serveren afviser adgang og svarer tilbage med en nonce som er et tilfældigt tal. Selvom det generelt er en dårlig ide at gemme passwords på servere, anvendes dette for eksempel på IP telefoni servere.



Figur 38 - Overførsel af password som hash værdi med nonce

I eksemplet i Figur 38 kender IP telefonen og serveren brugernavnet og passwordet. For at undgå at en eventuel cracker aflyttet kommunikationen genererer IP telefonen og serveren en hash værdi der er baseret på brugernavn, password og nonce. De kommer begge frem til samme hash værdi, da de bruger samme hash funktion med samme input data. Crackeren kan aflytte brugernavn, nonce og hash værdi, men kan har ikke adgang til det hemmelige password. Næste gang IP telefonen logger ind vil serveren generere en anden nonce.

Eksempel opfanget med Wireshark

I eksemplet i Figur 39 afvises telefonen af serveren – 401 Unauthorized – da den prøvede at logge ind ved kun at anvende brugernavnet. Serveren fortæller i samme pakke at den ønsker en MD5 hash værdi udregnet baseret på medsendte nonce.

```
⊞ Frame 161: 540 bytes on wire (4320 bits), 540 bytes captured (4320 b
⊞ Ethernet II, Src: Motorola_be:4c:84 (00:24:37:be:4c:84), Dst: LnSrit
⊞ Internet Protocol Version 4, Src: 87.48.131.54 (87.48.131.54), Dst:
⊞ User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
⊟ Session Initiation Protocol (401)
  ⊞ Status-Line: SIP/2.0 401 Unauthorized
  ⊟ Message Header
    ⊞ From: "5401 heth"<sip:henrikth@vk102113.hvoip.dk>;tag=95859cb8-ac
    ⊞ To: "5401 heth"<sip:henrikth@vk102113.hvoip.dk>;tag=5e13d931038de
      Call-ID: 68656e72696b-aabb-7065-01a7eab23b0-0-2eba@10.197.0.104
    ⊞ CSeq: 1 REGISTER
    ⊞ Via: SIP/2.0/UDP 10.197.0.104:5060;branch=z9hG4bK-33-c7e4-4abde8b
      Content-Length: 0
    ⊟ WWW-Authenticate: Digest nonce="3B75025A1DDC2D5100000000F79C7455"
        Authentication Scheme: Digest
        nonce="3B75025A1DDC2D5100000000F79C7455"
        realm="hvoip.ip.tdk.dk"
        algorithm=MD5
        qop="auth"
```

Figur 39 - Eksempel på opsamlet trafik med wireshark. hvor login af IP telefon afvises af server

IP telefonen prøver at logge ind igen efter den har udregnet hash værdien baseret på brugernavn, password og nonce. I Figur 40 er hash værdien af Wireshark angivet som responce.

```
⊞ Internet Protocol Version 4, Src: 10.197.0.104 (10.197.0.104), Dst: 87.48.
⊞ User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
⊟ Session Initiation Protocol (REGISTER)
  ⊞ Request-Line: REGISTER sip:vk102113.hvoip.dk SIP/2.0
  ⊟ Message Header
    ⊞ From: "5401 heth"<sip:henrikth@vk102113.hvoip.dk>;tag=95859cb8-ac50068-1
    ⊞ To: "5401 heth"<sip:henrikth@vk102113.hvoip.dk>
      Call-ID: 68656e72696b-aabb-7065-01a7eab23b0-0-2eba@10.197.0.104
    ⊞ CSeq: 2 REGISTER
    ⊞ Via: SIP/2.0/UDP 10.197.0.104:5060;branch=z9hG4bK-33-c826-5b7b8d92
      Max-Forwards: 70
      Supported: replaces
      User-Agent: LG-Ericsson IP8815 v1.2.25sbt_a SN/001A7EAB23B0
      Expires: 0
    ⊟ [truncated] Authorization: Digest username="henrikth@vk102113.hvoip.dk",
        Authentication Scheme: Digest
        username="henrikth@vk102113.hvoip.dk"
        realm="hvoip.ip.tdk.dk"
        nonce="3B75025A1DDC2D5100000000F79C7455"
        uri="sip:vk102113.hvoip.dk"
        response="2c881a030008dd77a29ada104d3992ec"
        algorithm=MD5
```

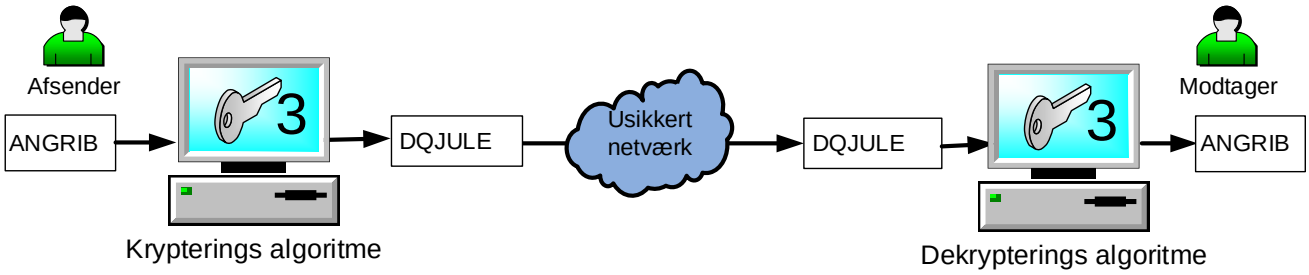
Figur 40 - IP telefonen logger ind med hash værdi (response) baseret på serverens nonce

Kryptering med nøgler

Kryptering af data forgår med hemmelige nøgler som er kendt af afsender og modtager. Nøglen er oftest er meget stort tal på flere hundrede cifre.

Cæsar krypterings algoritme

En af de ældste kryptering algoritmer blev anvendt af Julius Cæsar for mere end to tusind år siden.



Figur 41 – Kryptering med Cæsar algoritmen med nøglen "3".

Cæsar algoritmen er simpel og meget usikker og bygger på en såkaldt monoalfabetisk substitution hvor hvert enkelt bogstav udskiftes med et andet bogstav bestemt af nøglen.

I eksemplet i Figur 41 er klarteksten ”ANGRIB” krypteret med krypteringsalgoritmen Cæsar med nøglen ”3” som giver chifferteksten ”DQJULE” som transporteres gennem det usikre netværk til modtageren. Nøglen ”3” betyder at chiffertekst alfabetet er roteret 3 tegn mod venstre og chifferteksten er fundet ved at finde hver enkelt klartekst bogstav i klartekst alfabetet og tilføje det underliggende chiffertekst alfabet bogstav til chifferteksten som er den krypterede besked. A bliver for eksempel til D

```
Kryterings algoritme : Cæsar cipher
Krypterings nøgle    : 3
Klartekst alfabet    : ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
Chiffertekst alfabet : DEFGHIJKLMNOPQRSTUVWXYZ0123456789ABC
Klartekst            : ANGRIB
Chiffertekst         : DQJULE
```

Cæsar krypteringsalgoritmen er meget usikker da der kun er 27 forskellige nøgler og anvendes derfor ikke til noget praktisk formål. Moderne krypteringsalgoritmer anvender avanceret matematik og store nøgler.

Symmetriske nøgler

Krypteringsalgoritmer som anvender samme nøgle til kryptering og dekryptering kaldes for symmetriske nøgler og har det problem at afsender og modtager skal have adgang til samme hemmelige nøgle. Afsender og modtager skal derfor udveksle den hemmelige nøgle mellem hinanden for at sikre kommunikationen.

Udveksling af nøgler

Da afsender og modtager skal anvende samme nøgle er det nødvendigt med en metode til sikkert at udveksle nøgler uden at andre kan opsnappe og misbruge nøglen. Dette blev førhen gjort ved at en kurer personligt bragte nøglen mellem afsender og modtager. Dette er naturligvis urealistisk på Internettet at udveksling af nøgler foregår ved at sende en kurer.

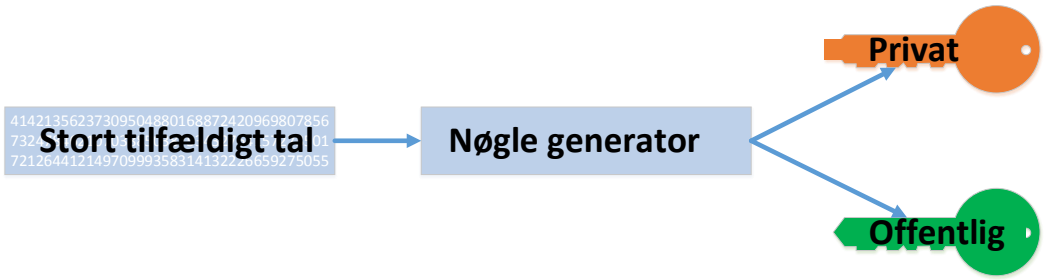
Asymmetriske nøgler

Problemet med nøgleudveksling mellem afsender og modtager når der anvendes symmetriske nøgler har ført til udviklingen af asymmetriske nøgler.

Asymmetriske nøgler er et nøglepar der består af en offentlig og en privat nøgle. Nøglerne er matematisk forbundet således at den ene nøgle kan anvendes til kryptering og den anden nøgle kan anvendes til dekryptering.

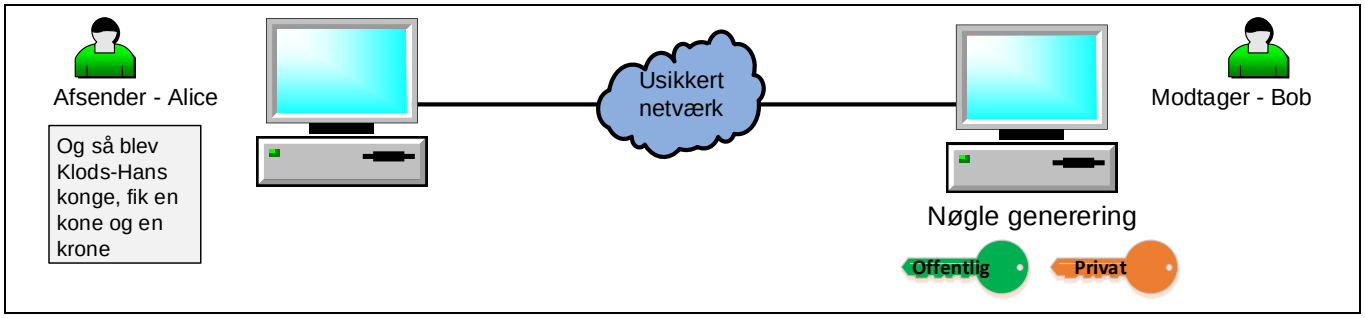
Offentlig nøgle kryptering

Ved offentlig nøgle kryptering genereres et nøglepar ud fra et stort tilfældigt tal. Den ene nøgle kaldes den private nøgle og er hemmelig. Den anden nøgle kaldes den offentlige nøgle og er ikke hemmelig.



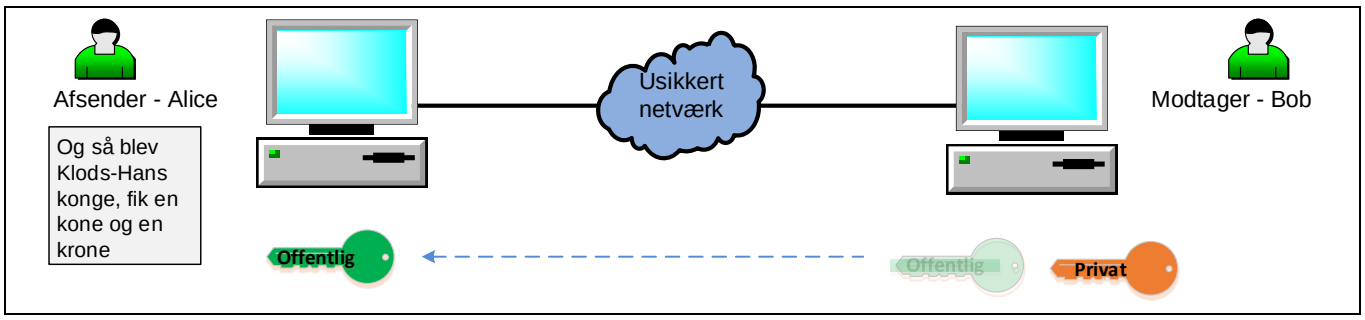
Figur 42 - Generering af asymmetrisk nøglepar

Ved anvendelse af offentlig nøgle kryptering genererer modtageren af den hemmelige besked et nøglepar. I eksemplet i Figur 3 genererer Bobs computer et nøglepar bestående af en privat og en offentlig nøgle.



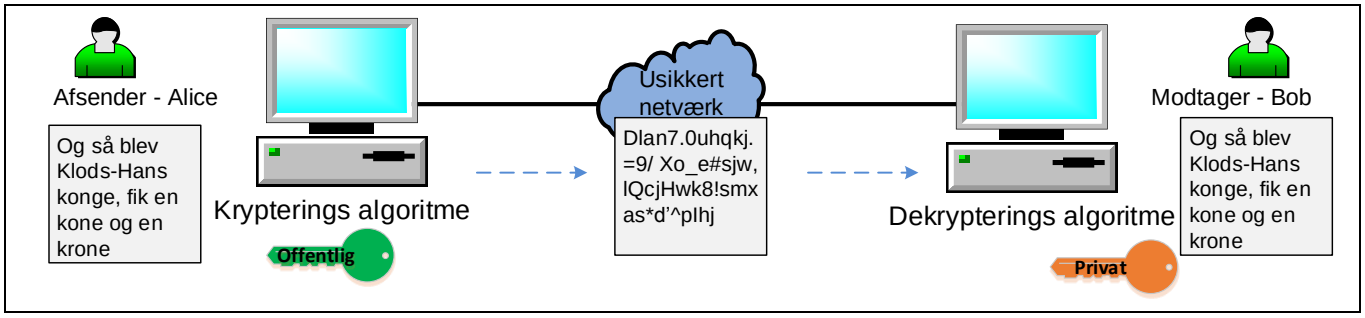
Figur 43 - Modtageren Bob genererer et nøglepar

Som vist i Figur 4 sender Bobs computer den offentlige nøgle til Alice gennem det usikre netværk. Den offentlige nøgle kan opsnappes af crackere, men det gør ikke noget da den offentlige nøgle kun kan anvendes til at kryptere og ikke til at dekryptere.



Figur 44 - Bob sender den offentlige nøgle til Alice

Når Alice har modtaget den offentlige nøgle krypterer hun den hemmelige tekst med Bobs offentlige nøgle og sender de krypterede data gennem det usikre netværk til Bob. Bob anvender den private nøgle til at dekryptere den hemmelige besked. Se Figur 5.



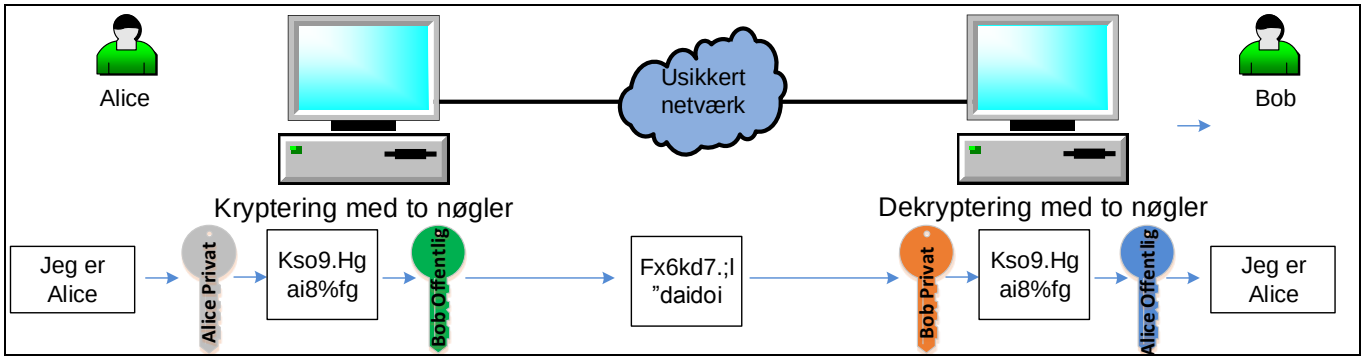
Figur 45 - Alice krypterer den hemmelige besked med den offentlige nøgle og Bob dekrypterer med den private nøgle

Anvendelse af asymmetriske nøgler

Kryptering og dekryptering af data ved anvendelse af asymmetriske nøgler kræver flere ressourcer og er langsommere end anvendelsen af symmetrisk kryptering. Derfor anvender flere krypteringsalgoritmer den offentlige nøgle til at kryptere den hemmelige symmetriske nøgle der senere skal anvendes til symmetrisk kryptering af store mængder data.

Identitet

Asymmetriske nøgler har den egenskab at den ene nøgle kan bruges til kryptering og den anden til dekryptering. Det betyder at også den private nøgle kan anvendes til at kryptere en besked som den offentlige nøgle kan dekryptere. I eksemplet i Figur 6 Kender Bob Alices offentlige nøgle og Alice beviser hun er indehaver af Alices private nøgle da hun krypterer sin identitet med hendes private nøgle.

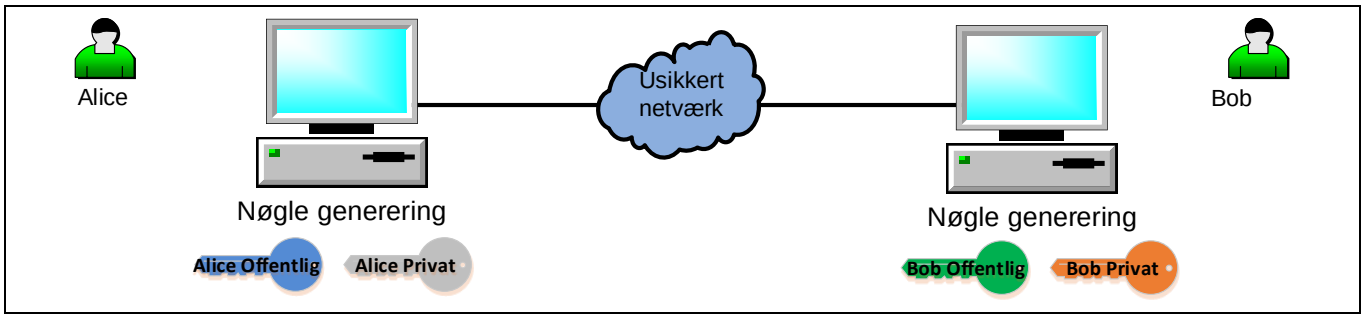


Figur 46 - Alice beviser sin identitet da kun hun har Alices private nøgle

Diffie-Hellman nøgle udveksling

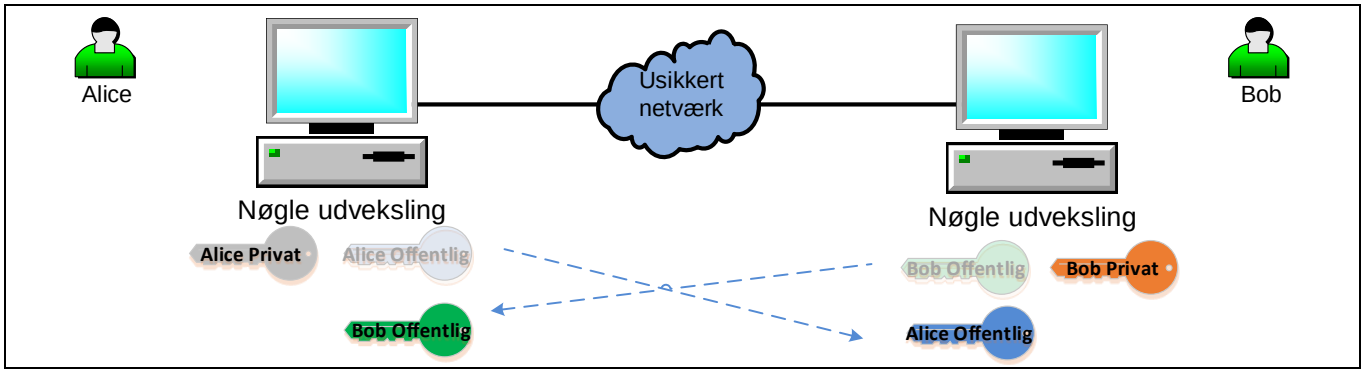
Diffie-Hellman eller DH nøgle udveksling er en anvendt algoritme til at generere symmetriske nøgler ved anvendelse af asymmetriske nøgler og blev offentliggjort i 1976 af Whitfield Diffie og Martin Hellman.

Det grundlæggende princip i DH nøgle udvesling er at begge parter genererer et asymmetrisk nøglepar. Se Figur 1.



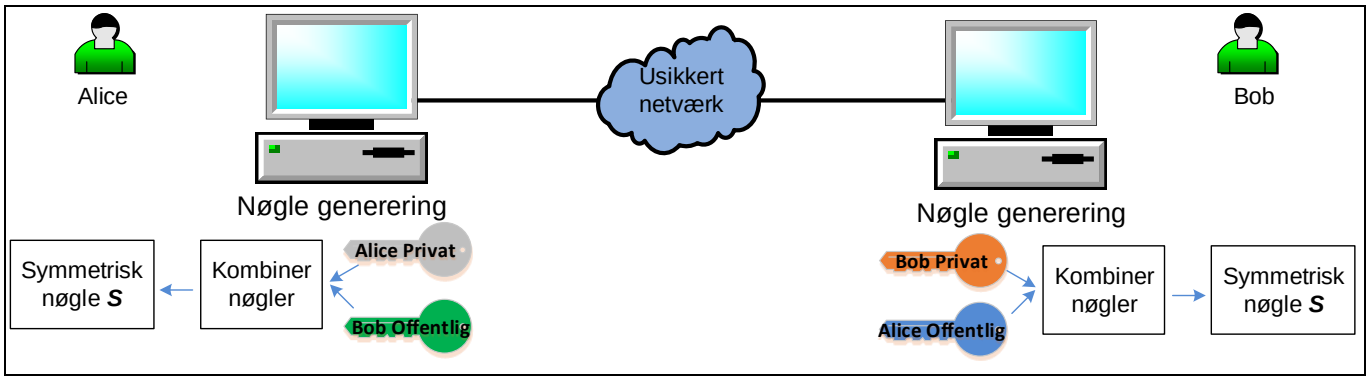
Figur 47 - Både Alice og Bob genererer et nøglesæt bestående af en offentlig og en privat nøgle

Herefter udveksler Alice og Bob deres offentlige nøgler med hinanden. Se Figur 2.



Figur 48 - Alice og bob udveksler deres offentlige nøgler

Alice kombinerer matematisk hendes private nøgle med Bobs offentlige nøgle og når frem til en symmetrisk nøgle kaldet ***S***. Bob kombinerer på samme matematiske måde som Alice hans private nøgle med Alices offentlige og kommer frem til den samme nøgle ***S*** som Alice. Se figur 3.



Figur 49 - Alice og Bob kombinerer deres nøgler og når på "magisk" vis frem til samme symmetriske nøgle

Alice og Bob har herefter samme symmetriske nøgle som de kan anvende til at kryptere deres data over det usikre netværk.

Hele ovenstående algoritme foregår automatisk imellem Alices og Bobs computere.

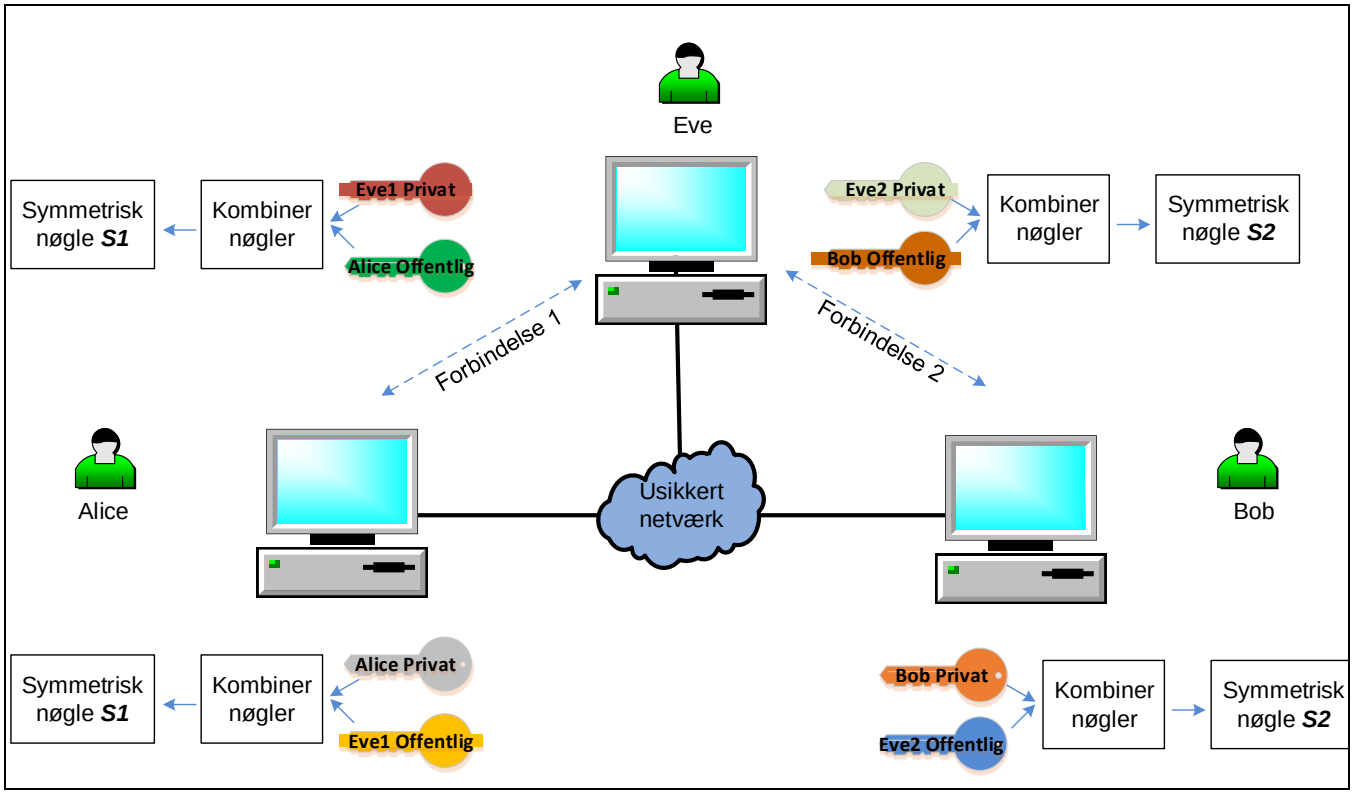
Anvendelse

Diffie-Hellman nøgle udvekslingen kan anvendes af blandt andet IPsec

Ulemper

Diffie-Hellman nøgle udveksling indeholder ingen brugervalidering (Authentication) og er sårbar overfor man-in-the-middle angreb. Hvis Alices computer tror at Bobs computer har Eves IP adresse, vil Alices computer udveksle nøgler med Eves computer og finde den symmetriske nøgle ***S1*** og tro alt er i orden. Se Figur 4 forbindelse 1. Ligeledes hvis Bobs computer tror at Alices computers IP adresse er Eves IP adresse, vil Bobs computer udveksle nøgler med Eves computer og finde den symmetriske nøgle ***S2***. Se, forbindelse 2.

Data mellem Alice og Bob dekrypteres af Eves computer før det videresendes og Eve kan derfor læse og ændre i klarteksten.



Figur 50 - Eve udfører man-in-the-middle angreb