

Velkommen til

Netvirkssikkerhed i firmanetvirk

Maj 2009

Henrik Lund Kramshj
hlk@security6.net

Kontaktinformation og profil



- Henrik Lund Kramshj, freelance IT-sikkerhedskonsulent
- Email: hlk@security6.net Mobil: +45 2026 6000
- Cand.scient fra Datalogisk Institut ved Kbenhavns Universitet, DIKU
- CISSP og CEH certificeret
- Selvstndig sikkerhedskonsulent siden januar 2003

Vi skal have glde af hinanden i flgende kursusforl

- 2 aftener med workshop

I skal udover at lre en masse om protokoller og netvrk

Forhbentlig lrer i nogle gode vaner!

Jeres arbejde med netvrk kanlettes betydeligt - hvis I starter rigtigt!



Free graphics by Lumen Design Studio

Dette materiale består af flere dele:

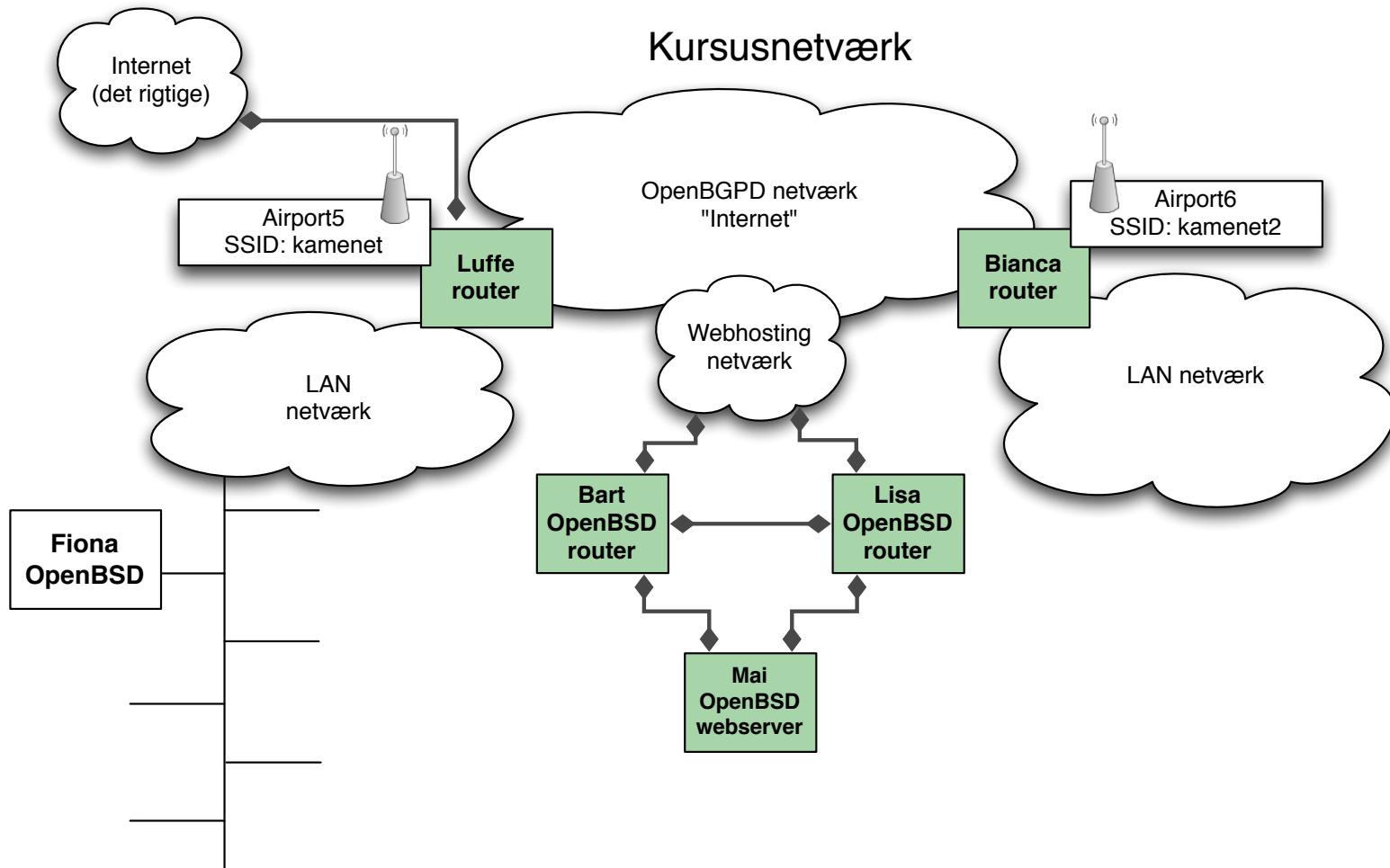
- Kursusmaterialet - præsentationen til undervisning - dette st
- velseshfte med velser

Hertil kommer diverse ressourcer fra internet

Boot CD'er baseret på Linux

Bemærk: kursusmaterialet er ikke en substitut for andet materiale, der er udeladt mange detaljer som forklares undervejs, eller kan ses op på internet

Forml: netvrkssikkerhed for TCP/IP netvrk



TCP/IP-baserede netvrk - internet er overalt

At introducere god sikkerhed i TCP/IP netvirk for firmaer

Kendskab til almindeligt brugte protokoller

- VLAN, WLAN, DNS, RADIUS, LDAP m.v.

Kendskab til almindelige vrktjer i disse miljøer

- ping, traceroute, iperf, Smokeping, Nagios, Apache Benchmark m.v.

Gennemgang af netværksdesign ved hjælp af almindeligt brugte setups

- en skalamodel af internet

NB: ja, jeg bruger en masse Unix og webapplikationer p Unix

**men de fleste af programmerne KAN installeres p Windows,
eller der kan findes alternativer der benytter samme protokoller!**

Forudstninger

Dette er en workshop og fuldt udbytte krver at deltagerne udfører praktiske velser

Kurset anvender OpenBSD til velser, men Unix kendskab er ikke nødvendigt

De fleste velser kan udføres fra en Windows PC

velserne foregår via

- Login til Unix maskinen
- Direkte fra jeres systemer Windows eller Linux boot CD
- Via administrationsprogrammer, ofte webinterfaces

Forudsætninger penetrationstest



Til penetrationstest og det meste Internet-sikkerhedsarbejde er der flgende forudsætninger

- Netværkserfaring
- TCP/IP principper - ofte i detaljer
- Programmeringserfaring er en fordel
- Unix kendskab er ofte en **ndvendighed**
 - fordi de nyeste værktøjer er skrevet til Unix i form af Linux og BSD

Der er opbygget et kursusnetvirk med flgende primre systemer:

- Unix server Fiona med HTTP server og vrktjer
- Unix boot CD'er eller VMware images - jeres systemer

P Unix serveren tillades login diverse kursusbrugere - kursus1, kursus2, kursus3, ...
kodeordet er **kursus**

Login: **kursus1**

Password: **kursus**

Det er en fordel at benytte hver sin bruger, s man kan gemme scripts

P de resterende systemer kan benyttes brugeren **kursus**

Login: **kursus**

Password: **kursus42** el **kursus**

BackTrack boot CD'er



Brug CD'en eller VMware player til de grafiske vrktjer som Wireshark

BackTrack <http://www.remote-exploit.org/backtrack.html>

BackTrack er baseret p Linux og m kopieres frit :-)

Til begyndere indenfor Linux anbefales Ubuntu eller Kubuntu til arbejdsstationer

Stop - tid til check



Er alle kommet

Har alle en PC med

Har alle et kabel eller trdlst netkort som virker

Der findes et trdlst netvrk ved navn **kamenet**

Mangler der strmkabler

Mangler noget af ovenstende, st nogen igang med at finde det :-)

Da Unix indgr er her et lille *cheat sheet* til Unix

- DOS/Windows kommando - tilsvarende Unix, og forklaring
- dir - ls - str for list files, viser filnavne
- del - rm - str for remove, sletter filer
- cd - cd - change directory, skifter katalog
- type - cat - concatenate, viser indholdet af tekstfiler
- more - less - viser tekstfiler en side af gangen
- attrib - chmod - change mode, ændrer rettighederne på filer

Prv bare:

- **ls** list, eller long listing med **ls -l**
- **cat /etc/hosts** viser hosts filen
- **chmod +x head.sh** - st execute bit på en fil så den kan udføres som et program med kommandoen
./head.sh

Straffelovens paragraf 263 Stk. 2. Med bde eller fngsel indtil 6 mneder straffes den, som uberettiget skaffer sig adgang til en andens oplysninger eller programmer, der er bestemt til at bruges i et anlg til elektronisk databehandling.

Hacking kan betyde:

- At man skal betale erstatning til personer eller virksomheder
- At man fr konfiskeret sit udstyr af politiet
- At man, hvis man er over 15 r og bliver dmt for hacking, kan få en bde - eller fngselsstraf i alvorlige tilfde
- At man, hvis man er over 15 r og bliver dmt for hacking, får en plettet straffeattest. Det kan give problemer, hvis man skal finde et job eller hvis man skal rejse til visse lande, fx USA og Australien
- Frit efter: <http://www.stophacking.dk> lavet af Det Kriminalprventive Rd
- Frygten for terror har forstrket ovenstende - så lad vre!

Agenda - dag 1 Basale begreber og Ethernet



Opstart - hvad er IP og TCP/IP repetition, TCP, UDP, Subnets og CIDR

Basale vrktjer traceroute, ping, dig, host

Wireshark sniffer

SSL Secure Sockets Layer

VLAN 802.1q

Mlinger iperf, apache benchmark (ab)

Tuning og perfomancemlinger

Plus diverse webinterfaces og administrationsvrktjer

Agenda - dag 2 Avancerede netvrksteknologier og 802.11



Management, SNMP, RRDTool og Smokeping

Overvægning og diagnosticering Nagios, syslog m.v.

Trælse netvrk og sikkerhed Wi-Fi Protected Access (WPA)

Sikkerhedsvrktjer til trælse netvrk aircrack-ng suites af vrktjer

Directory services RADIUS, LDAP m.v.

Avancerede teknologier som 802.1x portbaseret autentifikation

VoIP - kort introduktion

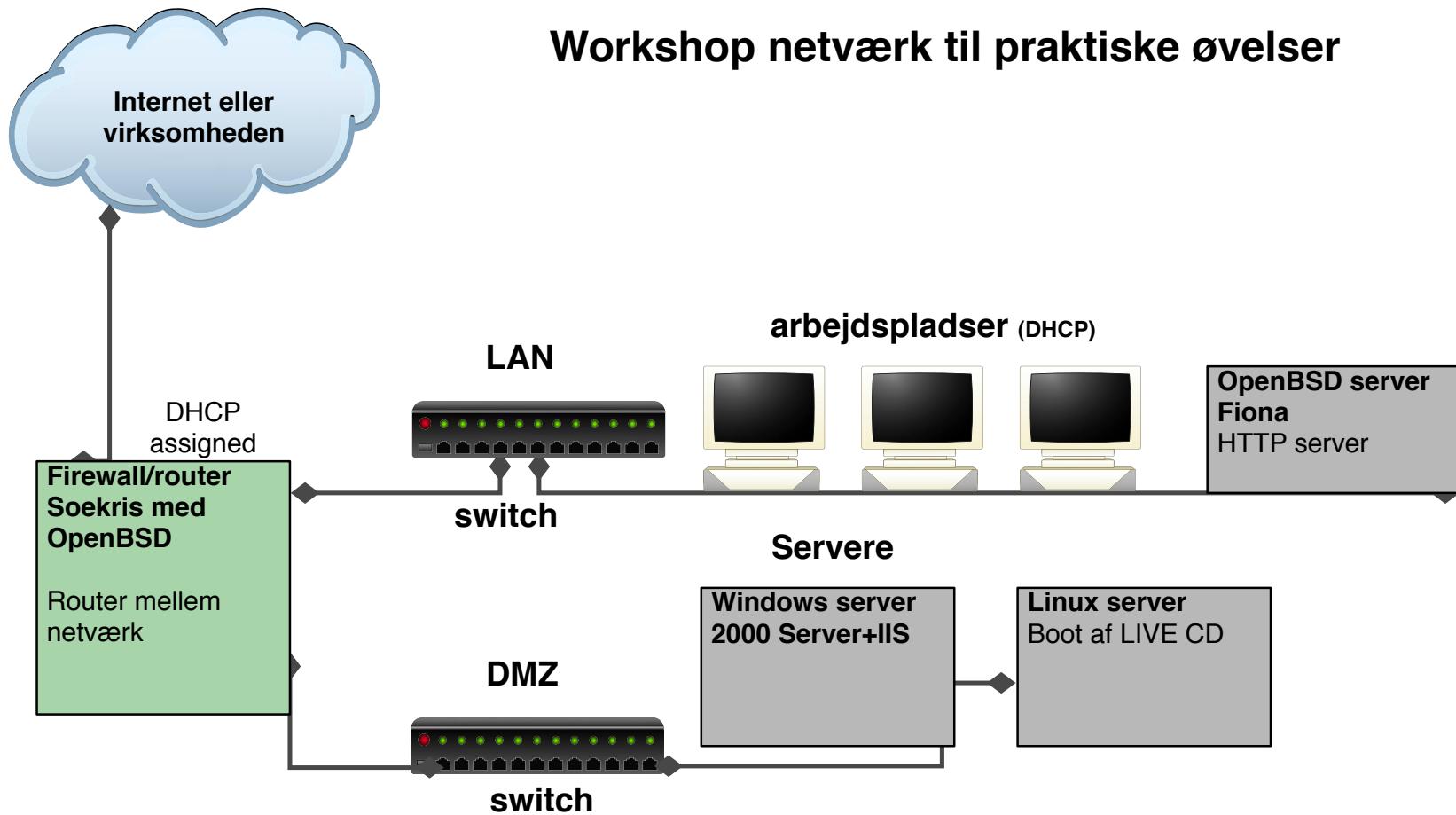
Firewalls, VPN protokoller og IPSec - kort introduktion

Infrastrukturer i praksis og netvrksdesign

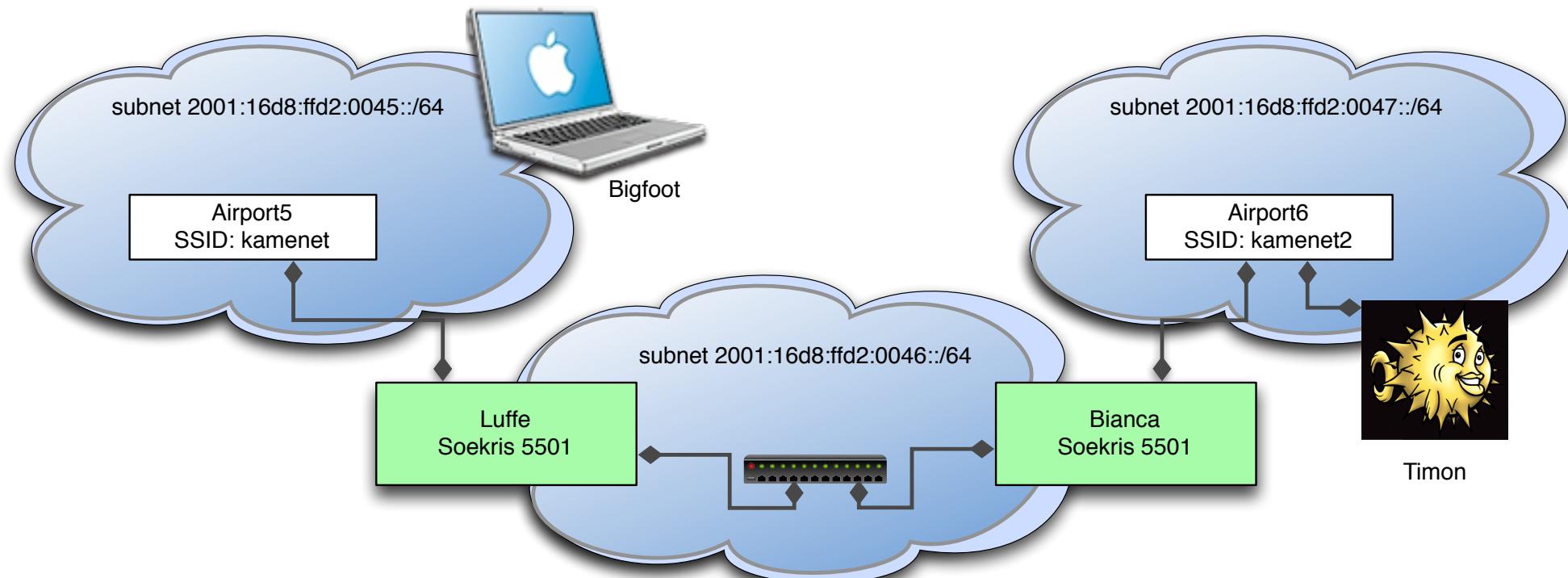
Afslutning og opsummering p kursus

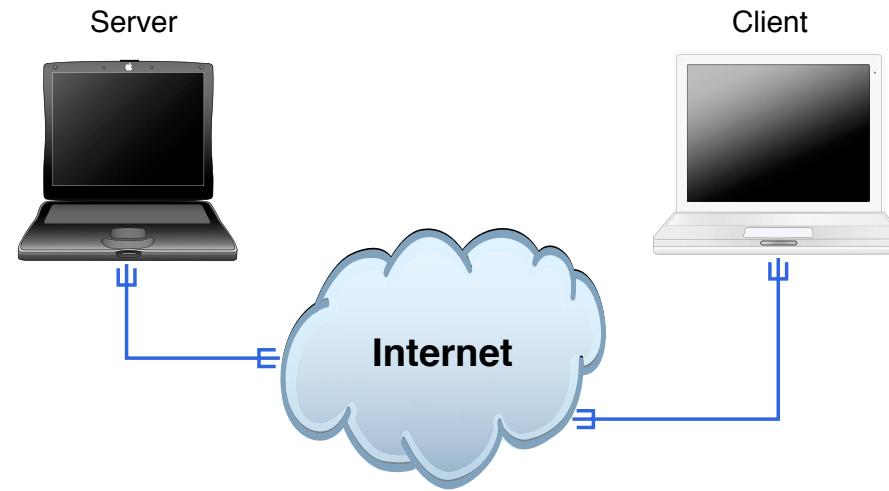
Dag 1 Basale begreber og Ethernet

Workshop netværk til praktiske øvelser



Netvrk til routning





Klienter og servere

Rdder i akademiske miljer

Protokoller der er op til 20 år gamle

Meget lidt kryptering, mest på http til brug ved e-handel

Kurset omhandler udelukkende netværk baseret på IP protokollerne

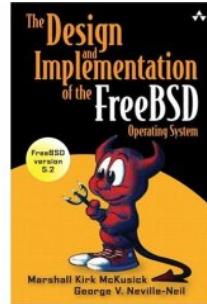
Kommunikation mellem mennesker!

Baseret på TCP/IP

- best effort
- packet switching (IPv6 kalder det packets, ikke datagram)
- forbindelsesorienteret, *connection-oriented*
- forbindelsesløs, *connection-less*

RFC-1958:

A good analogy for the development of the Internet is that of constantly renewing the individual streets and buildings of a city, rather than razing the city and rebuilding it. The architectural principles therefore aim to provide a framework for creating cooperation and standards, as a small "spanning set" of rules that generates a large, varied and evolving space of technology.



P Berkeley Universitetet blev der udviklet en del p Unix og det har givet anledning til en hel gren kaldet BSD Unix, BSD str for Berkeley Software Distribution

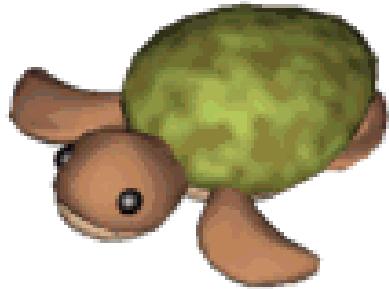
BSD Unix har blandt andet resulteret i virtual memory management og en masse TCP/IP relaterede applikationer

Specielt har BSD TCP/IP kernefunktionalitet vret genbrugt mange steder

Tilsvarende genbruges KAME IPv6 implementationen mange steder

<http://en.wikipedia.org/wiki/BSD>

KAME - en IPv6 reference implementation



<http://www.kame.net>

- Er idag at betragte som en reference implementation
 - i stil med BSD fra Berkeley var det
- KAME har vret p forkant med implementation af draft dokumenter
- KAME er inkluderet i OpenBSD, NetBSD, FreeBSD og BSD/OS - har vret det siden version 2.7, 1.5, 4.0 og 4.2
- Projektet er afsluttet, men nye projekter fortstter i WIDE regi <http://www.wide.ad.jp/>
- Der er udkommet to bger som i detaljer gennemgr IPv6 protokollerne i KAME

80'erne IP/TCP starten af 80'erne

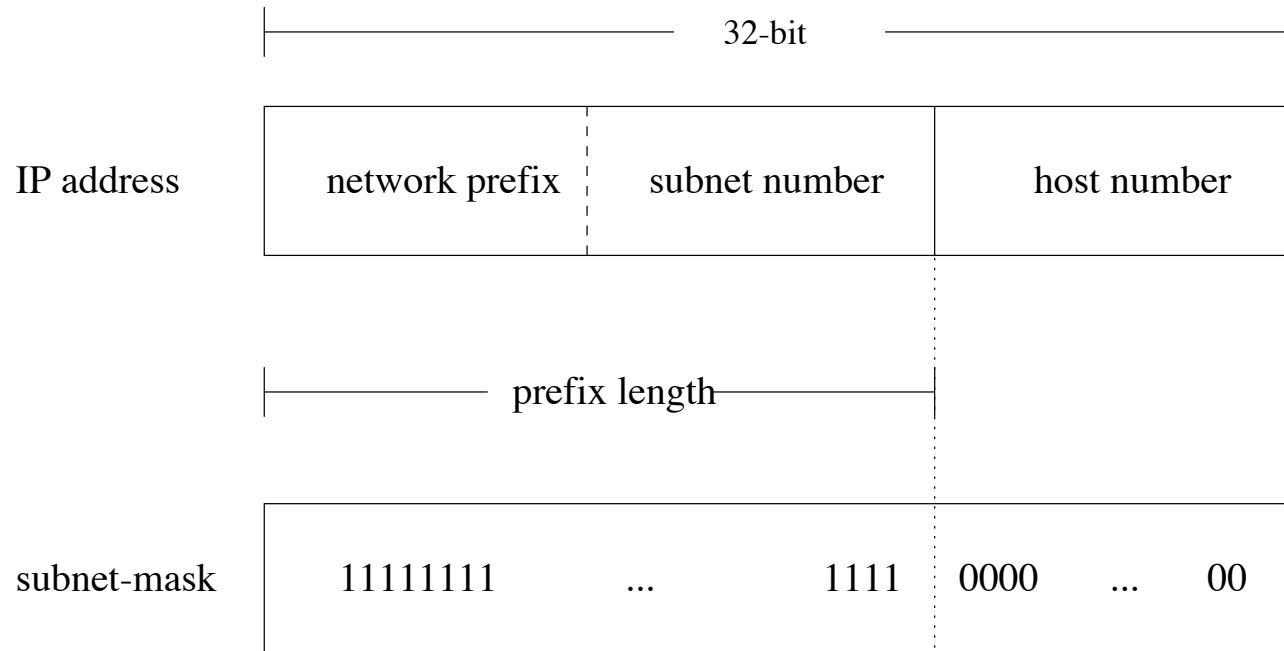
90'erne IP version 6 udarbejdes

- IPv6 ikke brugt i Europa og US
- IPv6 er ekstremt vigtigt i Asien
- historisk f adresser tildelt til 3.verdenslande
- Strre Universiteter i USA har ofte strre allokering end Kina!

1991 WWW "opfindes" af Tim Berners-Lee hos CERN

E-mail var hovedparten af traffik - siden overtog web/http frstepladsen

Filles adresserum



Hvad kendetegner internet idag

Der er et filles adresserum baseret p 32-bit adresser

En IP-adresse kunne vre 10.0.0.1

IPv4 addresser og skrivemde



```
hlk@bigfoot:hlk$ ipconvert.pl 127.0.0.1
Adressen er: 127.0.0.1
Adressen er: 2130706433
hlk@bigfoot:hlk$ ping 2130706433
PING 2130706433 (127.0.0.1): 56 data bytes
64 bytes from 127.0.0.1: icmp_seq=0 ttl=64 time=0.135 ms
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.144 ms
```

IP-adresser skrives typisk som decimaltal adskilt af punktum

Kaldes **dot notation**: 10.1.2.3

Kan ogs skrive som oktal eller heksadecimale tal

IP-adresser som bits

IP-adresse: 127.0.0.1

Heltal: 2130706433

Binary: 11111110000000000000000000000001

IP-adresser kan også konverteres til bits

Computeren regner binært, vi bruger dot-notationen

Tidligere benyttede man klasseinddelingen af IP-adresser: A, B, C, D og E

Desværre var denne opdeling uflexibel:

- A-klasse kunne potentielt indeholde 16 millioner hosts
- B-klasse kunne potentielt indeholder omkring 65.000 hosts
- C-klasse kunne indeholde omkring 250 hosts

Derfor bad de fleste om adresser i B-klasser - så de var ved at blive træt!

D-klasse benyttes til multicast

E-klasse er blot reserveret

Se evt. http://en.wikipedia.org/wiki/Classful_network

CIDR Classless Inter-Domain Routing



Classfull routing		Classless routing (CIDR)	
4 Class C networks	Inherent subnet mask	Supernet	Subnet mask
192.0.08.0	255.255.255.0	192.0.08.0	255.255.252.0 (252d=11111100b)
192.0.09.0	255.255.255.0		
192.0.10.0	255.255.255.0		
192.0.11.0	255.255.255.0		
		Base network/prefix 192.0.8.0/	

Subnetmasker var oprindeligt indforstet

Dernst var det noget man brugte til at opdele sit A, B eller C net med

Ved at tildele flere C-klasser kunne man spare de resterende B-klasser - men det betød en routing table explosion

Idag er subnetmaske en sammenhngende række 1-bit der angiver strrelse på nettet

10.0.0.0/24 betyder netvirket 10.0.0.0 med subnetmaske 255.255.255.0

Nogle steder kaldes det tillige supernet, supernetting

Subnet calculator, CIDR calculator

Subnet Calculator

Network Class A <input type="radio"/> B <input type="radio"/> C <input checked="" type="radio"/>	First Octet Range 192 - 223
IP Address 192 . 168 . 0 . 1	Hex IP Address C0.A8.00.01
Subnet Mask 255.255.255.0	Wildcard Mask 0.0.0.255
Subnet Bits 0	Mask Bits 24
Maximum Subnets 1	Hosts per Subnet 254
Host Address Range 192.168.0.1 - 192.168.0.254	
Subnet ID 192.168.0.0	Broadcast Address 192.168.0.255
Subnet Bitmap 110nnnnn.nnnnnnnn.nnnnnnnn.hhhhhh	

Der findes et vld af programmer som kan hjlpe med at udregne subnetmasker til IPv4
Screenshot fra <http://www.subnet-calculator.com/>

Der findes et antal adresserum som alle m benytte frit:

- 10.0.0.0 - 10.255.255.255 (10/8 prefix)
- 172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
- 192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

Address Allocation for Private Internets RFC-1918 adresserne!

NB: man m ikke sende pakker ud p internet med disse som afsender, giver ikke mening

IPv4 addresser opsummering



- Altid 32-bit adresser
- Skrives typisk med 4 decimaltal dot notation 10.1.2.3
- Netværk angives med CIDR Classless Inter-Domain Routing RFC-1519
- CIDR notation 10.0.0.0/8 - fremfor 10.0.0.0 med subnet maske 255.0.0.0
- Specielle adresser
 - 127.0.0.1 localhost/loopback
 - 0.0.0.0 default route
- RFC-1918 angiver private adresser som alle kan bruge

IPv6 addresser og skrivemde



subnet prefix	interface identifier
---------------	----------------------

2001:16d8:ff00:012f:0000:0000:0000:0002
2001:16d8:ff00:12f::2

- 128-bit adresser, subnet prefix nsten altid 64-bit
- skrives i grupper af 4 hexcifre ad gangen adskilt af kolon :
- foranstillede 0 i en gruppe kan udelades, en rkke 0 kan erstattes med ::
- dvs 0:0:0:0:0:0:0 er det samme som
0000:0000:0000:0000:0000:0000:0000:0000
- Dvs min webservers IPv6 adresse kan skrives som: 2001:16d8:ff00:12f::2
- Specielle adresser: ::1 localhost/loopback og :: default route
- Ls mere i RFC-3513

Stop - netvrket idag



Bemrk hvilket netvrk vi bruger idag

Primre server fiona har IP-adressen 10.0.45.36

Primre router luffe har IP-adressen 10.0.45.2 (og flere andre)

Sekundre router idag er Bianca som har IP-adressen 10.0.46.2 (og flere andre)

Hvis du kender til IP i forvejen s udforsk gerne p egen hnd netvrket

Det er tilladt at logge ind p alle systemer, undtagen Henrik's laptop bigfoot :-)

Det er forbudt at ndre IP-konfiguration og passwords

Nu burde I kunne forbinde jer til netvrket fysisk, check med ping 10.0.45.2

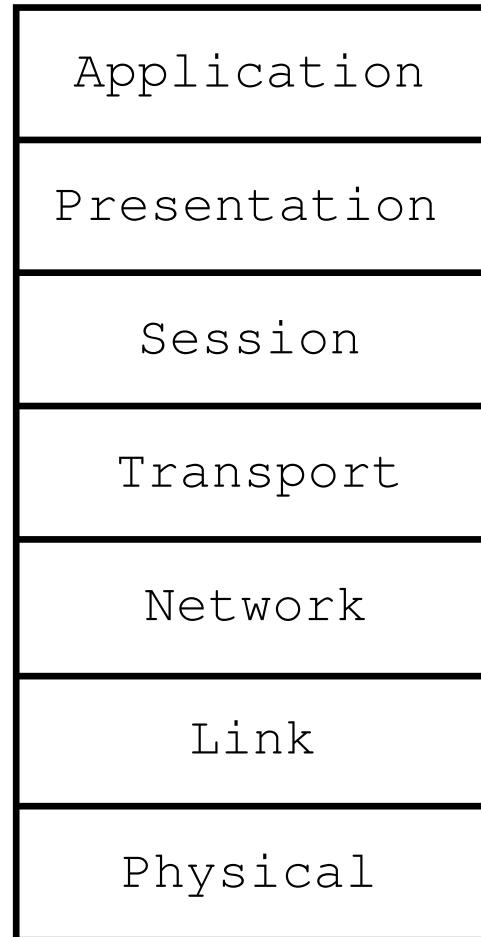
Det er nok at en PC i hver gruppe er p kursusnetvrket

Pause for dem hvor det virker, mens vi ordner resten

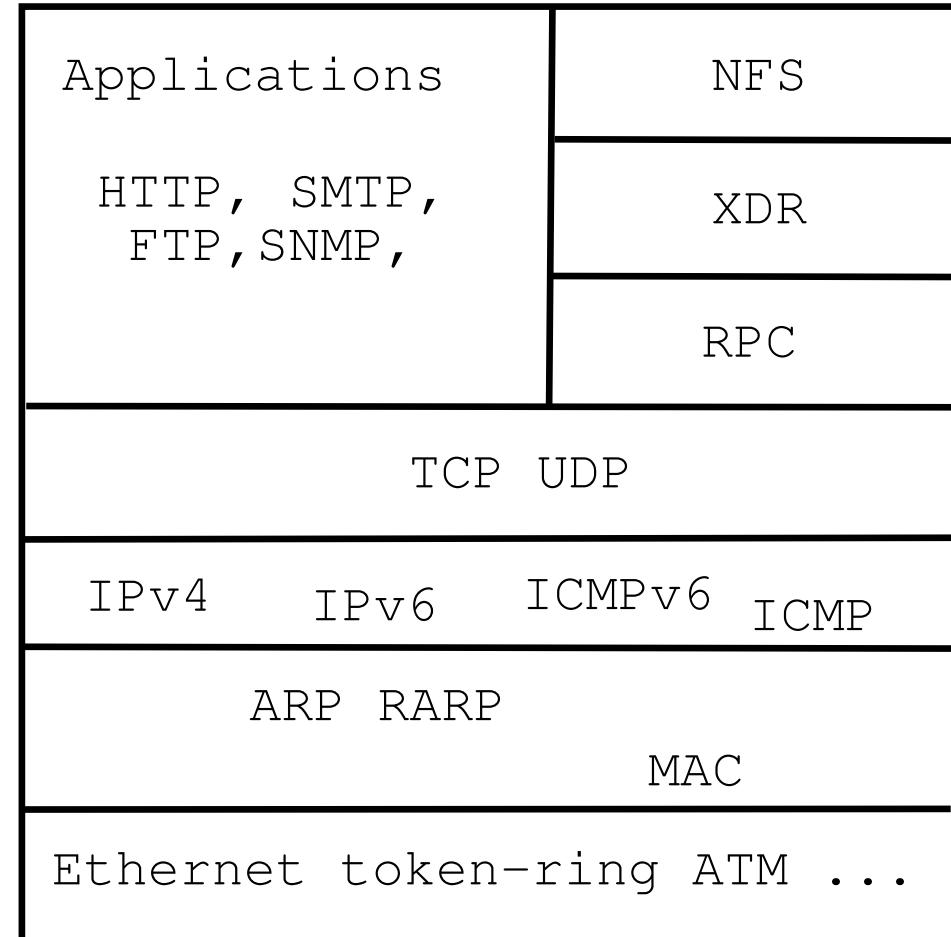
OSI og Internet modellerne



OSI Reference Model



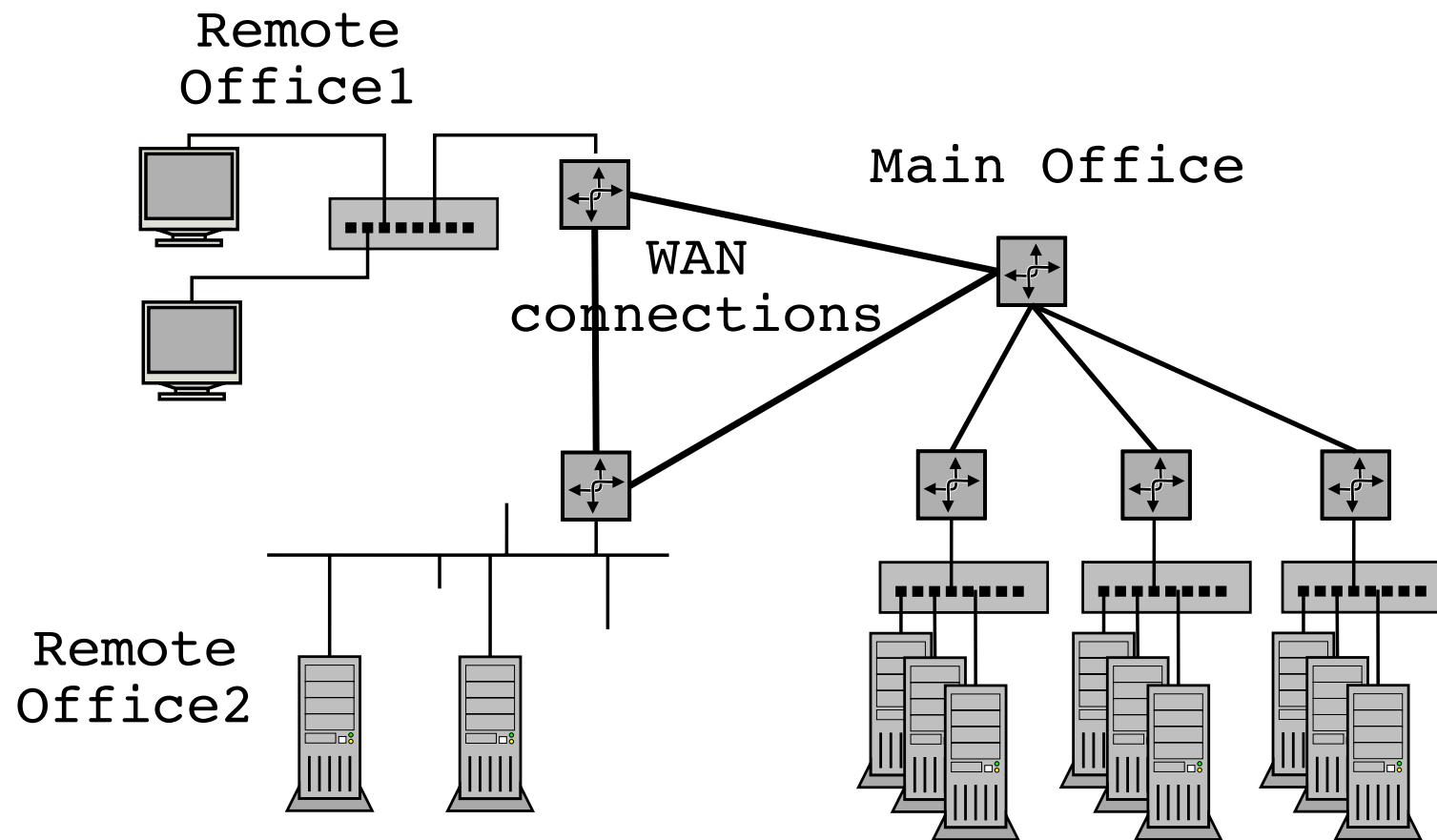
Internet protocol suite





Et typisk 802.11 Access-Point (AP) der har Wireless og Ethernet stik/switch

Første dag bruger vi blot trdlse netvirk, p dag 2 gennemgr vi 802.11



Fysisk er der en begrnsing for hvor lange ledningerne m vre

Ethernet er broadcast teknologi, hvor data sendes ud på et delt medie - teren

Broadcast giver en grænse for udbredningen vs hastighed

Ved hjælp af en bro kan man forbinde to netværkssegmenter på layer-2

Broen kopierer data mellem de to segmenter

Virker som en forstørre på signalet, men mere intelligent

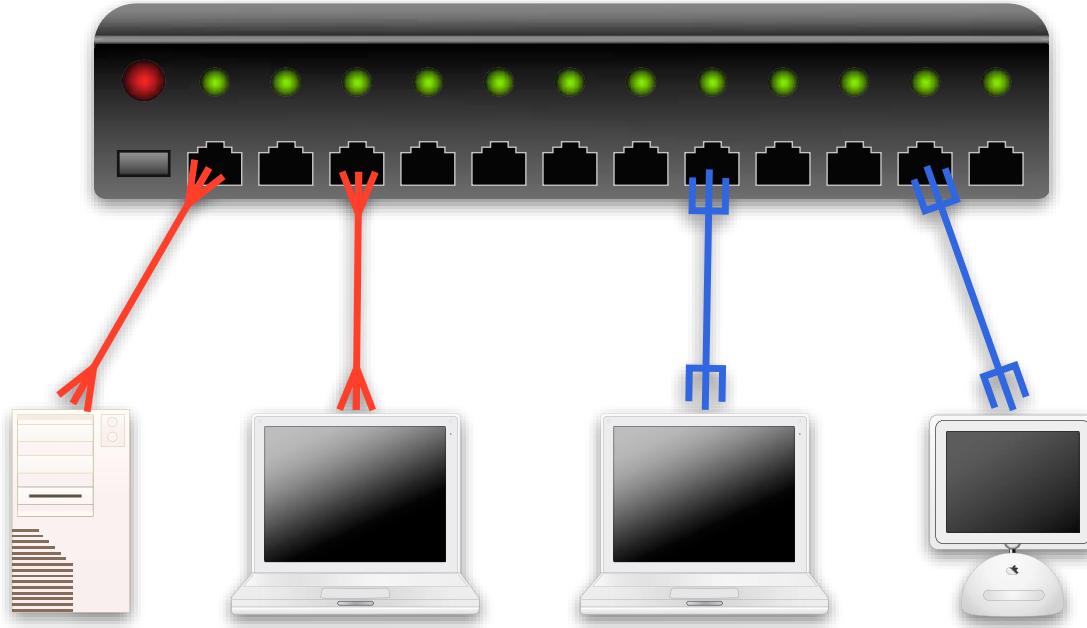
Den intelligente bro kender MAC adresserne på hver side

Broen kopierer kun hvis afsender og modtager er på hver sin side

Kilde: For mere information se efter Aloha-net

<http://en.wikipedia.org/wiki/ALOHAnet>

En switch

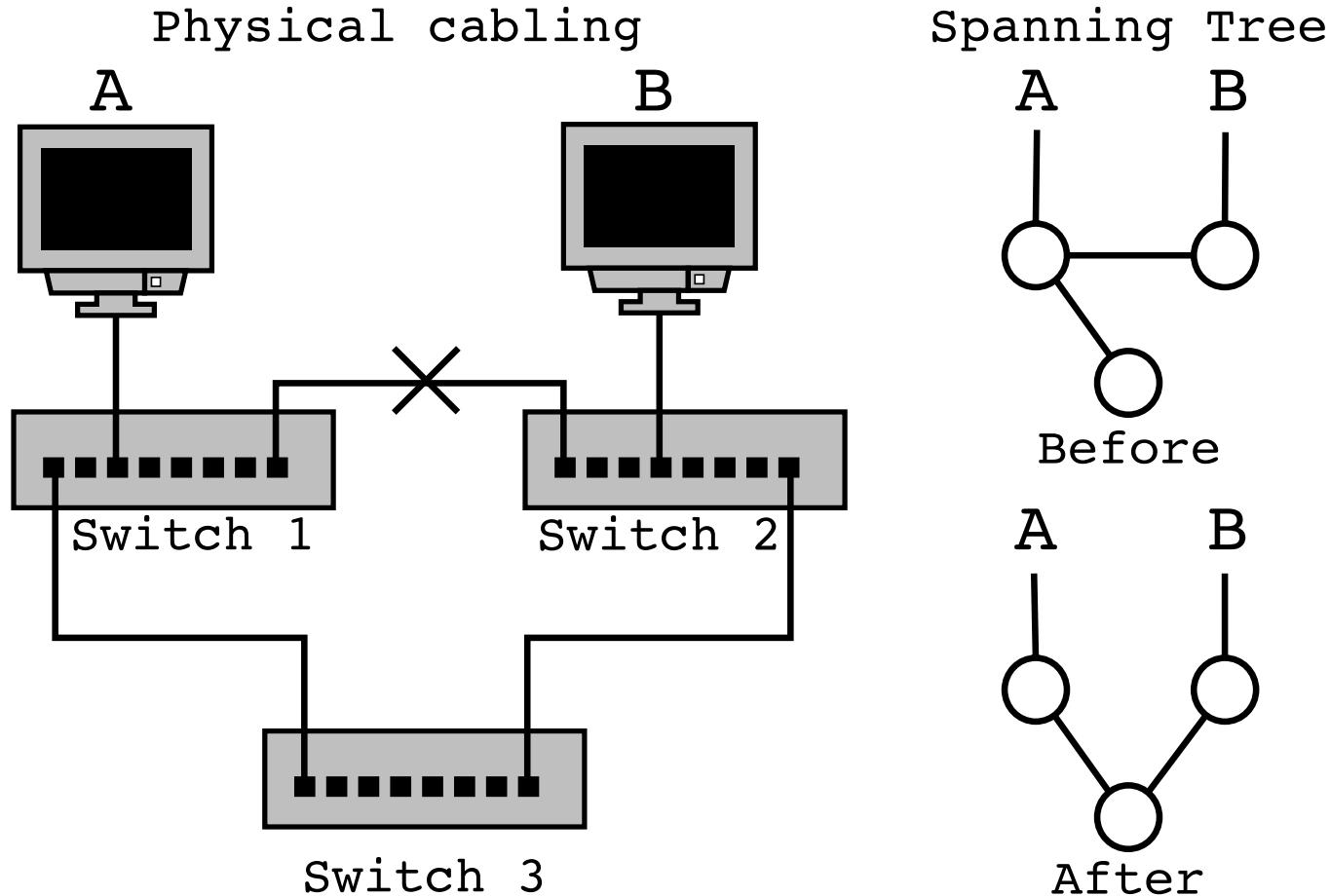


Ved at fortalte udviklingen kunne man samle broer til en switch

En switch idag kan sende og modtage på flere porte samtidig, og med full-duplex

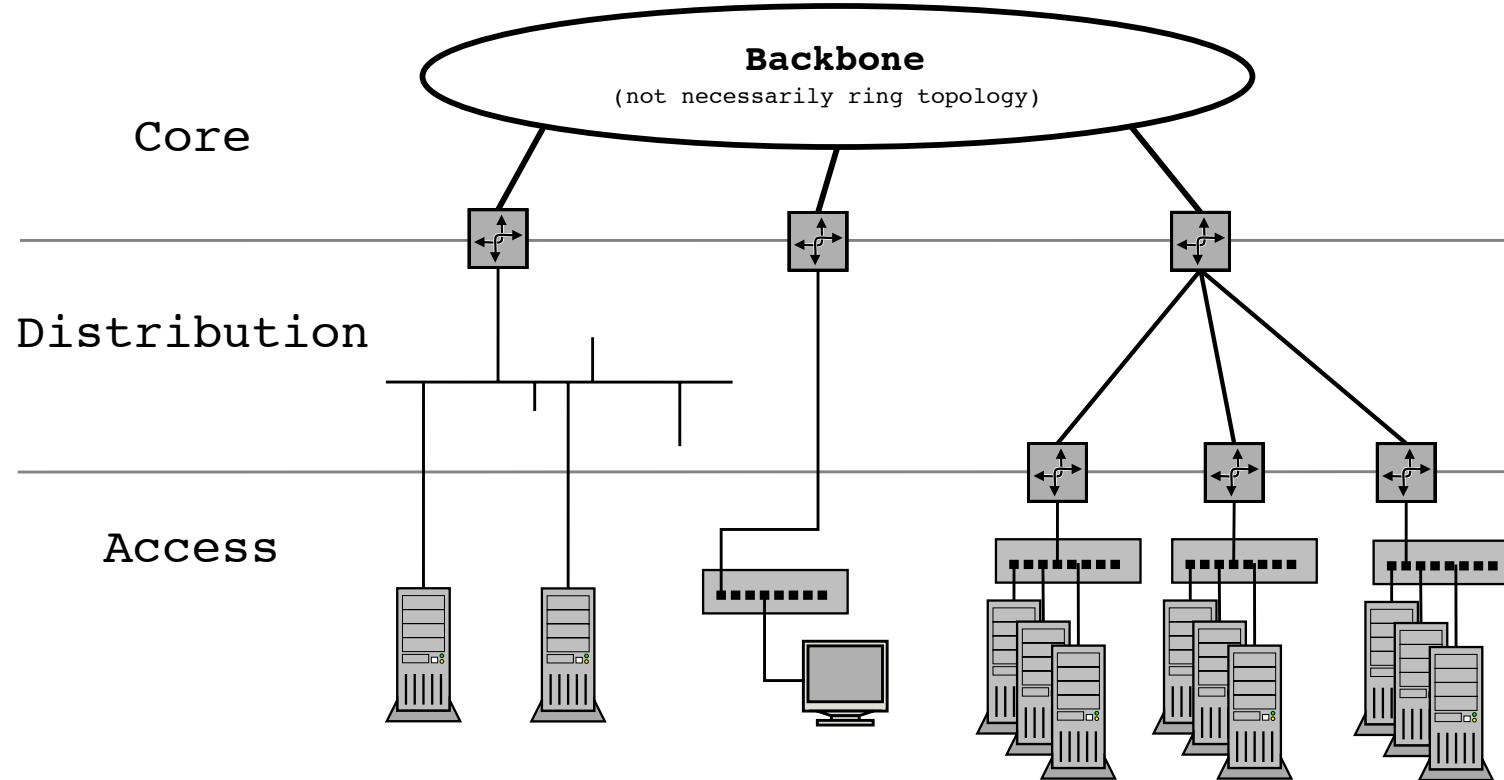
Bemærk performance begrænses af backplane i switchen

Topologier og Spanning Tree Protocol



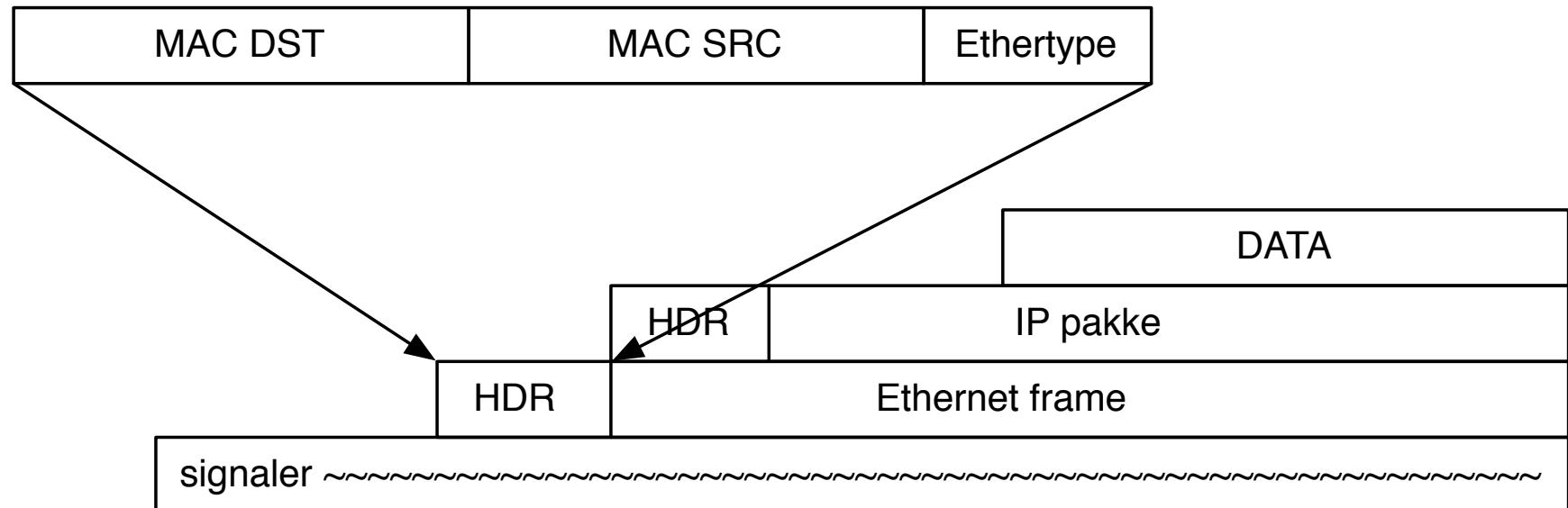
Se mere i bogen af Radia Perlman, *Interconnections: Bridges, Routers, Switches, and Internetworking Protocols*

Core, Distribution og Access net



Det er ikke altid man har prcis denne opdeling, men den er ofte brugt

Pakker i en datastrm



Ser vi data som en datastrm er pakkerne blot et mnster lagt henover data

Netvrksteknologien definerer start og slut p en frame

Fra et lavere niveau modtager vi en pakke, eksempelvis 1500-bytes fra Ethernet driver

ARP cache



```
hlk@bigfoot:hlk$ arp -an
? (10.0.42.1) at 0:0:24:c8:b2:4c on en1 [ethernet]
? (10.0.42.2) at 0:c0:b7:6c:19:b on en1 [ethernet]
```

ARP cache kan vises med kommandoen `arp -an`

-a viser alle

-n viser kun adresserne, prver ikke at sl navne op - typisk hurtigere

ARP cache er dynamisk og adresser fjernes automatisk efter 5-20 minutter hvis de ikke bruges mere

Ls mere med `man 4 arp`

Routere understter ofte Proxy ARP

Med Proxy ARP svarer de for en adresse bagved routeren

Derved kan man få trafik nemt igennem fra internet til adresser

Det er smart i visse situationer hvor en subnetting vil spilde for mange adresser

Hvis man kun har få adresser er subnetting måske heller ikke muligt

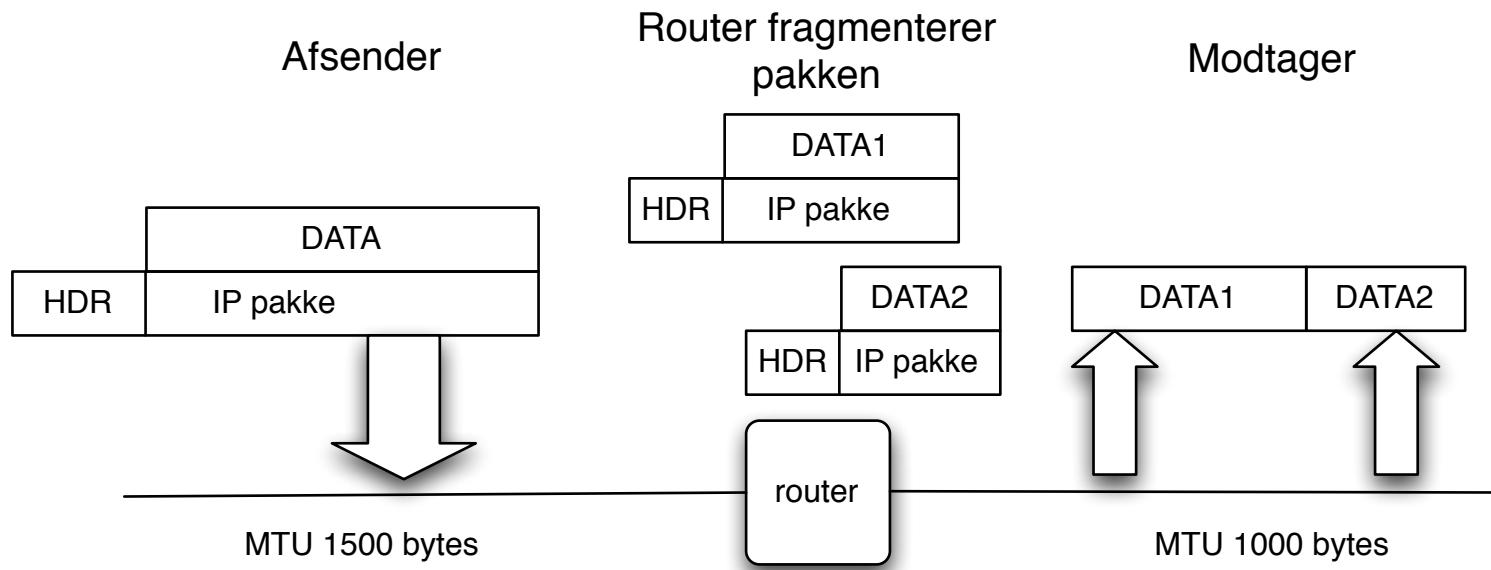
http://en.wikipedia.org/wiki/Proxy_ARP

ARP vs NDP



```
h1k@bigfoot:basic-ipv6-new$ arp -an
? (10.0.42.1) at 0:0:24:c8:b2:4c on en1 [ethernet]
? (10.0.42.2) at 0:c0:b7:6c:19:b on en1 [ethernet]
h1k@bigfoot:basic-ipv6-new$ ndp -an
Neighbor                               Linklayer Address  Netif Expire   St Flgs Prbs
::1                                     (incomplete)        lo0 permanent R
2001:16d8:fffd2:cf0f:21c:b3ff:fec4:e1b6 0:1c:b3:c4:e1:b6 en1 permanent R
fe80::1%lo0                            (incomplete)        lo0 permanent R
fe80::200:24ff:fec8:b24c%en1  0:0:24:c8:b2:4c       en1 8h54m51s S R
fe80::21c:b3ff:fec4:e1b6%en1  0:1c:b3:c4:e1:b6        en1 permanent R
```

Fragmentering og PMTU



Hidtil har vi antaget at der blev brugt Ethernet med pakkestørrelse på 1500 bytes

Pakkestørrelsen kaldes MTU Maximum Transmission Unit

Skal der sendes mere data opdeles i pakker af denne størrelse, fra afsender

Men hvad hvis en router på vejen ikke bruger 1500 bytes, men kun 1000

Kontrolprotokol og fejlmeldinger

Nogle af de mest almindelige beskedtyper

- echo
- netmask
- info

Bruges generelt til *signalering*

Defineret i RFC-792

NB: nogle firewall-administratorer blokerer alt ICMP - det er forkert!

Type

- 0 = net unreachable;
- 1 = host unreachable;
- 2 = protocol unreachable;
- 3 = port unreachable;
- 4 = fragmentation needed and DF set;
- 5 = source route failed.

Ved at fjerne ALT ICMP fra et net fjerner man ndvendig funktionalitet!

Tillad ICMP types:

- 3 Destination Unreachable
- 4 Source Quench Message
- 11 Time Exceeded
- 12 Parameter Problem Message

ICMP - Internet Control Message Protocol

Benyttes til fejlbeskeder og til diagnosticering af forbindelser

ping programmet virker ved hjlp af ICMP ECHO request og forventer ICMP ECHO reply

```
$ ping 192.168.1.1
```

```
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=150 time=8.849 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=150 time=0.588 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=150 time=0.553 ms
```

Flere sm forskelle

ping eller ping6

Nogle systemer viger at ping kommandoen kan ping'e bde IPv4 og Ipv6

Andre viger at ping kun benyttes til IPv4, mens IPv6 ping kaldes for ping6

Lg ogs mrke til jargonen *at pinge*

traceroute programmet virker ved hjlp af TTL

levetiden for en pakke tilles ned i hver router p vejen og ved at stte denne lavt opnr man at pakken *timer ud* - besked fra hver router p vejen

default er UDP pakker, men p Unix systemer er der ofte mulighed for at bruge ICMP

```
$ traceroute 217.157.20.129
```

```
traceroute to 217.157.20.129 (217.157.20.129),  
30 hops max, 40 byte packets  
1 safri (10.0.0.11) 3.577 ms 0.565 ms 0.323 ms  
2 router (217.157.20.129) 1.481 ms 1.374 ms 1.261 ms
```

Husk at p Windows hedder kommandoen tracert

traceroute - med UDP



```
# tcpdump -i en0 host 217.157.20.129 or host 10.0.0.11
tcpdump: listening on en0
23:23:30.426342 10.0.0.200.33849 > router.33435: udp 12 [ttl 1]
23:23:30.426742 safri > 10.0.0.200: icmp: time exceeded in-transit
23:23:30.436069 10.0.0.200.33849 > router.33436: udp 12 [ttl 1]
23:23:30.436357 safri > 10.0.0.200: icmp: time exceeded in-transit
23:23:30.437117 10.0.0.200.33849 > router.33437: udp 12 [ttl 1]
23:23:30.437383 safri > 10.0.0.200: icmp: time exceeded in-transit
23:23:30.437574 10.0.0.200.33849 > router.33438: udp 12
23:23:30.438946 router > 10.0.0.200: icmp: router udp port 33438 unreachable
23:23:30.451319 10.0.0.200.33849 > router.33439: udp 12
23:23:30.452569 router > 10.0.0.200: icmp: router udp port 33439 unreachable
23:23:30.452813 10.0.0.200.33849 > router.33440: udp 12
23:23:30.454023 router > 10.0.0.200: icmp: router udp port 33440 unreachable
23:23:31.379102 10.0.0.200.49214 > safri.domain: 6646+ PTR?

200.0.0.10.in-addr.arpa. (41)
23:23:31.380410 safri.domain > 10.0.0.200.49214: 6646 NXDomain* 0/1/0 (93)
14 packets received by filter
0 packets dropped by kernel
```

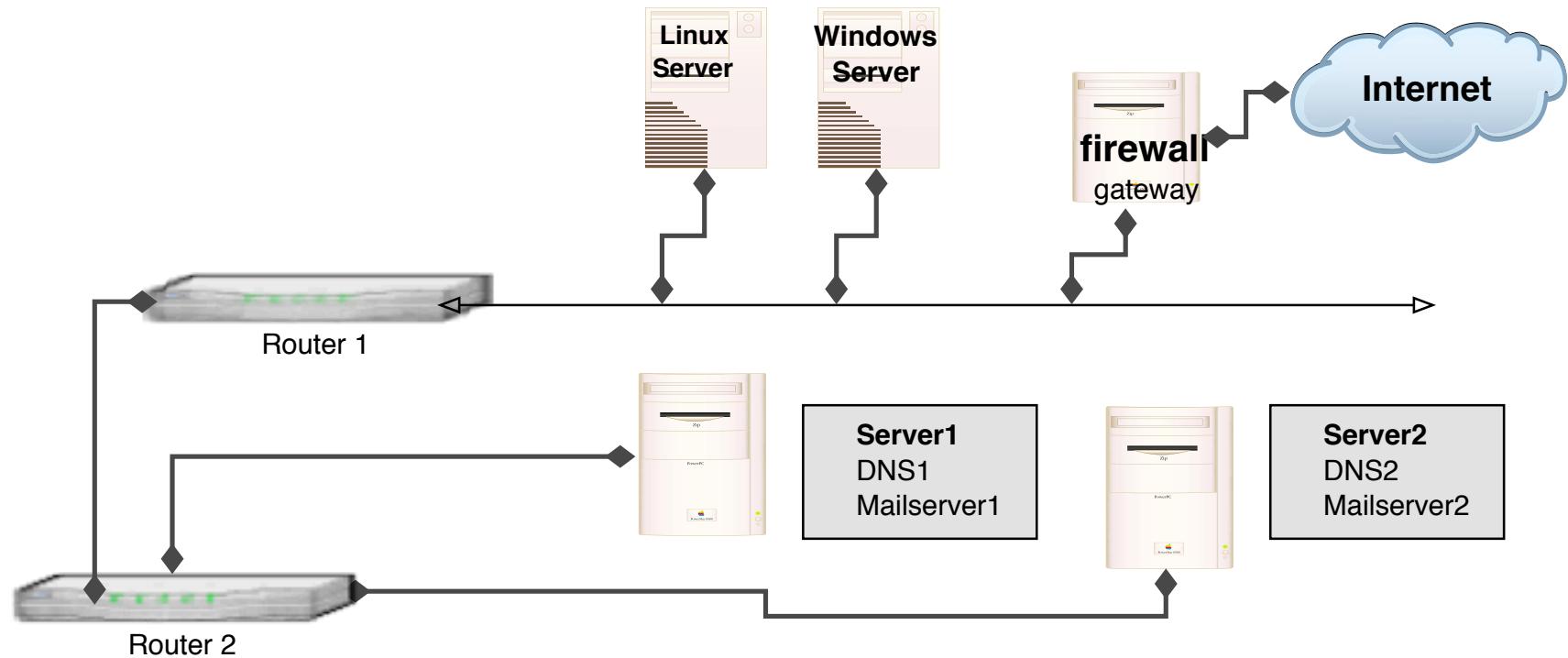
Diagnosticering af netvrksproblemer - formlet med traceroute

Indblik i netvrkets opbygning!

Svar fra hosts - en modtaget pakke fremfor et *sort hul*

Traceroute er ikke et angreb - det er også vigtigt at kunne genkende normal trafik!

Network mapping



Ved brug af traceroute og tilsvarende programmer kan man ofte udlede topologien i det netværk man undersger

mtr My traceroute - grafisk <http://www.bitwizard.nl/mtr/>

Ift - *layer four trace* benytter TCP SYN og FIN prober

trace ved hjlp af TCP og andre protokoller findes

paratrace - *Parasitic Traceroute via Established TCP Flows and IPID Hopcount*

Der findes webservices hvor man kan trace fra, eksempelvis: <http://www.samspade.org>

Stop - vi gennemgr og tester vores setup



Vi gennemgr hvordan vores setup ser ud

Vi laver traceroute fr og efter:

Vi fjerner en ledning *link down*

Vi stopper en router og ser de annoncerede netvrk forsvinder

Vi bootter en router og ser de annoncerede netvrk igen

Stop - vi ser i fllesskab p admin interfaces



Vi prver lige at se p diverse interfaces sammen

hvis alle prver samtidig bliver det lidt kaos :-)

Huskeliste til Henrik:

- Cisco switch
- Airport Extreme access-point
- Juniper SSG5 firewall
- Linksys WRV-200 router, access-point og switch

Shells kommandofortolkere:

- sh - Bourne Shell
- bash - Bourne Again Shell
- ksh - Korn shell, lavet af David Korn
- csh - C shell, syntaks der minder om C sproget
- flere andre, zsh, tcsh

Svarer til command.com og cmd.exe p Windows

Kan bruges som komplette programmeringssprog

Kommandoprompten

```
[hlk@fischer hlk]$ id  
uid=6000(hlk) gid=20(staff) groups=20(staff),  
0(wheel), 80(admin), 160(cvs)  
[hlk@fischer hlk]$
```

```
[root@fischer hlk]# id  
uid=0(root) gid=0(wheel) groups=0(wheel), 1(daemon),  
2(kmem), 3(sys), 4(tty), 5(operator), 20(staff),  
31(guest), 80(admin)  
[root@fischer hlk]#
```

typisk viser et dollartegn at man er logget ind som almindelig bruge
mens en havelge at man er root - superbruger

```
echo [-n] [string ...]
```

Kommandoerne der skrives p kommandolinien skrives sdan:

- Starter altid med kommandoen, man kan ikke skrive henrik echo
- Options skrives typisk med bindestreg foran, eksempelvis -n
- Flere options kan sttes sammen, tar -cvf eller tar cvf
- I manualsystemet kan man se valgfrie options i firkantede klammer []
- Argumenterne til kommandoen skrives typisk til sidst (eller der bruges redirection)

It is a book about a Spanish guy called Manual. You should read it. – Dilbert

Manualsystemet i Unix er utroligt strkt!

Det SKAL altid installeres sammen med vrktjerne!

Det er nsten identisk p diverse Unix varianter!

man -k sger efter keyword, se ogs apropos

Prv man crontab og man 5 crontab

kommando [options] [argumenter]

\$ cal -j 2005

CAL(1)

BSD General Commands Manual

CAL(1)

NAME

cal - displays a calendar

SYNOPSIS

cal [-jy] [[month] year]

DESCRIPTION

cal displays a simple calendar. If arguments are not specified, the current month is displayed. The options are as follows:

- j Display julian dates (days one-based, numbered from January 1).
- y Display a calendar for the current year.

The Gregorian Reformation is assumed to have occurred in 1752 on the 3rd of September. By this time, most countries had recognized the reformation (although a few did not recognize it until the early 1900's.) Ten days following that date were eliminated by the reformation, so the calendar for that month is a bit unusual.

HISTORY

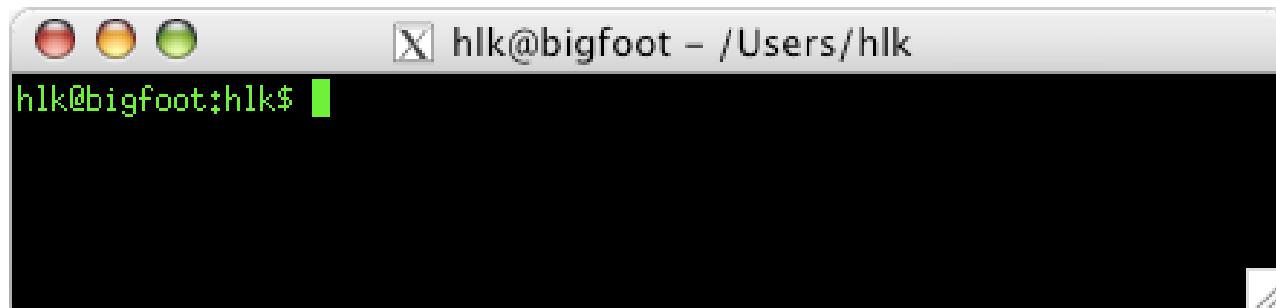
A cal command appeared in Version 6 AT&T Unix.



Adgang til Unix kan ske via grafiske brugergrænseflader

- KDE <http://www.kde.org>
- GNOME <http://www.gnome.org>

eller kommandolinien





Vi laver nu velsen

1Putty installation - Secure Shell loginchapter.1

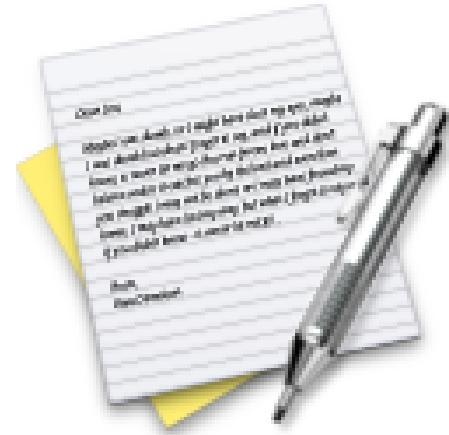
som er velse **1Putty installation - Secure Shell loginchapter.1** fra velseshftet.



Vi laver nu velsen

2WinSCP installation - Secure Copy chapter.2

som er velse 2WinSCP installation - Secure Copy chapter.2 fra velseshftet.



Vi laver nu velsen

3Login p Unix systemerne chapter.3

som er velse 3Login p Unix systemerne chapter.3 fra velseshftet.



Vi laver nu velsen

??

som er velse ?? fra velseshftet.



Vi laver nu velsen

??

som er velse ?? fra velseshftet.



Vi laver nu velsen

??

som er velse ?? fra velseshftet.

```
ifconfig en0 10.0.42.1 netmask 255.255.255.0  
route add default gw 10.0.42.1
```

konfiguration af interfaces og netvrk p Unix foregr med:

ifconfig, route **og** netstat

- ofte pakket ind i konfigurationsmenuer m.v.

fejlsning foregr typisk med ping **og** traceroute

P Microsoft Windows benyttes ikke ifconfig

men kommandoerne ipconfig **og** ipv6

Netvrkskonfiguration p OpenBSD:

```
# cat /etc/hostname.sk0
inet 10.0.0.23 0xfffffff00 NONE
# cat /etc/mygate
10.0.0.1
# cat /etc/resolv.conf
domain security6.net
lookup file bind
nameserver 212.242.40.3
nameserver 212.242.40.51
```

GUI vrktjer - autoconfiguration



Built-in Ethernet

TCP/IP DNS WINS AppleTalk 802.1X Proxies Ethernet

Configure IPv4: Using DHCP

IPv4 Address:

Subnet Mask:

Router:

DHCP Client ID:
(If required)

Configure IPv6: Automatically

IPv6 Address:

Prefix Length:

GUI vrktjer - manuel konfiguration



Built-in Ethernet

TCP/IP DNS WINS AppleTalk 802.1X Proxies Ethernet

Configure IPv4: Manually

IPv4 Address: 0.0.0.0

Subnet Mask:

Router:

Configure IPv6: Manually

Router:

IPv6 Address:

Prefix Length:

Advanced

ifconfig output

```
hlk@bigfoot:hlk$ ifconfig -a
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
        inet 127.0.0.1 netmask 0xff000000
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        ether 00:0a:95:db:c8:b0
        media: autoselect (none) status: inactive
        supported media: none autoselect 10baseT/UTP <half-duplex> 10baseT/UTP
en1: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        ether 00:0d:93:86:7c:3f
        media: autoselect (<unknown type>) status: inactive
        supported media: autoselect
```

ifconfig output er nsten ens p tvrs af Unix

ARP Address Resolution Protocol

IP og ICMP Internet Control Message Protocol

UDP User Datagram Protocol

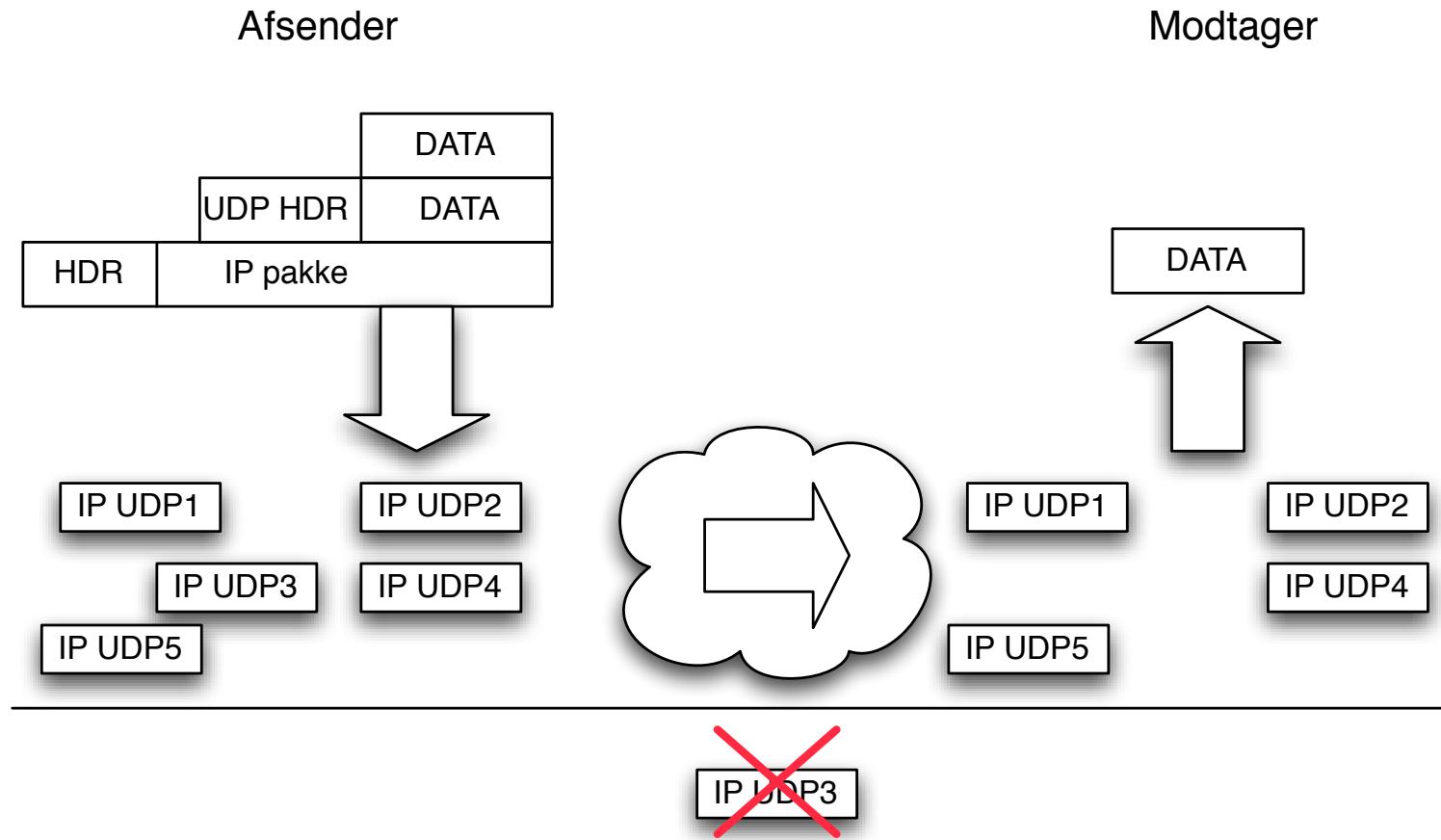
TCP Transmission Control Protocol

DHCP Dynamic Host Configuration Protocol

DNS Domain Name System

Ovenstende er omtrent minimumskrav for at komme p internet

UDP User Datagram Protocol



Forbindelsesløs RFC-768, *connection-less* - der kan tabes pakker

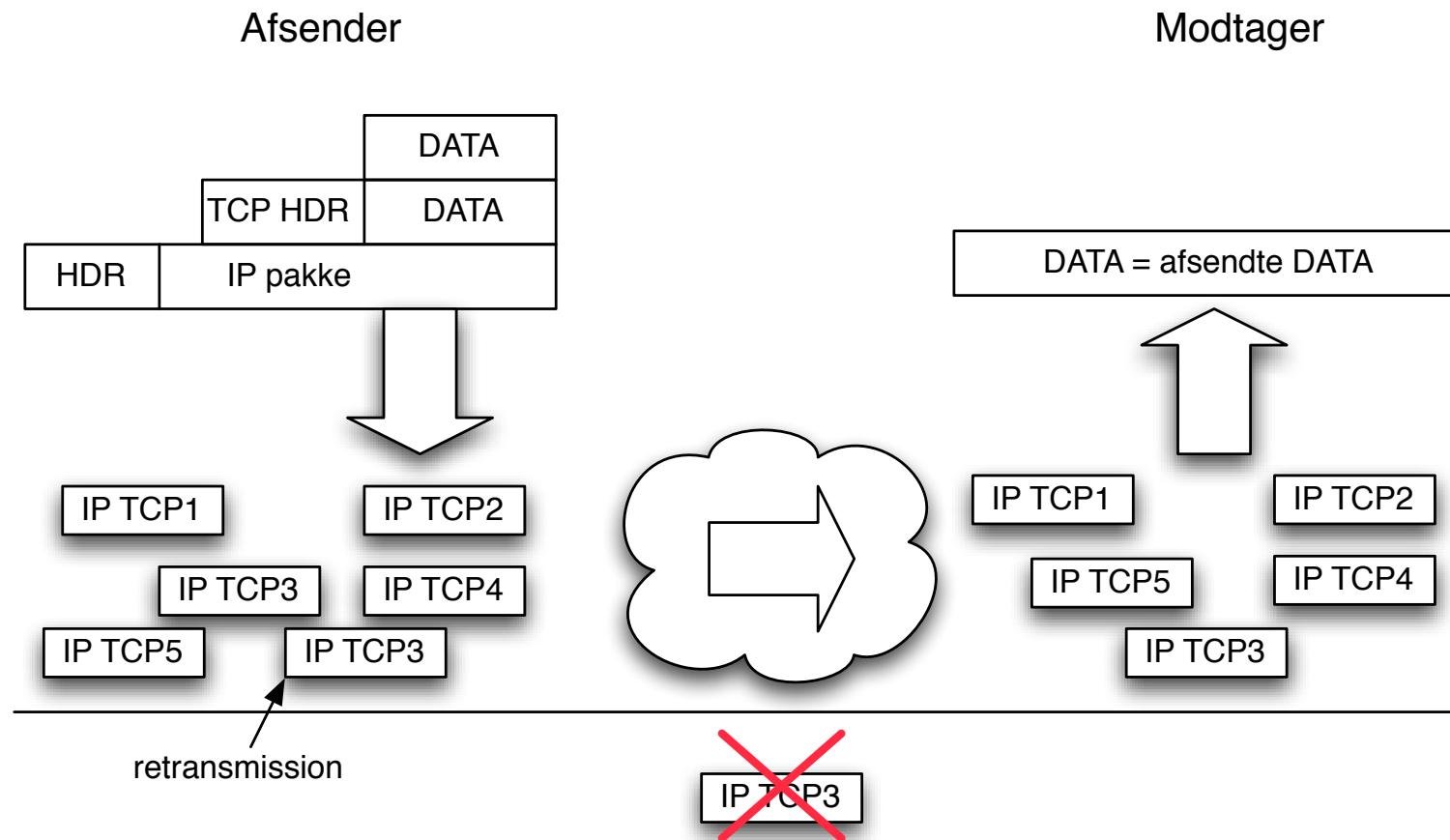
Kan benyttes til multicast/broadcast - flere modtagere

TCP Transmission Control Protocol



- Security

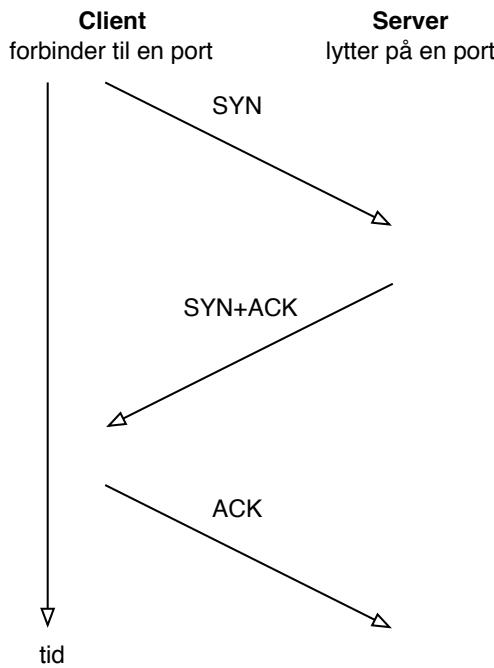
.net



Forbindelsesorienteret RFC-791 September 1981, *connection-oriented*

Enten overfres data eller man får fejlmeddelelse

TCP three way handshake



- **TCP SYN half-open scans**
- Tidligere loggede systemer kun var etableret en fuld TCP forbindelse - dette kan/kunne udnyttes til *stealth*-scans
- Hvis en maskine modtager mange SYN pakker kan dette fylde tabellen over connections op - og derved afholde nye forbindelser fra at blive oprette - **SYN-flooding**

Well-known port numbers



IANA vedligeholder en liste over magiske konstanter i IP

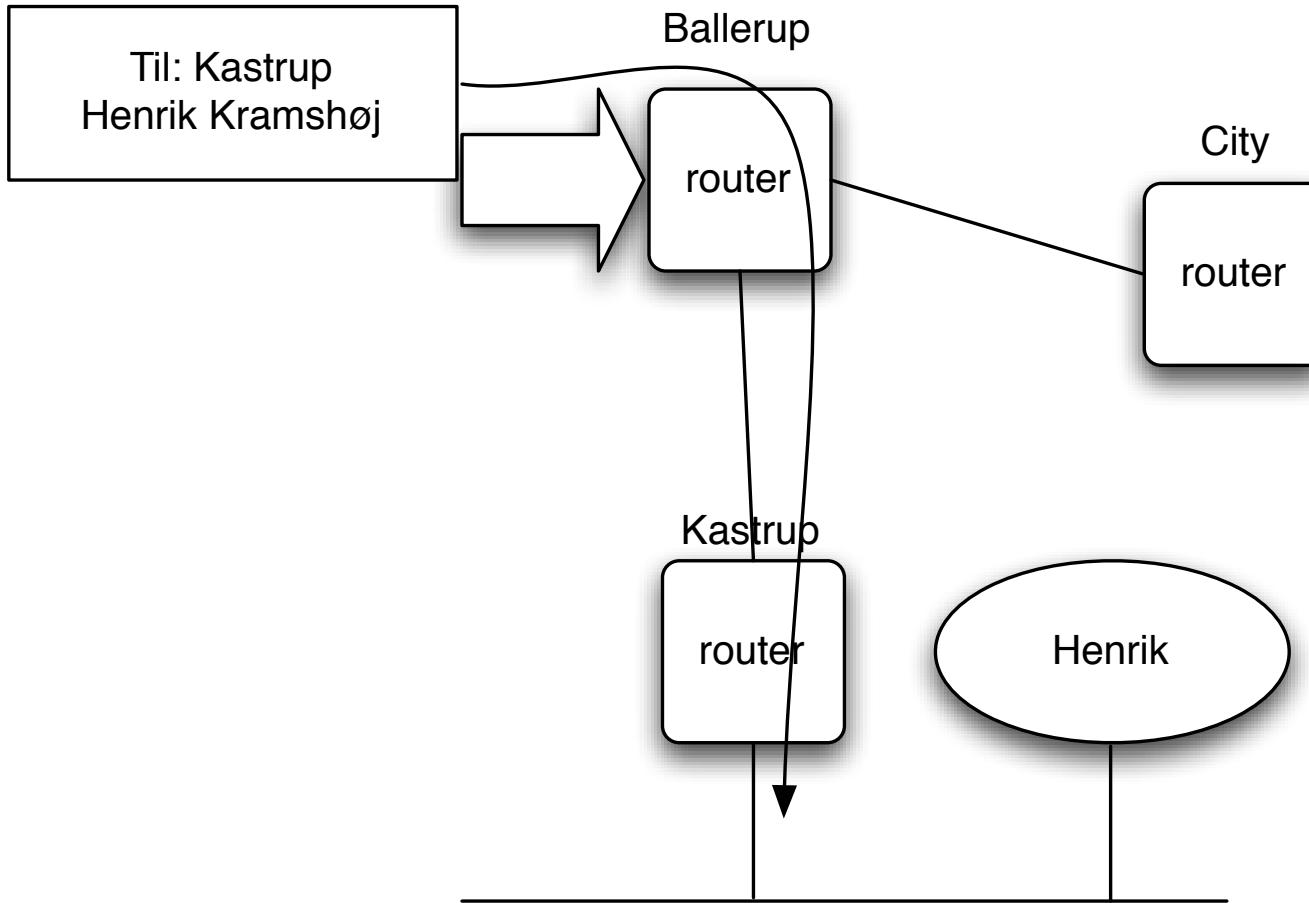
De har lister med hvilke protokoller har hvilke protokol ID m.v.

En liste af interesse er port numre, hvor et par eksempler er:

- Port 25 SMTP Simple Mail Transfer Protocol
- Port 53 DNS Domain Name System
- Port 80 HTTP Hyper Text Transfer Protocol over TLS/SSL
- Port 443 HTTP over TLS/SSL

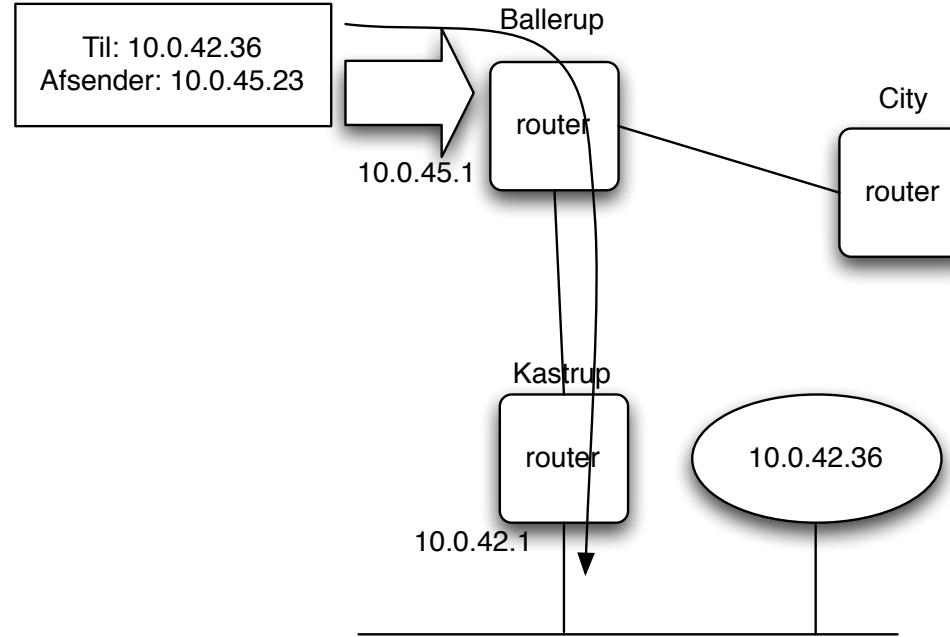
Se flere p <http://www.iana.org>

Hierarkisk routing



Hvordan kommer pakkerne frem til modtageren

IP default gateway



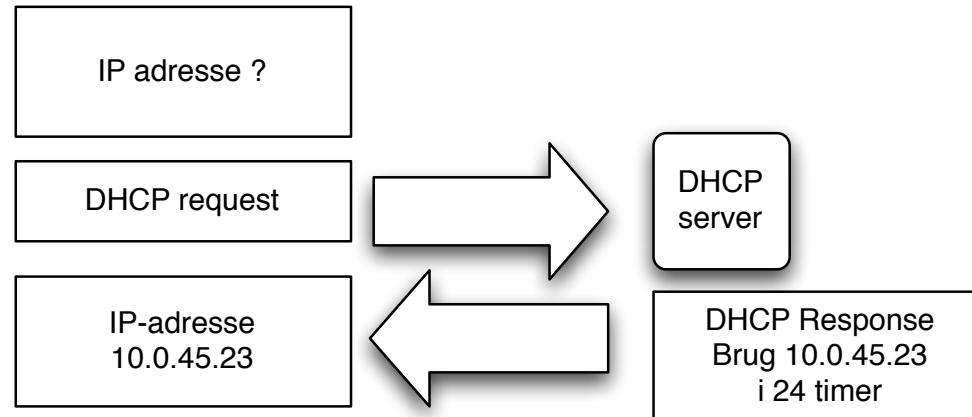
IP routing er nemt

En host kender en default gateway i nrheden

En router har en eller flere upstream routere, f adresser den sender videre til

Core internet har default free zone, kender *alle netværk*

DHCP Dynamic Host Configuration Protocol



Hvordan fr man information om default gateway

Man sender et DHCP request og modtager et svar fra en DHCP server

Dynamisk konfiguration af klienter fra en centralt konfigureret server

Bruges til IP adresser og meget mere

IPv6 router advertisement daemon



```
/etc/rtadvd.conf:  
en0:  
    :addrs#1:addr="2001:1448:81:b00f::":prefixlen#64:  
en1:  
    :addrs#1:addr="2001:1448:81:beef::":prefixlen#64:  
  
root# /usr/sbin/rtadvd -Df en0 en1  
root# sysctl -w net.inet6.ip6.forwarding=1  
net.inet6.ip6.forwarding: 0 -> 1
```

Stateless autoconfiguration er en stor ting i IPv6

Kommandoen starter den i debug-mode og i forgrunden
- normalt vil man starte den fra et script

Typisk skal forwarding aktiveres, som vist med BSD sysctl kommando

routing table - tabel over netvrkskort og tilhrende adresser

default gateway - den adresse hvortil man sender *non-local* pakker
kaldes også default route, gateway of last resort

routing styres enten manuelt - opdatering af route tabellen, eller konfiguration af adresser og subnet masker på netkort

eller automatisk ved brug af routing protocols - interne og eksterne route protokoller

De lidt lidre routing protokoller har ingen sikkerhedsmekanismer

IP benytter longest match i routing tabeller!

Den mest specifikke route glder for forward af en pakke!

Routing forstelse

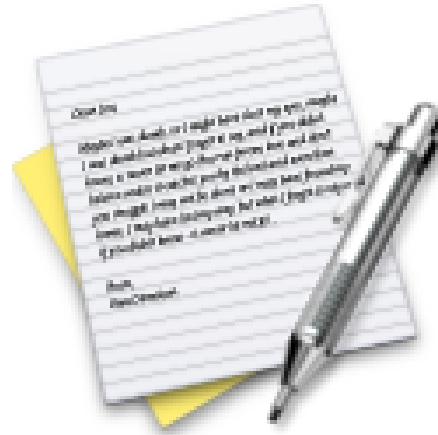


```
$ netstat -rn  
Routing tables
```

Internet:

Destination	Gateway	Flags	Refs	Use	Netif
default	10.0.0.1	UGSc	23	7	en0
10/24	link#4	UCS	1	0	en0
10.0.0.1	0:0:24:c1:58:ac	UHLW	24	18	en0
10.0.0.33	127.0.0.1	UHS	0	1	lo0
10.0.0.63	127.0.0.1	UHS	0	0	lo0
127	127.0.0.1	UCS	0	0	lo0
127.0.0.1	127.0.0.1	UH	4	7581	lo0
169.254	link#4	UCS	0	0	en0

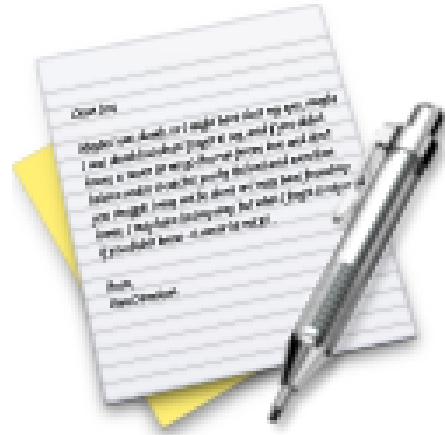
Start med kun at se på Destination, Gateway og Netinterface



Vi laver nu velsen

5Netvrksinformation: ifconfig/ipconfigchapter.5

som er velse **5Netvrksinformation: ifconfig/ipconfigchapter.5** fra velseshftet.



Vi laver nu velsen

6Netvrksinformation: netstatchapter.6

som er velse **6Netvrksinformation: netstatchapter.6** fra velseshftet.



Vi laver nu velsen

7ping og traceroute chapter.7

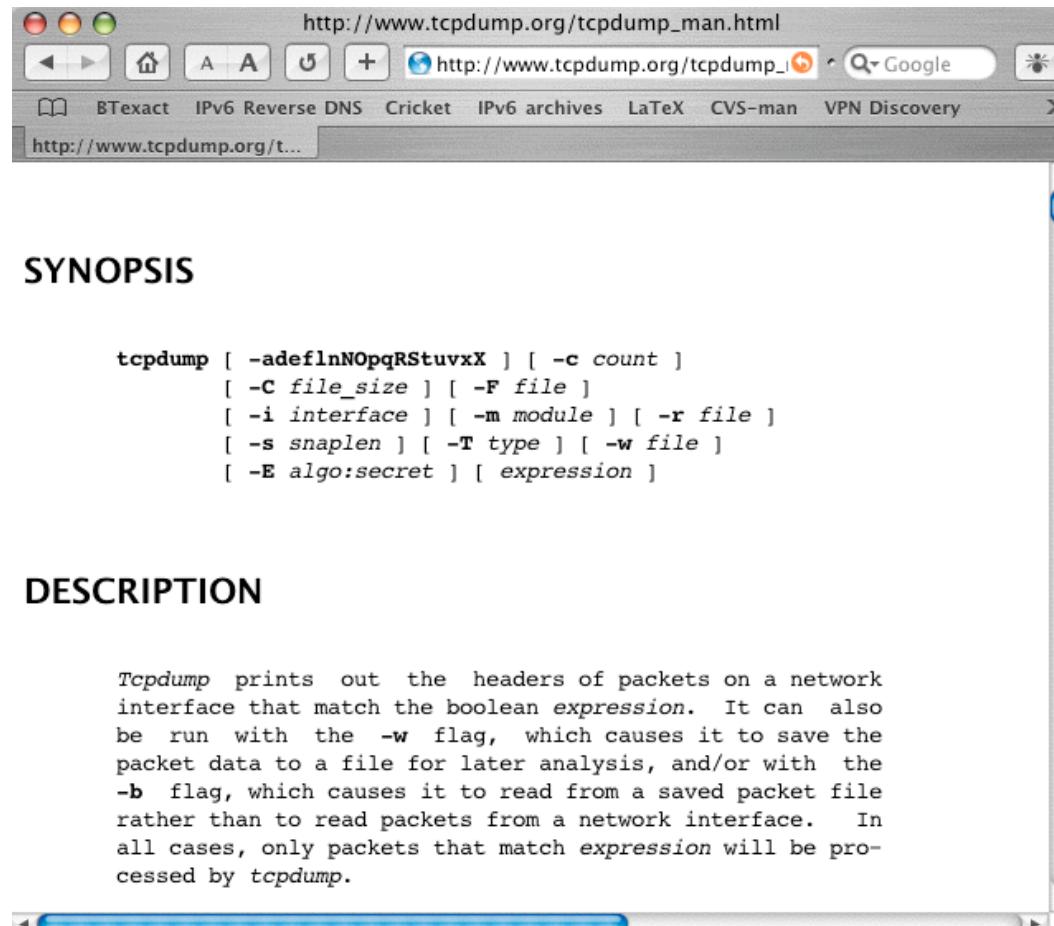
som er velse **7ping og traceroute chapter.7** fra velseshftet.



Vi laver nu velsen

8ping6 og traceroute6chapter.8

som er velse **8ping6 og traceroute6chapter.8** fra velseshftet.



<http://www.tcpdump.org> - bde til Windows og Unix

tcpdump - normal brug



- tekstmode
- kan gemme netvrkspakker i filer
- kan lse netvrkspakker fra filer
- er de-facto standarden for at gemme netvrksdata i filer

```
[root@otto hlk]# tcpdump -i en0
tcpdump: listening on en0
13:29:39.947037 fe80::210:a7ff:fe0b:8a5c > ff02::1: icmp6: router advertisement
13:29:40.442920 10.0.0.200.49165 > dns1.cybercity.dk.domain: 1189+[|domain]
13:29:40.487150 dns1.cybercity.dk.domain > 10.0.0.200.49165: 1189 NXDomain*[|domain]
13:29:40.514494 10.0.0.200.49165 > dns1.cybercity.dk.domain: 24765+[|domain]
13:29:40.563788 dns1.cybercity.dk.domain > 10.0.0.200.49165: 24765 NXDomain*[|domain]
13:29:40.602892 10.0.0.200.49165 > dns1.cybercity.dk.domain: 36485+[|domain]
13:29:40.648288 dns1.cybercity.dk.domain > 10.0.0.200.49165: 36485 NXDomain*[|domain]
13:29:40.650596 10.0.0.200.49165 > dns1.cybercity.dk.domain: 4101+[|domain]
13:29:40.694868 dns1.cybercity.dk.domain > 10.0.0.200.49165: 4101 NXDomain*[|domain]
13:29:40.805160 10.0.0.200 > mail: icmp: echo request
13:29:40.805670 mail > 10.0.0.200: icmp: echo reply
...
```

filtrere til husbehov

- type - host, net og port
- src pakker med afsender IP eller afsender port
- dst pakker med modtager IP eller modtager port
- host - afsender eller modtager
- proto - protokol: ether, fddi, tr, ip, ip6, arp, rarp, decnet, tcp og udp

IP adresser kan angives som dotted-decimal eller navne

porte kan angives med numre eller navne

komplekse udtryk opbygges med logisk and, or, not

tcpdump udtryk eksempler



Host 10.1.2.3

Alle pakker hvor afsender eller modtager er 10.1.2.3

host 10.2.3.4 and not host 10.3.4.5

Alle pakker til/fra 10.2.3.4 undtagen dem til/fra 10.3.4.5

- meget praktisk hvis man er logget ind på 10.2.3.4 via netværk fra 10.3.4.5

host foo and not port ftp and not port ftp-data

trafik til/fra maskine *foo* undtagen hvis det er FTP trafik

Wireshark - grafisk pakkesniffer

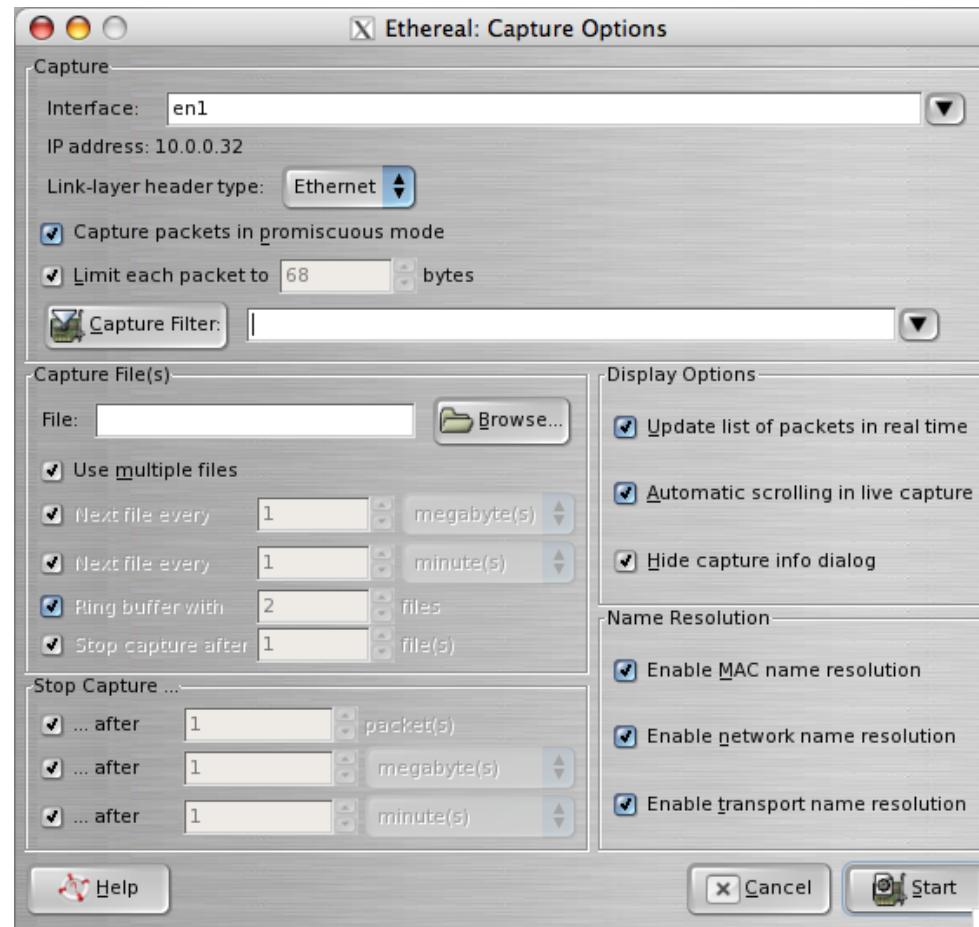


The screenshot shows the official Wireshark website. At the top, there's a large blue header with the 'WIRESHARK' logo. Below it is a black navigation bar with links for HOME, ABOUT, WHAT'S NEW, DOWNLOAD, and FAQ. To the right of the navigation is a photograph of a shark swimming in the ocean. On the left side, there's a sidebar with a dark blue background containing links: Get It (with Download), Get Help (with FAQs, Documentation, Mailing Lists, Wiki, Bug tracker), Develop (with Developer Info), Products (with AirPcap, Network Toolkit, OEM WinPcap), and Sniffing Problems A Mile Away. The main content area has a white background. It features a section titled 'Sniffing Problems A Mile Away' which explains the name change from Ethereal to Wireshark and highlights its features. Below this is a screenshot of the Wireshark interface showing network traffic. Further down is a 'News' section with a link to 'Wireshark 0.99.3 Released' and a date of 'Aug 23, 2006'. The news text mentions fixed security-related vulnerabilities. To the right of the main content is a sidebar with a light blue background titled 'Download Now' showing version 0.99.3, and a Q&A section about capturing 802.11 traffic using AirPcap.

<http://www.wireshark.org>

bde til Windows og Unix, tidligere kendt som Ethereal

Brug af Wireshark



Man starter med Capture - Options

Brug af Wireshark



X (Untitled) - Ethereal

File Edit View Go Capture Analyze Statistics Help

No. Time Source Destination Protocol Info

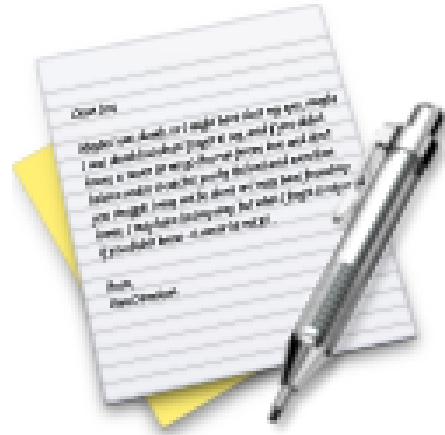
561	6.700947	10.0.0.32	sunny.kramse.uk	TCP	54021 > imaps [ACK] Seq=420 Ack=10775 Win=65!
562	6.763144	sunny.kramse.dk	10.0.0.32	TLS	Continuation Data, [Unreassembled Packet]
563	6.820037	10.0.0.32	sunny.kramse.dk	TCP	54021 > imaps [ACK] Seq=426 Ack=11106 Win=65!
564	6.919635	10.0.0.32	sunny.kramse.dk	TCP	54023 > imaps [SYN] Seq=0 Ack=0 Win=65535 Len
565	6.921708	sunny.kramse.dk	10.0.0.32	TCP	imaps > 54023 [SYN, ACK] Seq=0 Ack=1 Win=1638
566	6.921794	10.0.0.32	sunny.kramse.dk	TCP	54023 > imaps [ACK] Seq=1 Ack=1 Win=65535 Len
567	6.922614	10.0.0.32	sunny.kramse.dk	TLS	Client Hello

Frame 563 (66 bytes on wire, 66 bytes captured)
Ethernet II, Src: AppleCom_86:7c:3f (00:0d:93:86:7c:3f), Dst: Olicom_c3:57:d8 (00:00:24:c3:57:d8)
Internet Protocol, Src: 10.0.0.32 (10.0.0.32), Dst: sunny.kramse.dk (217.157.20.131)
Transmission Control Protocol, Src Port: 54021 (54021), Dst Port: imaps (993), Seq: 426, Ack: 11106, Len: 0

0000 00 00 24 c3 57 d8 00 0d 93 86 7c 3f 08 00 45 00 ..\$.W...|?.E.
0010 00 34 7e 8b 40 00 40 06 c3 f8 0a 00 00 20 d9 9d .4~.@@.
0020 14 83 d3 05 03 e1 cd 31 c9 ea 0d 7b a2 bf 80 101 ...{....
0030 ff ff 32 0d 00 00 01 01 08 0a 62 e0 c3 42 bb e3 ..2.....b..B..

Filter: Expression... Clear Apply File: "/var/tmp/ether0ARkxt..."

Lg mrke til filtermulighederne



Vi laver nu velsen

9Wireshark netvrksnifferchapter.9

som er velse **9Wireshark netvrksnifferchapter.9** fra velseshftet.

en sniffer til mange usikre protokoller

inkluderer **arpspoof**

Lavet af Dug Song, dugsong@monkey.org

dsniff is a password sniffer which handles FTP, Telnet, SMTP, HTTP, POP, poppass, NNTP, IMAP, SNMP, LDAP, Rlogin, RIP, OSPF, PPTP, MS-CHAP, NFS, VRRP, YP/NIS, SOCKS, X11, CVS, IRC, AIM, ICQ, Napster, PostgreSQL, Meeting Maker, Citrix ICA, Symantec pcAnywhere, NAI Sniffer, Microsoft SMB, Oracle SQL*Net, Sybase and Microsoft SQL protocols.

Kommenteret dsniff

```
[root@hlk hlk]# dsniff
dsniff: listening on fxp0
-----
05/20/03 08:53:38 tcp client.49154 -> server.110 (pop)
USER hlk
PASS secr3t! Her er opsamlet et kodeord til e-mail
-----
05/20/03 08:54:11 tcp client.49155 -> server.23 (telnet)
[poppe]

hlk
secr3t! Her er opsamlet kodeord og
kommandoer fra en session
ls
exit
-----
05/20/03 08:55:33 tcp client.49156 -> server.23 (telnet)
[poppe]

an ja
an jnaan ja
an ja
```

Chaosreader

Chaosreader Report

Created at: Sun Nov 16 21:04:18 2003, Type: snoop

[Image Report](#) - Click here for a report on captured images.

[GET/POST Report](#) (Empty) - Click here for a report on HTTP GETs and POSTs.

[HTTP Proxy Log](#) - Click here for a generated proxy style HTTP log.

TCP/UDP/... Sessions

1.	Sun Nov 16 20:38:22 2003	30 s	192.168.1.3:1368 <-> 192.77.84.99:80	web	383 bytes	• as html
2.	Sun Nov 16 20:38:22 2003	29 s	192.168.1.3:1366 <-> 192.77.84.99:80	web	381 bytes	• as html

Med adgang til et netvrksdump kan man lse det med chaosreader

Output er HTML med oversigter over sessioner, billeder fra datastrmmen osv.

<http://chaosreader.sourceforge.net/>

Kryptering af e-mail

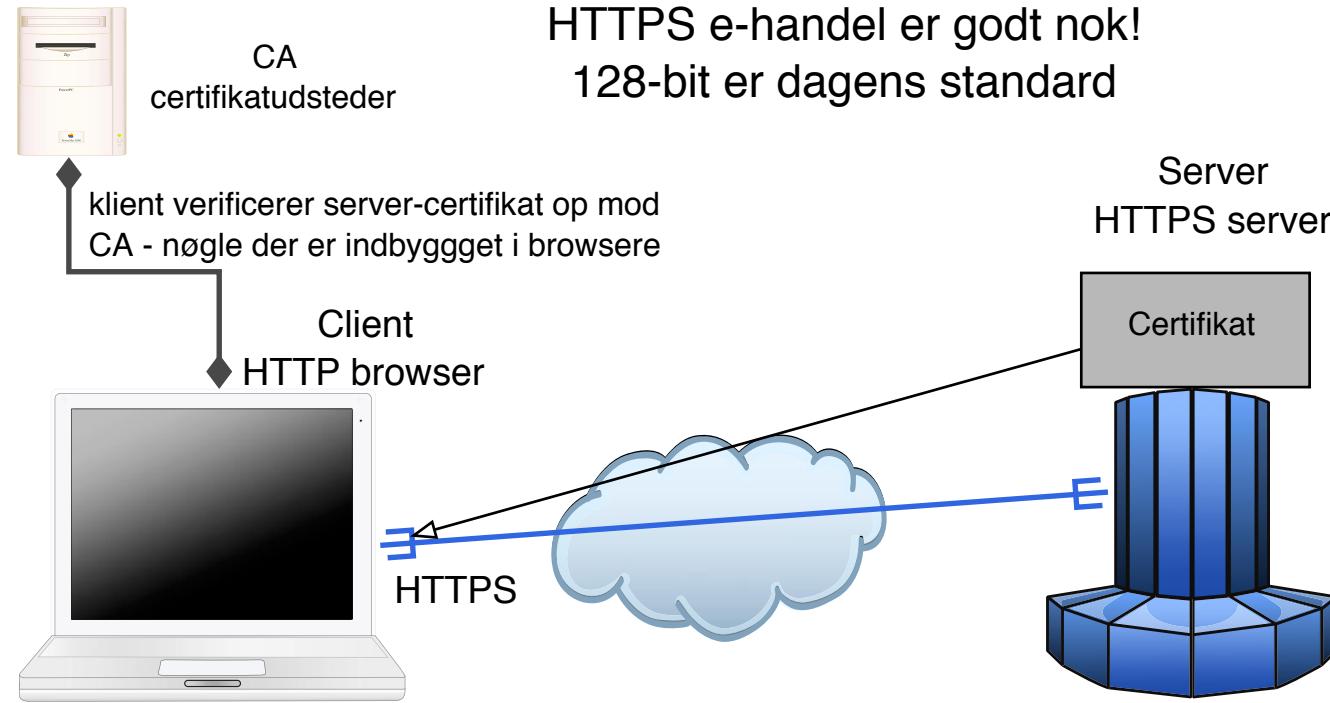
- Pretty Good Privacy - Phil Zimmermann
- GNU Privacy Guard - Open Source implementation af OpenPGP
- OpenPGP = mail sikkerhed, OpenPGP RFC-2440, PGP/MIME RFC 3156)

Kryptering af sessioner SSL/TLS

- Secure Sockets Layer SSL / Transport Layer Services TLS
- krypterer data der sendes mellem webservere og klienter
- SSL kan bruges generelt til mange typer sessioner, eksempelvis POP3S, IMAPS, SSH m.fl.

Kryptering af netvirkstrafik - Virtual Private Networks VPN

- IPsec IP Security Framework, se også L2TP
- PPTP Point to Point Tunneling Protocol - drlig og usikker, brug den ikke mere!
- OpenVPN m.fl.



Oprindeligt udviklet af Netscape Communications Inc.

Secure Sockets Layer SSL er idag blevet adopteret af IETF og kaldes derfor også for Transport Layer Security TLS. TLS er baseret på SSL Version 3.0.

RFC-2246 The TLS Protocol Version 1.0 fra Januar 1999

SSL/TLS udgaver af protokoller



Check with your system administrator before changing any of the advanced options below:

IMAP Path Prefix: INBOX

Port: 993 Use SSL

Authentication: Password

Mange protokoller findes i udgaver hvor der benyttes SSL

HTTPS vs HTTP

IMAPS, POP3S, osv.

Bemrk: nogle protokoller benytter to porte IMAP 143/tcp vs IMAPS 993/tcp

Andre benytter den samme port men en kommando som starter:

SMTP STARTTLS RFC-3207



Hvad er Secure Shell SSH?

Oprindeligt udviklet af Tuomo Ylinen i Finland,
se <http://www.ssh.com>

SSH aflser en række protokoller som er usikre:

- Telnet til terminal adgang
- r* programmerne, rsh, rcp, rlogin, ...
- FTP med brugerid/password

SSH - de nye kommandoer er



kommandoerne er:

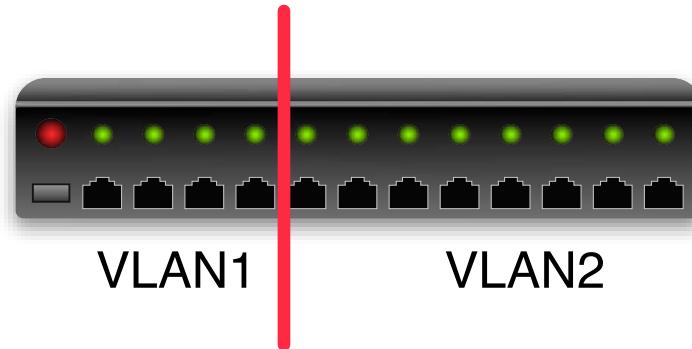
- ssh - Secure Shell
- scp - Secure Copy
- sftp - secure FTP

Husk: SSH er bde navnet p protokollerne - version 1 og 2 samt programmet `ssh` til at logge ind p andre systemer

SSH tillader ogs port-forward, tunnel til usikre protokoller, eksempelvis X protokollen til Unix grafiske vinduer

NB: Man br idag bruge SSH protokol version 2!

Portbased VLAN



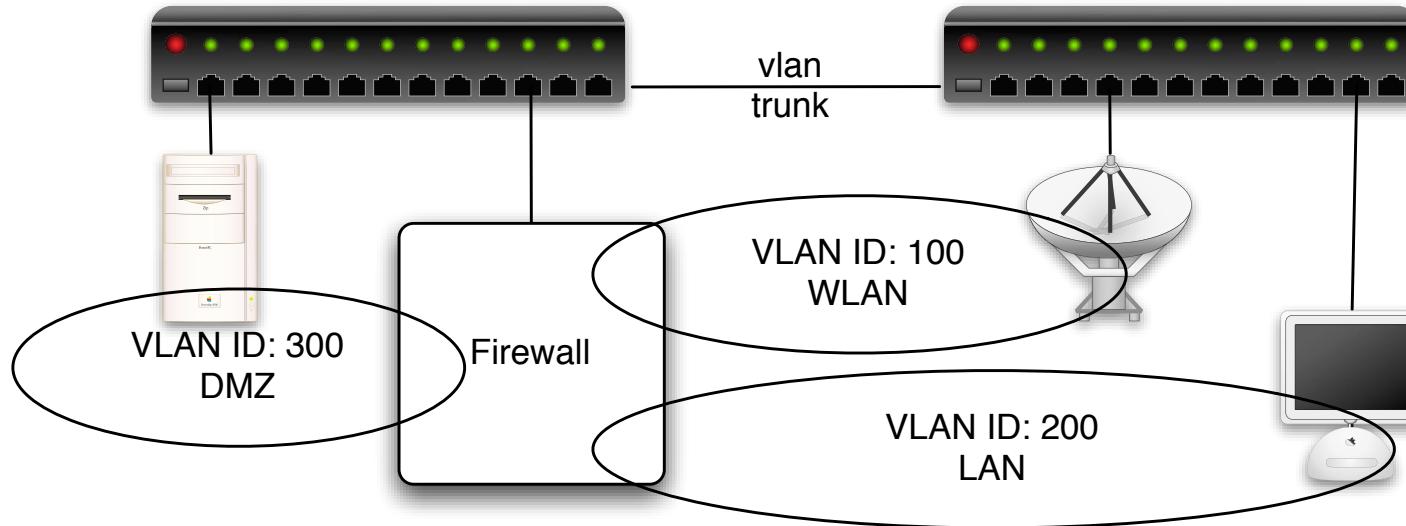
Nogle switcher tillader at man opdeler portene

Denne opdeling kaldes VLAN og portbaseret er det mest simple

Port 1-4 er et LAN

De resterende er et andet LAN

Data skal omkring en firewall eller en router for at krydse fra VLAN1 til VLAN2



Nogle switcher tillader konfiguration med 802.1q VLAN tagging på Ethernet niveau

Data skal omkring en firewall eller en router for at krydse fra VLAN1 til VLAN2

VLAN trunking giver mulighed for at dele VLANs ud på flere switches

Der findes administrationsværktøjer der letter dette arbejde: OpenNAC FreeNAC, Cisco VMPS

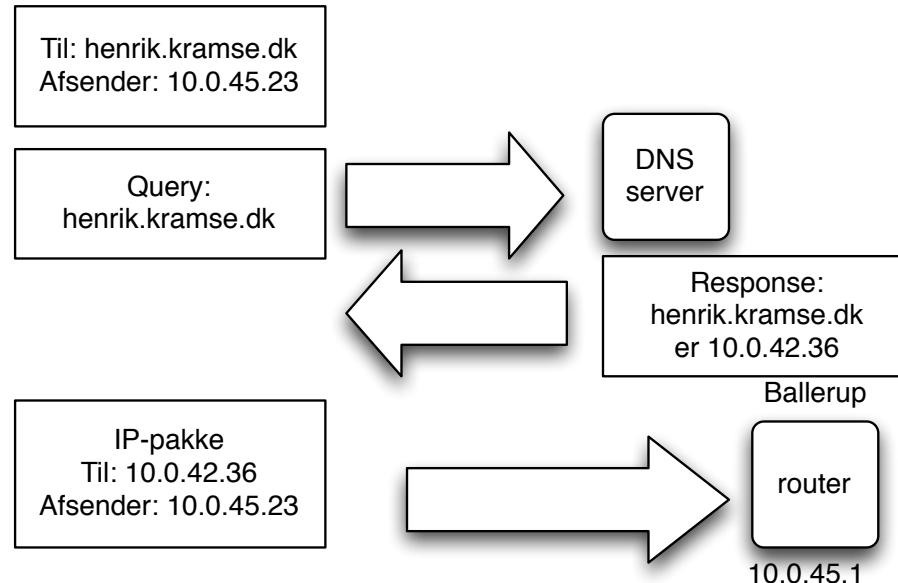


Vi laver nu velsen

10VLAN 802.1qchapter.10

som er velse **10VLAN 802.1qchapter.10** fra velseshftet.

Domain Name System



Gennem DHCP fr man typisk ogs information om DNS servere

En DNS server kan sl navne, domner og adresser op

Foregr via query og response med datatyper kaldet resource records

DNS er en distribueret database, s opslag kan resultere i flere opslag

bestr af resource records med en type:

- adresser A-records
- IPv6 adresser AAAA-records
- autoritative navneservere NS-records
- post, mail-exchanger MX-records
- flere andre: md , mf , cname , soa , mb , mg , mr , null , wks , ptr , hinfo , minfo , mx

ns1	IN	A	217.157.20.130
	IN	AAAA	2001:618:433::1
www	IN	A	217.157.20.131
	IN	AAAA	2001:618:433::14
	IN	MX	10 mail.security6.net.
	IN	MX	20 mail2.security6.net.

Basal DNS opstning p klienter

/etc/resolv.conf

NB: denne fil kan hedde noget andet p Unix varianter!

eksempelvis /etc/netsvc.conf

typisk indhold er domnenavn og IP-adresser for navneservere

```
domain security6.net
nameserver 212.242.40.3
nameserver 212.242.40.51
```

Berkeley Internet Name Daemon server

Mange bruger BIND fra Internet Systems Consortium - alts Open Source
konfigureres gennem named.conf
det anbefales at bruge BIND version 9

- *DNS and BIND*, Paul Albitz & Cricket Liu, O'Reilly, 4th edition Maj 2001
- *DNS and BIND cookbook*, Cricket Liu, O'Reilly, 4th edition Oktober 2002

Kilde: <http://www.isc.org>

BIND konfiguration - et udgangspunkt



```
acl internals { 127.0.0.1; ::1; 10.0.0.0/24; };
options {
    // the random device depends on the OS !
    random-device "/dev/random"; directory "/namedb";
    listen-on-v6 any;
    port 53; version "Dont know"; allow-query { any; };
};

view "internal" {
    match-clients { internals; }; recursion yes;
    zone " ." {
        type hint; file "root.cache"; };
    // localhost forward lookup
    zone "localhost." {
        type master; file "internal/db.localhost";   };
    // localhost reverse lookup from IPv4 address
    zone "0.0.127.in-addr.arpa" {
        type master; file "internal/db.127.0.0"; notify no;   };
    ...
}
```



Vi laver nu velsen

11DNS og navneopslagchapter.11

som er velse **11DNS og navneopslagchapter.11** fra velseshftet.



Vi laver nu velsen

12DNS og navneopslag - IPv6chapter.12

som er velse **12DNS og navneopslag - IPv6chapter.12** fra velseshftet.

Hvordan skal vi kunne huske og administrere servere?

Det er ikke nemt at navngive hverken brugere eller servere!

Selvom det lyder smart med A01S13, som forkortelse af Afdeling 01's Server nr 13, er det umuligt at huske

... men måske nødvendigt i de største netværk

- Windows serveren er domænecontroller - skal hedde:
- Linux server som er terminalserver - skal hedde:
- PC-system med NetBSD skal måske være vores ene server - skal hedde: ?
- PC-system 1 med en Linux server - skal hedde:
- PC-system 2 med en Linux server - skal hedde:

RFC-2142 Mailbox Names for Common Services, Roles and Functions

Du BR konfigurere dit domne til at modtage post for flgende adresser:

- postmaster@domne.dk
- abuse@domne.dk
- webmaster@domne.dk, evt. www@domne.dk

Du gr det nemmere at rapportere problemer med dit netvrk og services

E-mail best current practice

MAILBOX	AREA	USAGE
ABUSE	Customer Relations	Inappropriate public behaviour
NOC	Network Operations	Network infrastructure
SECURITY	Network Security	Security bulletins or queries
...		
MAILBOX	SERVICE	SPECIFICATIONS
POSTMASTER	SMTP	[RFC821], [RFC822]
HOSTMASTER	DNS	[RFC1033-RFC1035]
USENET	NNTP	[RFC977]
NEWS	NNTP	Synonym for USENET
WEBMASTER	HTTP	[RFC 2068]
WWW	HTTP	Synonym for WEBMASTER
UUCP	UUCP	[RFC976]
FTP	FTP	[RFC959]

Kilde: RFC-2142 Mailbox Names for Common Services, Roles and Functions. D. Crocker. May 1997

IP adresserne administreres i dagligdagen af et antal Internet registries, hvor de største er:

- RIPE (Réseaux IP Européens) <http://ripe.net>
- ARIN American Registry for Internet Numbers <http://www.arin.net>
- Asia Pacific Network Information Center <http://www.apnic.net>
- LACNIC (Regional Latin-American and Caribbean IP Address Registry) - Latin America and some Caribbean Islands

disse fire kaldes for Regional Internet Registries (RIRs) i modstning til Local Internet Registries (LIRs) og National Internet Registry (NIR)

NTP opstning

foregår typisk i /etc/ntp.conf eller /etc/ntpd.conf

det vigtigste er navnet på den server man vil bruge som tidskilde

Brug enten en NTP server hos din udbyder eller en fra <http://www.pool.ntp.org/>

Eksempelvis:

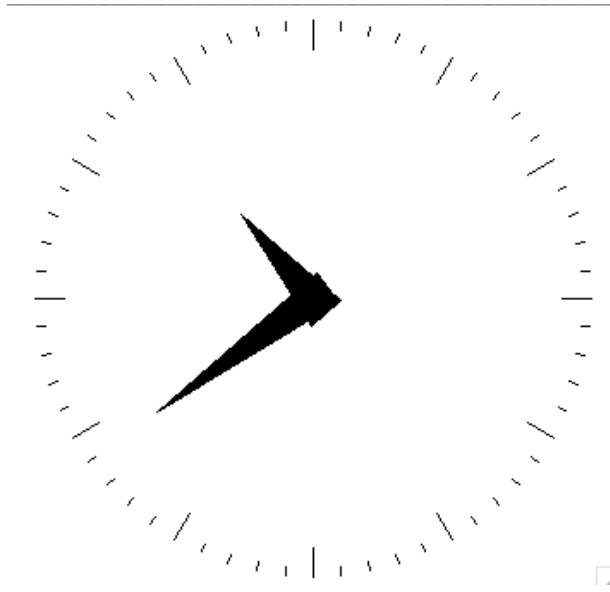
```
server ntp.cybercity.dk
```

```
server 0.dk.pool.ntp.org
```

```
server 0.europe.pool.ntp.org
```

```
server 3.europe.pool.ntp.org
```

What time is it?



Hvad er klokken?

Hvad betydning har det for sikkerheden?

Brug NTP Network Time Protocol p produktionssystemer

What time is it? - sprg ICMP



ICMP timestamp option - request/reply

hvad er klokken p en server

Slayer icmpush - er installeret p server

viser tidstempel

```
# icmpush -v -tstamp 10.0.0.12
```

```
ICMP Timestamp Request packet sent to 10.0.0.12 (10.0.0.12)
```

```
Receiving ICMP replies ...
```

```
fischer          -> 21:27:17
```

```
icmpush: Program finished OK
```

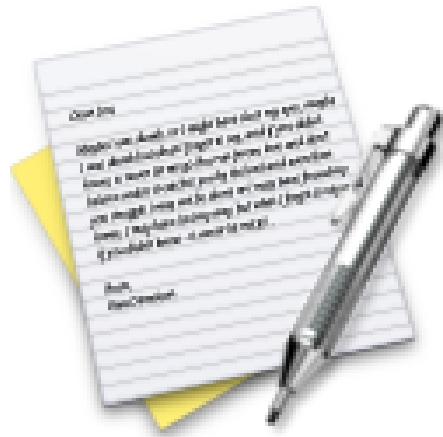
Stop - NTP Konfigurationseksempler



Vi har en masse udstyr, de meste kan NTP, men hvordan

Vi gennemgr, eller I undersger selv:

- Airport
- Switche (managed)
- Mac OS X
- OpenBSD - check `man rdate` og `man ntpd`



Vi laver nu velsen

13Opslag i whois databaserchapter.13

som er velse **13Opslag i whois databaserchapter.13** fra velseshftet.



Vi laver nu velsen

??

som er velse ?? fra velseshftet.



IP har eksisteret mange år

Vi har udskiftet langsomme forbindelser med hurtige forbindelser

Vi har udskiftet langsomme MHz maskiner med Quad-core GHz maskiner

IP var tidligere meget konservativt, for ikke at overbelaste modtageren

Billedet er en HP arbejdsstation med 19" skrm og en 60MHz HP PA-RISC processor

Anbefalet netvrkstuning - hvad skal tunes



Der er visse indstillinger som tidligere var standard, de br idag sls fra

En del er allerede tunet i nyere versioner af IP-stakkene, men check lige

Ideer til ting som skal sls fra:

- broadcast ICMP, undg smurfing
- Source routing, kan mske omg firewalls og filtre

Ideer til ting som skal sls til/ndres:

- Bufferstrrelser - hvorfor have en buffer p 65535 bytes p en maskine med 32GB ram?
- Nye funktioner som RFC-1323 TCP Extensions for High Performance

Det anbefales at finde leverandrens vejledning til hvad der kan tunes

Netvrkskonfiguration med sysctl



```
# tuning
net.inet.tcp.recvspace=65535
net.inet.tcp.sendspace=65535
net.inet.udp.recvspace=65535
net.inet.udp.sendspace=32768
# postgresql tuning
kern.seminfo.semnni=256
kern.seminfo.semnmns=2048
kern.shminfo.shmmax=50331648
```

P mange Unix varianter findes et specielt tuningsprogram, sysctl

Findes blandt andet p alle BSD'erne: FreeBSD, OpenBSD, NetBSD og Darwin/OSX

ndringerne skrives ind i filen /etc/sysctl.conf

P Linux erstatter det til dels konfiguration med echo

```
echo 1 > /proc/net/ip/forwarding
```

P AIX benyttes kommandoen network options no

Hvad er flaskehalsen for programmet?

I/O bundet - en enkelt disk eller flere

CPU bundet - regnekraften

Netvirket - 10Mbit half-duplex adapter

Memory - begynder systemet at *swappe* eller *thrasher*

brug top og andre statistikprogrammer til at se disse data

Mling af throughput



Nr der skal tunes er det altid ndvendigt med en baseline

Man kan ikke begynde at tune ud fra subjektive mlinger

Det krer langsomt, Svartiden er for hj

Mlinger der giver prcise tal er ndvendige, fr og efter mlinger!

Der findes et antal vrktjer til, blandt andet Iperf

Mlinger med Iperf



```
hlk@fluffy:hlk$ iperf -s
-----
Server listening on TCP port 5001
TCP window size: 64.0 KByte (default)
-----
[ 4] local 10.0.42.23 port 5001 connected with 10.0.42.67 port 51148
[ 4] 0.0-10.2 sec 6.95 MBytes 5.71 Mbits/sec
[ 4] local 10.0.42.23 port 5001 connected with 10.0.42.67 port 51149
[ 4] 0.0-10.2 sec 7.02 MBytes 5.76 Mbits/sec
```

Ovenstende er set fra server, client kaldes med iperf -c fluffy

Stop - vi prver i fllesskab Iperf



Vi prver lige Iperf sammen

hvis alle prver samtidig giver det stor variation i resultaterne

Antal pakker per sekund

Til tider er det ikke bndbredden som sdan man vil mle

Specielt for routere er det vigtigt at de kan behandle mange pakker per sekund, pps

Til dette kan man lege med det indbyggede Ping program i flooding mode

Nr programmet kaldes (som systemadministrator) med ping -f server vil den sende ping pakker s hurtigt som netkortet tillader

Programmer der kan teste pakker per sekund kaldes generelt for blaster tools

Apache benchmark og andre programmer



```
hlk@bigfoot:hlk$ ab -n 100 http://www.kramse.dk/
This is ApacheBench, Version 2.0.41-dev <$Revision: 1.121.2.12 $> apache-2.0
Copyright (c) 1996 Adam Twiss, Zeus Technology Ltd, http://www.zeustech.net/
Copyright (c) 2006 The Apache Software Foundation, http://www.apache.org/
```

Benchmarking www.kramse.dk (be patient) ...

...

Der findes specialiserede vrktjer til mange protokoller

Eksempelvis flger der et apache benchmark med Apache HTTPD serveren

Mange andre vrktjer til at simulere flere samtidige brugere

Apache Benchmark output - 1



Server Software: Apache
Server Hostname: www.kramse.dk
Server Port: 80

Document Path: /
Document Length: 7547 bytes

Concurrency Level: 1
Time taken for tests: 13.84924 seconds
Complete requests: 100
Failed requests: 0
Write errors: 0
Total transferred: 778900 bytes
HTML transferred: 754700 bytes
Requests per second: 7.64 #/sec (mean)
Time per request: 130.849 ms (mean)
Time per request: 130.849 ms (mean, across all concurrent requests)
Transfer rate: 58.08 Kbytes/sec received

Apache Benchmark output - 3



Connection Times (ms)

	min	mean	+/-sd	median	max
Connect:	22	24	4.0	24	58
Processing:	96	105	33.0	99	421
Waiting:	63	71	32.7	65	386
Total:	119	130	33.5	124	446

Percentage of the requests served within a certain time (ms)

50%	124
66%	126
75%	128
80%	130
90%	143
95%	153
98%	189
99%	446
100%	446 (longest request)



Vi laver nu velsen

??

som er velse ?? fra velseshftet.



Vi laver nu velsen

16Performance tool - iperfchapter.16

som er velse **16Performance tool - iperfchapter.16** fra velseshftet.



Vi laver nu velsen

?

som er velse ?? fra velseshftet.

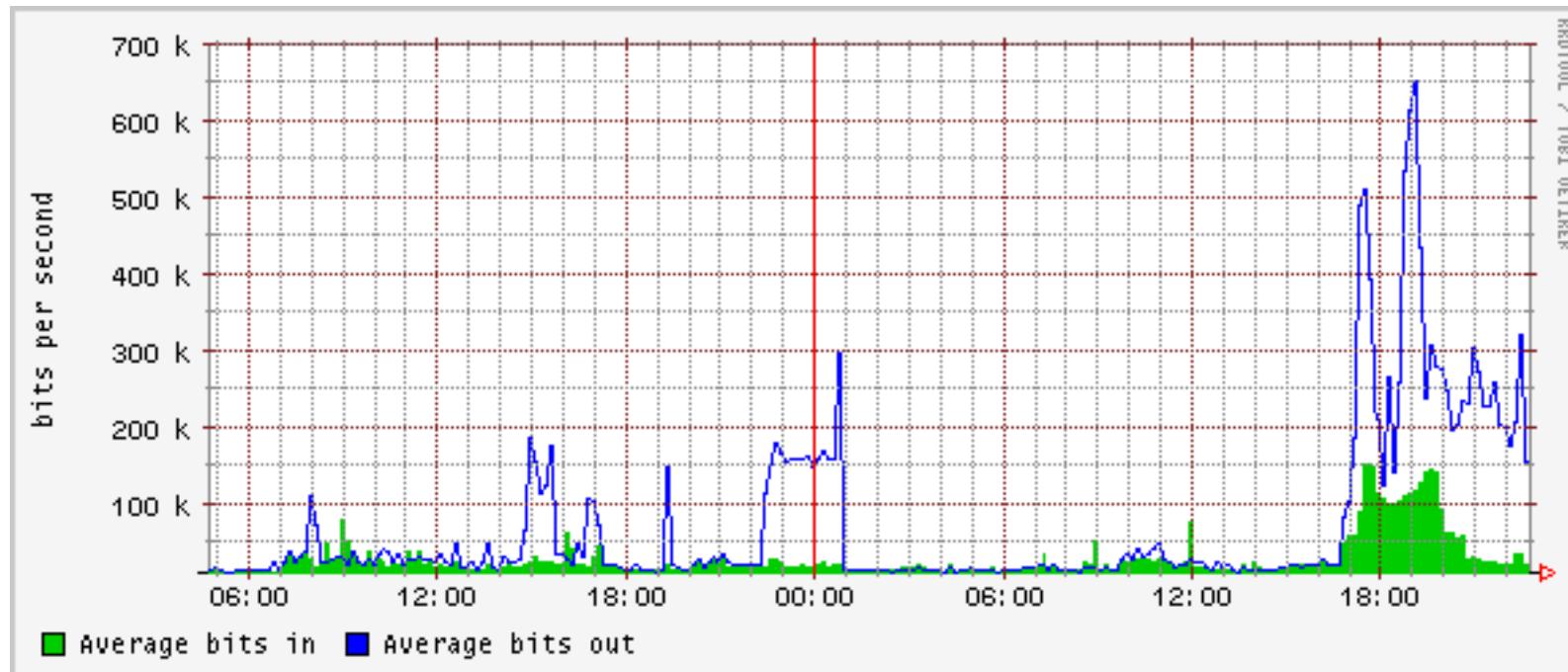
Opsamling p dagens arbejde



Hvad har vi lrt?

Fri leg p udstyret

Agenda - dag 2 Avancerede netvirksteknologier og 802.11



Nu skal vi til management og diagnosticering



Always check the spark plugs!

Nr man skal spore fejl i netvrk er det essentiel at starte fra bunden:

- Er der link?
- Er der IP-adresse?
- Er der route?
- Modtager systemet pakker
- Er der en returvej fra systemet! Den her kan snyde mange!
- Lytter serveren p den port man vil forbinde til, UDP/TCP

Hvis der ikke er link vil man aldrig få svar fra databasen/webserveren/postserveren

De vigtigste kommandoer til udtrk af netvrkskonfigurationen

P Unix:

- cat - til at vise tekstfiler
- ifconfig - interface configuration
- netstat - network statistics
- lsof - list open files

Windows:

- kontrolpanelet
- ipconfig/ipv6

Basale testvirkter TCP - Telnet og OpenSSL



Telnet blev tidligere brugt til login og er en klartekst forbindelse over TCP

Telnet kan bruges til at teste forbindelsen til mange andre serverprotokoller som benytter ASCII kommandoer

- telnet mail.kramse.dk 25 laver en forbindelse til port 25/tcp
- telnet www.kramse.dk 80 laver en forbindelse til port 80/tcp

Til krypterede forbindelser anbefales det at teste med openssl

- openssl s_client -host www.kramse.dk -port 443
laver en forbindelse til port 443/tcp med SSL
- openssl s_client -host mail.kramse.dk -port 993
laver en forbindelse til port 993/tcp med SSL

Med OpenSSL i client-mode kan services tilgs med samme tekstkommandoer som med telnet

UDP er lidt drilsk, for de fleste services er ikke *ASCII protokoller*

Der findes dog en række testprogrammer, a la ping

- nsPing - name server ping
- dhcpping - dhcp server ping
- ...

Derudover kan man bruge de almindelige programmer som host til navneopslag osv.

Logfiler er en ndvendighed for at have et transaktionsspor

Logfiler giver mulighed for statistik

Logfiler er desuden ndvendige for at fejlfinde

Det kan være relevant at sammenholde logfiler fra:

- routere
- firewalls
- webservere
- intrusion detection systemer
- adgangskontrolsystemer
- ...

Husk - tiden er vigtig! Network Time Protocol (NTP) anbefales

Husk at logfilerne typisk kan slettes af en angriber - hvis denne får kontrol med systemet

syslog er system loggen p Unix og den er effektiv

- man kan definere hvad man vil se og hvor man vil have det dirigeret hen
- man kan samle det i en fil eller opdele alt efter programmer og andre kriterier
- man kan ligeledes bruge named pipes - dvs filer i filesystemet som tunneller fra chroot'ed services til syslog i det centrale system!
- man kan nemt sende data til andre systemer

Hvis man vil lave en centraliseret lsning er flgende link vigtigt:

<http://loganalysis.org>

syslogd.conf eksempel

```
*.err;kern.debug;auth.notice;authpriv.none;mail.crit      /dev/console
*.notice;auth,authpriv,cron,ftp,kern,lpr,mail,user.none   /var/log/messages
kern.debug;user.info;syslog.info                           /var/log/messages
auth.info                                                 /var/log/authlog
authpriv.debug                                           /var/log/secure
...
# Uncomment to log to a central host named "loghost".
#*.notice;auth,authpriv,cron,ftp,kern,lpr,mail,user.none   @loghost
#kern.debug,user.info,syslog.info                          @loghost
#auth.info,authpriv.debug,daemon.info                     @loghost
```

Andre syslogs syslog-ng

der findes andre syslog systemer eksempelvis syslog-ng

konfigureres gennem /etc/syslog-nginx/syslog-nginx.conf

Eksempel p indholdet af filen kunne vre:

```
options {  
    long_hostnames(off);  
    sync(0);  
    stats(43200);  
};  
  
source src unix-stream("/dev/log"); internal(); pipe("/proc/kmsg"); ;  
destination messages file("/var/log/messages"); ;  
destination console_all file("/dev/console"); ;  
log source(src); destination(messages); ;  
log source(src); destination(console_all); ;
```



Vi laver nu velsen

18Logning med syslogd og syslog.confchapter.18

som er velse 18Logning med syslogd og syslog.confchapter.18 fra velseshftet.

Logfiler er en ndvendighed for at have et transaktionsspor

Logfiler er desuden ndvendige for at fejlfinde

Det kan være relevant at sammenholde logfiler fra:

- routere
- firewalls
- intrusion detection systemer
- adgangskontrolsystemer
- ...

Husk - tiden er vigtig! Network Time Protocol (NTP) anbefales

Husk at logfilerne typisk kan slettes af en angriber - hvis denne får kontrol med systemet

Simple Network Management Protocol



SNMP er en protokol der supporteres af de fleste professionelle netvrksenheder, ssom switcher, routere

hosts - skal sls til men flger som regel med

SNMP bruges til:

- *network management*
- statistik
- rapportering af fejl - SNMP traps

sikkerheden baseres p community strings der sendes som klartekst ...

det er nemmere at brute-force en community string end en brugerid/kodeord kombination

Simple Network Management Protocol

sikkerheden afhnger alene af en Community string SNMPv2

typisk er den nem at gtte:

- public - default til at aflse statistik
- private - default nr man skal ndre p enheden, skrive
- cisco
- ...

Der findes lister og ordbger p nettet over kendte default communities

kan vre svrt at finde ... det er UDP 161

Hvis man finder en s prv at bruge **snmpwalk** programmet - det kan vise alle tilgngelige SNMP oplysninger fra den pglende host

det kan vre en af mderne at identificere uautoriserede WLAN Access Points p - sweep efter port 161/UDP

snmpwalk er et af de mest brugte programmer til at hente snmp oplysninger - i forbindelse med hackning og penetrationstest

snmpwalk

Typisk brug er:

```
snmpwalk -v 1 -c secret switch1
```

```
snmpwalk -v 2c -c secret switch1
```

Eventuelt bruges **snmpget** og **snmpset**

Ovenstende er en del af Net-SNMP pakken

<http://net-snmp.sourceforge.net/>



Vi laver nu velsen

17SNMP walkchapter.17

som er velse **17SNMP walkchapter.17** fra velseshftet.

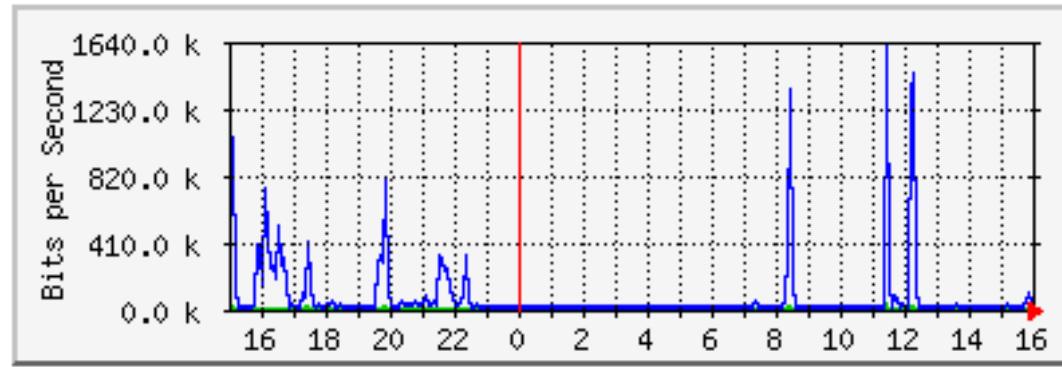
Eksempler p SNMP og management



Ofte foregr administration af netvrksenheder via HTTP, Telnet eller SSH

- sm dumme enheder er idag ofte web-enablet
- bedre enheder giver bde HTTP og kommandolinieadgang
- de bedste giver mulighed for SSH, fremfor Telnet

'Daglig' graf (5 minuts Middel)



	Max	Middel	Nu
Ind	35.5 kb/s (0.0%)	2392.0 b/s (0.0%)	5280.0 b/s (0.0%)
Ud	1604.6 kb/s (1.6%)	57.6 kb/s (0.1%)	51.4 kb/s (0.1%)

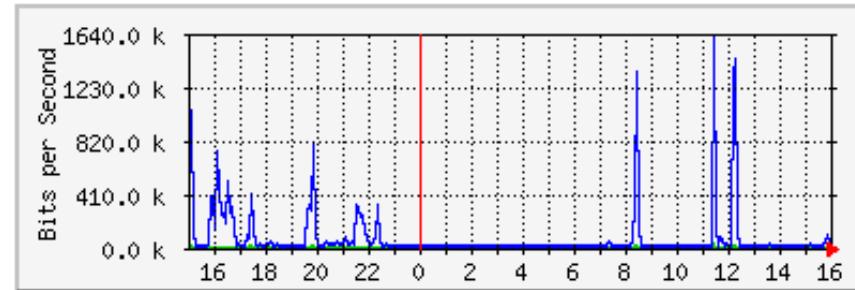
Monitorering af SNMP enheder og grafer

Inkluderer en nem configmaker og benytter idag RRDTool til data

Hjemmesiden: <http://oss.oetiker.ch/mrtg/>

RRDTool Round Robin Database Tool

'Daglig' graf (5 minuts Middel)



Round Robin Database Tool er en mde at gemme data p

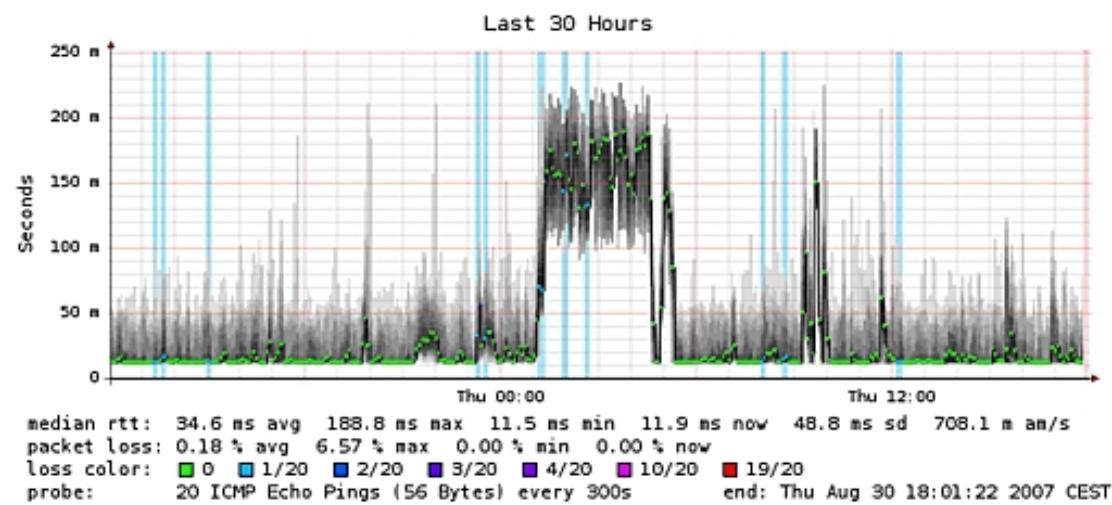
Med RRDTool kan man derefter f lavet grafer

Typisk bruger man et andet vrktj som benytter RRDTool til data

<http://oss.oetiker.ch/rrdtool/doc/index.en.html>

Kan bruges til temperaturmlinger og alt muligt andet

Smokeping



Mling af latency for netvrksservice

Understtter et stort antal prober: ICMP, DNS, HTTP, LDAP, SMTP, ...

Min SmokePing server <http://pumba.kramse.dk/smokeping/>

Hjemmesiden for SmokePing <http://oss.oetiker.ch/smokeping/>

Lavet af Tobias Oetiker og Niko Tyni

Overvgningsvrktj der giver godt overblik

- Monitoring af diverse services (SMTP, POP3, HTTP, NNTP, PING, etc.)
- Monitoring af host resources (processor load, disk and memory usage, running processes, log files, etc.)
- Monitoring af andre ressourcer som temperatur
- Simpel plugin design som gr det nemt at udvide
- Kan sende e-mail, SMS m.v.

Benyttes mange steder

Hjemmesiden for Nagios <http://www.nagios.org/>

Stop - overvgningsvrktjer



Brug lidt tid p at se p vores netvrk

Valgfrit om I vil se p Administrationsinterface p switcher

eller SNMP indstillinger eksempelvis

eller Nagios og SmokePing p mine servere

Sm DNS tools bind-version - Shell script



```
#!/bin/sh
# Try to get version info from BIND server
PROGRAM=`basename $0`
. `dirname $0`/functions.sh
if [ $# -ne 1 ]; then
    echo "get name server version, need a target! "
    echo "Usage: $0 target"
    echo "example $0 10.1.2.3"
    exit 0
fi
TARGET=$1
# using dig
start_time
dig @$1 version.bind chaos txt
echo Authors BIND er i versionerne 9.1 og 9.2 - mske ...
dig @$1 authors.bind chaos txt
stop_time
```

<http://www.kramse.dk/files/tools/dns/bind-version>

Sm DNS tools dns-timecheck - Perl script



```
#!/usr/bin/perl
# modified from original by Henrik Kramshj, hlk@kramse.dk
# 2004-08-19
#
# Original from: http://www.rfc.se/fpdns/timecheck.html
use Net::DNS;

my $resolver = Net::DNS::Resolver->new;
$resolver->nameservers($ARGV[0]);

my $query = Net::DNS::Packet->new;
$query->sign_tsig("n","test");

my $response = $resolver->send($query);
foreach my $rr ($response->additional)
    print "localtime vs nameserver $ARGV[0] time difference: ";
    print $rr->time_signed - time() if $rr->type eq "TSIG";
```

<http://www.kramse.dk/files/tools/dns/dns-timecheck>



Vi laver nu velsen

?

som er velse ?? fra velseshftet.

802.11 er arbejdsgruppen under IEEE

De mest kendte standarder idag indenfor trdlse teknologier:

- 802.11b 11Mbps versionen
- 802.11g 54Mbps versionen
- 802.11n endnu hurtigere, og draft
- 802.11i Security enhancements

Der er proprietære versioner 22Mbps og den slags

- det anbefales IKKE at benytte disse da det giver vendor lock-in - man bliver fast

Kilde: <http://grouper.ieee.org/groups/802/11/index.html>

802.11 modes og frekvenser



Access point krer typisk i *access point mode* ogs kaldet infrastructure mode - al trafik gr via AP

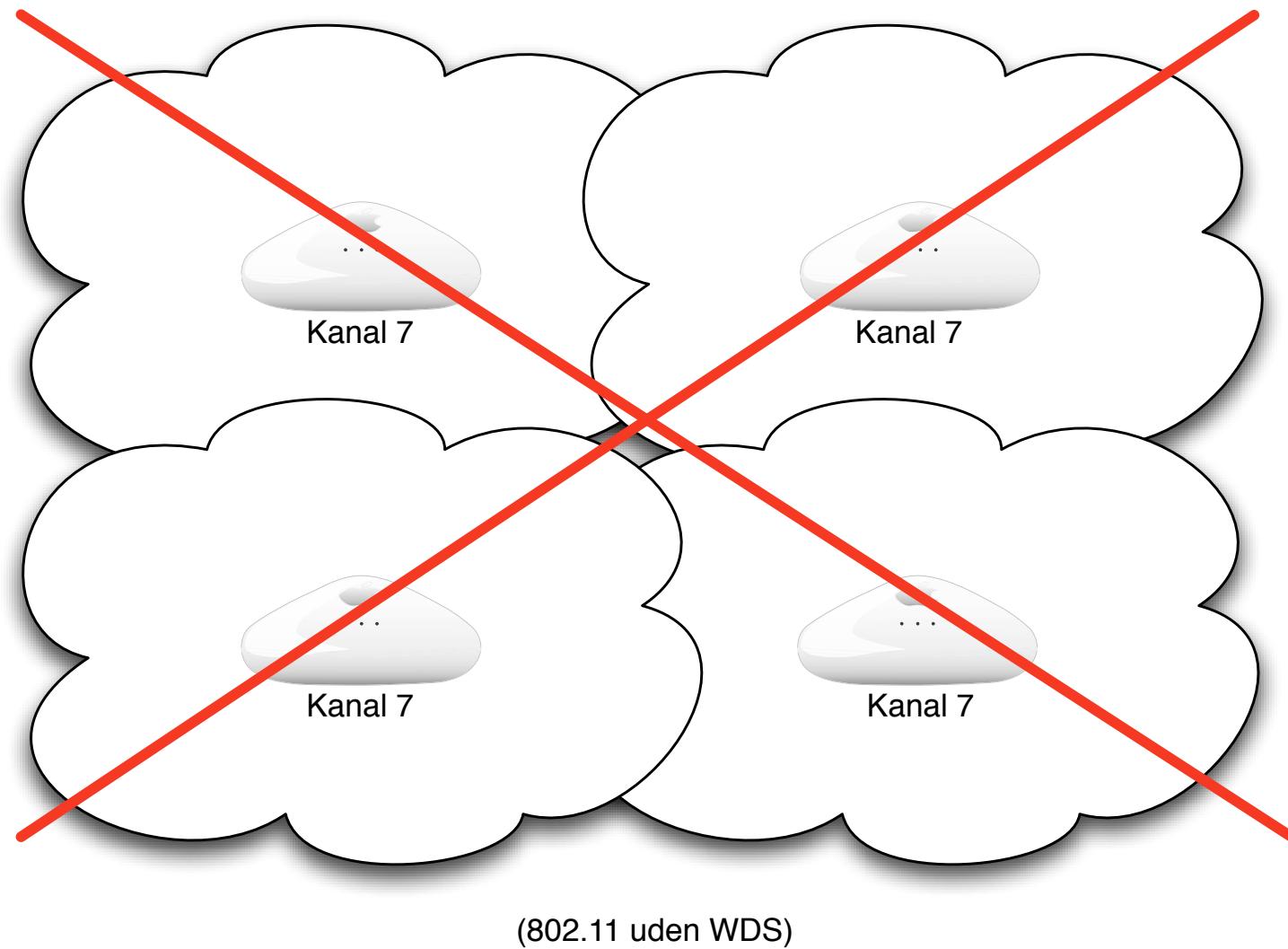
Alternativt kan wireless kort oprette ad-hoc netvrk - hvor trafikken gr direkte mellem netkort

Frekvenser op til kanal 11 og 12+13 i DK/EU

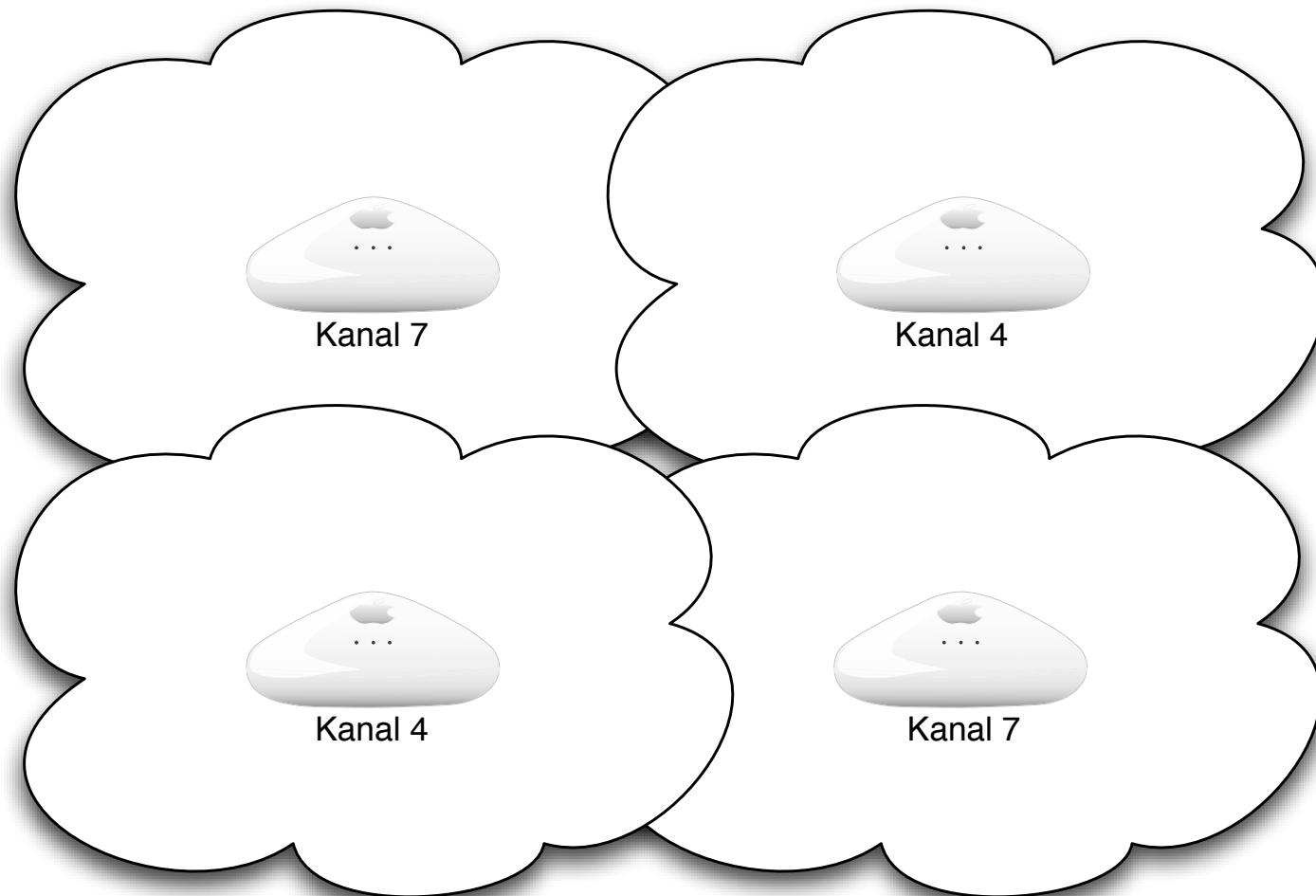
Høgst 2 kanaler spring for 802.11b AP der placeres indenfor rkkevidde

Høgst 4 kanaler spring for 802.11g AP der placeres indenfor rkkevidde

Eksempel p netvrk med flere AP'er

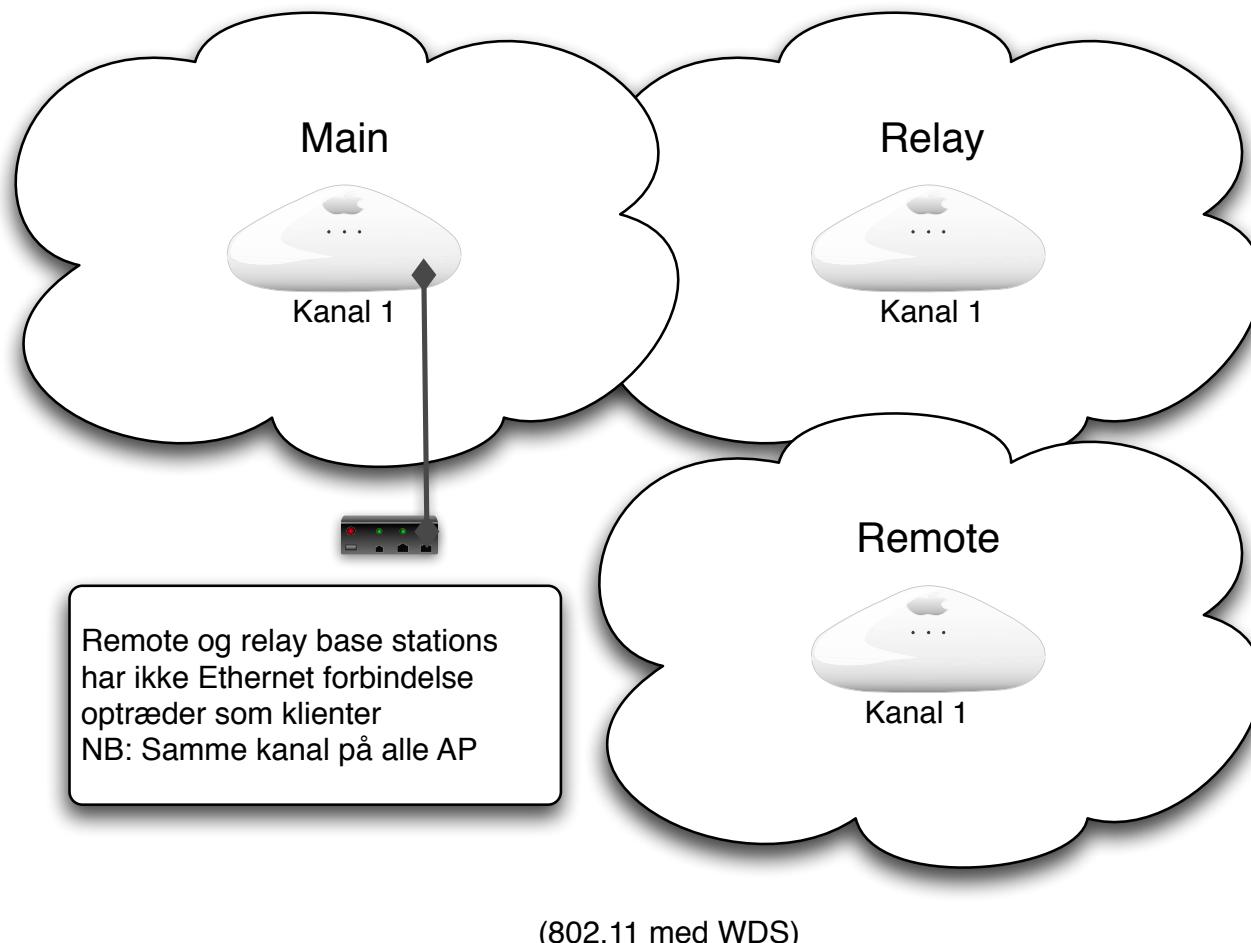


Eksempel p netvrk med flere AP'er



(802.11 uden WDS)

Wireless Distribution System WDS



Se også: http://en.wikipedia.org/wiki/Wireless_Distribution_System

Er trdlse netvrk interessante?

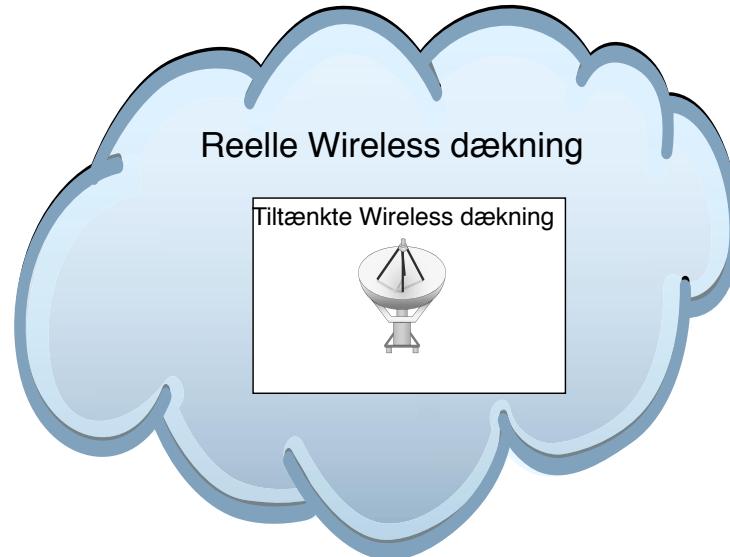


Sikkerhedsproblemer i de trdlse netvrk er mange

- Fra lavt niveau - eksempelvis ARP, 802.11
- drlige sikringsmekanismer - WEP
- drligt udstyr - mange fejl
- usikkherhed om implementering og overvgning

Trdlst udstyr er blevet meget billigt!

Det er et krav fra brugerne - trdlst er lkkert



- Vrre end Internetangreb - anonymt
- Krver ikke fysisk adgang til lokationer
- Konsekvenserne ved sikkerhedsbrud er generelt strre
- Typisk fr man direkte LAN eller Internet adgang!

Laptop gerne med PC-CARD slot

Trdlse kort Atheros chipset anbefales, de indbyggede er til tider ringe ;-)

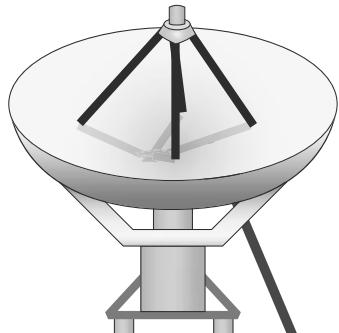
Access Points - jeg anbefaler Airport Express

Antenner hvis man har lyst

Bger: *Real 802.11 security*

Internetressourcer:

- BackTrack - CD image med Linux+vrktjer
- Packetstorm wireless tools <http://packetstormsecurity.org/wireless/>
- *Beginner's Guide to Wireless Auditing* David Maynor
<http://www.securityfocus.com/infocus/1877?ref=rss>
- Aircrack-ng suite af programmer <http://www.aircrack-ng.org/>



Wireless Access Point

netværket - typisk Ethernet

et access point - forbindes til netværket

Nr man tager fat p udstyr til trdlse netvrk opdager man:

SSID - nettet skal have et navn

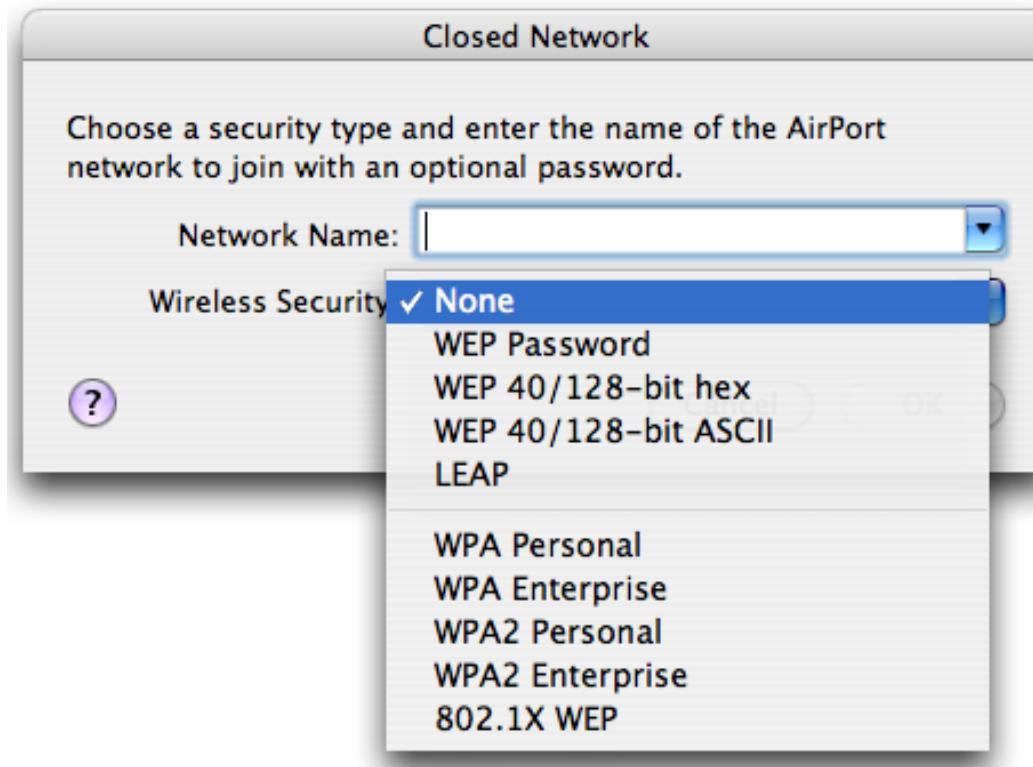
frekvens / kanal - man skal vlge en kanal, eller udstyret vlger en automatisk
der er nogle forskellige metoder til sikkerhed



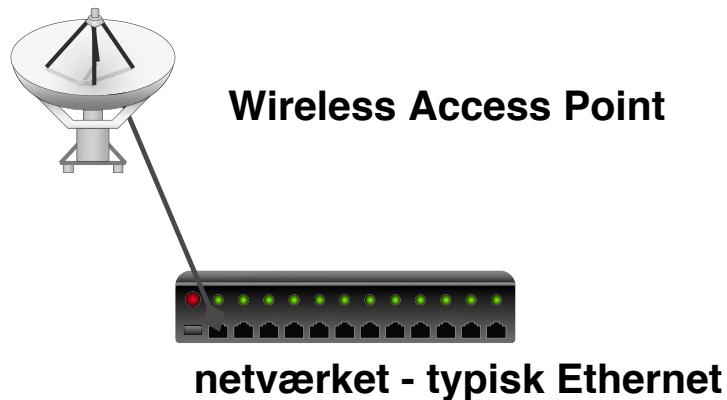
Vi laver nu velsen

19AirPort Extremechapter.19

som er velse **19AirPort Extremechapter.19** fra velseshftet.



- Trdls sikkerhed - WPA og WPA2
- Nem konfiguration
- Nem konfiguration af Access Point



Sikkerheden er baseret på nogle få forudsætninger

- SSID - netnavnet
- WEP kryptering - Wired Equivalent Privacy
- mætte MAC filtrering, kun bestemte kort må tilgå accesspoint

Til gengæld er disse forudsætninger ofte ikke tilstrækkelige ...

- WEP er mætte *ok* til visse små hjemmenetværk
- WEP er baseret på en DELT hemmelighed som alle stationer kender
- Den endres sjældent, og det er svært at distribuere en ny

Til gengld er disse forudstninger ofte ikke tilstrækkelige ...

Hvad skal man beskytte?

Hvordan kan sikkerheden omgs?

Mange firmaer og virksomheder stille forskellige krav til sikkerheden - der er ikke en sikkerhedsmekanisme der passer til alle

Service Set Identifier (SSID) - netnavnet

32 ASCII tegn eller 64 hexadecimale cifre

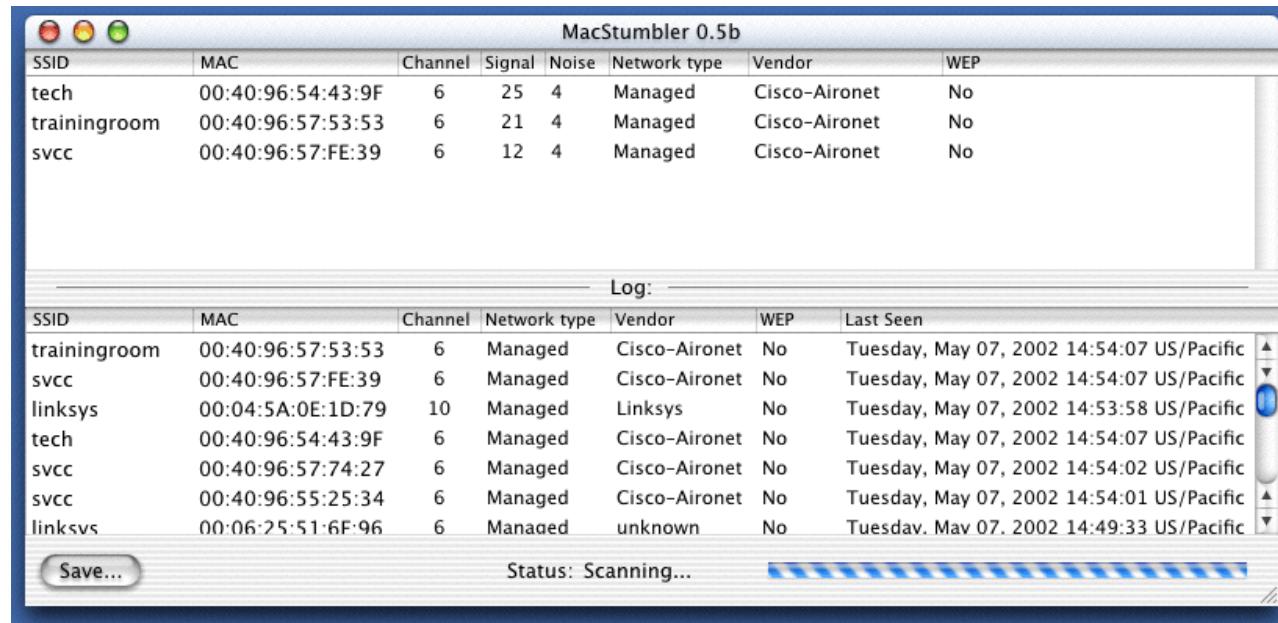
Udstyr leveres typisk med et standard netnavn

- Cisco - tsunami
- Linksys udstyr - linksys
- Apple Airport, 3Com m.fl. - det er nemt at genkende dem

SSID kaldes også for NWID - network id

SSID broadcast - udstyr leveres oftest med broadcast af SSID

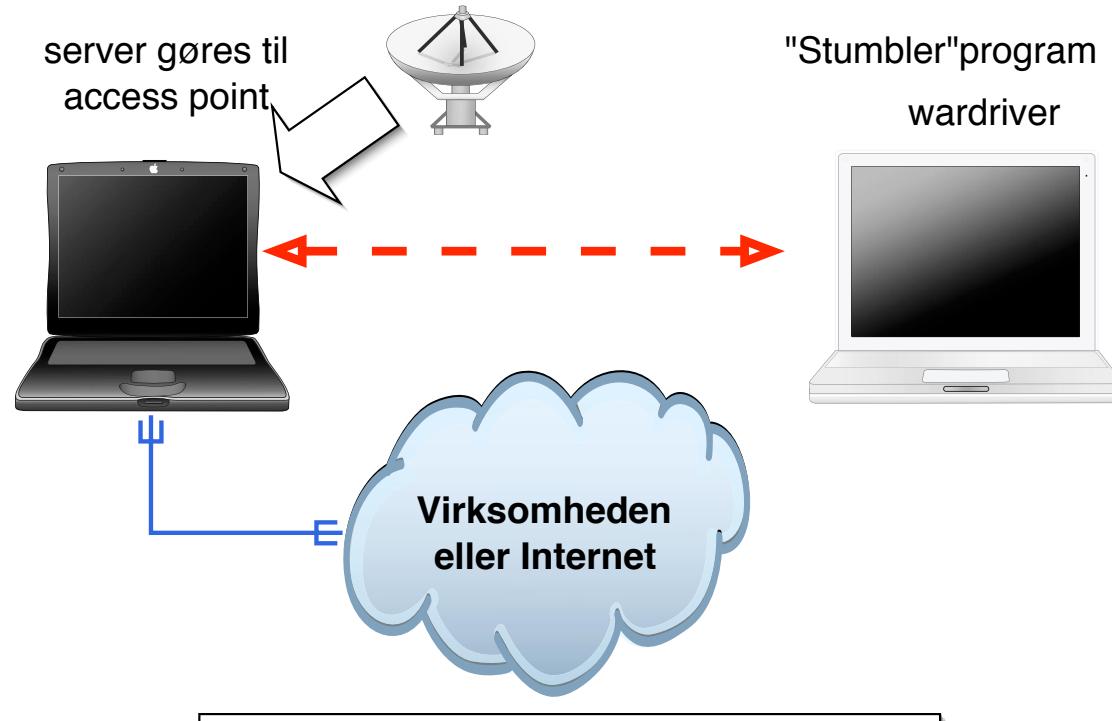
Demo: wardriving med stumbler programmer



man tager et trdlst netkort og en brbar computer og noget software:

- Netstumbler - Windows <http://www.netstumbler.com>
- dstumbler - UNIX <http://www.dachboden.com/projects/dstumbler.html>
- iStumbler - Mac <http://www.istumbler.net/>
- Kismet ... mange andre

Start p demo - wardriving



- Almindelige laptops bruges til demo
- Der startes et *access point*

De fleste netkort tillader at man udskifter sin MAC adresse

MAC adressen p kortene er med i alle pakker der sendes

MAC adressen er aldrig krypteret, for hvordan skulle pakken s n frem?

MAC adressen kan derfor overtages, nr en af de tilladte stationer forlader området ...

Hvad opdager man ved wardriving?

- at WEP IKKE krypterer hele pakken
- at alle pakker indeholder MAC adressen
- WEP ngen skifter sjldent
- ca. 2/3 af de netvrk man finder har ikke WEP slet til - og der er fri og uhindret adgang til Internet

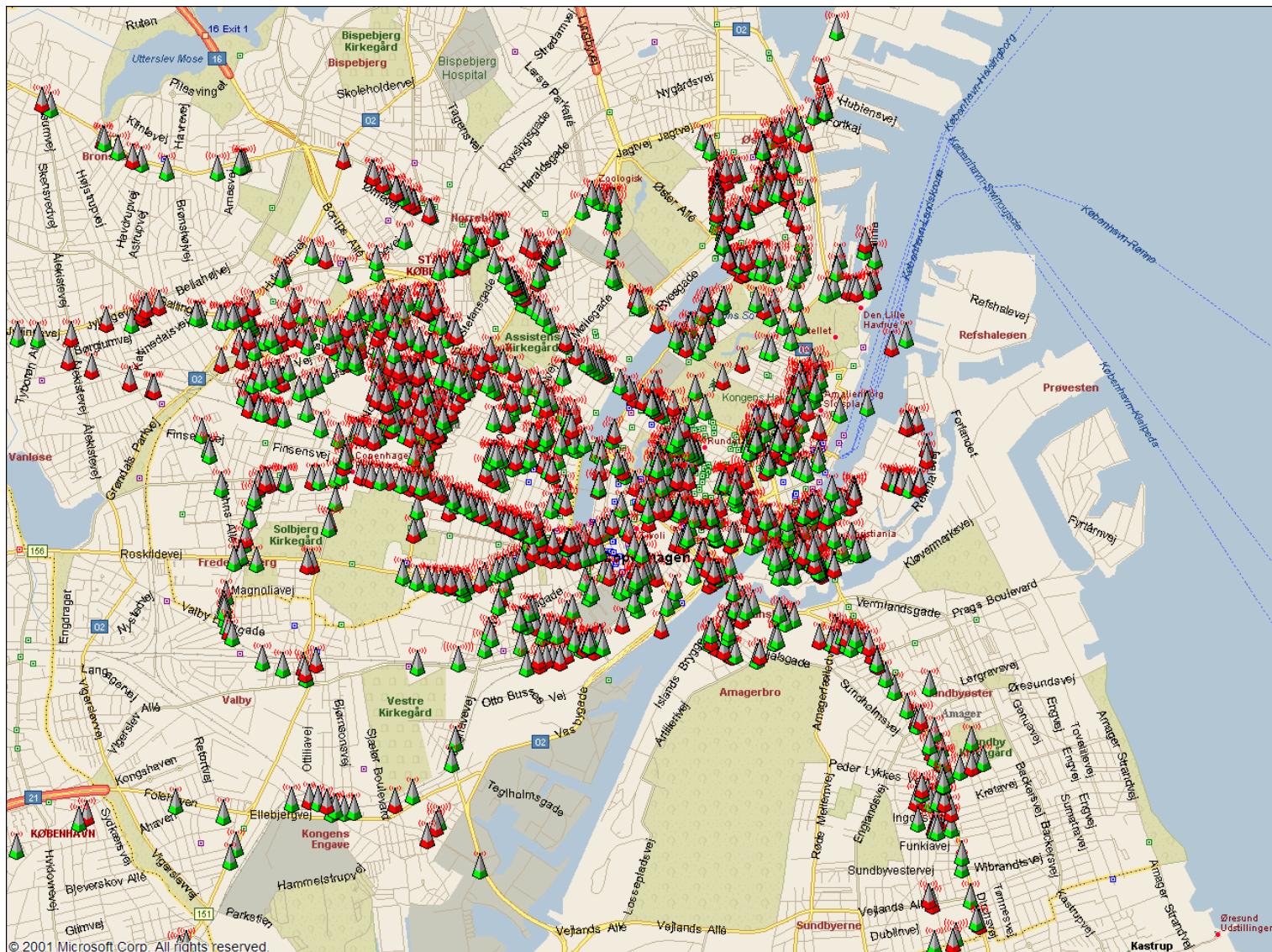
Man kan alts lytte med p et netvrk med WEP, genbruge en anden maskines MAC adresse - og mske endda bryde WEP krypteringen.

Medmindre man kender virksomheden og WEP ngen ikke er skiftet ... det er besvrligt at skifte den, idet alle stationer skal opdateres.

Storkbenhavn



- Security





Vi laver nu velsen

??

som er velse ?? fra velseshftet.



Vi laver nu velsen

?

som er velse ?? fra velseshftet.

Det vi har udført er informationsindsamling

Indsamlingen kan være aktiv eller passiv i forhold til målet for angrebet
passiv kunne være at lytte med på trafik eller se i databaser på Internet
aktiv indsamling er eksempelvis at sende ICMP pakker og registrere hvad man får af svar

WEP *kryptering* - med nøgler der specificeres som tekst eller hexadecimale cifre typisk 40-bit, svarende til 5 ASCII tegn eller 10 hexadecimale cifre eller 104-bit 13 ASCII tegn eller 26 hexadecimale cifre

WEP er baseret på RC4 algoritmen der er en *stream cipher* lavet af Ron Rivest for RSA Data Security

De frste fejl ved WEP



Oprindeligt en drlig implementation i mange Access Points

Fejl i krypteringen - rettet i nyere firmware

WEP er baseret p en DELT hemmelighed som alle stationer kender

Nglen ndres sjldent, og det er svrt at distribuere en ny



AirSnort Homepage



AirSnort is a wireless LAN (WLAN) tool which recovers encryption keys. AirSnort operates by passively monitoring transmissions, computing the encryption key when enough packets have been gathered.

802.11b, using the Wired Equivalent Protocol (WEP), is crippled with numerous security flaws. Most damning of these is the weakness described in "Weaknesses in the Key Scheduling Algorithm of RC4" by Scott Fluhrer, Itsik Mantin and Adi Shamir. Adam Stubblefield was the first to implement this attack, but he has not made his software public. AirSnort, along with WEPCrack, which was released about the same time as AirSnort, are the first publicly available implementations of this attack. <http://airsnort.shmoo.com/>

major cryptographic errors



weak keying - 24 bit er allerede kendt - $128\text{-bit} = 104\text{ bit}$ i praksis

small IV - med kun 24 bit vil hver IV blive genbrugt oftere

CRC-32 som integritetscheck er ikke *strkt* nok kryptografisk set

Authentication gives pad - giver fuld adgang - hvis der bare opdages *encryption pad* for en bestemt IV. Denne IV kan så bruges til al fremtidig kommunikation

Konklusion: Kryptografi er svrt

WEP cracking - airodump og aircrack



airodump - opsamling af krypterede pakker

aircrack - statistisk analyse og forsøg på at finde WEP nøglen

Med disse værktøjer er det muligt at knække *128-bit nøgler!*

Blandt andet fordi det reelt er 104-bit nøgler ☺

tommelfingerregel - der skal opsamles mange pakker ca. 100.000 er godt

Links:

<http://www.cr0.net:8040/code/network/aircrack/> aircrack

<http://www.securityfocus.com/infocus/1814> WEP: Dead Again

airodump afvikling



Nr airodump krer opsamles pakkerne
samtidig vises antal initialisationsvektorer IV's:

BSSID	CH	MB	ENC	PWR	Packets	LAN IP / # IVs	ESSID
00:03:93:ED:DD:8D	6	11		209	801963	540180	wanlan

NB: dataopsamlingen er foretaget p 100% opdateret Mac udstyr

aircrack - WEP cracker



```
$ aircrack -n 128 -f 2 aftendump-128.cap
                           aircrack 2.1
* Got 540196! unique IVs | fudge factor = 2
* Elapsed time [00:00:22] | tried 12 keys at 32 k/m
KB      depth    votes
 0      0/   1    CE( 45) A1( 20) 7E( 15) 98( 15) 72( 12) 82( 12)
 1      0/   2    62( 43) 1D( 24) 29( 15) 67( 13) 94( 13) F7( 13)
 2      0/   1    B6( 499) E7( 18) 8F( 15) 14( 13) 1D( 12) E5( 10)
 3      0/   1    4E( 157) EE( 40) 29( 39) 15( 30) 7D( 28) 61( 20)
 4      0/   1    93( 136) B1( 28) 0C( 15) 28( 15) 76( 15) D6( 15)
 5      0/   2    E1( 75) CC( 45) 39( 31) 3B( 30) 4F( 16) 49( 13)
 6      0/   2    3B( 65) 51( 42) 2D( 24) 14( 21) 5E( 15) FC( 15)
 7      0/   2    6A( 144) 0C( 96) CF( 34) 14( 33) 16( 33) 18( 27)
 8      0/   1    3A( 152) 73( 41) 97( 35) 57( 28) 5A( 27) 9D( 27)
 9      0/   1    F1( 93) 2D( 45) 51( 29) 57( 27) 59( 27) 16( 26)
10     2/   3    5B( 40) 53( 30) 59( 24) 2D( 15) 67( 15) 71( 12)
11     0/   2    F5( 53) C6( 51) F0( 21) FB( 21) 17( 15) 77( 15)
12     0/   2    E6( 88) F7( 81) D3( 36) E2( 32) E1( 29) D8( 27)
```

KEY FOUND! [CE62B64E93E13B6A3AF15BF5E6]

Hvor lang tid tager det?



Opsamling a data - ca. en halv time p 802.11b ved optimale forhold

Tiden for krsel af aircrack fra auditor CD p en Dell CPi 366MHz Pentium II laptop:

```
$ time aircrack -n 128 -f 2 aftendump-128.cap
...
real      5m44.180s    user     0m5.902s    sys     1m42.745s
```

Tiden for krsel af aircrack p en moderne 1.6GHz CPU med almindelig laptop disk tager typisk mindre end 60 sekunder



Vi laver nu velsen

??

som er velse ?? fra velseshftet.

Erstatning for WEP- WPA



Det anbefales at bruge:

Kendte VPN teknologier eller WPA

baseret på trovrdige algoritmer

implementeret i professionelt udstyr

fra trovrdige leverandører

udstyr der vedligeholdes og opdateres

Man kan måske endda bruge de eksisterende løsninger - fra hjemmepc adgang, mobil
adgang m.v.

Der findes idag andre metoder til sikring af trdlse netvrk

802.1x Port Based Network Access Control

WPA - Wi-Fi Protected Access)

WPA = 802.1X + EAP + TKIP + MIC

nu WPA2 som krver CCMP

WPA2 is based on the final IEEE 802.11i amendment to the 802.11 standard and is eligible for FIPS 140-2 compliance.

Kilde: <http://www.wifialliance.org/OpenSection/protectedaccess.aspx>

WPA eller WPA2?

WPA2 is based upon the Institute for Electrical and Electronics Engineers (IEEE) 802.11i amendment to the 802.11 standard, which was ratified on July 29, 2004.

Q: How are WPA and WPA2 similar?

A: Both WPA and WPA2 offer a high level of assurance for end-users and network administrators that their data will remain private and access to their network restricted to authorized users. Both utilize 802.1X and Extensible Authentication Protocol (EAP) for authentication. Both have Personal and Enterprise modes of operation that meet the distinct needs of the two different consumer and enterprise market segments.

Q: How are WPA and WPA2 different?

A: WPA2 provides a **stronger encryption mechanism** through **Advanced Encryption Standard (AES)**, which is a requirement for some corporate and government users.

Kilde: <http://www.wifialliance.org> WPA2 Q and A

WPA Personal eller Enterprise



Personal - en delt hemmelighed, preshared key kaldes WPA-PSK

Enterprise - brugere valideres op mod filles server

Hvorfor er det bedre?

- Flere valgmuligheder - passer til store og sm
 - WPA skifter den faktiske krypteringsngle jvnligt - TKIP
 - Initialisationsvektoren (IV) fordobles 24 til 48 bit
 - Imdekommer alle kendte problemer med WEP!
 - Integrerer godt med andre teknologier - RADIUS
-
- EAP - Extensible Authentication Protocol - individuel autentifikation
 - TKIP - Temporal Key Integrity Protocol - ngleskift og integritet
 - MIC - Message Integrity Code - Michael, ny algoritme til integritet
 - CCMP - Counter-Mode/CBC-MAC Protocol, IEEE 802.11i AES kryptering
 - CBC-MAC - Cipher Block Chaining - Message Authentication Code
 - AES - Advanced Encryption Standard, Rijndael algoritmen
 - RSN - Robust Secure Network, en del af IEEE 802.11i

WPA-PSK cracking



Nu skifter vi s til WPA og alt er vel s godt? ■

Desvrre ikke!

Du skal vlge en laaaaang passphrase, ellers kan man sniffe WPA handshake nr en computer gr ind p netvrket!

Med et handshake kan man med aircrack igen lave off-line bruteforce angreb!

WPA-PSK cracking demo



Vi konfigurerer AP med Henrik42 som WPA-PSK/passphrase

Vi finder netvirk kismet eller airodump

Vi starter airodump mod specifik kanal

Vi spoofer deauth og opsamler WPA handshake

Vi knkker WPA :-)

Brug manualsiderne for programmerne i aircrack-ng pakken!

WPA-PSK cracking med aircrack - start



```
slax ~ # aircrack-ng -w dict wlan-test.cap
Opening wlan-test.cap
Read 1082 packets.
```

#	BSSID	ESSID	Encryption
1	00:11:24:0C:DF:97	wlan	WPA (1 handshake)
2	00:13:5F:26:68:D0	Noea	No data - WEP or WPA
3	00:13:5F:26:64:80	Noea	No data - WEP or WPA
4	00:00:00:00:00:00		Unknown

Index number of target network ? **1**

WPA cracking med aircrack - start



```
[00:00:00] 0 keys tested (0.00 k/s)
```

```
KEY FOUND! [ Henrik42 ]
```

```
Master Key      : 8E 61 AB A2 C5 25 4D 3F 4B 33 E6 AD 2D 55 6F 76
                  6E 88 AC DA EF A3 DE 30 AF D8 99 DB F5 8F 4D BD
```

```
Transient Key   : C5 BB 27 DE EA 34 8F E4 81 E7 AA 52 C7 B4 F4 56
                  F2 FC 30 B4 66 99 26 35 08 52 98 26 AE 49 5E D7
                  9F 28 98 AF 02 CA 29 8A 53 11 EB 24 0C B0 1A 0D
                  64 75 72 BF 8D AA 17 8B 9D 94 A9 31 DC FB 0C ED
```

```
EAPOL HMAC     : 27 4E 6D 90 55 8F 0C EB E1 AE C8 93 E6 AC A5 1F
```

Min Thinkpad X31 med 1.6GHz Pentium M knkker ca. 150 Keys/sekund

Pyrit takes a step ahead in attacking WPA-PSK and WPA2-PSK, the protocol that today de-facto protects public WIFI-airspace. The project's goal is to estimate the real-world security provided by these protocols. Pyrit does not provide binary files or wordlists and does not encourage anyone to participate or engage in any harmful activity. **This is a research project, not a cracking tool.**

Pyrit's implementation allows to create massive databases, pre-computing part of the WPA/WPA2-PSK authentication phase in a space-time-tradeoff. The performance gain for real-world-attacks is in the range of three orders of magnitude which urges for re-consideration of the protocol's security. Exploiting the computational power of GPUs, *Pyrit* is currently by far the most powerful attack against one of the world's most used security-protocols.

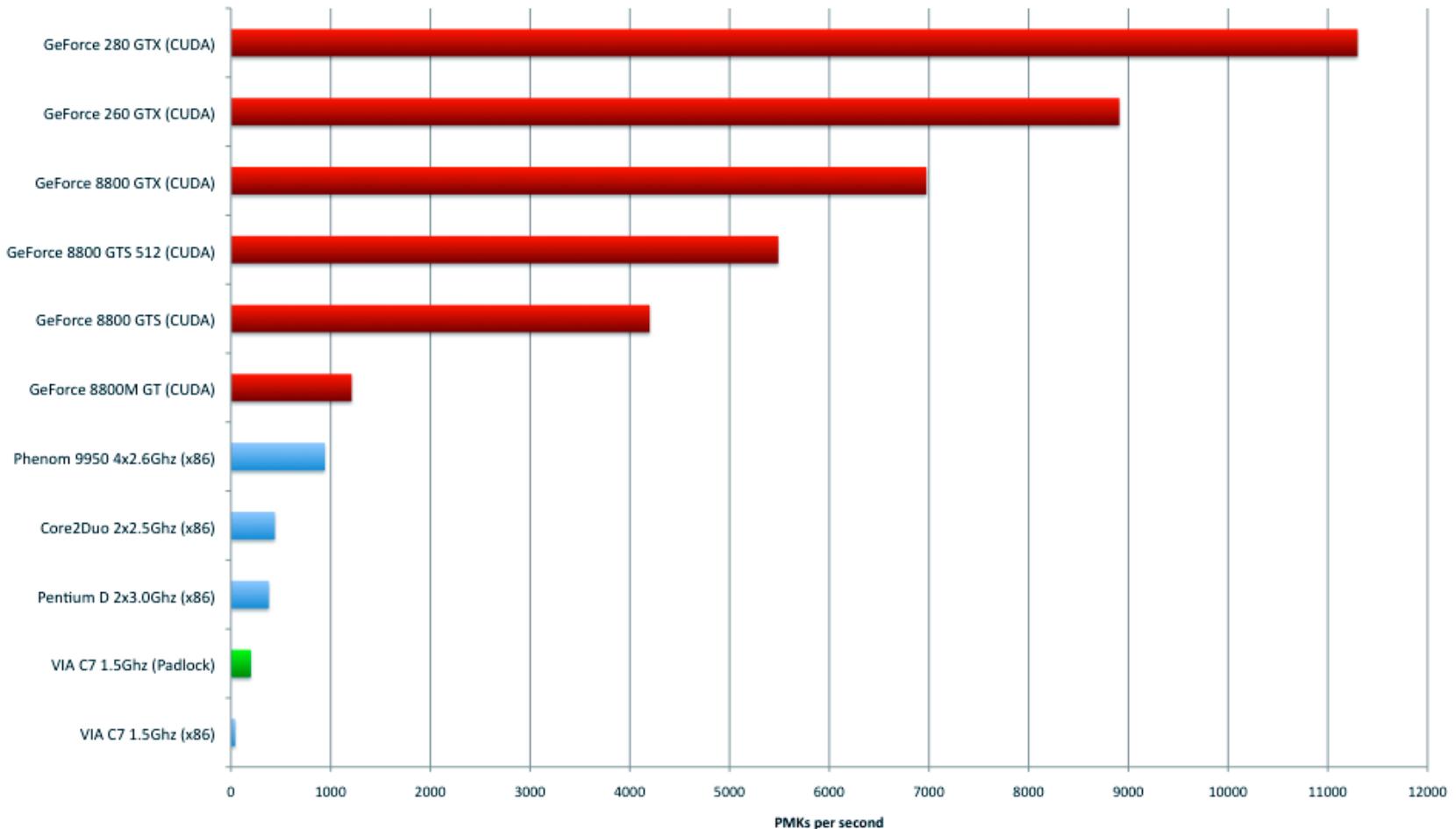
sloooow, plejede det at vre - 150 keys/s p min Thinkpad X31

Kryptering afhnger af SSID! S check i tabellen er minutter.

<http://pyrit.wordpress.com/about/>

Tired of WoW?

Pyrit performing on different platforms - Computed PMKs per second



Kilde: <http://code.google.com/p/pyrit/>

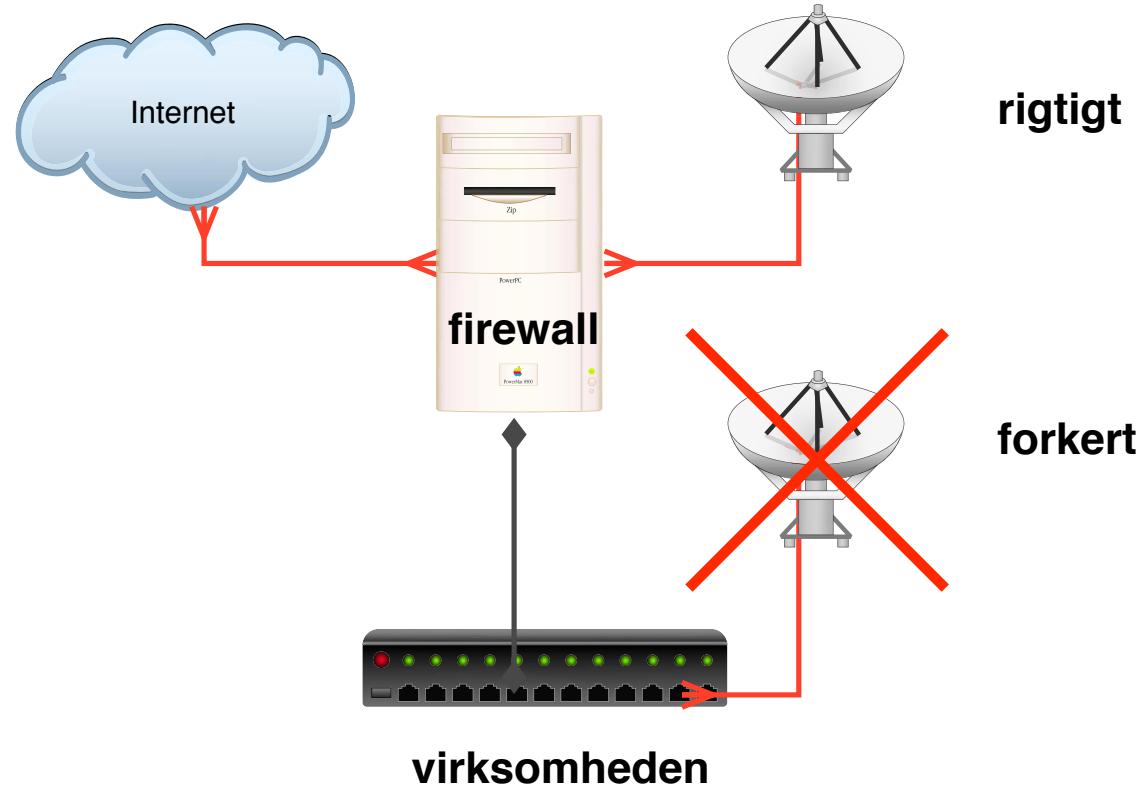
Nr adgangen er skabt



S gr man igang med de almindelige vrktjer

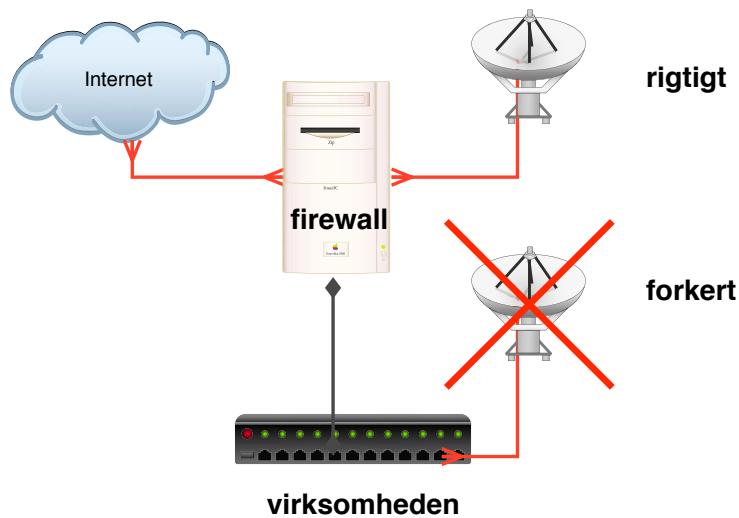
Fyodor Top 100 Network Security Tools <http://www.sectools.org>

Forsvaret er som altid - flere lag af sikkerhed!



Sdan br et access point forbinderes til netvrket

Anbefalinger mht. trdlse netvrk



- Brug noget tilfldigt som SSID - netnavnet
- Brug ikke WEP til virksomhedens netvrk
 - men istedet en VPN lsning med individuel autentificering eller WPA
- NB: WPA Personal/PSK krver passphrase på +40 tegn!
- Placer de trdlse adgangspunkter hensigtsmssigt i netvrket - s de kan overvges
- Lav et st regler for brugen af trdlse netvrk - hvor m medarbejdere bruge det?
- Se eventuelt pjecerne *Beskyt dit trdlse Netvrk* fra Ministeriet for Videnskab, Teknologi og Udvikling
<http://www.videnskabsministeriet.dk/>

Lad vre med at bruge et wireless-kort i en PC til at lave AP, brug et AP

Husk et AP kan vre en router, men den kan ofte ogs blot vre en bro

Brug WPA og overvej at lave en decideret DMZ til WLAN

Placer AP hensigtsmddigt og gerne hjt, oppe p et skab eller lignende

RADIUS er en protokol til autentificering af brugere op mod en filles server

Remote Authentication Dial In User Service (RADIUS)

RADIUS er beskrevet i RFC-2865

RADIUS kan vre en fordel i strre netvrk med

- dial-in
- administration af netvrksudstyr
- trdlse netvrk
- andre RADIUS kompatible applikationer

LDAP er en protokol til directory access, opslag i database

Light udgave af den X.500 directory access standard

LDAP er beskrevet i RFC-3377: Lightweight Directory Access Protocol (v3): Technical Specification

Standard interface for opslag, men desvrre ikke for data

Bruges meget typisk til brugere, grupper og passwords



Vi laver nu velsen

20RADIUS clientchapter.20

som er velse **20RADIUS clientchapter.20** fra velseshftet.

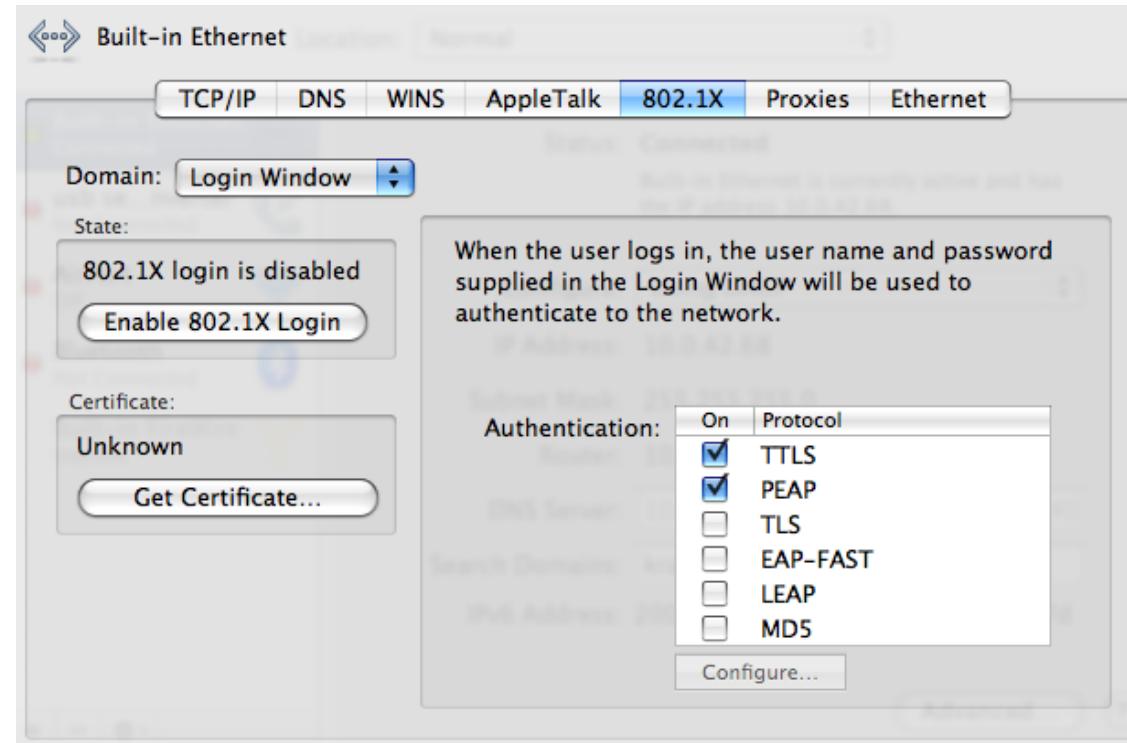


Vi laver nu velsen

21LDAP clientchapter.21

som er velse **21LDAP clientchapter.21** fra velseshftet.

IEEE 802.1x Port Based Network Access Control



Nogle switcher tillader at man benytter 802.1x brugervalidering p portniveau

Adgang til porten baseret p brugernavn og kodeord/certifikat

Denne protokol indgår også i WPA Enterprise

802.1x og andre teknologier



802.1x giver vsentlige fordele

MAC filtrering kan spoofes, hvor 802.1x krver det rigtige kodeord

WEP og WPA-PSK er en ngle til alle brugere, 802.1x er individuel adgang

Typisk benyttes RADIUS integration mod LDAP eller Active Directory

Vi vil nu gennemg netvrksdesign med udgangspunkt i vores setup

Vores setup indeholder:

- Routere
- Firewall
- Wireless
- DMZ
- DHCPD, BIND, BGPD, ...

Den kunne udvides med flere andre teknologier vi har til rådighed:

- VLAN inkl VLAN trunking/distribution
- WPA Enterprise

Tidligere havde vi adskilte netværk, nu samles de

Idag er det meget normalt at både firmaer og private bruger IP-telefoni

Fordele er primært billigere og mere fleksibelt

Eksempler på IP telefoner:

- Skype benytter IP, men egenudviklet protokol
- Cisco IP-telefoner benyttes ofte i firmaer
- Cybercity telefoner kræver over IP, med analog adapter

Det anbefales at se på Asterisk telefoniserver, hvis man har mod på det :-)

<http://www.asterisk.org/>

Der er generelt problemer med:

- Stabilitet - quality of service, netvirket skal være bygget til det
- Sikkerhed - hvem lytter med, hvem kan afbryde forbindelsen
Se evt. <http://www.voipsa.org/>
- Spam over VoIP, connect, send WAV fil med spam kaldes SPIT
- Kompatibilitet - hvilke protokoller, codecs, standarder, ...

Der er flere store spillere

SIP Session Initiation Protocol, IETF standard signaleringsprotokol

H.323 ITU-T standard signaleringsprotokol

IAX Inter-Asterisk Exchange Protocol, Asterisk protokol

SSCP Cisco protokol

ZRTP Phil Zimmermann, zfone - sikker kommunikation

<http://zfoneproject.com/>

Trivial File Transfer Protocol - uautentificerede filoverførsler

De bruges til:

- TFTP bruges til boot af netværksklienter uden egen harddisk
- TFTP benytter UDP og er derfor ikke garanteret at data overføres korrekt

TFTP sender alt i klartekst, hverken password

FTP bruger TCP men sender også i klartekst: **USER brugernavn** og **PASS hemmeligt-kodeord**

Mange routere og firewalls idag kan lave bndbredde allokering til protokoller, porte og derved bestemte services

Mest kendte er i Open Source:

- ALTQ bruges p OpenBSD - integreret i PF
- FreeBSD har dummynet
- Linux har tilsvarende
 - ADSL-Bandwidth-Management-HOWTO, ADSL Bandwidth Management HOWTO
 - Adv-Routing-HOWTO, Linux Advanced Routing & Traffic Control HOWTO
 - <http://www.knowplace.org/shaper/resources.html> Linux resources

Det kaldes ogs traffic shaping

Firewalls - packet filtering

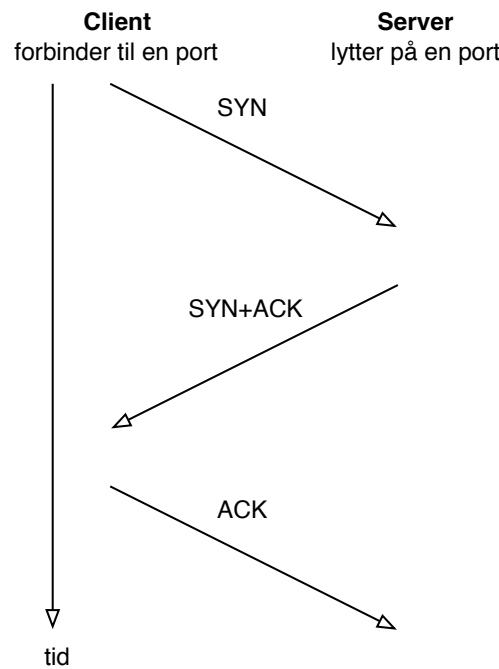


0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	
+-----+																						
Version IHL Type of Service													Total Length									
+-----+																						
Identification								Flags	Fragment Offset													
+-----+																						
Time to Live	Protocol	Header Checksum																				
+-----+																						
Source Address																						
+-----+																						
Destination Address																						
+-----+																						
Options												Padding										
+-----+																						

Packet filtering er firewalls der filterer på IP niveau

I dag inkluderer de fleste statefull inspection

TCP three way handshake



- Hvis en maskine modtager mange SYN pakker kan dette fyde tabellen over connections op - og derved afholde nye forbindelser fra at blive oprettet - **SYN-flooding**
- Mange firewalls kan udfre SYN handshake idag, fr forbindelsen overlades til serveren bagved
- Beskytter mod **TCP SYN flooding**

- Checkpoint Firewall-1 <http://www.checkpoint.com>
- Nokia appliances - Nokia IPSO <http://www.nokia.com>
- Cisco PIX <http://www.cisco.com>
- Clavister firewalls <http://www.clavister.com>
- Netscreen - nu ejet af Juniper <http://www.juniper.net>

Ovenstende er dem som jeg oftest ser ude hos mine kunder

Open source baserede firewalls



- Linux firewalls - fra begyndelsen til det nuvrende netfilter til kerner version 2.4 og 2.6
<http://www.netfilter.org>
- Firewall GUIs ovenp Linux - mange! IPcop, Guarddog, Watchguard nogle Linux firewalls er kommersielle produkter
- IP Filter (IPF) <http://coombs.anu.edu.au/avalon/>
- OpenBSD PF - findes idag p andre operativsystemer <http://www.openbsd.org>
- FreeBSD IPFW og IPFW2 <http://www.freebsd.org>
- FreeBSD inkluderer ogs OpenBSD PF
- Mac OS X benytter IPFW og har en application socket firewall
- NetBSD - bruger IPF og OpenBSD PF

NB: kun eksempler og dem jeg selv har brugt

Hardware eller software

Man hrer indimellem begrebet *hardware firewall*

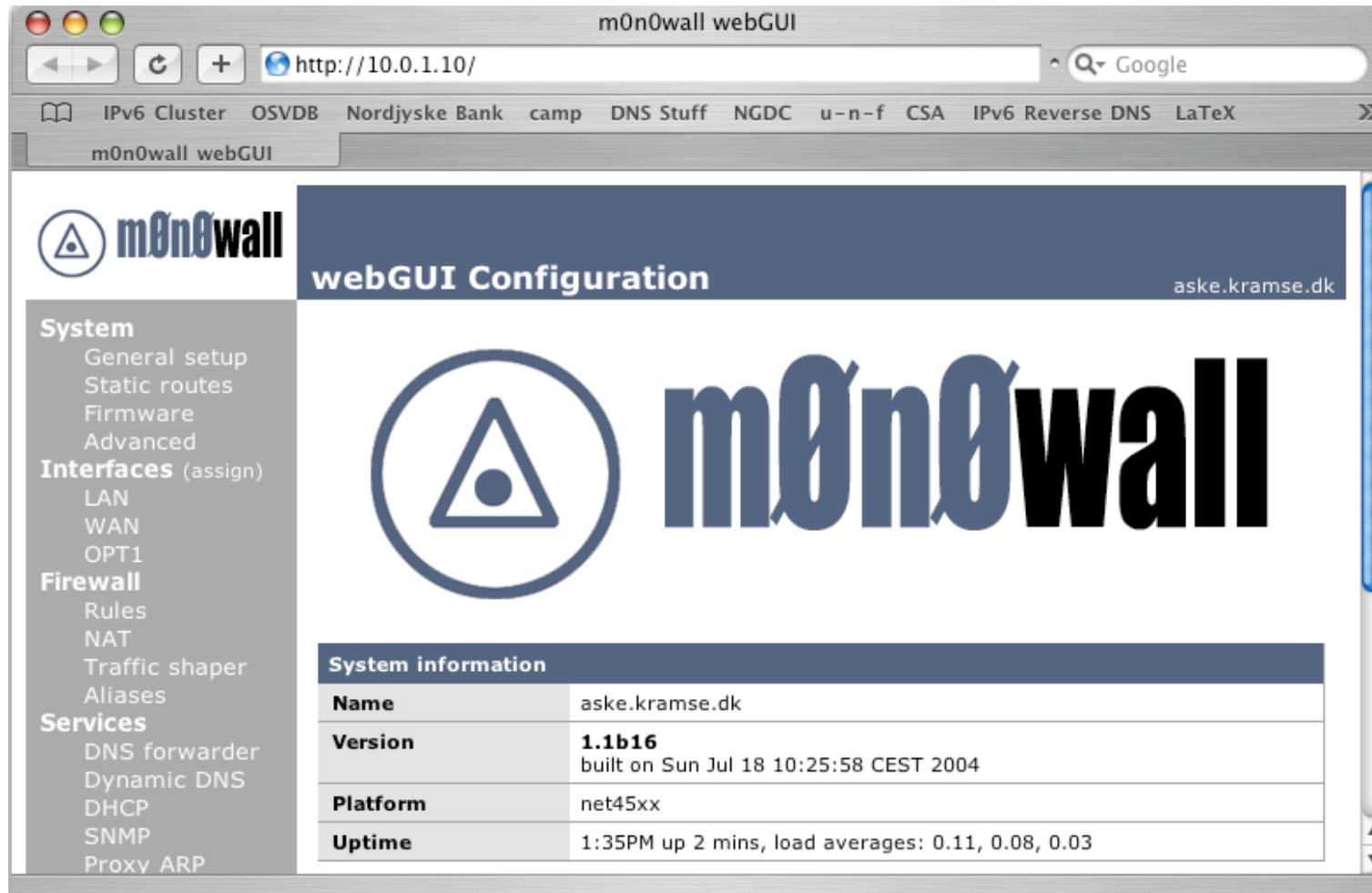
Det er dog et faktum at en firewall bestr af:

- Netvrkskort - som er hardware
- Filtreringssoftware - som er *software!*

Det giver ikke mening at kalde en Zyxel 10 en hardware firewall og en Soekris med OpenBSD for en software firewall!

Det er efter min mening et marketingtrick

Man kan til gengld godt argumentere for at en dedikeret firewall som en separat enhed kan give bedre sikkerhed



Kilde: billede fra <http://m0n0.ch/wall/>

Rækkefølgen af regler betyder noget!

- To typer af firewalls: First match - nr en regel matcher, gr det som angives block/pass Last match - marker pakken hvis den matcher, til sidst afgres block/pass

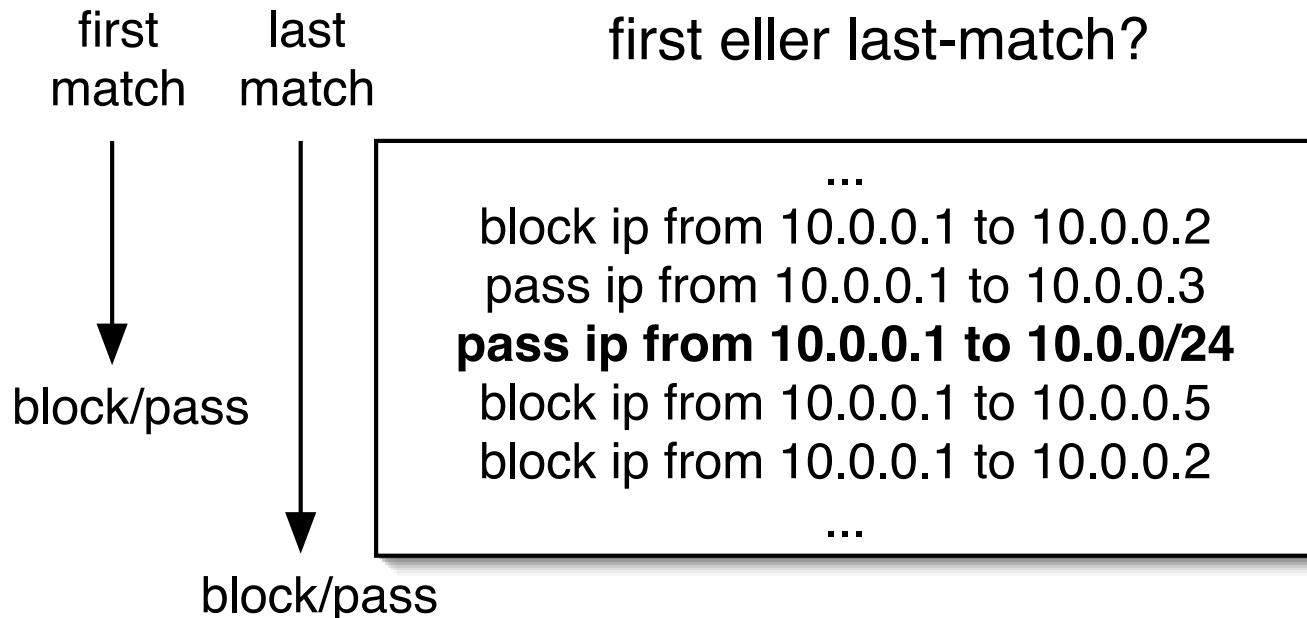
Det er ekstremt vigtigt at vide hvilken type firewall man bruger!

OpenBSD PF er last match

FreeBSD IPFW er first match

Linux iptables/netfilter er last match

First or Last match firewall?



Med dette regelsæt vil en first-match firewall blokere pakker fra 10.0.0.1 til 10.0.0.2 - men tillade alt andet fra 10.0.0.1 til 10.0.0/24

Med dette regelsæt vil en last-match firewall blokere pakker fra 10.0.0.1 til 10.0.0.2, **10.0.0.1 til 10.0.0.5**, **10.0.0.1 til 10.0.0.2** - men ellers tillade alt andet fra 10.0.0.1 til 10.0.0/24

- To typer af firewalls: First match - eksempelvis IPFW, Last match - eksempelvis PF

First match - IPFW



```
00100 16389 1551541 allow ip from any to any via lo0
00200      0      0 deny log ip from any to 127.0.0.0/8
00300      0      0 check-state
...
65435    36    5697 deny log ip from any to any
65535    865    54964 allow ip from any to any
```

Den sidste regel ns aldrig!

Last match - OpenBSD PF



```
ext_if="ext0"
int_if="int0"

block in
pass out keep state

pass quick on { lo $int_if }

# Tillad forbindelser ind p port 80=http og port 53=domain
# p IP-adressen for eksterne netkort ($ext_if) syntaksen
pass in on $ext_if proto tcp to ($ext_if) port http keep state
pass in on $ext_if proto { tcp, udp } to ($ext_if) port domain keep state
```

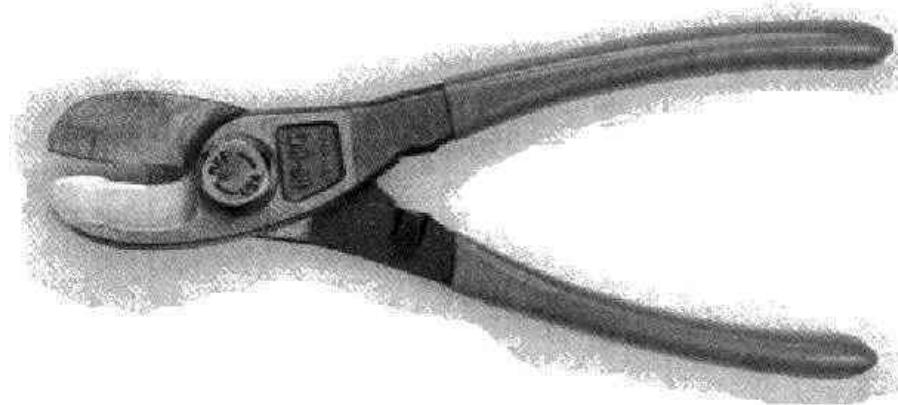
Pakkerne markeres med block eller pass indtil sidste regel
ngleordet *quick* afslutter match - god til store regelst

```
ipfw add allow icmp from any to any icmp types 3,4,11,12
```

Ovenstende er IPFW syntaks for at tillade de interessant ICMP beskeder igennem

Tillad ICMP types:

- 3 Destination Unreachable
- 4 Source Quench Message
- 11 Time Exceeded
- 12 Parameter Problem Message



Hvor skal en firewall placeres for at gre strst nytte?

Hvad er forudstningen for at en firewall virker?

At der er konfigureret et st fornuftige regler!

Hvor kommer reglerne fra? Sikkerhedspolitikken!

Kilde: Billedet er fra Marcus Ranum The ULTIMATELY Secure Firewall

Der er porte og services som altid br blokeres

Det kan vre kendte srbare services

- Windows SMB filesharing - ikke til brug p Internet!
- Unix NFS - ikke til brug p Internet!

Kendte problemer:

- KaZaA og andre P2P programmer - hvis muligt!
- Portmapper - port 111

Firewall konfiguration

Den bedste firewall konfiguration starter med:

- Papir og blyant
- En fornuftig adressestruktur

Brug dernst en firewall med GUI frste gang!

Husk dernst:

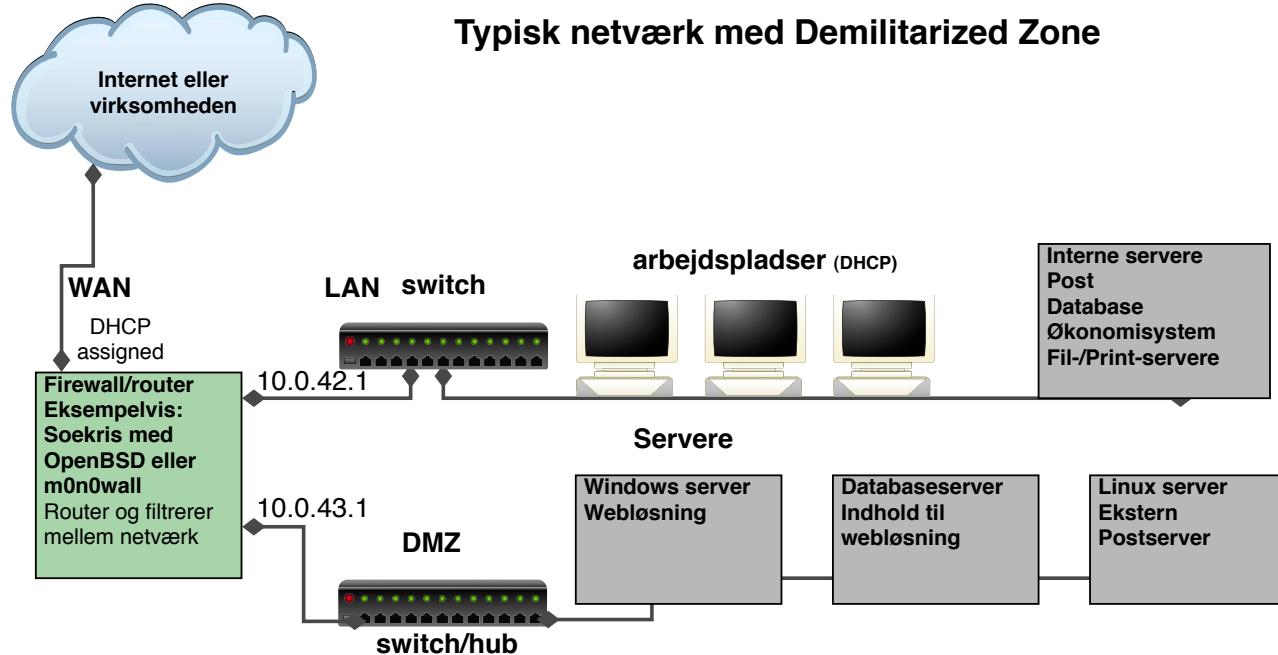
- En firewall skal passes
- En firewall skal opdateres
- Systemerne bagved skal hrdes!

Hvad kan man gøre for at få bedre netværkssikkerhed?

- Bruge switcher - der skal ARP spoofes og bedre performance
- Opdele med firewall til flere DMZ zoner for at holde utsatte servere adskilt fra hinanden, det interne netværk og Internet
- Overvåge, læse logs og reagere på hændelser

Husk du skal også kunne opdatere dine servere

En typisk firewall konfiguration



Du br opdele dit netværk i segmenter efter traffik

Du br altid holde interne og eksterne systemer adskilt!

Du br isolere farlige services i jails og chroots

Seperation of privileges



Forskellige computere til forskellige formål, en server er mail-server en anden er web-server

Brug en sikker konfiguration, minimumskonfiguration

Brug sikre protokoller, kryptering SSH fremfor Telnet

Opstning af netværk, hvordan? Security Configuration Guides + paranoia

- <http://csrc.nist.gov/publications/PubsSPs.html>
- <http://www.nsa.gov/research/publications/index.shtml>
- [http://www.nsa.gov/ia/guidance/security_{configuration guides}/index.shtml](http://www.nsa.gov/ia/guidance/security_configuration_guides/index.shtml)

Proxy servers

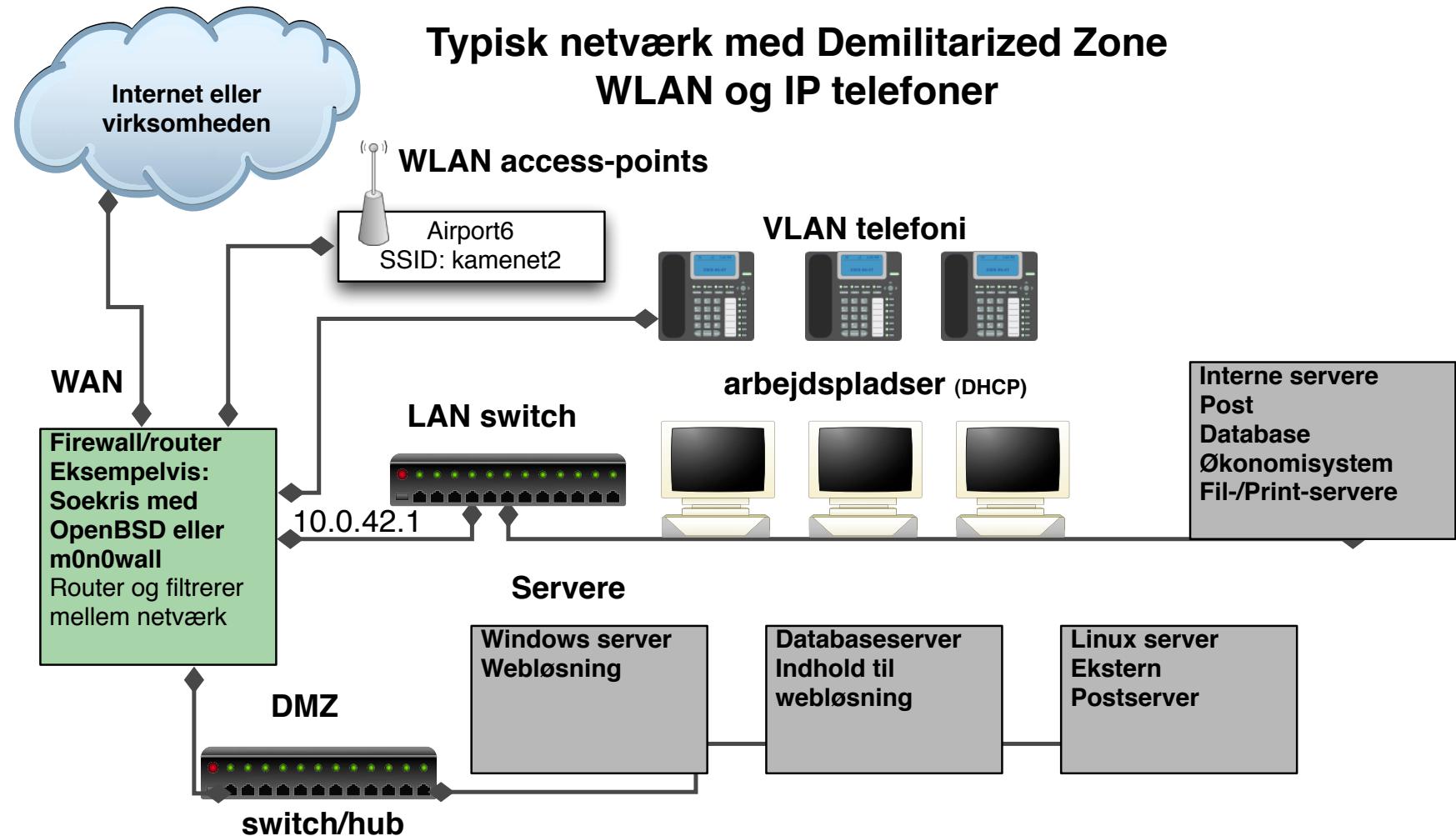
Filtrering på højere niveauer i OSI modellen er muligt

Idag findes proxy applikationer til de mest almindelige funktioner

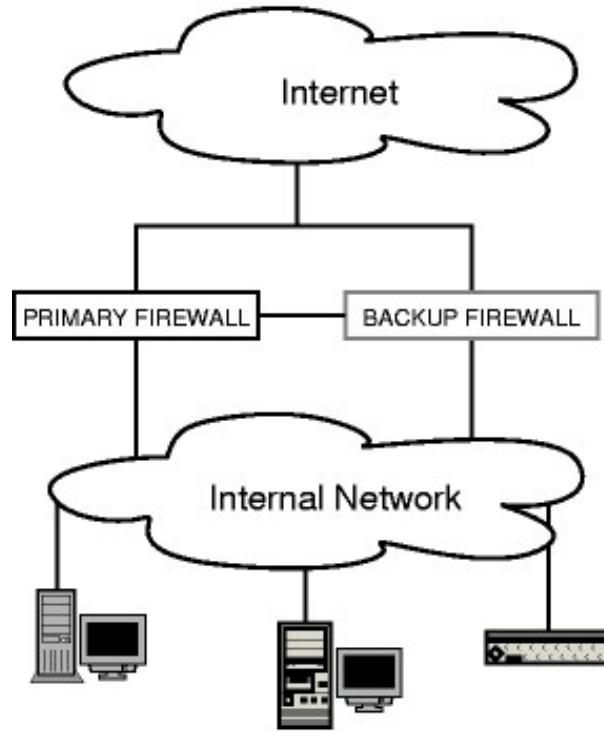
Den typiske proxy er en caching webproxy der kan foretage HTTP request på vegne af arbejdsstationer og gemme resultatet

NB: nogle protokoller egner sig ikke til proxy servere

SSL forbindelser til *secure websites* kan per design ikke proxies



Redundante firewalls



- OpenBSD Common Address Redundancy Protocol CARP - bde IPv4 og IPv6 overtagelse af adresse bde IPv4 og IPv6
- pfsync - sender opdateringer om firewall states mellem de to systemer
- Kilde: <http://www.countersiege.com/doc/pfsync-carp/>



Vi laver nu velsen

??

som er velse ?? fra velseshftet.



Vi laver nu velsen

??

som er velse ?? fra velseshftet.



Vi laver nu velsen

??

som er velse ?? fra velseshftet.

De fleste firewalls giver mulighed for at lave krypterede tunneler

Nyttigt til fjernkontorer der skal have usikker traffik henover usikre netværk som Internet

Konceptet kaldes Virtual Private Network VPN

IPsec er de facto standarden for VPN og beskrevet i RFC'er

Sikkerhed i netvrket

- RFC-2401 Security Architecture for the Internet Protocol
- RFC-2402 IP Authentication Header (AH)
- RFC-2406 IP Encapsulating Security Payload (ESP)
- RFC-2409 The Internet Key Exchange (IKE) - dynamisk keying

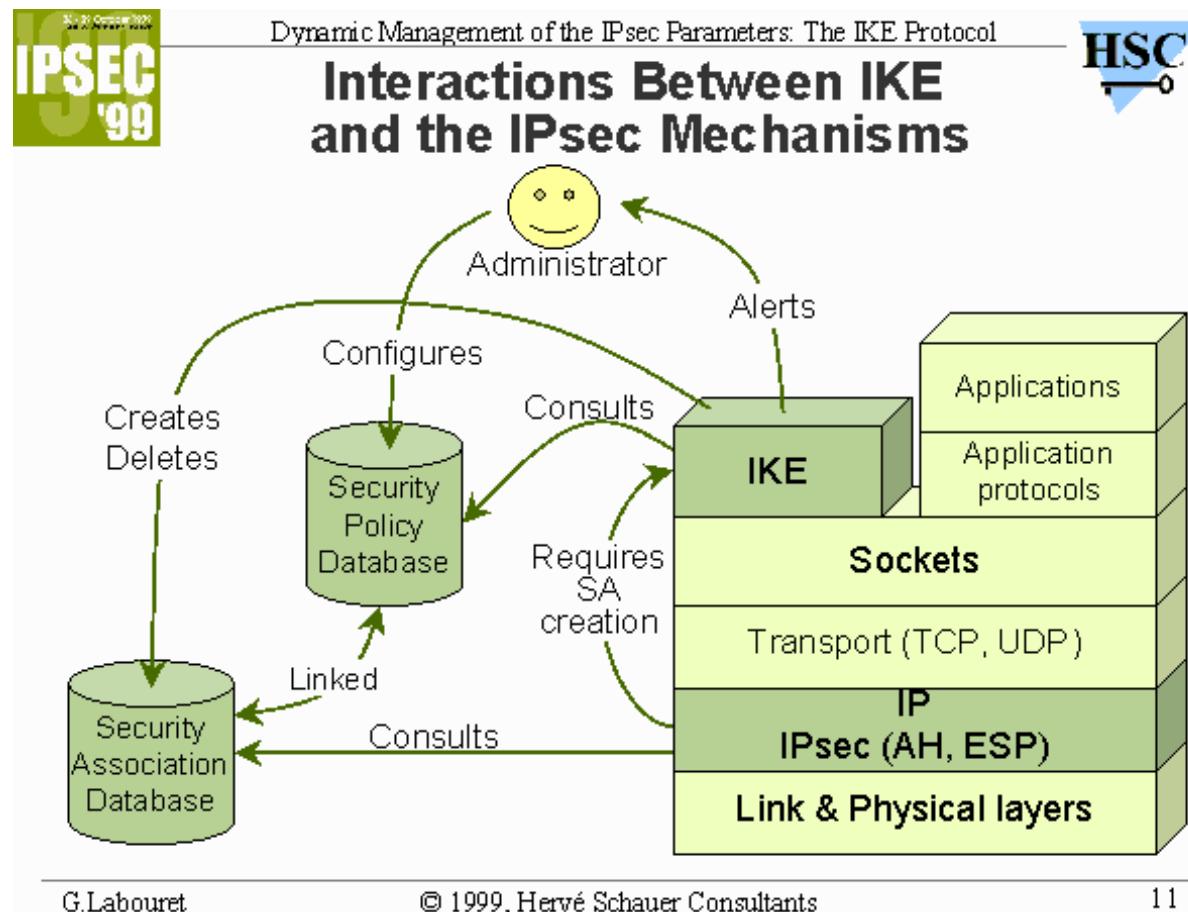
Bde til IPv4 og IPv6

MANDATORY i IPv6! - et krav hvis man implementerer fuld IPv6 support

Der findes IKEscan til at scanne efter IKE porte/implementationer

<http://www.nta-monitor.com/ike-scan/index.htm>

IPsec er ikke simpelt!



G.Labouret

© 1999, Hervé Schauer Consultants

11

Kilde: <http://www.hsc.fr/presentations/ike/>

Pakkerne frø og efter:

BEFORE APPLYING ESP

IPv6		ext	hdrs			
	orig	IP	hdr	if present	TCP	Data

AFTER APPLYING ESP

IPv6	orig	hop-by-hop, dest*,	dest		ESP	ESP
	IP	hdr routing, fragment.	ESP opt*	TCP Data	Trailer Auth	

| <---- encrypted ----> |
| <---- authenticated ----> |

OpenVPN is a full-featured SSL VPN solution which can accommodate a wide range of configurations, including remote access, site-to-site VPNs, WiFi security, and enterprise-scale remote access solutions with load balancing, failover, and fine-grained access-controls (articles) (examples) (security overview) (non-english languages).

Et andet populrt VPN produkt er OpenVPN

Bemrk dog at hvis der benyttes TCP i TCP risikerer man at stde ind i et problem som kaldes *TCP in TCP meltdown*

Kilde: <http://openvpn.net/>

Network patterns



Hvad taler for og imod - de nste slides gennemgr nogle standardsetups

En slags Patterns for networking

Pattern: erstat Telnet med SSH

Telnet er dd!

Brug altid Secure Shell fremfor Telnet

Opgrader firmware til en der kan SSH, eller køb bedre udstyr næste gang

Selv mine sm billige Linksys switcher forstør SSH!

Pattern: erstat FTP med HTTP



Hvis der kun skal distribueres filer kan man ofte benytte HTTP istedet for FTP

Hvis der skal overfres med password er SCP/SFTP fra Secure Shell at foretrække

Anti-patterns

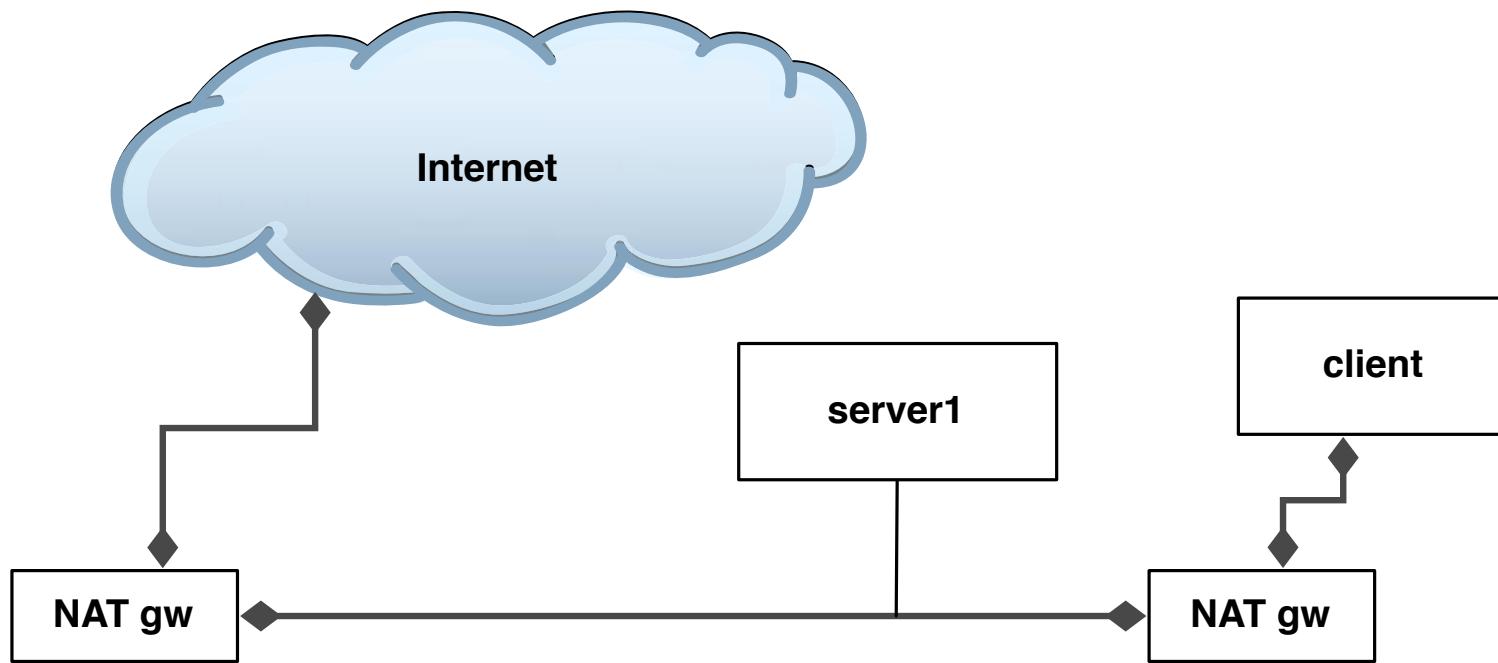


Nu præsenteres et antal setups, som ikke anbefales

Faktisk vil jeg advare mod at bruge dem

Husk følgende slides er min mening

Anti-pattern dobbelt NAT i eget netvrk



Det er nødvendigt med NAT for at overstte traffik der sendes videre ud p internet.

Der er ingen som helst grund til at benytte NAT indenfor eget netvrk!

Anti-pattern blokering af ALT ICMP



```
ipfw add allow icmp from any to any icmptypes 3,4,11,12
```

Lad vre med at blokere for alt ICMP, s delgger du funktionaliteten i dit net

Anti-pattern blokering af DNS opslag p TCP

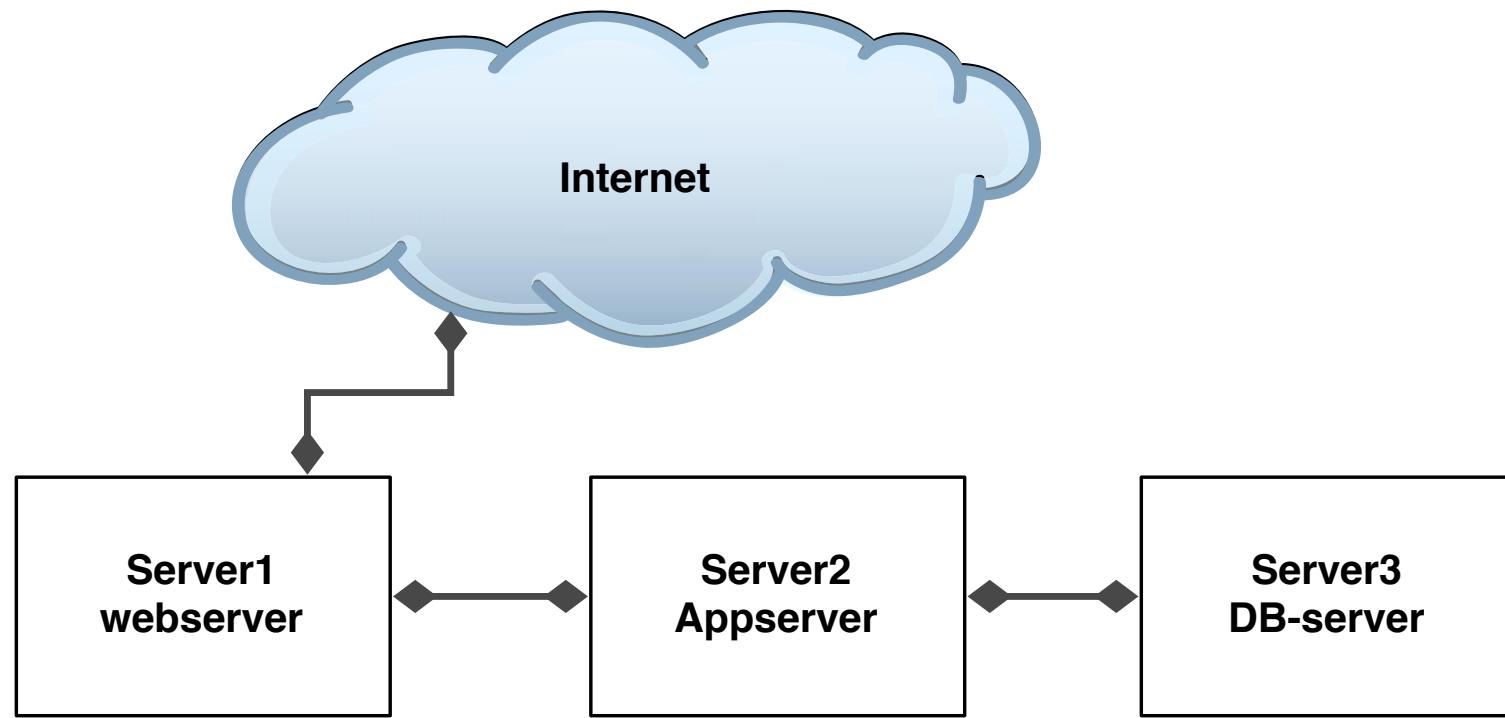


Det bliver (er) ndvendigt med DNS opslag over TCP p grund af store svar. Det betyder at firewalls skal tillade DNS opslag via TCP

Guide:

Brug en caching nameserver, sledes at det kun er den som kan lave DNS opslag ud i verden

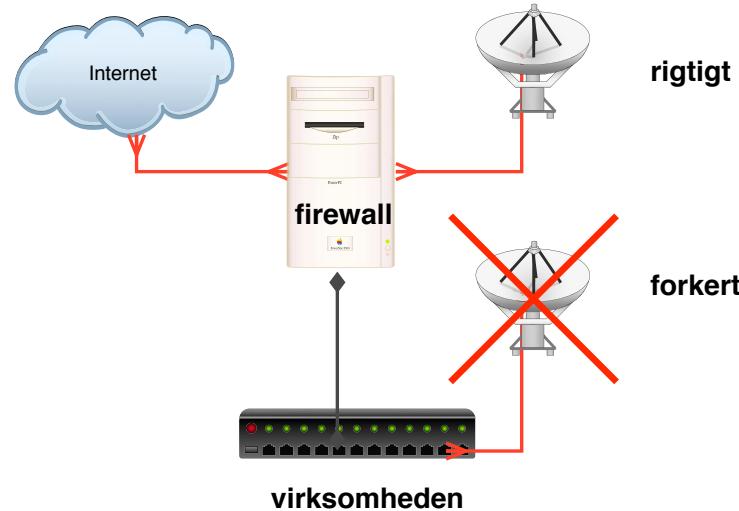
Anti-pattern daisy-chain



Daisy-chain af servere, erstat med firewall, switch og VLAN

Det giver et vld af problemer med overvægning, administration, backup og opdatering

Anti-pattern WLAN forbundet direkte til LAN



WLAN AP'er forbundet direkte til LAN giver strre risiko for at sikkerheden brydes

Ved at stte WLAN direkte p LAN risikerer man at eksterne fr direkte adgang

Kan selvflgelig g an i et privat hjem

Det forvrres jo flere AP'er man har, har du 100 skal du vre sikker p allesammen er sikre!

Husk følgende:

- Unix og Linux er blot eksempler - navneservice eller HTTP server krer fint p Windows
- DNS er grundlaget for Internet
- Sikkerheden p internet er generelt drlig, brug SSL!
- Procedurerne og vedligeholdelse er essentiel for alle operativsystemer!
- Man skal *hrde* operativsystemer *fr* man stter dem p Internet
- Husk: IT-sikkerhed er ikke kun netvrkssikkerhed!
- God sikkerhed kommer fra langsigtede intiativer

Jeg hber I har lrt en masse om netvrk og kan bruge det i praksis :-)

Henrik Lund Kramshj
hlk@security6.net

<http://www.security6.net>

I er altid velkomne til at sende sprgsml p e-mail

Referencer: netvrksbger



- O'Reilly Network Warrior - god allround bog, men ogs Cisco centrisk
- Stevens, Comer klassiske bger om TCP/IP
- TCP/IP bogen p dansk mske
- O'Reilly IPv6 Network Administration
- KAME bgerne om IPv6 protokollerne, meget detaljerede
- O'Reilly cookbooks: Cisco, BIND og Apache HTTPD m.fl.
- Cisco Press og website
- Juniper website
- Firewall bger Cheswick
- Der findes mange gode bger om netvrk

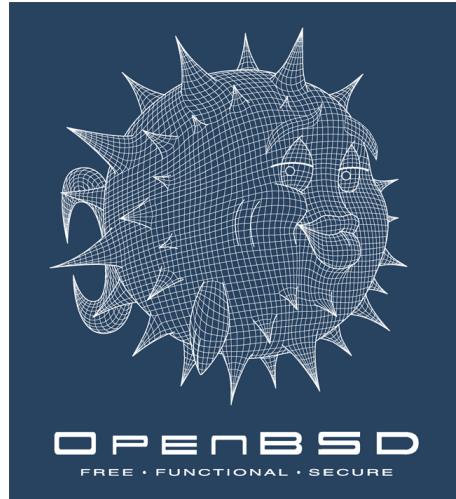
IPv6 Network Administration af David Malone og Niall Richard Murphy - god til real-life admins, typisk O'Reilly bog

IPv6 Essentials af Silvia Hagen, O'Reilly 2nd edition (May 17, 2006) god reference om emnet

IPv6 Core Protocols Implementation af Qing Li, Tatuya Jinmei og Keiichi Shima

IPv6 Advanced Protocols Implementation af Qing Li, Jinmei Tatuya og Keiichi Shima

- flere andre



Primære website: <http://www.openbsd.org>

Ved at sætte OpenBSD sætter du:

- OpenSSH - inkluderet i mere end 80-100 distributioner
- Udviklingen af OpenBSD PF - en super firewall, er med i FreeBSD, NetBSD
- Udvikling af stackprotection i Open Source operativsystemer
- OpenBGPD - en fri routing daemon, OpenNTPD - en fri NTP daemon, OpenCVS - en fri NTP daemon, CARP - redundancy must be free!

- Nmap portscanner <http://nmap.org>
- Diverse testvrktjer <http://www.sectools.org>
- Cain og Abel fra gratis password cracker <http://oxid.it>
- Wireshark avanceret netvrkssniffer <http://www.wireshark.org>
- OpenBSD operativsystem med fokus p sikkerhed <http://www.openbsd.org>
- Open Source Security Testing Methodology Manual - gennemgang af elementer der br indg i en struktureret test <http://www.isecom.org/>
- Putty terminal emulator med indbygget SSH
<http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>
- BackTrack security collection - en boot CD med omkring 300 hackervrktjer
<http://www.remote-exploit.org/>

Tnk som en hacker

Rekognoscering

- ping sweep
- portscan
- OS detection - TCP/IP eller banner grab
- Servicescan - rpcinfo, netbios, ...
- telnet/netcat interaktion med services

Udnyttelse/afprvning: Nessus, whisker, exploit programs

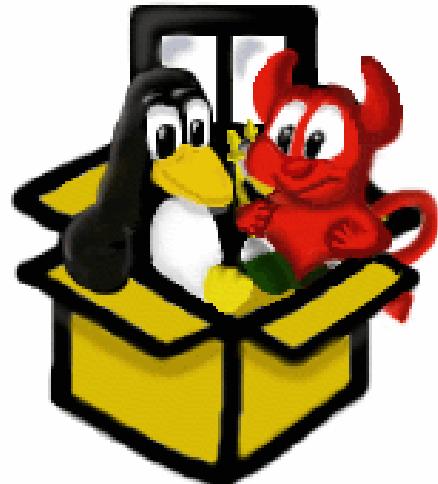
Oprydning

- Lav en rapport
- Gennemg rapporten, registrer ndringer
- Opdater programmer, konfigurationer, arkitektur, osv.

I skal jo ogs VISE andre at I gr noget ved sikkerheden.

Security6.net afholder flgende kurser med mig som underviser

- IPv6 workshop - 1 dag
Introduktion til Internetprotokollerne og forberedelse til implementering i egne netvrk. Internetprotokollerne har eksisteret i omkring 20 r, og der er kommet en ny version kaldet version 6 af disse - IPv6.
- Wireless teknologier og sikkerhed workshop - 2 dage
En dag med fokus p netvksdesign og fornuftig implementation af trdlse netvrk og integration med eksempelvis hjemmepc og wirksamhedens netvrk
- Hacker workshop 2 dage
Workshop med detaljeret gennemgang af hackermetoderne angreb over netvrk, exploitprogrammer, portscanning, Nessus m.fl.
- Forensics workshop 2 dage
Med fokus p tilngelige open source vrktjer gennemgs metoder og praksis af undersgelse af diskimages og spor p computer systemer
- Moderne Firewalls og Internetsikkerhed 2 dage
Informere om trusler og aktivitet p Internet, samt give et bud p hvorledes en avanceret moderne firewall idag kunne konfigureres.



6cm

BSD-DK - dansk forening for BSD'erne,
<http://www.bsd-dk.dk>
medlemsskab giver god rabat på bøger gennem
<http://www.polyteknisk.dk>, typisk 15-20%

SSLUG, Skåne Sjælland Linux User Group
<http://www.sslug.dk>

Soekris bestilling



Et lille embedded system

- Soekris 5501-30 + case 2250,-
- Soekris 4801-50 + case 1400,-
- Strmforsyning 1.5A (lille) 130,-
- Strmforsyning 3A (stor) 170,-
- vpn1411 miniPCI 400,-

- 4801 Harddisk mount kit 2.5" 70,-
- Alle priser er cirkapriser og ekskl. moms.
- kontakt leverandør for njagtige oplysninger!
- Anbefalet leverandør <http://www.kd85.com>
- Alternativ leverandør <http://www.cortexsystems.dk>