Welcome to

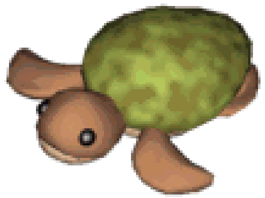
IPv6 in real networks

Henrik Lund Kramshøj
hlk@solidonetworks.com

http://www.solidonetworks.com

Slides are available as PDF

Goal



Introduce IPv6

IPv6 addressing

Neighbor Discovery Protocol

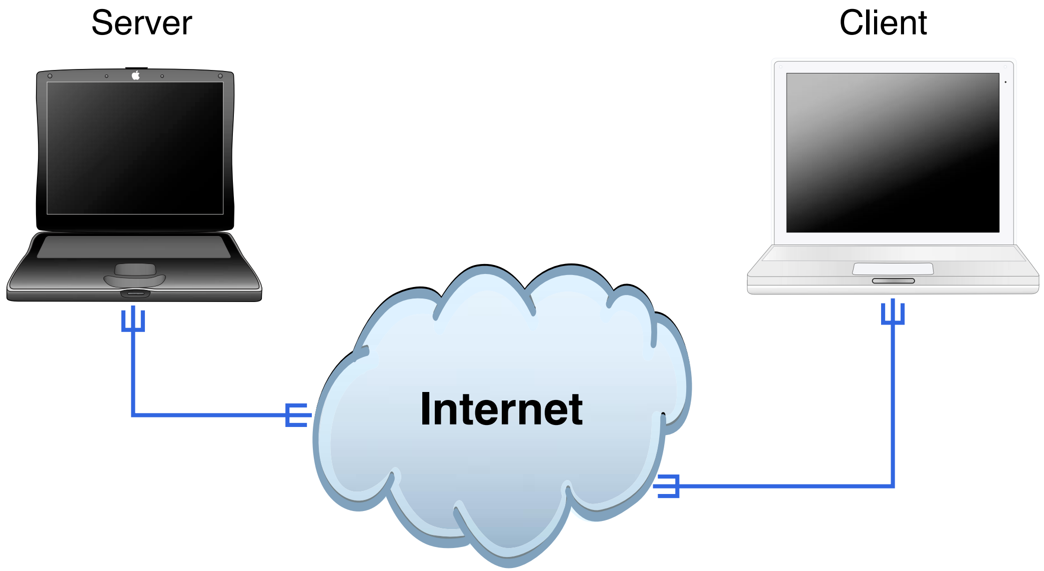
IPv4 vs IPv6 - Differences and similarities

Practical information about implementing IPv6 networks

Configuration examples

Ressources, links and documents

Internet idag



Clients and servers

Rooted in academic networks

Protocols which are more than 20 years old

Very little encryption and security built into the network

Internet is built on Open Standards

We reject kings, presidents, and voting.
We believe in rough consensus and running code.
– The IETF credo Dave Clark, 1992.

RFC - Request for comments

RFC, Best Current Practice, FYI, informational

Standards track:
Proposed Standard $\rightarrow$ Draft Standard $\rightarrow$ Standard

Internetworking: history

1961 L. Kleinrock, MIT packet-switching theory

1962 J. C. R. Licklider, MIT - notes

1964 Paul Baran: On Distributed Communications

1969 ARPANET 4 nodes

1971 14 nodes

1973 Design of Internet Protocols started

1973 Email is about 75% of all ARPANET traffic

1974 TCP/IP: Cerf/Kahn: A protocol for Packet Network Interconnection

1983 EUUG → DKUUG/DIKU forbindelse

1988 About 60.000 systems on the internet - The Morris Worm hits about 10%

2002 Ialt ca. 130 millioner på Internet

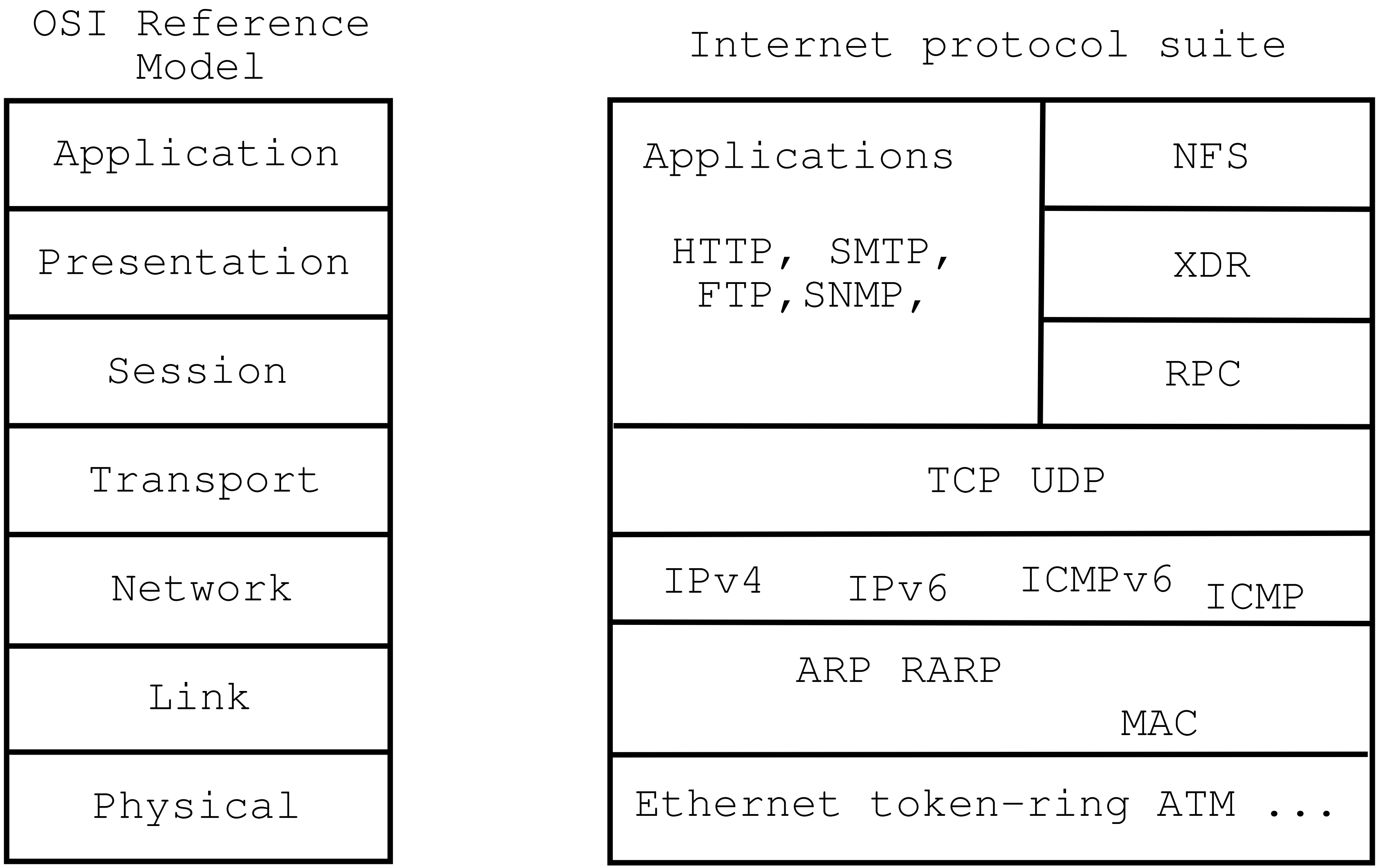
2010 IANA reserved blocks 7% (Maj 2010) - `http://www.potaroo.net/tools/ipv4/`

Fremtiden - 2010 og fremefter

The Mobile Network in 2010 and 2011
Global mobile data traffic grew 2.6-fold in 2010, nearly tripling for the third year in a row. The 2010 mobile data traffic growth rate was higher than anticipated. Last year's forecast projected that the growth rate would be 149 percent. This year's estimate is that global mobile data traffic grew 159 percent in 2010.
...
Last year's mobile data traffic was three times the size of the entire global Internet in 2000. Global mobile data traffic in 2010 (237 petabytes per month) was over three times greater than the total global Internet traffic in 2000 (75 petabytes per month).
...
There will be 788 million mobile-only Internet users by 2015. The mobile-only Internet population will grow 56-fold from 14 million at the end of 2010 to 788 million by the end of 2015.

Kilde: *Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2010 - 2015*

OSI & Internet Protocols



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!

The Internet has done this before!

Because all hosts can not be converted to TCP simultaneously, and some will implement only IP/TCP, it will be necessary to provide temporarily for communication between NCP-only hosts and TCP-only hosts. To do this certain hosts which implement both NCP and IP/TCP will be designated as relay hosts. These relay hosts will support Telnet, FTP, and Mail services on both NCP and TCP. These relay services will be provided beginning in November 1981, and will be fully in place in January 1982.

Initially there will be many NCP-only hosts and a few TCP-only hosts, and the load on the relay hosts will be relatively light. As time goes by, and the conversion progresses, there will be more TCP capable hosts, and fewer NCP-only hosts, plus new TCP-only hosts. But, presumably most hosts that are now NCP-only will implement IP/TCP in addition to their NCP and become ”dual protocol” hosts. So, while the load on the relay hosts will rise, it will not be a substantial portion of the total traffic.

NCP/TCP Transition Plan November 1981 RFC-801 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        IN A       91.102.95.20
           IN AAAA    2a02:9d0:10::9
```

IPv4 header - RFC-791

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 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    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

                  Example Internet Datagram Header
```

IPv6 header - RFC-2460

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

IPv6 - new and improved

IPv6 - extension headers RFC-2460

- Hop-by-Hop Options
- Routing (Type 0)
- Fragment - fragmentation only at end-points!
- Destination Options
- Authentication
- Encapsulating Security Payload

Note: IPsec (AH and ESP) are mandatory for IPv6 hosts

Path MTU, PMTU implemented larger default MTU, at least 1280 bytes

Fragmentation only at the source host, no router fragmentation

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**.

IPv6 addressing RFC-4291, cont.

subnet prefix	interface identifier

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

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

8 times 4 hex-digits seperated by colon x:x:x:x:x:x:x:x

Written as ipv6-address/prefix-length CIDR notation

Leading zeros can be removed

One or more groups of 16 bits of zeros can be replaced by ::

Examples:

- ABCD:EF01:2345:6789:ABCD:EF01:2345:6789
- Adddress 2001:DB8:0:0:8:800:200C:417A
- Address of loopback ::1
- IPv6 prefix 2a02:09d0:95::1/64, subnet 2a02:09d0:0095:0000::/64
- Address 2a02:09d0:95::1 or 2a02:09d0:0095:0000:0000:0000:0000:0001

- Danish sites
- Name servers for .dk
  p.nic.dk has IPv6 address 2001:500:14:6036:ad::1
  s.nic.dk has IPv6 address 2a01:3f0:0:303::53
  b.nic.dk has IPv6 address 2a01:630:0:80::53
- ns1.gratisdns.dk has IPv6 address 2a02:9d0:3002:1::2
- www.solidonetworks.com has IPv6 address 2a02:9d0:10::9

IPv6 address - regional prefixes

Aggregatable Global Unicast

2001::/16 RIR subTLA space

- 2001:200::/23 APNIC
- 2001:400::/23 ARIN
- 2001:600::/23 RIPE

2002::/16 6to4 prefix

3ffe::/16 6bone allocation - old not used anymore

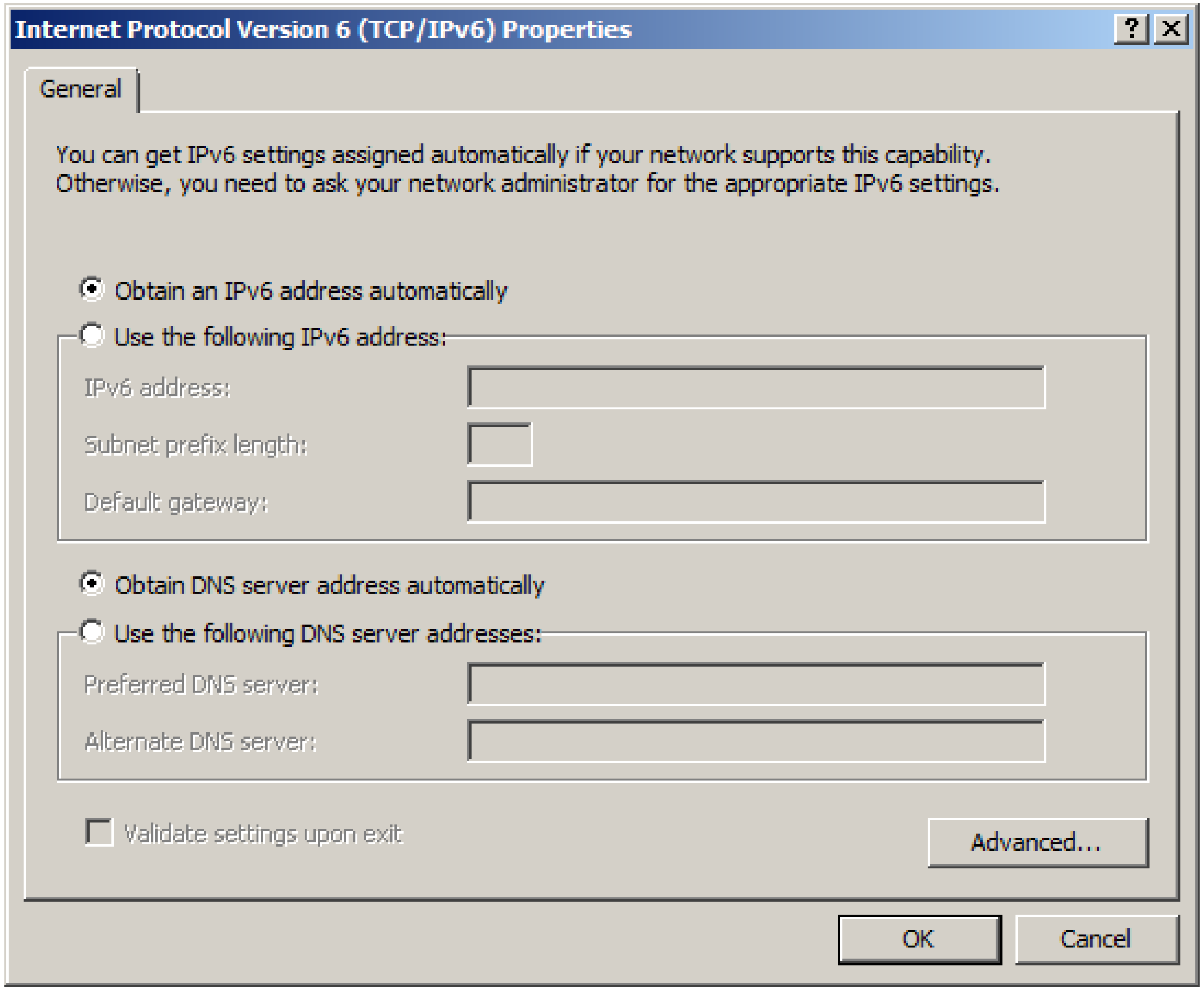
IPv6 address - special prefixes

- link-local unicast addresses
  fe80::/10 generated from the interface MAC address EUI-64
- FEC0::/10 site-local - deprecated in RFC-3879
- FC00::/7 Unique Local IPv6 Unicast Addresses RFC-4193
  `http://www.simpledns.com/private-ipv6.aspx`
- 2001:0DB8::/32 NON-ROUTABLE range to be used for documentation purpose RFC-3849.

Windows - ipconfig

```
Command Prompt
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Henrik Kramshoej>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : kramse.dk
   IPv6 Address. . . . . . . . . . . : 2001:16d8:dd0f:cf0f:f049:94d0:75d8:683e
   Temporary IPv6 Address. . . . . . : 2001:16d8:dd0f:cf0f:84bd:adea:fb61:8960
   Link-local IPv6 Address . . . . . : fe80::f049:94d0:75d8:683e%11
   IPv4 Address. . . . . . . . . . . : 10.0.42.107
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::200:24ff:fec8:b24c%11
                                       10.0.42.1

Tunnel adapter isatap.kramse.dk:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : kramse.dk

Tunnel adapter Local Area Connection* 11:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:0:5ef5:73b8:1000:322b:f5ff:d594
   Link-local IPv6 Address . . . . . : fe80::1000:322b:f5ff:d594%13
   Default Gateway . . . . . . . . . :

C:\Users\Henrik Kramshoej>_
```

Windows - control panel



Unix - practical examples ifconfig and ping

```
$ ifconfig en0
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
inet6 fe80::216:cbff:feac:1d9f%en0 prefixlen 64 scopeid 0x4
inet 10.0.42.15 netmask 0xffffff00 broadcast 10.0.42.255
inet6 2001:16d8:dd0f:cf0f:216:cbff:feac:1d9f prefixlen 64 autoconf
ether 00:16:cb:ac:1d:9f
media: autoselect (1000baseT <full-duplex>) status: active

$ ping6 ::1
PING6(56=40+8+8 bytes) ::1 --> ::1
16 bytes from ::1, icmp_seq=0 hlim=64 time=0.089 ms
16 bytes from ::1, icmp_seq=1 hlim=64 time=0.155 ms

$ traceroute6 2001:16d8:dd0f:cf0f::1
traceroute6 to 2001:16d8:dd0f:cf0f::1 (2001:16d8:dd0f:cf0f::1)
from 2001:16d8:dd0f:cf0f:216:cbff:feac:1d9f, 64 hops max, 12 byte packets
 1  2001:16d8:dd0f:cf0f::1  0.399 ms  0.371 ms  0.294 ms
```

ping6 global unicast address

```
root# ping6 2001:1448:81:beef:20a:95ff:fef5:34df
PING6(56=40+8+8 bytes) 2001:1448:81:beef::1 --> 2001:1448:81:beef:20a:95ff:fef5:34df
16 bytes from 2001:1448:81:beef:20a:95ff:fef5:34df, icmp_seq=0 hlim=64 time=10.639 ms
16 bytes from 2001:1448:81:beef:20a:95ff:fef5:34df, icmp_seq=1 hlim=64 time=1.615 ms
16 bytes from 2001:1448:81:beef:20a:95ff:fef5:34df, icmp_seq=2 hlim=64 time=2.074 ms
^C
--- 2001:1448:81:beef:20a:95ff:fef5:34df ping6 statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 1.615/4.776/10.639 ms
```

ping6 link-local address

```
hlk@bigfoot:hlk$ ping6 -I en1 fe80::20d:93ff:fe4d:55fe
PING6(56=40+8+8 bytes) fe80::223:6cff:fe9a:f52c%en1 --> fe80::20d:93ff:fe4d:55fe
16 bytes from fe80::20d:93ff:fe4d:55fe%en1, icmp_seq=0 hlim=64 time=1.557 ms
16 bytes from fe80::20d:93ff:fe4d:55fe%en1, icmp_seq=1 hlim=64 time=1.725 ms
^C
--- fe80::20d:93ff:fe4d:55fe ping6 statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.557/1.641/1.725/0.084 ms
```

Note: -I en1 specifies that this interface is being used.

ping6 til specielle adresser

```
root# ping6 -I en1 ff02::1

PING6(56=40+8+8 bytes) fe80::230:65ff:fe17:94d1 --> ff02::1
16 bytes from fe80::230:65ff:fe17:94d1, icmp_seq=0 hlim=64 time=0.483 ms
16 bytes from fe80::20a:95ff:fef5:34df, icmp_seq=0 hlim=64 time=982.932 ms
16 bytes from fe80::230:65ff:fe17:94d1, icmp_seq=1 hlim=64 time=0.582 ms
16 bytes from fe80::20a:95ff:fef5:34df, icmp_seq=1 hlim=64 time=9.6 ms
16 bytes from fe80::230:65ff:fe17:94d1, icmp_seq=2 hlim=64 time=0.489 ms
16 bytes from fe80::20a:95ff:fef5:34df, icmp_seq=2 hlim=64 time=7.636 ms
^C
--- ff02::1 ping6 statistics ---
4 packets transmitted, 4 packets received, +4 duplicates, 0% packet loss
round-trip min/avg/max = 0.483/126.236/982.932 ms

ff02::1 multicast address of all-hosts on the local link
ff02::2 multicast address of all-routers on the local link
```

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
```

Only Two places need updating the file /etc/sysconfig/network:

```
NETWORKING=yes
NETWORKING_IPV6=yes
HOSTNAME=host1.armadahosting.com
GATEWAY=10.234.123.254
```

From the file: /etc/sysconfig/network-scripts/ifcfg-eth0:

```
DEVICE=eth0
BOOTPROTO=none
ONBOOT=yes
BROADCAST=10.234.123.255
NETWORK=10.234.123.0
NETMASK=255.255.255.0
IPADDR=10.234.123.90
USERCTL=no
IPV6INIT=yes
IPV6ADDR=2a02:9d0:10::10:234:123:90
IPV6_DEFAULTGW=2a02:9d0:10::1
```


IPv6 autoconfiguration

```
Modified EUI-64 format-based interface identifiers
```

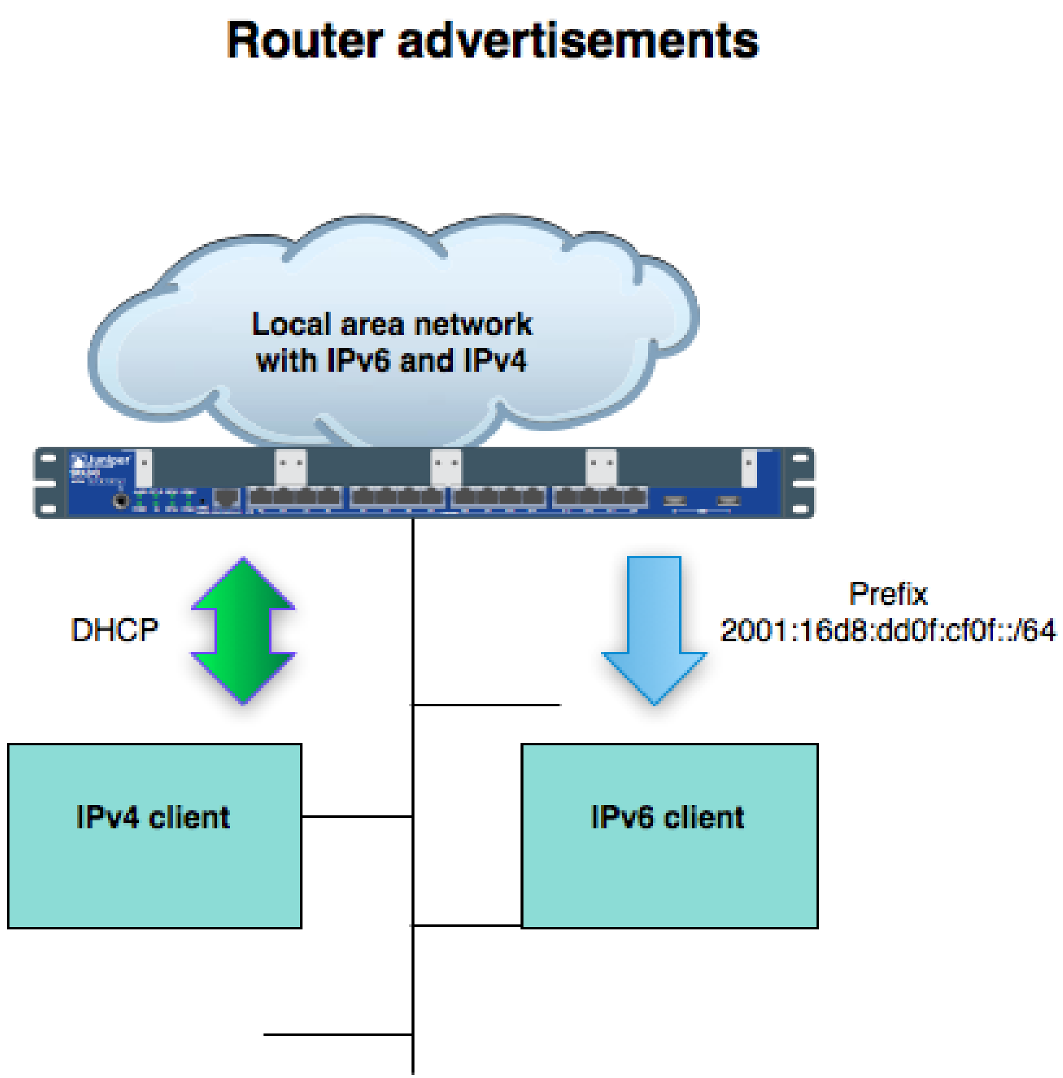
ifconfig en1
en1: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    ether 00:23:6c:9a:f5:2c
        00-23-6c-ff-fe-9a-f5-2c 48-bit MAC stretched to become EUI-64
        02-23-6c-ff-fe-9a-f5-2c inverting the "u" bit (universal/local bit)
        fe80:: + 0223:6cff:fe9a:f52c add link-local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



IPv6 sockets

```
root# netstat -an | grep -i listen

tcp46  0  0  *.80              *.*    LISTEN
tcp4   0  0  *.6000            *.*    LISTEN
tcp4   0  0  127.0.0.1.631     *.*    LISTEN
tcp4   0  0  *.25              *.*    LISTEN
tcp4   0  0  *.20123           *.*    LISTEN
tcp46  0  0  *.20123           *.*    LISTEN
tcp4   0  0  127.0.0.1.1033    *.*    LISTEN
```

Note: some platforms show tcp/tcp6 for IPv4/IPv6 and some show tcp4/tcp6

IPv6 - inet6 family

```
root# netstat -an -f inet6

Active Internet connections (including servers)
Proto Recv Send  Local  Foreign   (state)
tcp46  0    0     *.80      *.*      LISTEN
tcp46  0    0     *.22780   *.*      LISTEN
udp6   0    0     *.5353    *.*
udp6   0    0     *.5353    *.*
udp6   0    0     *.514     *.*
icm6   0    0     *.*       *.*
icm6   0    0     *.*       *.*
icm6   0    0     *.*       *.*
```

Note: this is from a Mac OS X and edited a little

IPv6 is default for a lot of services

```
root# telnet localhost 80

Trying ::1...
Connected to localhost.
Escape character is '^]'.
GET / HTTP/1.0

HTTP/1.1 200 OK
Date: Thu, 19 Feb 2004 09:22:34 GMT
Server: Apache/2.0.43 (Unix)
Content-Location: index.html.en
Vary: negotiate,accept-language,accept-charset
...
```

IPv6 is also default i OpenSSH

```
hlk$ ssh -v localhost -p 20123

OpenSSH_3.6.1p1+CAN-2003-0693, SSH protocols 1.5/2.0, OpenSSL 0x0090702f
debug1: Reading configuration data /Users/hlk/.ssh/config
debug1: Applying options for *
debug1: Reading configuration data /etc/ssh_config
debug1: Rhosts Authentication disabled, originating port will not be trusted.
```

debug1: Connecting to localhost [::1] port 20123.

```
debug1: Connection established.
debug1: identity file /Users/hlk/.ssh/id_rsa type -1
debug1: identity file /Users/hlk/.ssh/id_dsa type 2
debug1: Remote protocol version 2.0, remote software version OpenSSH_3.6.1p1+CA
debug1: match: OpenSSH_3.6.1p1+CAN-2003-0693 pat OpenSSH*
debug1: Enabling compatibility mode for protocol 2.0
debug1: Local version string SSH-2.0-OpenSSH_3.6.1p1+CAN-2003-0693
```

Note: specify -4 or -6 to use specific version

Apache HTTPD server

The world most popular HTTP server for many years `http://httpd.apache.org`

```
Listen 0.0.0.0:80
Listen [::]:80
...
Allow from 127.0.0.1
Allow from 2001:1448:81:0f:2d:9ff:f86:3f
Allow from 217.157.20.133
```

Apache access log

```
root# tail -f access_log
::1 - - [19/Feb/2004:09:05:33 +0100] "GET /images/IPv6ready.png
HTTP/1.1" 304 0
::1 - - [19/Feb/2004:09:05:33 +0100] "GET /images/valid-html401.png
HTTP/1.1" 304 0
::1 - - [19/Feb/2004:09:05:33 +0100] "GET /images/snowflake1.png
HTTP/1.1" 304 0
::1 - - [19/Feb/2004:09:05:33 +0100] "GET /~hlk/security6.net/images/logo-1.png
HTTP/1.1" 304 0
2001:1448:81:beef:20a:95ff:fef5:34df - - [19/Feb/2004:09:57:35 +0100]
"GET / HTTP/1.1" 200 1456
2001:1448:81:beef:20a:95ff:fef5:34df - - [19/Feb/2004:09:57:35 +0100]
"GET /apache_pb.gif HTTP/1.1" 200 2326
2001:1448:81:beef:20a:95ff:fef5:34df - - [19/Feb/2004:09:57:36 +0100]
"GET /favicon.ico HTTP/1.1" 404 209
2001:1448:81:beef:20a:95ff:fef5:34df - - [19/Feb/2004:09:57:36 +0100]
"GET /favicon.ico HTTP/1.1" 404 209
```

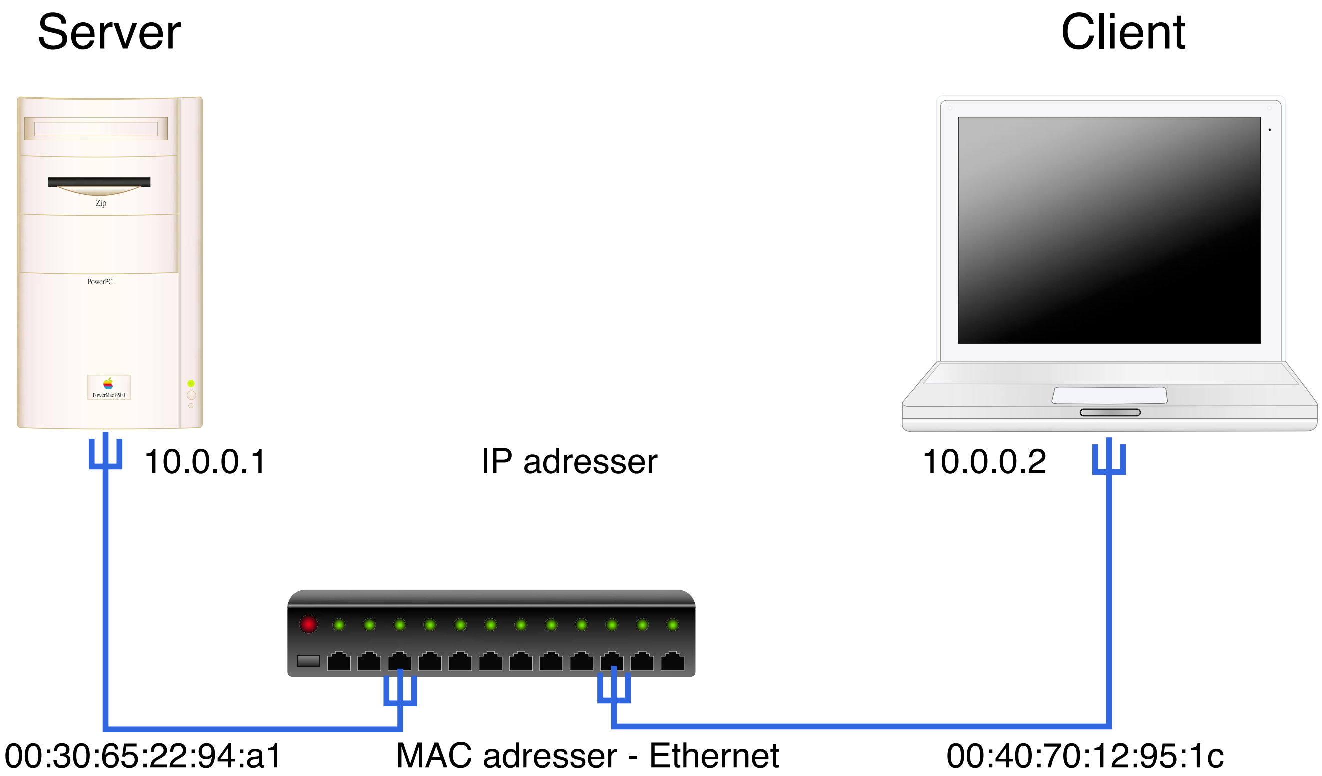
Routing - IPv4

```
$ 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
```

Routing - IPv6

```
$ netstat -f inet6 -rn
Routing tables

Internet6:
Destination                    Gateway              Flags       Netif
default                fe80::200:24ff:fec1:58ac     UGc           en0
::1                            ::1                  UH            lo0
2001:1448:81:cf0f::/64         link#4               UC            en0
2001:1448:81:cf0f::1           0:0:24:c1:58:ac      UHLW          en0
fe80::/64                      fe80::1              Uc            lo0
fe80::1                        link#1               UHL           lo0
fe80::/64                      link#4               UC            en0
fe80::20d:93ff:fe28:2812       0:d:93:28:28:12      UHL           lo0
fe80::/64                      link#5               UC            en1
fe80::20d:93ff:fe86:7c3f       0:d:93:86:7c:3f      UHL           lo0
ff01::/32                      ::1                  U             lo0
ff02::/32                      ::1                  UC            lo0
ff02::/32                      link#4               UC            en0
ff02::/32                      link#5               UC            en1
```

ARP in Ipv4


Server
Client
10.0.0.1
IP adresser
10.0.0.2
00:30:65:22:94:a1
MAC adresser - Ethernet
00:40:70:12:95:1c

ARP request and reply

ping 10.0.0.2 from server

ARP Address Resolution Protocol request/reply:

- ARP request broadcasted on layer 2 - Who has 10.0.0.2 Tell 10.0.0.1
- ARP reply (from 10.0.0.2) 10.0.0.2 is at 00:40:70:12:95:1c

IP ICMP request/reply:

- Echo (ping) request from 10.0.0.1 to 10.0.0.2
- Echo (ping) reply from 10.0.0.2 to 10.0.0.1
- ...

ARP is performed on Ethernet before IP can be transmitted

IPv6 neighbor discovery protocol (NDP)

<table>
<tr><th>OSI</th><th>IPv4</th><th>IPv6</th></tr>
<tr><td>Network</td><td>IP / ICMP</td><td rowspan="2">IPv6 / ICMPv6</td></tr>
<tr><td>Link</td><td>ARP</td></tr>
<tr><td>Physical</td><td>Physical</td><td>Physical</td></tr>
</table>

ARP er væk

NDP erstatter og udvider ARP, Sammenlign `arp -an` med `ndp -an`

Til dels erstatter ICMPv6 således DHCP i IPv6, DHCPv6 findes dog

NB: bemærk at dette har stor betydning for firewallregler!

RFC4861 Neighbor Discovery for IP version 6 (IPv6)

ARP vs NDP

```
hlk@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]

hlk@bigfoot:basic-ipv6-new$ ndp -an
Neighbor                             Linklayer Address  Netif Expire     St Flgs Prbs
::1                                  (incomplete)         lo0 permanent R
2001:16d8:ffd2: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
```

ICMPv6 has more

Autoconfiguration - what is the network prefix

Duplicate Address Detection - can I use this address

Neighbor Discovery - which neighbors exist

Link layer addresses - ”ARP” for IPv6

Neighbor Unreachability Detection, or NUD) - neighbors still alive

IPv6 firewalls - you MUST allow SOME ICMPv6

```
# Simple stateful network firewall rules for IPv6
# using IPv4 file for input and inspiration from
# http://www.ipv6style.jp/en/building/20040526/2.shtml
# input from
        $fwcmd6 -f flush
        $fwcmd6 add allow all from any to any via lo0
# Allow ICMPv6 destination unreach
        $fwcmd6 add pass ipv6-icmp from any to any icmptypes 1
# Allow NS/NA/toobig (don't filter it out)
        $fwcmd6 add pass ipv6-icmp from any to any icmptypes 2
# Allow timex Time exceeded
        $fwcmd6 add pass ipv6-icmp from any to any icmptypes 3
# Allow parameter problem
        $fwcmd6 add pass ipv6-icmp from any to any icmptypes 4
# IPv6 ICMP - echo request (128) and echo reply (129)
        $fwcmd6 add pass ipv6-icmp from any to any icmptypes 128,129
# IPv6 ICMP - router solicitation (133) and router advertisement (134)
        $fwcmd6 add pass ipv6-icmp from any to any icmptypes 133,134
# IPv6 ICMP - neighbour discovery solicitation (135) and advertisement (136)
        $fwcmd6 add pass ipv6-icmp from any to any icmptypes 135,136
```

IPv6 firewalls, cont. allowing services

```
#       Allow all established connections to persist (setup required
#       for new connections).
        $fwcmd6 add allow tcp from any to any established
        $fwcmd6 add allow tcp from any to any out setup
# allow access to my webserver and ssh
#       $fwcmd6 add allow tcp from any to any 80,443  setup
        $fwcmd6 add allow tcp from any to any $ssh  setup

# allow access to X11 forwarding over ::1
        $fwcmd6 add allow tcp from any to ::1 6010  setup

#       Politely rejects AUTH requests (e.g. email and ftp)
        $fwcmd6 add reset tcp from any to any 113

#       Deny everything else ipv6
        $fwcmd6 add 65435 deny log ipv6 from any to any
```

Practical information for your network

IPv6 is already there - see next slide

Take control of IPv6, do not just block it ☺

Strategy and actions points

- Collect information about IPv6
- Collect information about your network
- Collect information about your hosts and services
- Ask your providers for IPv6 plans
- Experiment with IPv6 - today
- Implement small proof of concept, in production!
- Expand coverage

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`

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 ☺

NIST Special Publication 800 series

Use the NIST special publications

SP 800-119 Feb. 22, 2010 DRAFT Guidelines for the Secure Deployment of IPv6
Great because it both introduces IPv6 and gives security advice

SP 800-58 Jan 2005 Security Considerations for Voice Over IP Systems
Almost step by step instructions for what questions to ask your VoIP providers and how to implement VoIP securely

Your network needs an update to support new features, critical needs, isolation VLANs, Quality of Service, new protocols such as iSCSI, VoIP, DNSSEC - get started now

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

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

Remember to add IPv6 to list of requirements for new devices

Collect information about your hosts and services

servers and services, today everything is IPv4 - in Europe

clients - do you only support PCs running Windows? think again. Smart phones and tablets are the future

Desktop and laptop operating systems: regular clients such as Windows, Linux and Mac OS X HAS great IPv6 support
(Dont ask about Windows Xp and Vista, kill them on sight)

Mobile operating systems: support is rapidly increasing, iPhone/iPad - OK, Android 2.x yes, we think so but double check ☺

Support for IPv6 is working on wireless and Ethernet - cellular data propbably not for a while?!

Ask your providers for IPv6 plans

```
Hvad er dit spørgsmål
Hvornår forventer I at få IPv6? Pt. er hastigheden jo
0Kb/s med IPv6 hos jer ;-)
Dit telefonnummer hos 3 20266000
Dit navn Henrik Kramshoej
Kontaktnummer 20266000
E-mailadresse hlk@solido.net
Har du kontaktet 3s kundeservice om denne henvendelse tidligere?
Nej
```

Answer from Mobile operator 3.dk

(ejTag:122712) Privat/Teknisk Support – Mobilt bredbånd/Hastighed — Inbox

From: kundeservice@3.dk
Subject: **(ejTag:122712) Privat/Teknisk Support - Mobilt bredbånd/Hastighed**
Date: 29. mar 2011 10.48.36 CEST
To: Henrik Kramshøj

Hej Henrik!

Tak for din mail!

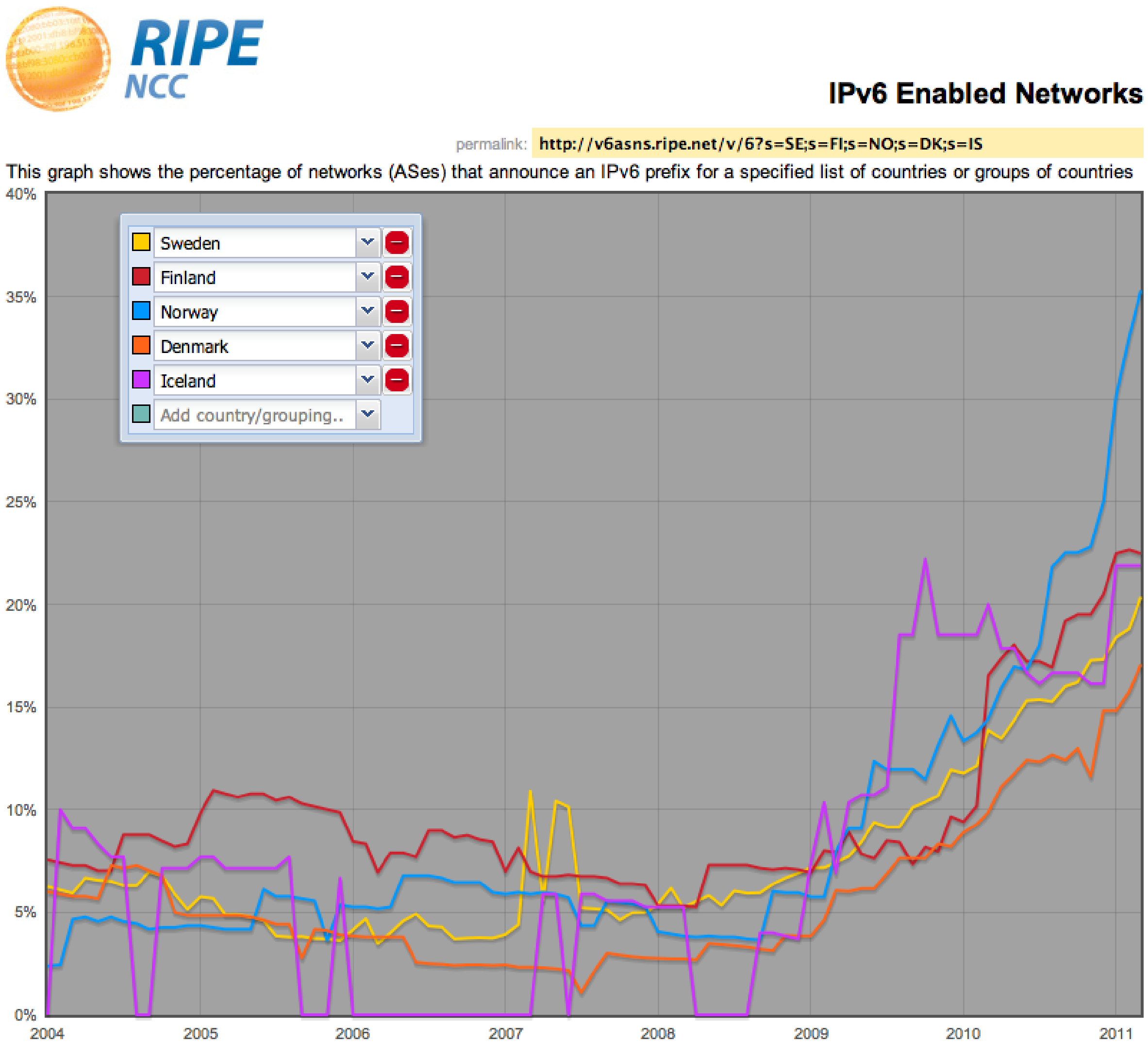
Det er korrekt at IPv6 ikke er understøttet af vores netværk på nuværende tidspunkt - om gør det muligt at benytte IPv6 i fremtiden vides ikke.

Med venlig hilsen

Frederik

Teknisk Frontline
Consumer Management, 3

IPv6 in the Nordic region, and Iceland



Curent status Denmark

Too little interest - less than 100 people thinking about IPv6?

Some providers have some IPv6 connectivity

NO ISPs have IPv6 to consumers

NO ISPs market IPv6 as a product, except me perhaps :-)

Perceived NO NEEED

Free, a major French ISP rolled-out IPv6 at end of year 2007

XS4All As of August 2010 native IPv6 DSL connections became available to almost all their customers.

Source: `http://en.wikipedia.org/wiki/IPv6_deployment`

Experiment with IPv6 - today

Native IPv6 - available at some hosting providers in DK

Automatic tunnels 6to4, Teredo etc.

- 6to4 benytter IPv4 infrastrukturen
- Teredo sender IPv6 gennem IPv4/UDP pakker

Configured tunnels and tunnelbrokers

- `http://sixxs.net` IPv6 Deployment & Tunnel Broker
- `http://he.net` hurricane electric internet services

Implement small proof of concept, in production!

Allocating IPv6 addresses

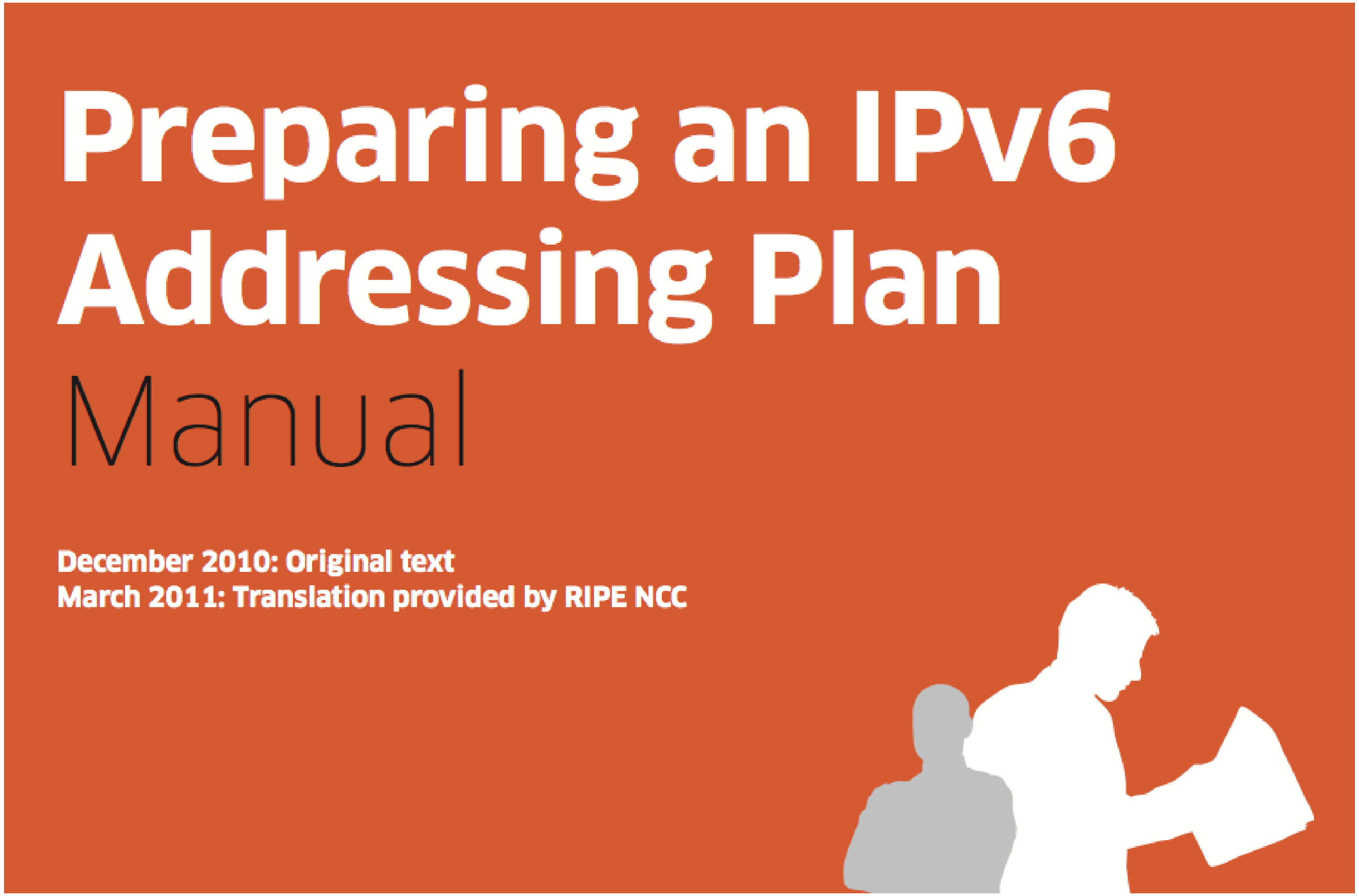
You have plenty!

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



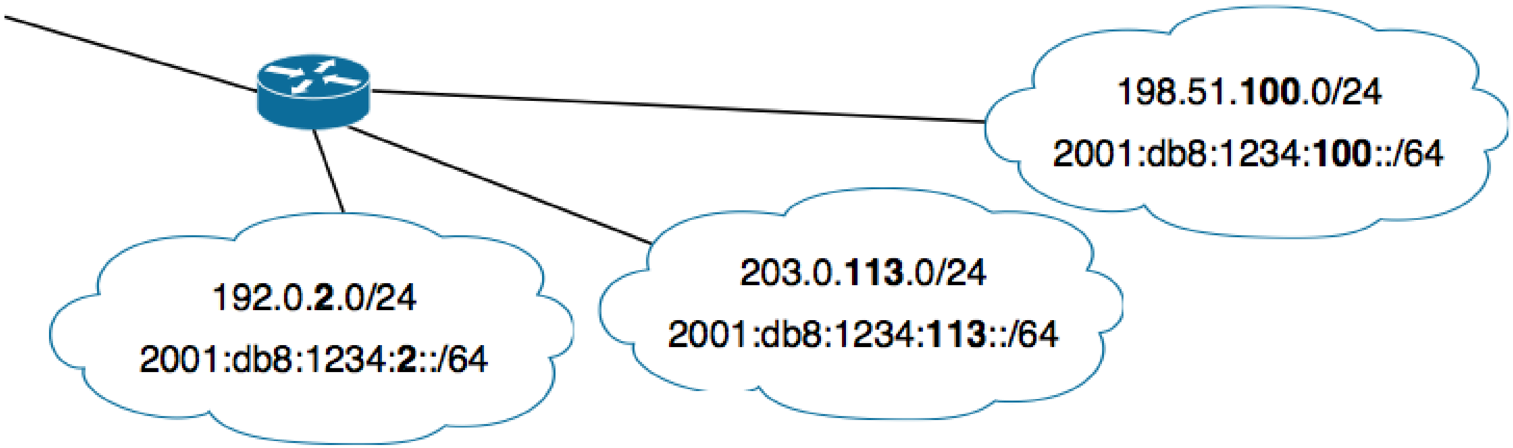
http://www.ripe.net/training/material/IPv6-for-LIRs-Training-Course/IPv6_addr_plan4.pdf

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

Ressources

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 - 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

Danish resources - get involved

Danish IPv6
Task Force

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

About World IPv6 Day

On 8 June, 2011, Google, Facebook, Yahoo!, Akamai and Limelight Networks will be amongst some of the major organisations that will offer their content over IPv6 for a 24-hour "test flight". The goal of the Test Flight Day is to motivate organizations across the industry - Internet service providers, hardware makers, operating system vendors and web companies - to prepare their services for IPv6 to ensure a successful transition as IPv4 addresses run out.

Please join us for this test drive and help accelerate the momentum of IPv6 deployment.

`http://isoc.org/wp/worldipv6day/` and `http://test-ipv6.com/`

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 is here already - use it

`http://www.ipv6actnow.org/`

`http://digitaliser.dk/group/374895`

`http://www.ipv6tf.dk`

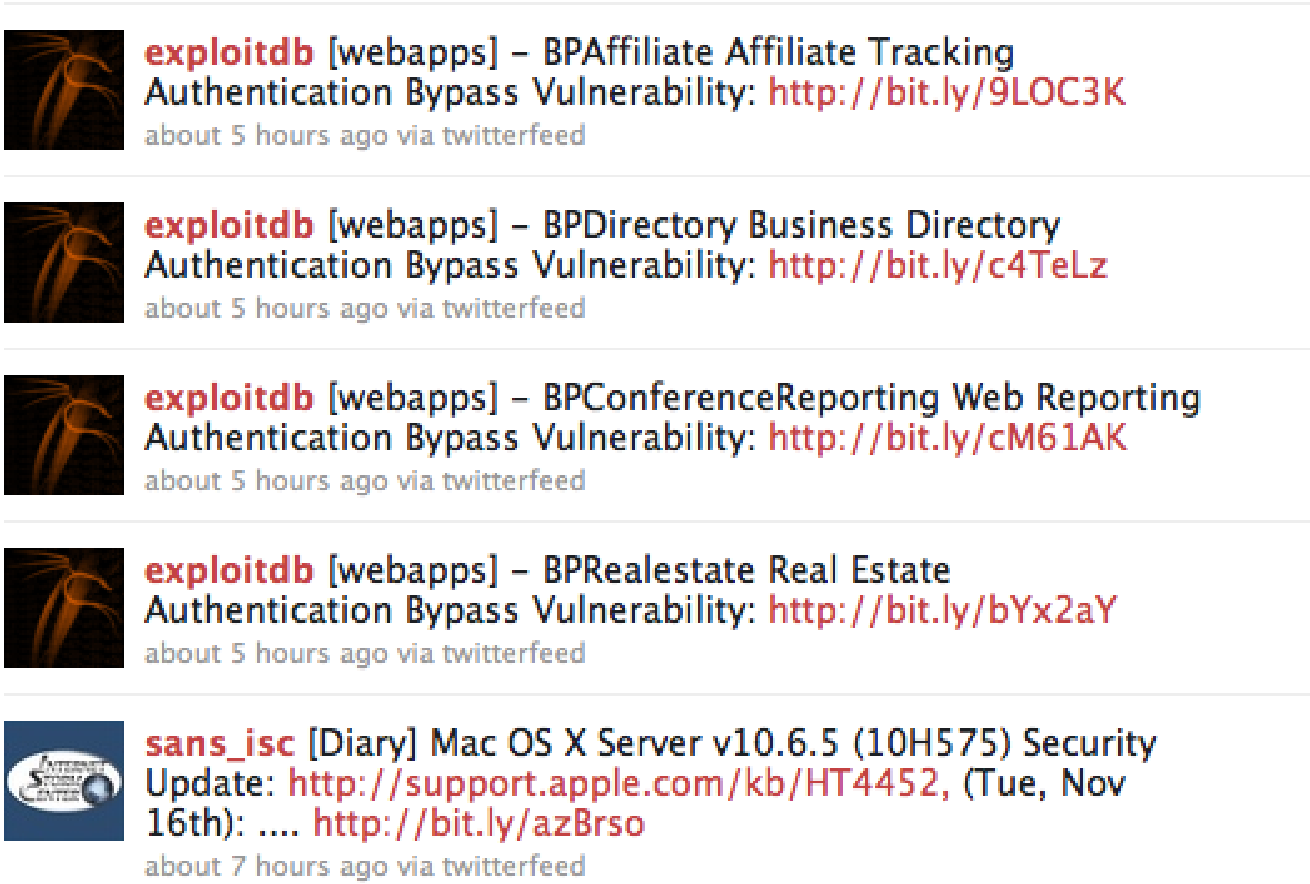
Questions?

Henrik Lund Kramshøj
hlk@solidonetworks.com

`http://www.solidonetworks.com`

You are always welcome to send me questions later via email

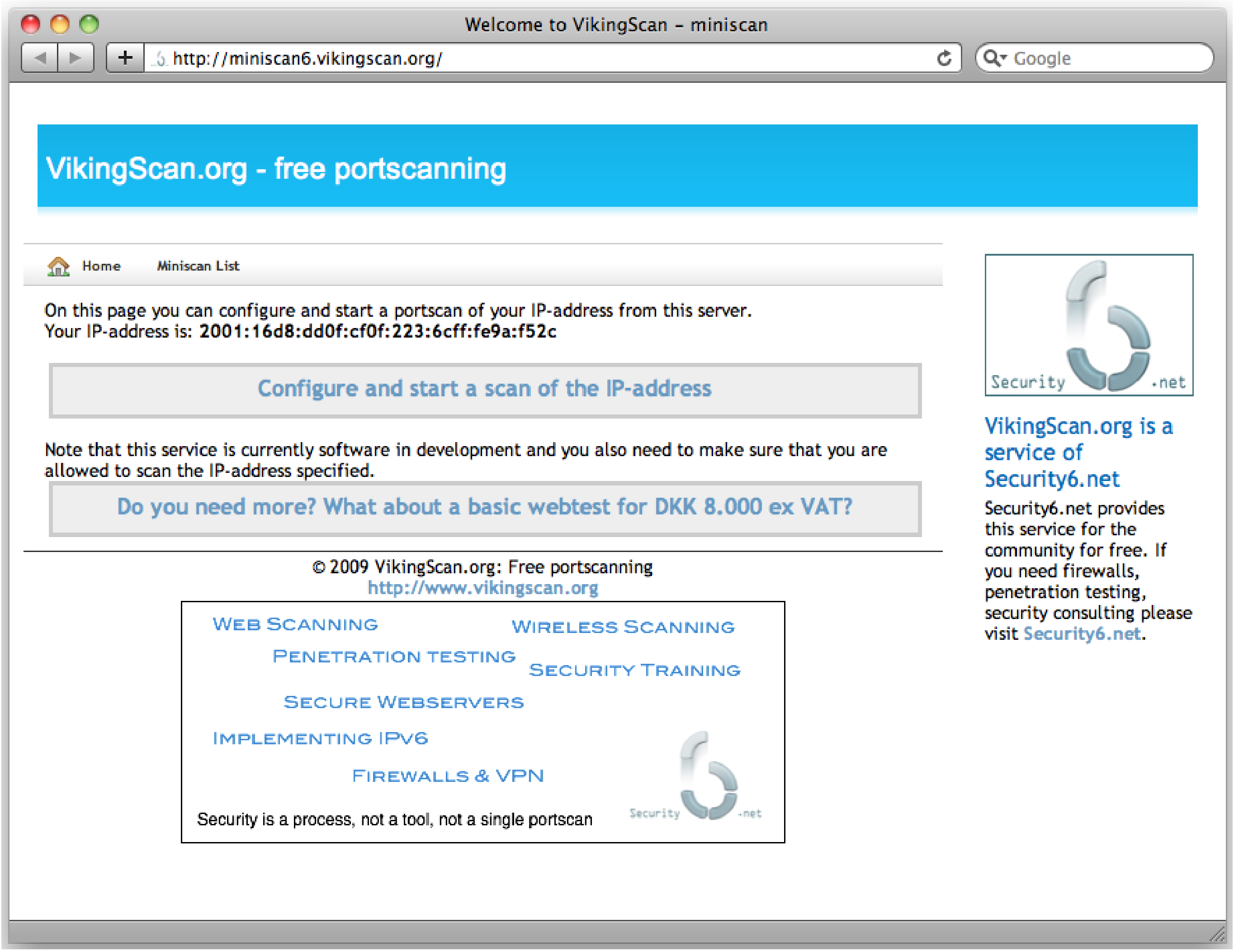
informationskilder



Nye kilder til information:

har twitter afløst RSS? NB: favoritsite `http://isc.sans.edu/index.html`

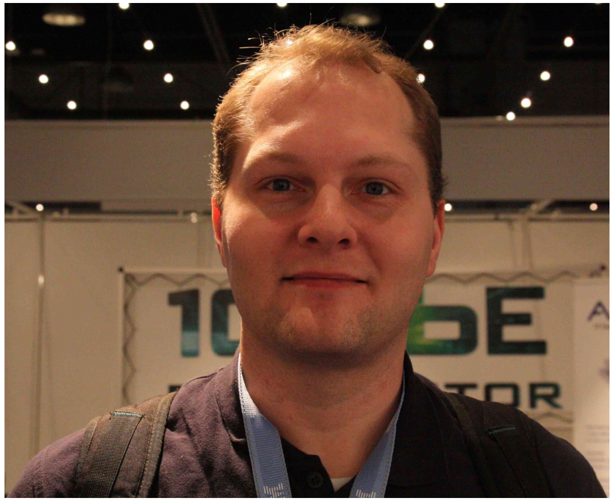
VikingScan.org - free portscanning



Referencer: netværksbøger

- Stevens, Comer,
- Network Warrior
- TCP/IP bogen på dansk
- KAME bøgerne
- O'Reilly generelt IPv6 Essentials og IPv6 Network Administration
- O'Reilly cookbooks: Cisco, BIND og Apache HTTPD
- Cisco Press og website
- Firewall bøger, Radia Perlman: IPsec,

Contact information



- Henrik Lund Kramshøj, IT-security and internet samurai
- Email: hlk@solidonetworks.com   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