Welcome to

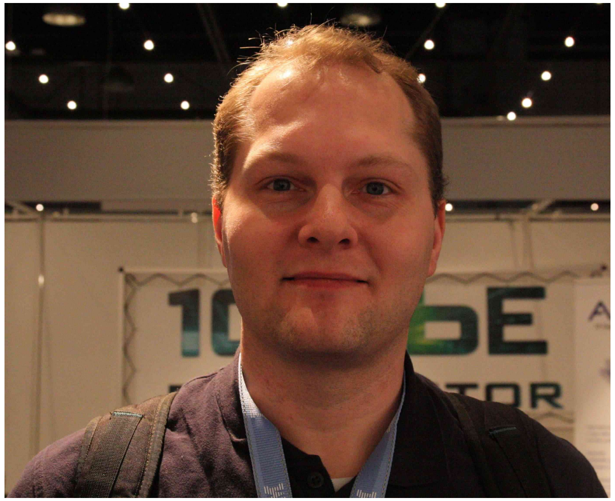
IPv6 Security in Enterprise Networks

Marts 2012

Henrik Lund Kramshøj
hlk@solido.net

http://www.solidonetworks.com

Contact information



- Henrik Lund Kramshøj, IT-security and internet samurai
- Email: hlk@solido.net Mobile: +45 2026 6000
- Educated from the Computer Science Department at the University of Copenhagen, DIKU
- CISSP and CEH certified
- 2003 - 2010 Independent security consultant
- 2010 - owner and partner in Solido Networks ApS

Planen idag

Don't Panic!

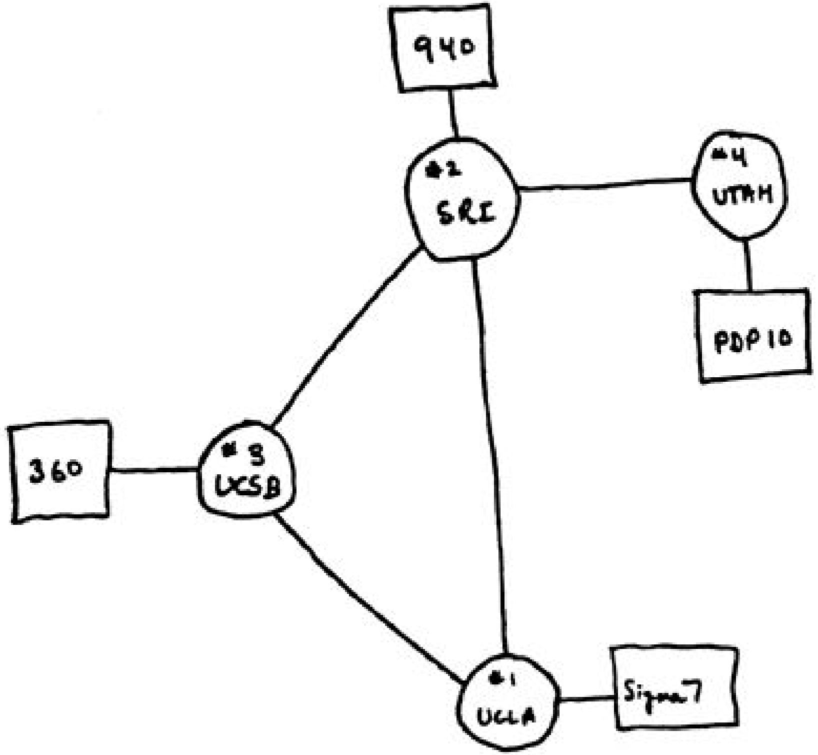
Kl 13:00-14:45

Mindre foredrag mere snak

Mindre enetale, mere foredrag 2.0 med socialt medie, informationsdeling og interaktion

Send gerne spørgsmål senere

Formål: netværkssikkerhed for TCP/IP netværk



TCP/IP-baserede netværk - internet er overalt

Formål: mere specifikt

At introducere TCP/IP version 6

Introducere specifikke sikkerhedsproblemer ved brug af IPv6

Hackerværktøjer

Der benyttes en del værktøjer:

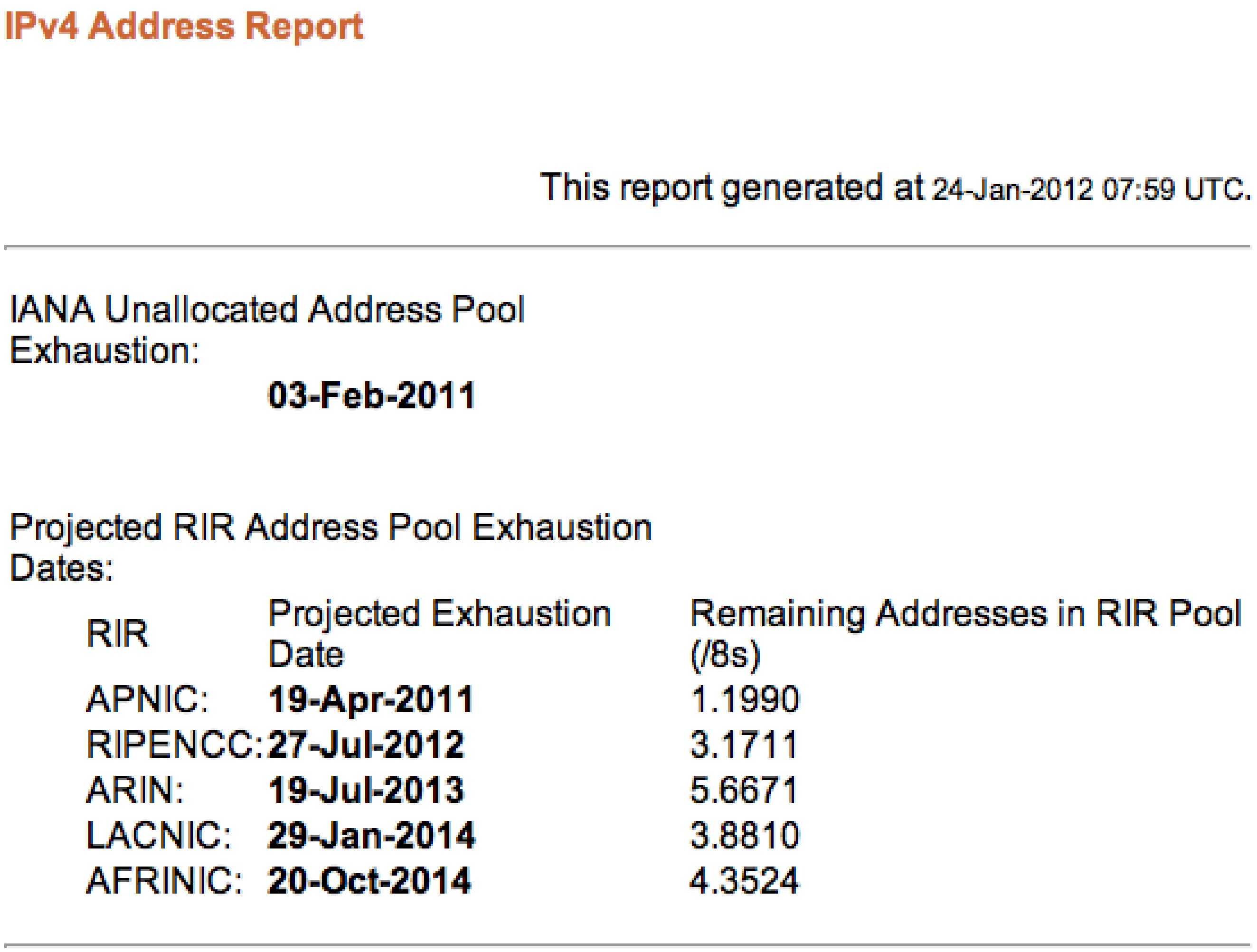
- Nmap, Nping - tester porte, godt til firewall admins `http://nmap.org`
- Metasploit Framework gratis på `http://www.metasploit.com/`
- Wireshark avanceret netværkssniffer - `http://http://www.wireshark.org/`
- Burpsuite `http://portswigger.net/burp/`
- Skipfish `http://code.google.com/p/skipfish/`
- Apache Tomcat J2EE servlet container `http://tomcat.apache.org`
- OpenBSD operativsystem med fokus på sikkerhed `http://www.openbsd.org`

BackTrack 5 og sniffer programmer

Wireshark - `http://www.wireshark.org` avanceret netværkssniffer
bruger vi til at sniffe, vi bruger Wireshark til primære demo, nævner Ettercap osv.

BackTrack `http://www.backtrack-linux.org/` BackTrack er baseret på Linux og må kopieres frit :-)

Status idag på internet



IPv4 Address Report

This report generated at 24-Jan-2012 07:59 UTC.

IANA Unallocated Address Pool Exhaustion:

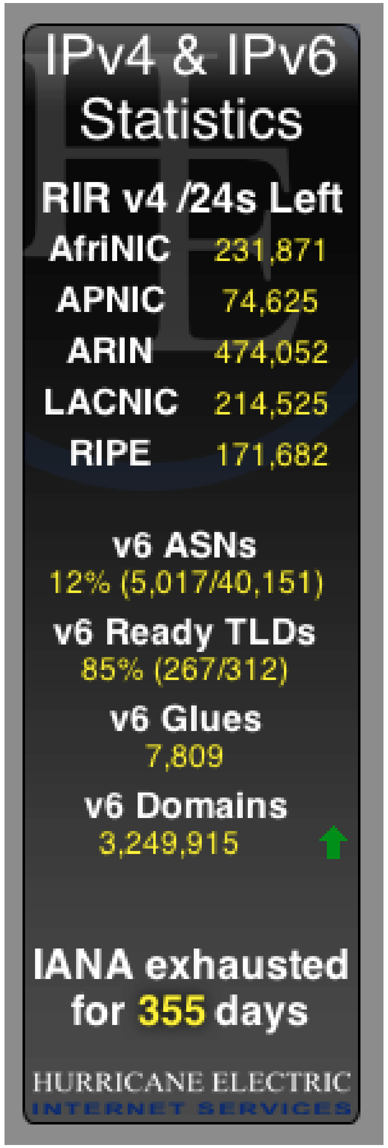
03-Feb-2011

Projected RIR Address Pool Exhaustion Dates:

RIR	Projected Exhaustion Date	Remaining Addresses in RIR Pool (/8s)
APNIC:	**19-Apr-2011**	1.1990
RIPENCC:	**27-Jul-2012**	3.1711
ARIN:	**19-Jul-2013**	5.6671
LACNIC:	**29-Jan-2014**	3.8810
AFRINIC:	**20-Oct-2014**	4.3524

Kilde: `http://www.potaroo.net/tools/ipv4/`

Why IPv6



IPv4 & IPv6 Statistics

RIR v4 /24s Left

AfriNIC	231,871
APNIC	74,625
ARIN	474,052
LACNIC	214,525
RIPE	171,682

v6 ASNs
12% (5,017/40,151)

v6 Ready TLDs
85% (267/312)

v6 Glues
7,809

v6 Domains
3,249,915 ↑

IANA exhausted for 355 days

HURRICANE ELECTRIC
INTERNET SERVICES

DDoS udviklingen, januar 2010 rapporten

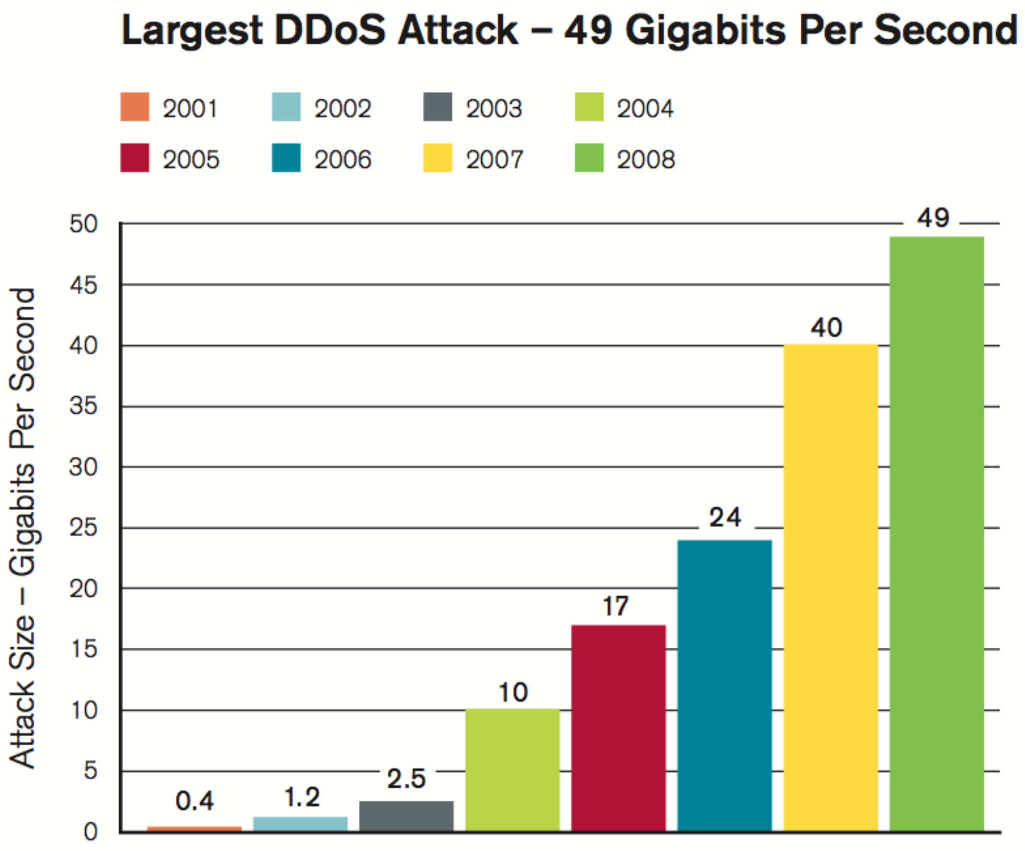


***Figure 1:** Largest DDoS Attack – 49 Gigabits Per Second*

Source: Arbor Networks, Inc.

Kilde: `http://www.arbornetworks.com/report` 2009 rapporten

DDoS udviklingen, februar 2011

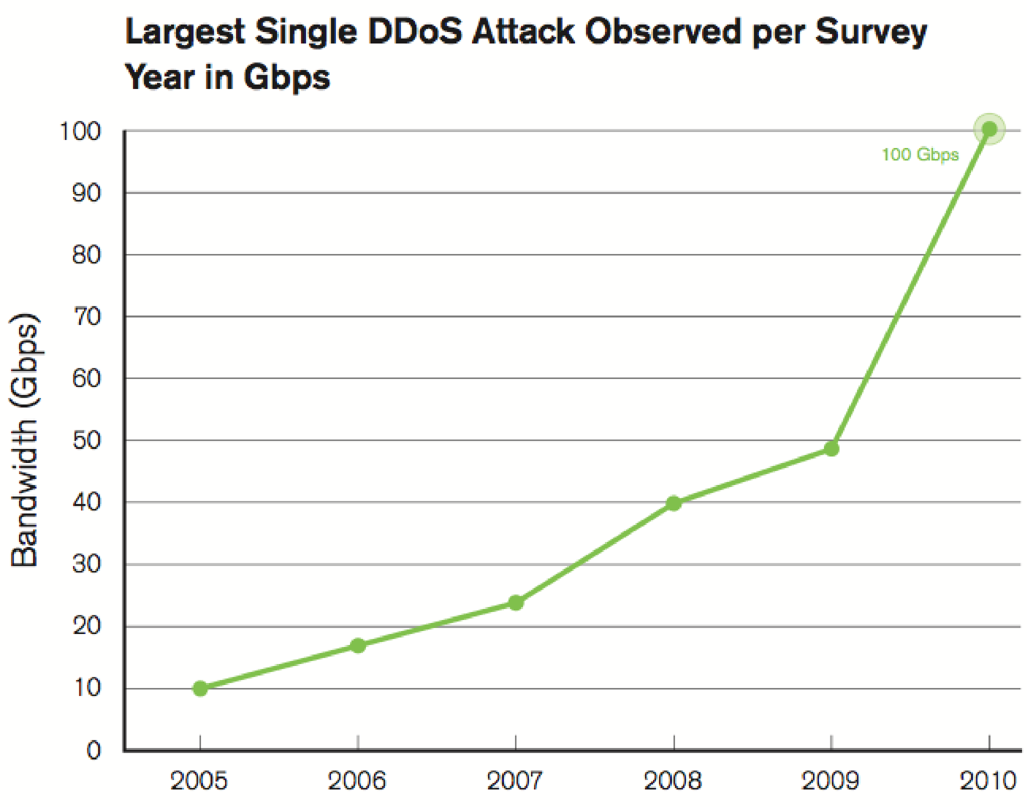


Figure 1
Source: Arbor Networks, Inc.

Kilde: `http://www.arbornetworks.com/report` 2010 rapporten

Worldwide Infrastructure Security Report, 2010 Report

> Key finding:
> **Application-Layer DDoS Attacks Are Increasing in Sophistication and Operational Impact**
> IDC and mobile/fixed wireless operators in particular are reporting significant outages, increased OPEX, customer churn and revenue loss due to application-layer DDoS attacks. These attacks are targeting both their customers and their own ancillary supporting services, such as DNS, Web portals, etc.
> ...
> Conclusions
> We further note that the fastest-growing category of ISPs-mobile and fixed wireless broadband operators-are also the least-prepared organizations in terms of network visibility, network control, and overall ability to successfully defend themselves and their customers against attack. These operators are balancing an overwhelming array of threats with conflicting budget pressures and business objectives.

Mere komplekse trusler, betyder det flere firewall?

Worldwide Infrastructure Security Report 2010 Volume VI

- Application-Layer DDoS Attacks Are Increasing in Sophistication and Operational Impact
- Mobile/Fixed Wireless Operators Are Facing Serious Challenges to Maintaining Availability in the Face of Attacks
- Firewalls and IPS Devices Are Falling Short on DDoS Protection
- DNS Has Broadly Emerged as an Attack Target and Enabler
- **Lack of Visibility into and Control over IPv6 Traffic Is a Significant Challenge**
- Chronic Underfunding of Operational Security Teams
- Operators Continue to Express Low Confidence in the Efficacy of Law Enforcement
- Operators Have Little Confidence in Government Efforts to Protect Critical Infrastructure

Kilde: `http://www.arbornetworks.com/report`

Worldwide Infrastructure Security Report 2011 Volume VII

- Ideologically-Motivated ”Hactivism” and Vandalism Are the Most Readily-Identified DDoS Attack Motivations
- 10 Gbps and Larger Flood-Based DDoS Attacks Are the ”New Normal”
- Increased Sophistication and Complexity of Application-Layer (Layer 7) DDoS Attacks and Multi-Vector DDoS Attacks Are Becoming More Common
- Visibility and Security of Mobile and Fixed Wireless Networks Are an Ongoing Concern
- **First-Ever Reports of IPv6 DDoS Attacks ”in the Wild” on Production Networks**
- **Rarity of IPv6-Enabled Attacks Indicates Low IPv6 Market Penetration and Lack of Critical Mass**
- Stateful Firewalls, IPS and Load-Balancer Devices Continue to Fall Short on DDoS Protection Capabilities
- The Overwhelming Majority of Network Operators Do Not Engage Law Enforcement

Kilde: `http://www.arbornetworks.com/report`

IPv6 is coming

An important consideration is that IPv6 is quite likely to be already running on the enterprise network, whether that implementation was planned or not. Some important characteristics of IPv6 include:

- IPv6 has a mechanism to automatically assign addresses so that end systems can easily establish communications.
- IPv6 has several mechanisms available to ease the integration of the protocol into the network.
- Automatic tunneling mechanisms can take advantage of the underlying IPv4 network and connect it to the IPv6 Internet.

Kilde:

`http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6553/white_paper_c11-629391.html`

Implications

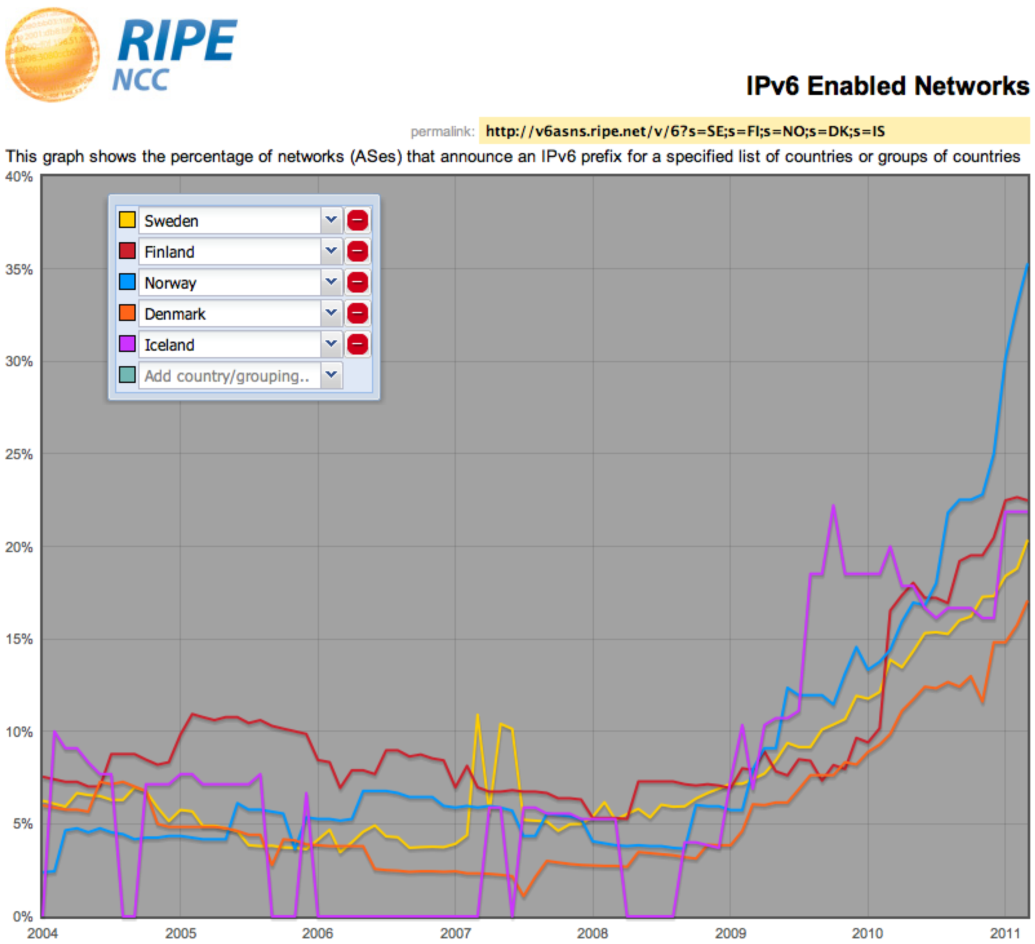
For an IPv4 enterprise network, the existence of an IPv6 overlay network has several of implications:

- The IPv4 firewalls can be bypassed by the IPv6 traffic, and leave the security door wide open.
- Intrusion detection mechanisms not expecting IPv6 traffic may be confused and allow intrusion
- In some cases (for example, with the IPv6 transition technology known as 6to4), an internal PC can communicate directly with another internal PC and evade all intrusion protection and detection systems (IPS/IDS). Botnet command and control channels are known to use these kind of tunnels.

Kilde:

`http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6553/white_paper_c11-629391.html`

IPv6 in the Nordic region



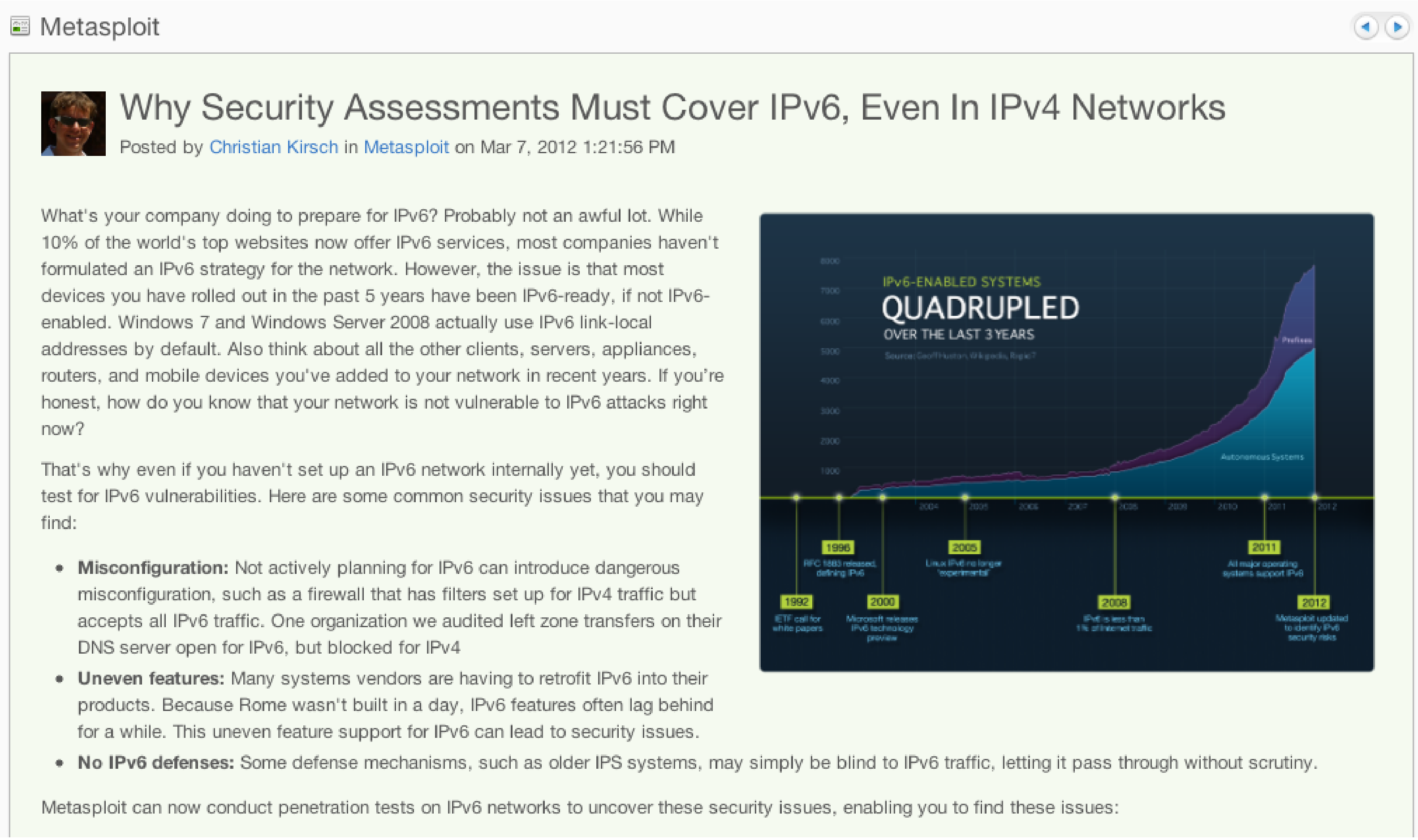
IPv6 Enabled Networks

permalink: http://v6asns.ripe.net/v/6?s=SE;s=FI;s=NO;s=DK;s=IS

This graph shows the percentage of networks (ASes) that announce an IPv6 prefix for a specified list of countries or groups of countries

http://v6asns.ripe.net/v/6?s=_ALL;s=DK;s=SE;s=NO;s=NL

Metasploit IPv6



Metasploit

Why Security Assessments Must Cover IPv6, Even In IPv4 Networks

Posted by Christian Kirsch in Metasploit on Mar 7, 2012 1:21:56 PM

What's your company doing to prepare for IPv6? Probably not an awful lot. While 10% of the world's top websites now offer IPv6 services, most companies haven't formulated an IPv6 strategy for the network. However, the issue is that most devices you have rolled out in the past 5 years have been IPv6-ready, if not IPv6-enabled. Windows 7 and Windows Server 2008 actually use IPv6 link-local addresses by default. Also think about all the other clients, servers, appliances, routers, and mobile devices you've added to your network in recent years. If you're honest, how do you know that your network is not vulnerable to IPv6 attacks right now?

That's why even if you haven't set up an IPv6 network internally yet, you should test for IPv6 vulnerabilities. Here are some common security issues that you may find:

- **Misconfiguration:** Not actively planning for IPv6 can introduce dangerous misconfiguration, such as a firewall that has filters set up for IPv4 traffic but accepts all IPv6 traffic. One organization we audited left zone transfers on their DNS server open for IPv6, but blocked for IPv4
- **Uneven features:** Many systems vendors are having to retrofit IPv6 into their products. Because Rome wasn't built in a day, IPv6 features often lag behind for a while. This uneven feature support for IPv6 can lead to security issues.
- **No IPv6 defenses:** Some defense mechanisms, such as older IPS systems, may simply be blind to IPv6 traffic, letting it pass through without scrutiny.

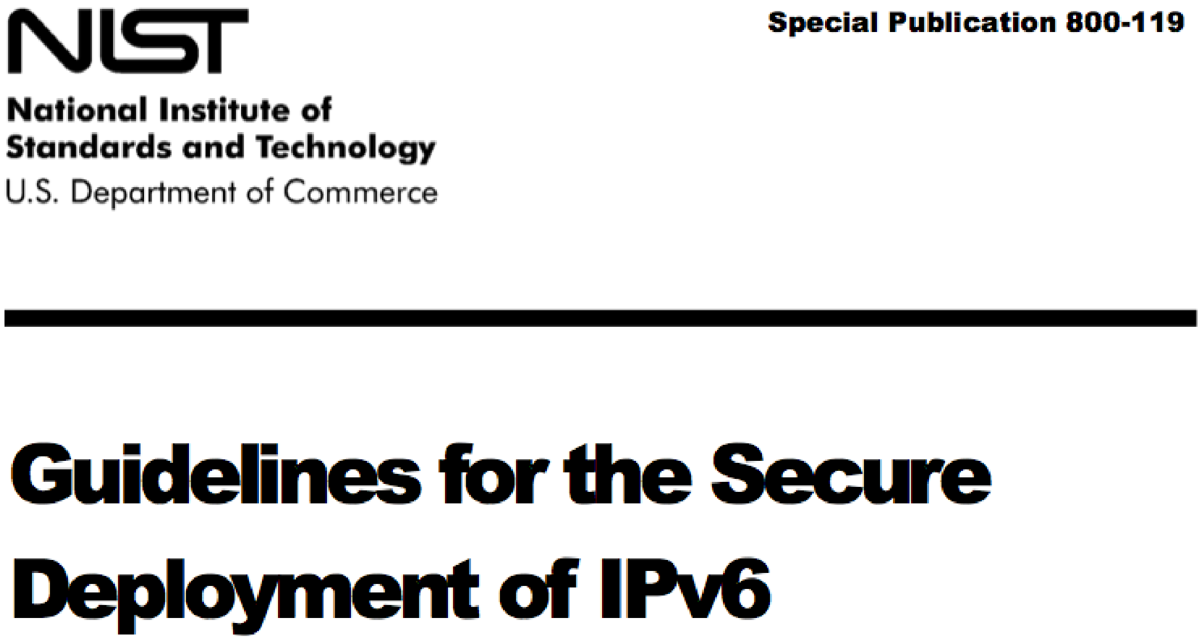
Metasploit can now conduct penetration tests on IPv6 networks to uncover these security issues, enabling you to find these issues:

IPv6-ENABLED SYSTEMS
QUADRUPLED
OVER THE LAST 3 YEARS
Source: Geoff Huston, Wikipedia, Rapid7
8000
7000
6000
5000
4000
3000
2000
1000
Prefixes
Autonomous Systems
2004
2005
2006
2007
2008
2009
2010
2011
2012
1996
RFC 1883 released, defining IPv6
2005
Linux IPv6 no longer "experimental"
2011
All major operating systems support IPv6
1992
IETF call for white papers
2000
Microsoft releases IPv6 technology preview
2008
IPv6 is less than 1% of Internet traffic
2012
Metasploit updated to identify IPv6 security risks

Kilde:

`https://community.rapid7.com/community/metasploit/blog/2012/03/07/`

NIST Special Publication 800 series



NIST

National Institute of Standards and Technology

U.S. Department of Commerce

Special Publication 800-119

Guidelines for the Secure Deployment of IPv6

SP 800-119 Dec. 2010 Guidelines for the Secure Deployment of IPv6
God introduktion til IPv6 og sikkerhed i forbindelse med IPv6

```
http://csrc.nist.gov/publications/PubsSPs.html
```

THC

> A complete tool set to attack the inherent protocol weaknesses of IPV6 and ICMP6, and includes an easy to use packet factory library.

Last update 2012-01-15 - opdateres løbende
Current public version: v1.8 - CCC Camp release

`http://thc.org/thc-ipv6/`

THC IPv6 [0x03] The Included Tools

- - parasite6: icmp neighbor solitication/advertisement spoofer, puts you as man-in-the-middle, same as ARP mitm (and parasite)
- - alive6: an effective alive scanng, which will detect all systems listening to this address
- - dnsdict6: parallized dns ipv6 dictionary bruteforcer
- - fake_router6: announce yourself as a router on the network, with the highest priority
- - redir6: redirect traffic to you intelligently (man-in-the-middle) with a clever icmp6 redirect spoofer
- - toobig6: mtu decreaser with the same intelligence as redir6
- - detect-new-ip6: detect new ip6 devices which join the network, you can run a script to automatically scan these systems etc.
- - dos-new-ip6: detect new ip6 devices and tell them that their chosen IP collides on the network (DOS).
- - trace6: very fast traceroute6 with supports ICMP6 echo request and TCP-SYN
- - flood_router6: flood a target with random router advertisements

- - flood_advertise6: flood a target with random neighbor advertisements
- - exploit6: known ipv6 vulnerabilities to test against a target
- - denial6: a collection of denial-of-service tests againsts a target
- - fuzz_ip6: fuzzer for ipv6
- - implementation6: performs various implementation checks on ipv6
- - implementation6d: listen daemon for implementation6 to check behind a fw
- - fake_mld6: announce yourself in a multicast group of your choice on the net
- - fake_mld26: same but for MLDv2
- - fake_mldrouter6: fake MLD router messages
- - fake_mipv6: steal a mobile IP to yours if IPSEC is not needed for authentication
- - fake_advertiser6: announce yourself on the network
- - smurf6: local smurfer
- - rsmurf6: remote smurfer, known to work only against linux at the moment
- - sendpees6: a tool by willdamn(ad)gmail.com, which generates a neighbor solicitation requests with a lot of CGAs (crypto stuff ;-) to keep the CPU busy. nice.

- - thcping6: sends a hand crafted ping6 packet

and about 15 more tools for you to discover

How to use IPv6

www.solidonetworks.com

hlk@solidonetworks.com

Really how to use IPv6?

Get IPv6 address and routing

Add AAAA (quad A) records to your DNS

Done

www.solidonetworks.com

```
www        IN A        91.102.95.20
           IN AAAA     2a02:9d0:10::9
```

IPv6 Status Denmark

IT- og Telestyrelsen are becoming more active

Unofficial IPv6 task force at `http://www.ipv6tf.dk/`

Other initiatives `http://world-ipv6-day.dk/`

Major providers are ready on back bones

Internet Providers are increasingly becoming ready

Collect information about IPv6

Guidelines for the Secure Deployment of IPv6, SP800-119, NIST
`http://csrc.nist.gov/publications/nistpubs/800-119/sp800-119.pdf`

The Second Internet: Reinventing Computer Networks with IPv6, Lawrence E. Hughes, October 2010,
`http://www.secondinternet.org/`

IPv6 Network Administration af David Malone og Niall Richard Murphy

`http://www.ripe.net`

This presentation ☺

Allocating IPv6 addresses

You have plenty!

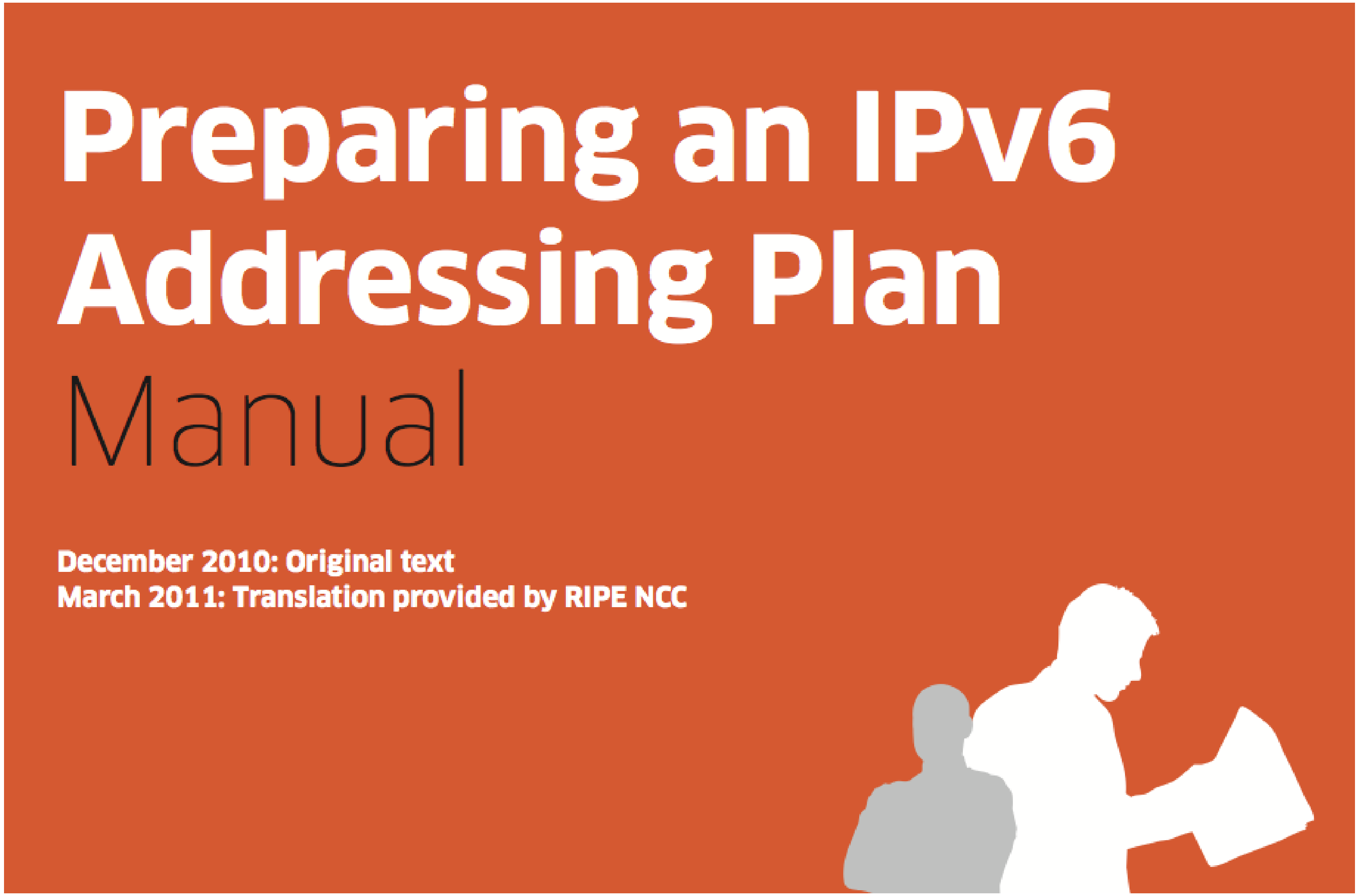
Providers and LIRs will typically get /32

Providers will typically give organisations /48 or /56

Your /48 can be used for:

- 65536 subnets - all host subnets are /64
- Each subnet has 2^{64} addresses

Preparing an IPv6 Addressing Plan



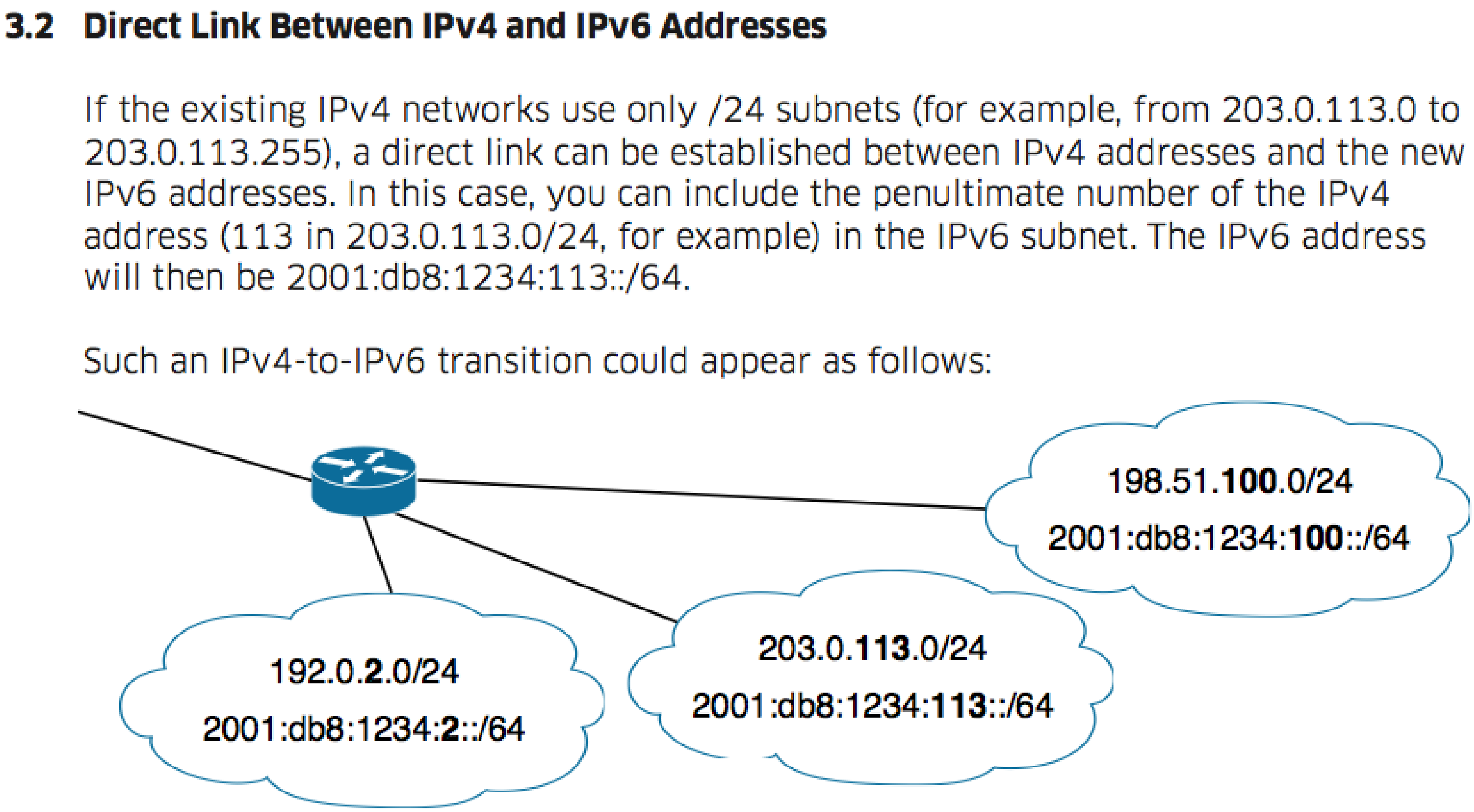
Preparing an IPv6 Addressing Plan

Manual

December 2010: Original text
March 2011: Translation provided by RIPE NCC

http://www.ripe.net/training/material/IPv6-for-LIRs-Training-Course/IPv6_addr_plan4.pdf

Example adress plan input



3.2 Direct Link Between IPv4 and IPv6 Addresses

If the existing IPv4 networks use only /24 subnets (for example, from 203.0.113.0 to 203.0.113.255), a direct link can be established between IPv4 addresses and the new IPv6 addresses. In this case, you can include the penultimate number of the IPv4 address (113 in 203.0.113.0/24, for example) in the IPv6 subnet. The IPv6 address will then be 2001:db8:1234:113::/64.

Such an IPv4-to-IPv6 transition could appear as follows:

Easy and coupled with VLAN IDs it will work ☺

Run IPv6 in production

Make sure you establish IPv6 in **production**

Enabling service on IPv6 without production - bad experience for users

Start by enabling your DNS servers for IPv6 - and DNSSEC - and DNS over TCP
Remember that your firewall might have problems with large DNS packets

Add a production IPv6 router - hardware device or generic server

Tunnels are OK, and SixXS consider their service production

IPv6 business case

- An almost unlimited scalability with a very large IPv6 address space ($2^{1}28$ addresses), enabling IP addresses to each and every device.
- Address self-configuration mechanisms, easing the deployment.
- Improved security and authentication features, such as mandatory IPSec capacities and the possibility to use of the address space to include encryption keys.
- Peer-to-peer connectivity, solving the NAT barrier with specific and permanent IP addresses for any device and/or user of the Internet.
- Mobility features, enabling a seamless connexion when moving from one access point to another access point on the Internet.
- Multi cast and any cast functionalities.
- IPv6 will provide an easier remote interaction with each and every device with a **direct integration to the Internet.** In other words, IPv6 will make possible to move from a network of servers, to a network of things.

Business case for IPv6 is **continuity**

Partial quote from http://www.smartipv6building.org/index.php/en/ipv6-potential

IPv6: Internet redesigned? - no!

Preserve the good stuff

back to basics, internet as it used to be!

fate sharing - connection rely on end points, not intermediary NAT boxes

end-to-end transparency - you have an address and I have an address

Wants: bandwidth +10G, low latency/predictable latency, Quality of Service, Security

IPv6 is evolution, not revolution

Note: IPv6 was not designed to solve all problems, so don't expect it to!

Up and running with IPv6

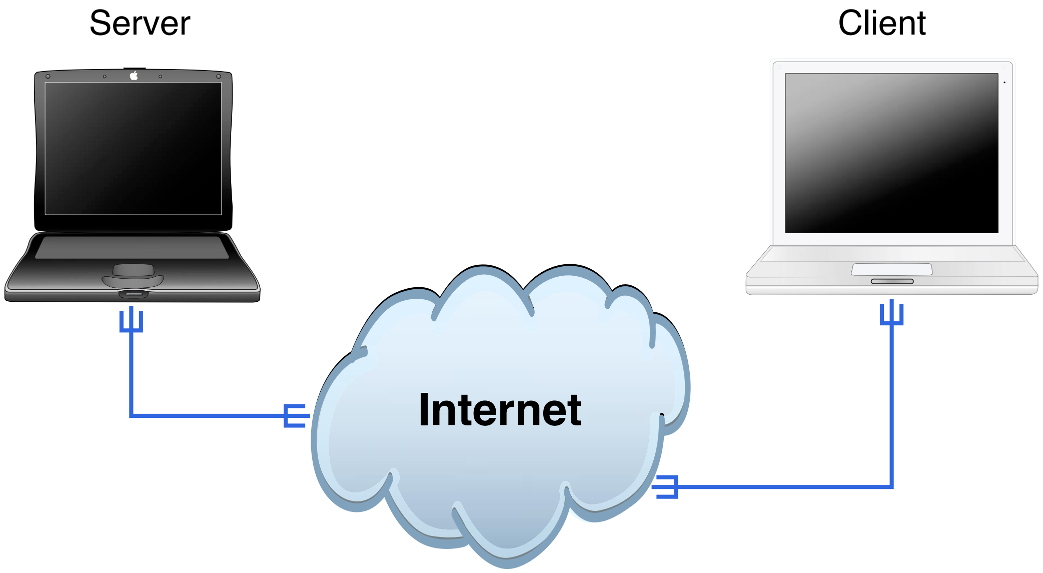
Use ping/ping6 and traceroute to test connectivity

Try in your browser:

- `http://www.kame.net` Dancing turtle
- `http://www.ripe.net` RIPE, look for address up right corner
- `http://loopsofzen.co.uk/` Play a game
- `https://www.sixxs.net/` Apply for IPv6 tunnel

Done ☺

Internet today



Clients and servers

Rooted in academic networks

Protocols which are more than 20 years old, moved to TCP/IP in 1981

Hvad er Internet

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.

Hvad er Internet

80’erne IP/TCP starten af 80’erne

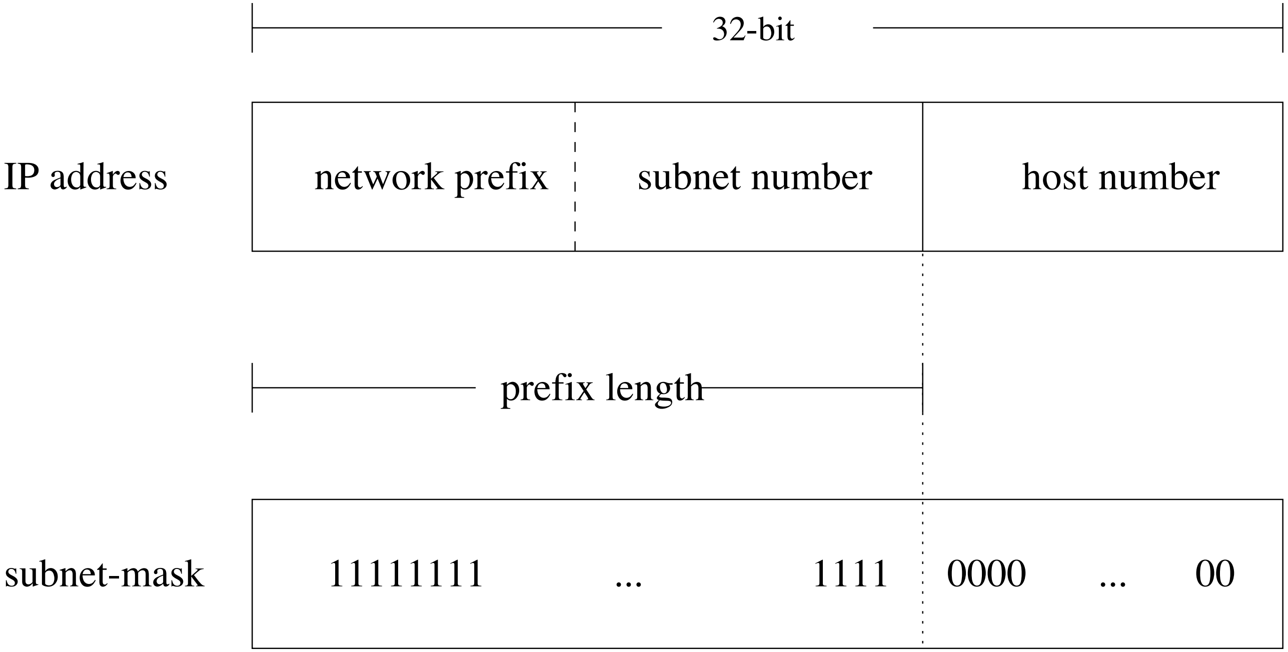
90’erne IP version 6 udarbejdes

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

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

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

Fælles adresserum

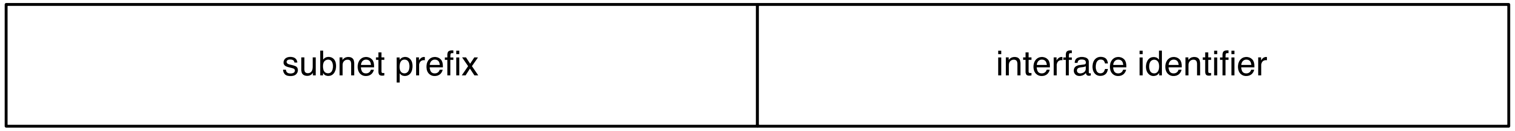


Hvad kendetegner internet idag

Der er et fælles adresserum baseret på 32-bit adresser

En IP-adresse kunne være 10.0.0.1

IPv6 addresser og skrivemåde



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

2001:16d8:ff00:12f::2

- 128-bit adresser, subnet prefix næsten altid 64-bit
- skrives i grupper af 4 hexcifre ad gangen adskilt af kolon :
- foranstillede 0 i en gruppe kan udelades, en række 0 kan erstattes med ::
- dvs 0:0:0:0:0:0:0:0 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
- Læs mere i RFC-3513

IPv6 header - RFC-2460

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Version| Traffic Class |           Flow Label                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Payload Length        |  Next Header  |   Hop Limit   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                         Source Address                        +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                      Destination Address                      +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

IPv6 addressing RFC-4291

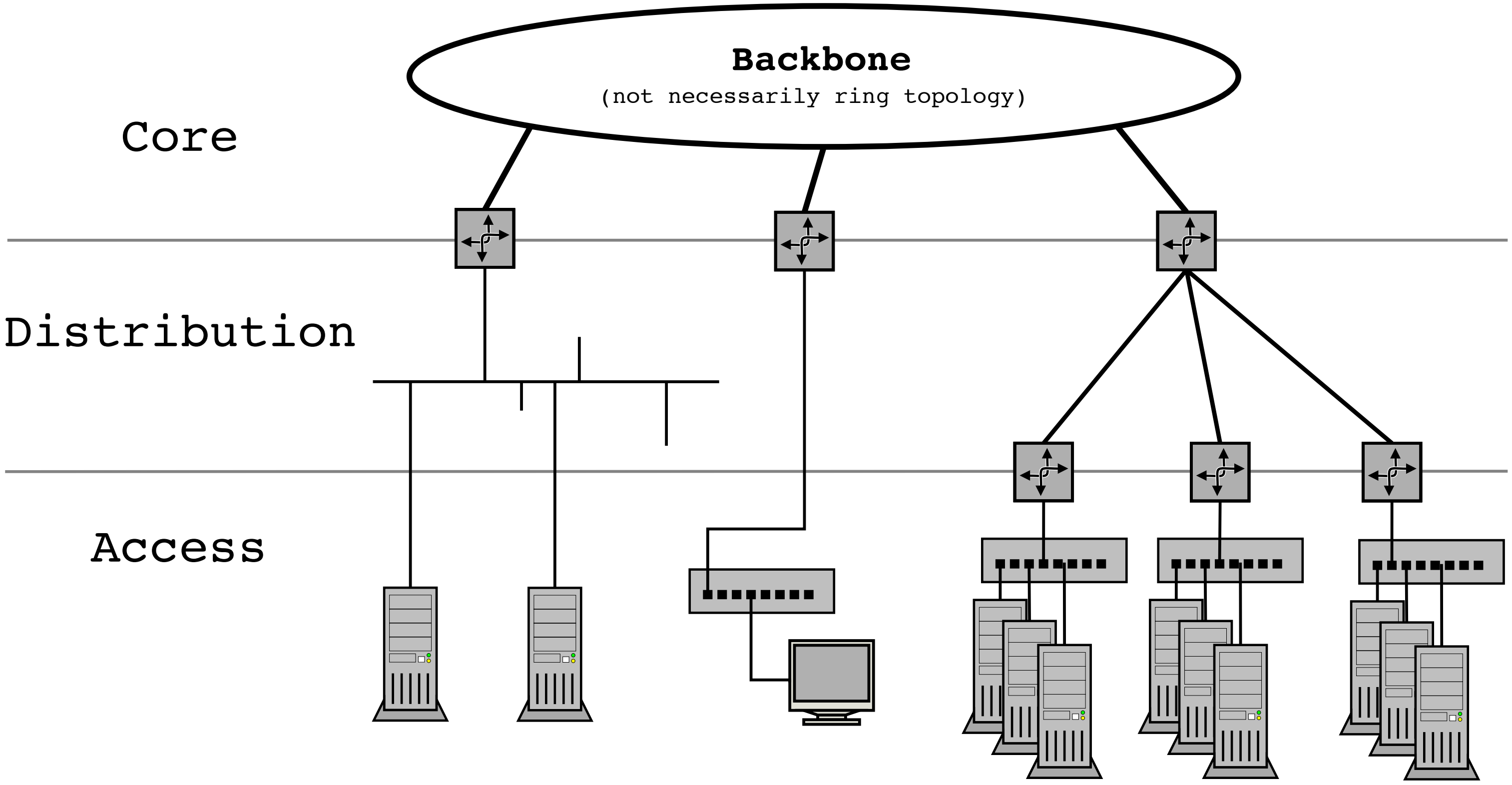
Addresses are always 128-bit identifiers for interfaces and sets of interfaces

Unicast: An identifier for a **single interface**.
A packet sent to a unicast address is delivered to the interface identified by that address.

Anycast: An identifier for a **set of interfaces** (typically belonging to different nodes).
A packet sent to an anycast address is **delivered to one** of the interfaces identified by that address (the ”nearest” one, according to the routing protocols' measure of distance).

Multicast: An identifier for a **set of interfaces** (typically belonging to different nodes).
A packet sent to a multicast address is **delivered to all interfaces identified by that address**.

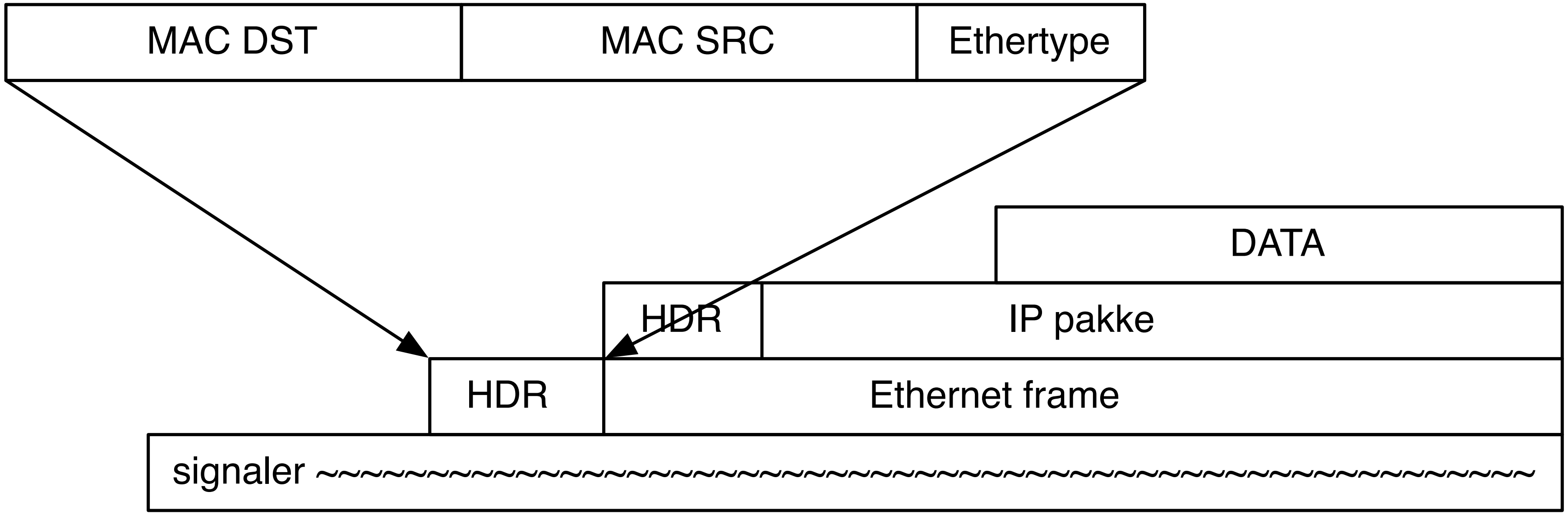
Core, Distribution og Access net



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

~~Where are the NAT gateways?~~

Pakker i en datastrøm


MAC DST
MAC SRC
Ethertype
DATA
HDR
IP pakke
HDR
Ethernet frame
signaler ~~~~~~

Ser vi data som en datastrøm er pakkerne blot et mønster lagt henover data

Netværksteknologien definerer start og slut på en frame

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

Collect information about your network

devices - what is a network device?

switches - Layer 2 does not matter much, management by RFC-1918 IPv4 is probably wise

routers - most important, connectivity MUST support IPv6. Check vendor home page - do NOT assume support is ready

Security devices: firewalls, IDS/IPS, VPN - critical and support in general poor. Some vendors such as Cisco ASA and Juniper SRX has good support

Hello neighbors

```
$ ping6 -w -I en1 ff02::1
PING6(72=40+8+24 bytes) fe80::223:6cff:fe9a:f52c%en1 --> ff02::1
30 bytes from fe80::223:6cff:fe9a:f52c%en1: bigfoot
36 bytes from fe80::216:cbff:feac:1d9f%en1: mike.kramse.dk.
38 bytes from fe80::200:aaff:feab:9f06%en1: xrx0000aaab9f06
34 bytes from fe80::20d:93ff:fe4d:55fe%en1: harry.local
36 bytes from fe80::200:24ff:fec8:b24c%en1: kris.kramse.dk.
31 bytes from fe80::21b:63ff:fef5:38df%en1: airport5
32 bytes from fe80::216:cbff:fec4:403a%en1: main-base
44 bytes from fe80::217:f2ff:fee4:2156%en1: Base Station Koekken
35 bytes from fe80::21e:c2ff:feac:cd17%en1: arnold.local
```

Vigtigste protokoller

ARP Address Resolution Protocol

IP og ICMP Internet Control Message Protocol

UDP User Datagram Protocol

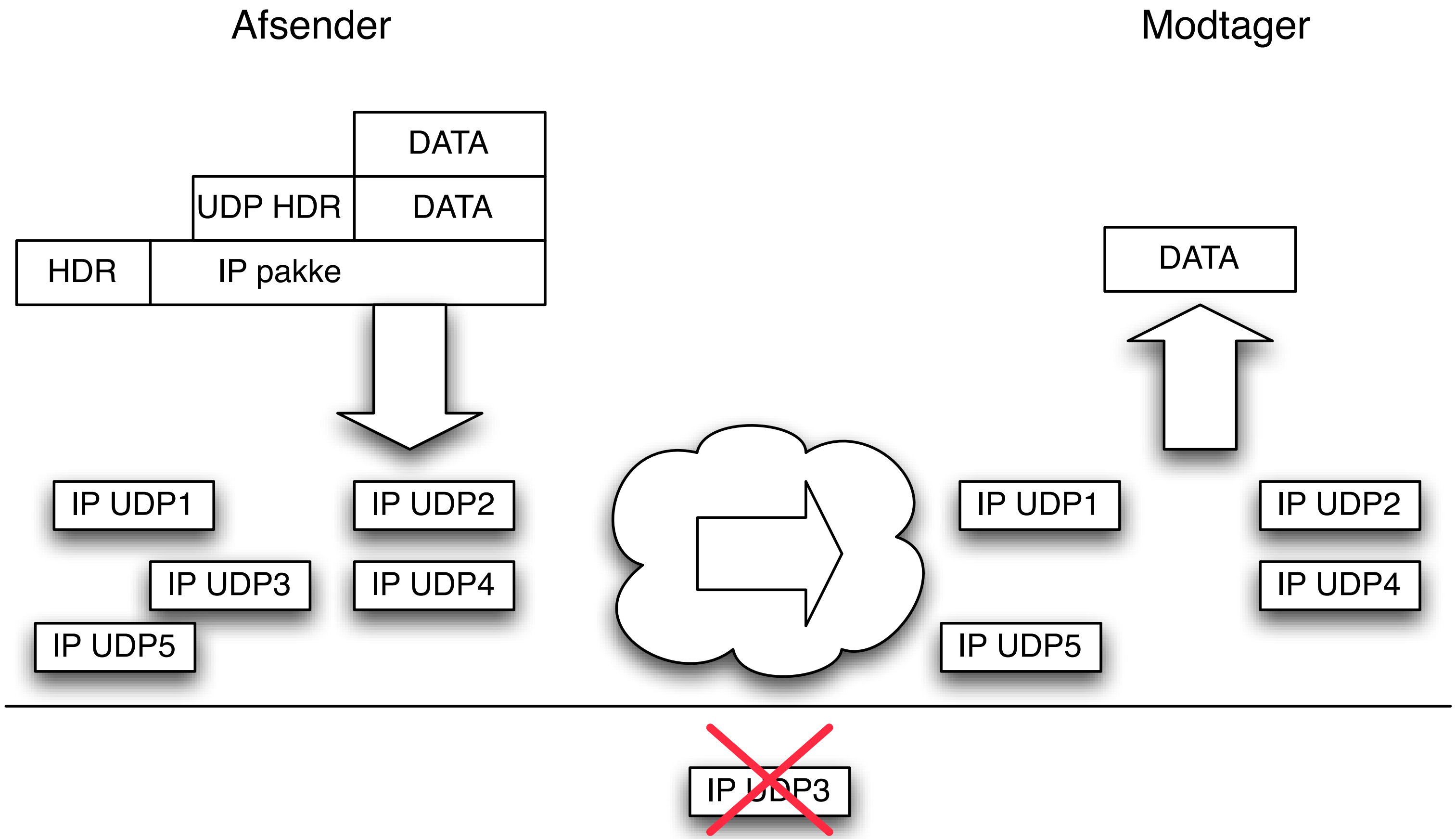
TCP Transmission Control Protocol

DHCP Dynamic Host Configuration Protocol

DNS Domain Name System

Ovenstående er omtrent minimumskrav for at komme på internet

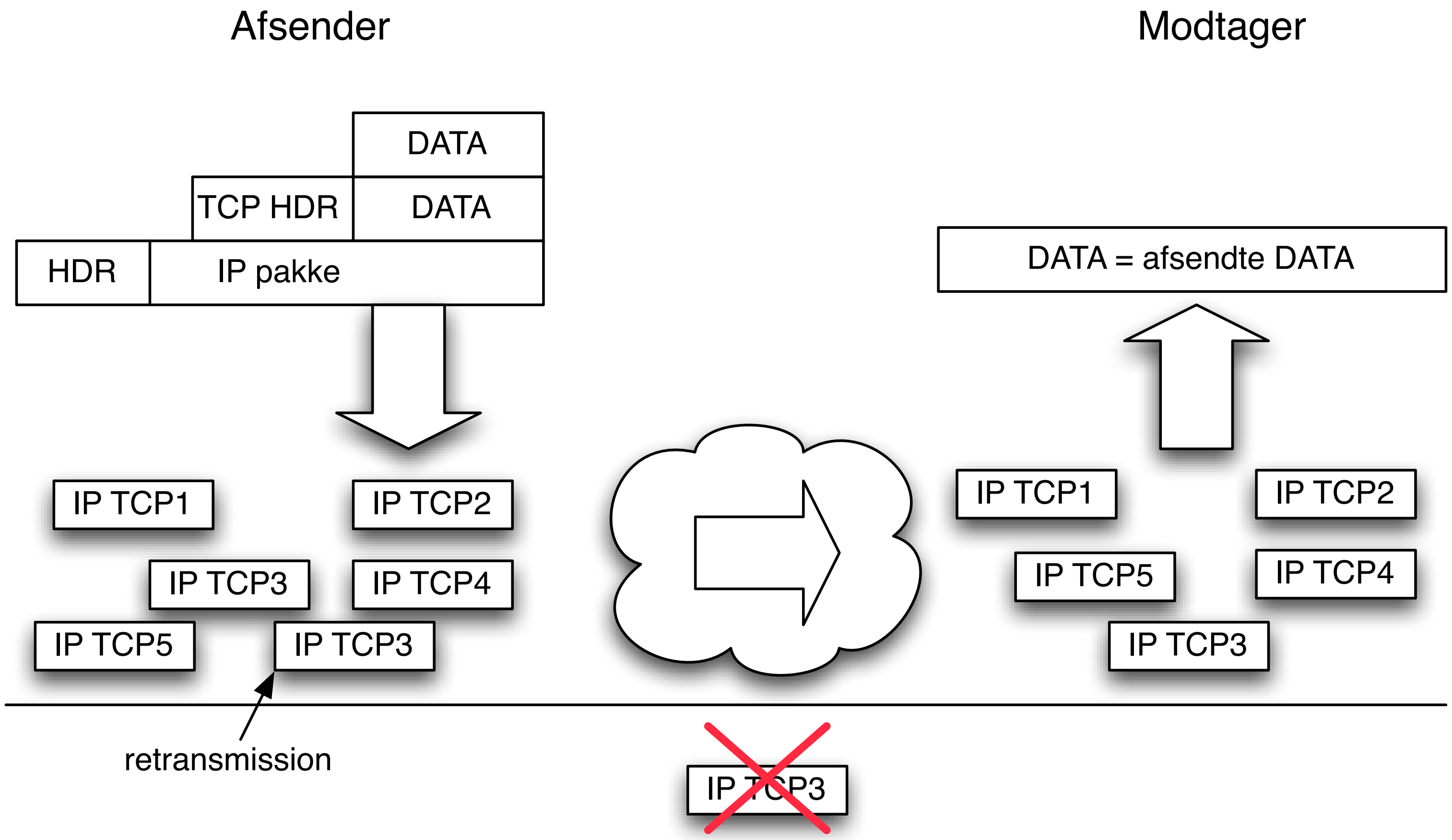
UDP User Datagram Protocol



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

Kan benyttes til multicast/broadcast - flere modtagere

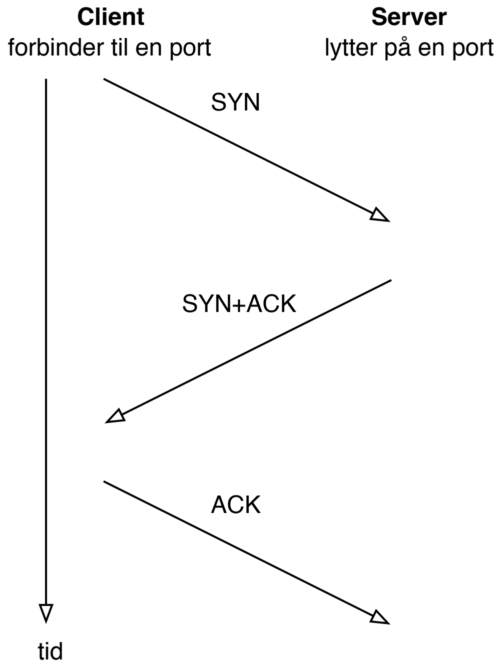
TCP Transmission Control Protocol



Forbindelsesorienteret RFC-791 September 1981, connection-oriented

Enten overføres data eller man får fejlmeddelelse

TCP three way handshake



- **TCP SYN half-open** scans
- Tidligere loggede systemer kun når der 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

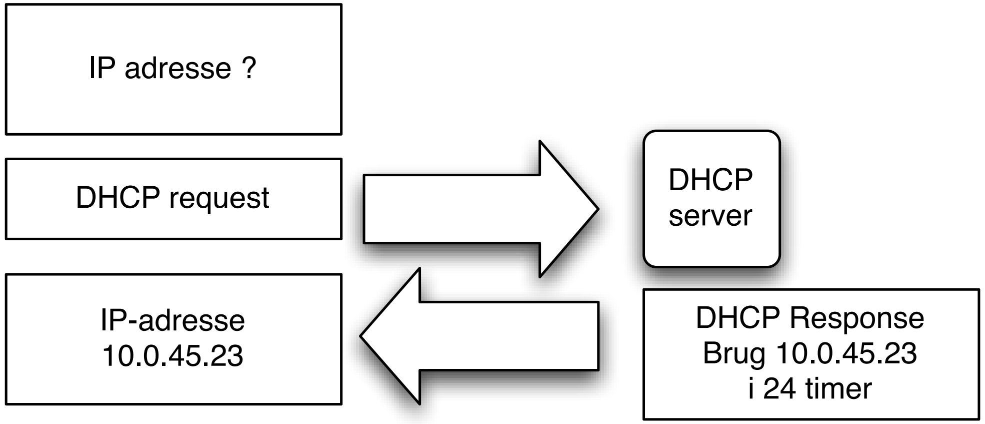
De har lister med hvilke protokoller har hvilke protokol ID m.v.

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 på `http://www.iana.org`

DHCP Dynamic Host Configuration Protocol



Hvordan får 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

NB: de fleste clients vil idag implementere IPv6 privacy addresses

IPv6 autoconfiguration

`Modified EUI-64 format-based interface identifiers`

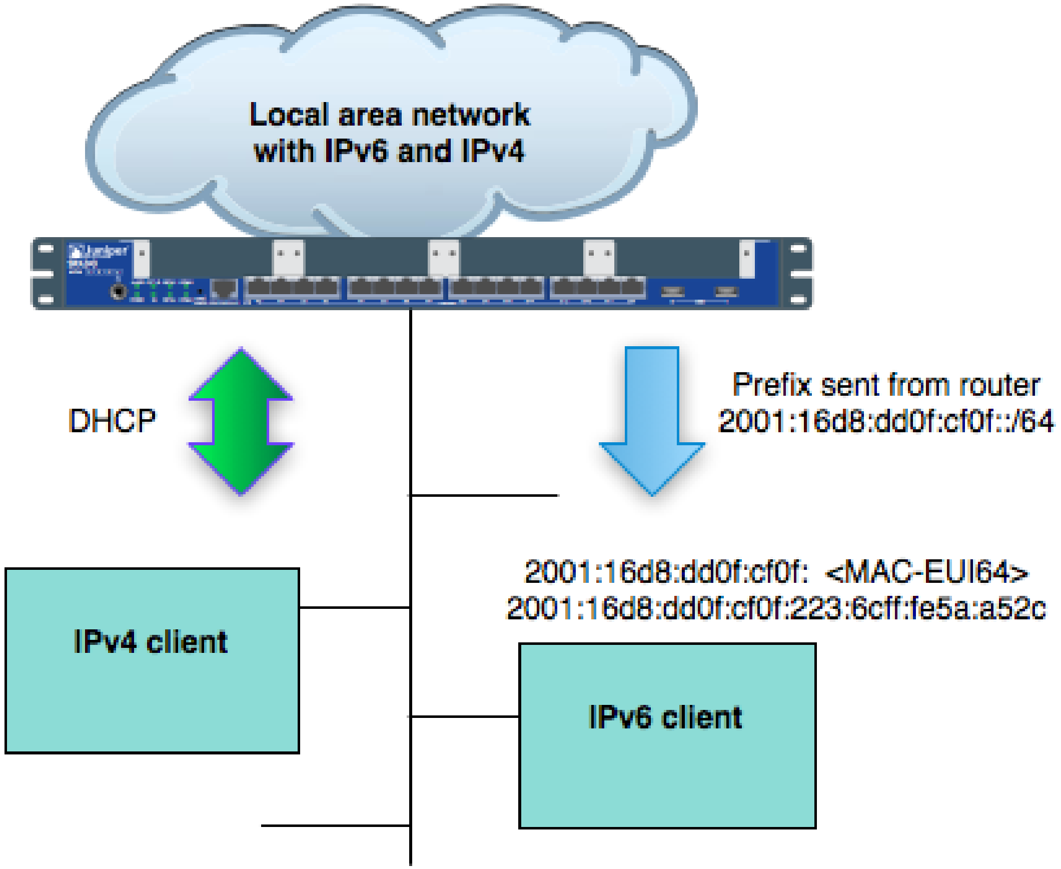
```
ifconfig en1
en1: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
      ether 00:23:6c:9a:f5:2c
             00-23-6c-ff-fe-9a-f5-2c  48-bit MAC stretched to become EUI-64
             02-23-6c-ff-fe-9a-f5-2c  inverting the "u" bit (universal/local bit)
             fe80::  +  0223:6cff:fe9a:f52c   add link-local prefix
      inet6 fe80::223:6cff:fe9a:f52c%en1 prefixlen 64 scopeid 0x6
```

DHCPv6 is available, but **stateless autoconfiguration** is king

Routers announce subnet prefix via **router advertisements**

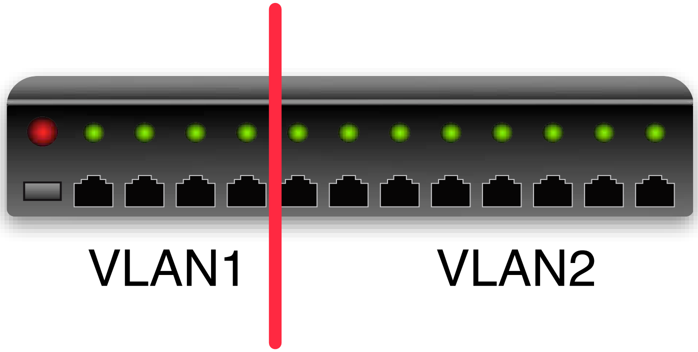
Individual nodes then combine this with their EUI64 identifier

Router advertisement daemon



VLAN Virtual LAN

Portbased VLAN



Nogle switche tillader at man opdeler portene

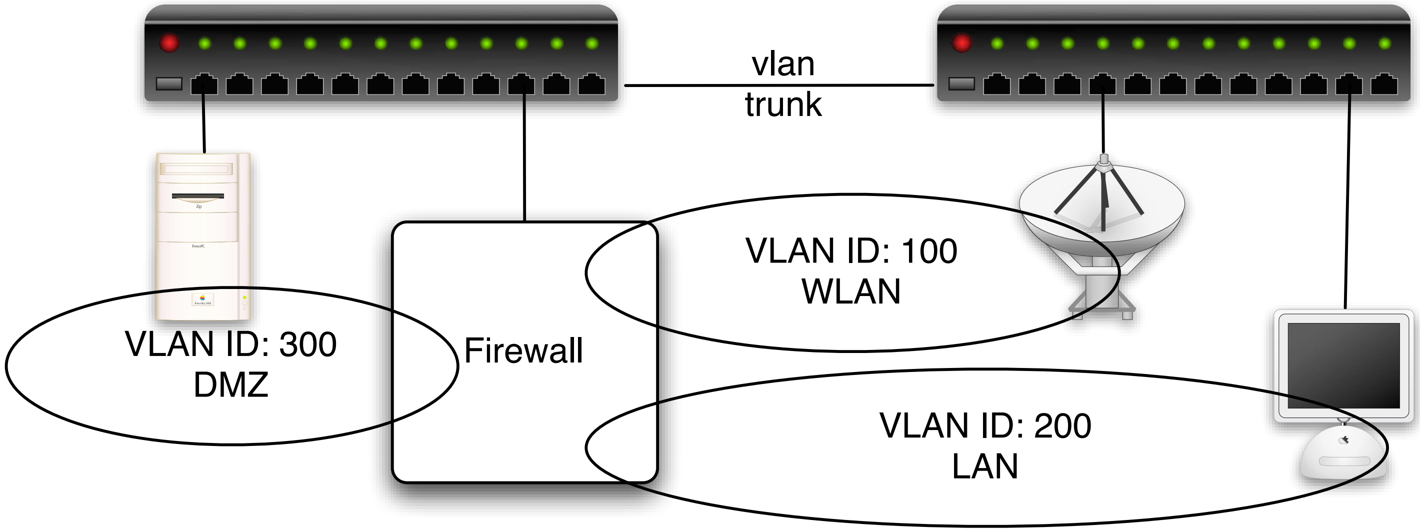
Denne opdeling kaldes VLAN og portbaseret er det mest simple

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

IEEE 802.1q



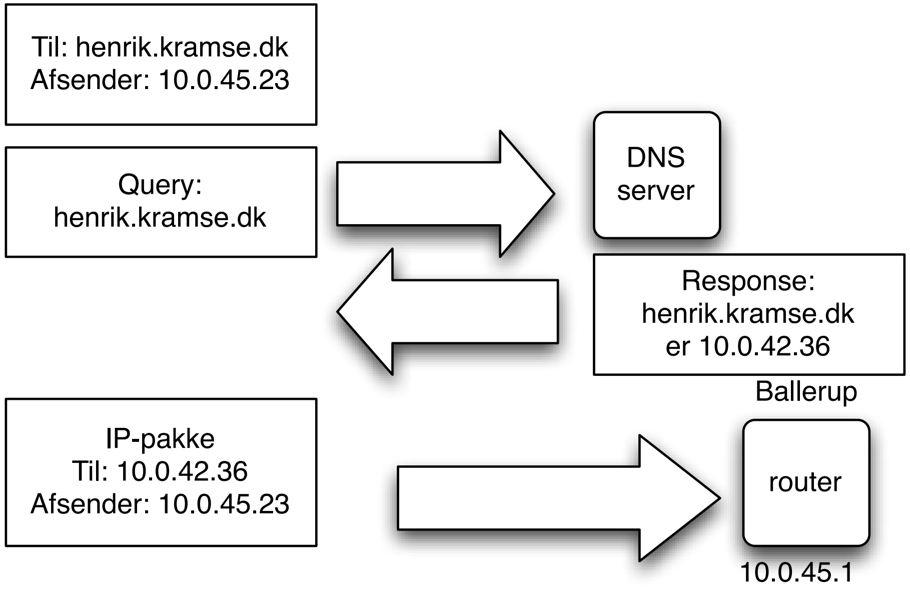
Nogle switche tillader konfiguration med 802.1q VLAN tagging på Ethernet niveau

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

Domain Name System



Gennem DHCP får man typisk også information om DNS servere

En DNS server kan slå navne, domæner og adresser op

Foregår via query og response med datatyper kaldet resource records

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

Mere end navneopslag

består 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.
```

Danish resources - get involved

Danish IPv6 task force - unofficial `http://www.ipv6tf.dk`

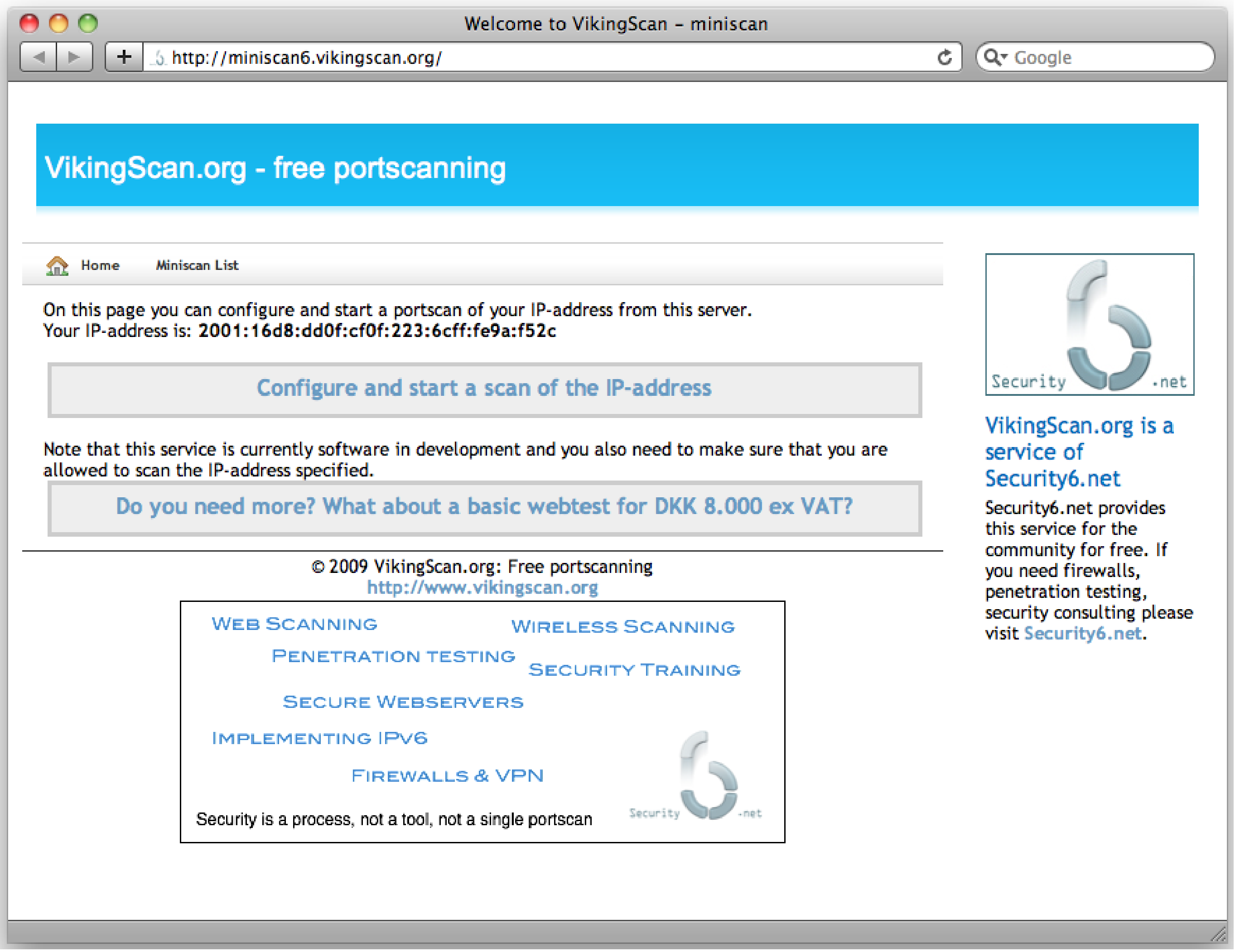
Spørgsmål?

Henrik Lund Kramshøj
hlk@solido.net

`http://www.solidonetworks.com`

I er altid velkomne til at sende spørgsmål på e-mail

VikingScan.org - free portscanning



Welcome to VikingScan – miniscan
http://miniscan6.vikingscan.org/
Google

VikingScan.org - free portscanning

On this page you can configure and start a portscan of your IP-address from this server.
Your IP-address is: **2001:16d8:dd0f:cf0f:223:6cff:fe9a:f52c**

Configure and start a scan of the IP-address

Note that this service is currently software in development and you also need to make sure that you are allowed to scan the IP-address specified.

Do you need more? What about a basic webtest for DKK 8.000 ex VAT?

© 2009 VikingScan.org: Free portscanning
http://www.vikingscan.org

Security is a process, not a tool, not a single portscan

VikingScan.org is a service of Security6.net

Security6.net provides this service for the community for free. If you need firewalls, penetration testing, security consulting please visit Security6.net.

Bøger om IPv6

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