How IPv6 addresses the future

INF5050 Lecture
IFI, April 25, 2014
Paal E. Engelstad, Prof. II
http://www.folk.uio/paalee

“TCP/IP will run over two tin cans and a string”
Internet explosion: IPv4 running out

Internet Users in the World (mill.)

1993: 14 mill. users (0.3% of world population)
2014: 292 mill. users (40% of world population)

Source: http://www.internetlivestats.com/internet-users/#trend
Internet Users per region
(July 1st 2013)

Source: http://www.internetlivestats.com/internet-users/#trend
IANA ran out of IPv4 addresses on 3rd Feb 2011

When different Regional Internet Registries (RIRs) reach their final /8 block

Status 16. April 2015:

RIR=Regional Internet Registry

- AFRINIC
- APNIC
- ARIN
- LACNIC
- RIPE NCC

Jan 2019

Empty!
Many measures have been proposed

• Class-E experimental addresses (240.0.0.0/8 – 255.0.0.0/8)
  – Not accepted by some computer and router OSs and firmware

• Reclamation of unused IPv4 addresses
  – Potential legal conflicts
  – Hard to track usage

• Trading of IPv4 addresses?
  – Might lead to fragmentation and expand the global routing table. However:
  – Trades might occur through mergers and acquisitions. In addition:
  – RIPE (European RIR) approved a policy for commercial trading in 2008
    • Runs a “Listing Service” for holders of IPv4 blocks available for “exchange” (for money)
  – ARIN (North America) followed in 2009, and APNIC (Asia) in 2010
  – Might prolong the life of IPv4...
Other measures to prolong the life of IPv4

- Special policy for last /8 block
  - APNIC: Allocation in terms of /22 address blocks since April 2011
    - 1024 addresses given per allocation
    - Prolongs the exhaustion period
    - But only one block per LIR (i.e. ISP)
      - Practically nothing!
  - Other RIRs followed this policy

- ISP wide NAT translation
  - Carrier Grade NAT (CGN)
  - = Large Scale NAT (LSN)
  - = Service Provider NAT44 (SP NAT44)
The address demand at the RIRs are still increasing

The IP address demand is fuelled by the ongoing growth of the Mobile Internet

• ... And the IP address demand will continue to grow in the future
  – E.g. The “Internet of Things”
  – 50 billion connected devices by 2020.
IP objects will be everywhere
Conversion to IPv6 is inevitable!

- IPv6 will solve the address outage problem of IPv4
- The primary reason for IPv6 is that it offers a considerably bigger address space
IPv6 offers a huge address space

IPv4 (32 bits):
4,200,000,000 addresses

IPv6 (128 bits):
3,4 \(10^{38}\) addresses

i.e. about 5,0 \(10^{28}\) addresses per person!

Still not impressed?
Not impressed?

One atom = IPv6 address

Total weight of IPv6 address space?

Not one Empire state building...
1 million Empire state buildings!
Still not impressed?

One video pixel = IPv6 address

The age of the universe is 14 billion years…

1,080 scan lines x 1,920 pixels/line = 2,073,600 pixels
60 frames per second

How long is the movie?

The movie is 6 times the age of the universe!
The transition to IPv6 must happen everywhere
The transition to IPv6 must happen everywhere

IPv6 OS
IPv6 DHCPv6
IPv6 OS
IPv6 DNS NS
IPv6 OS
IPv6 DNS NS

IPv6 IGP
(e.g. OSPFv3)
IPv6 DNS

IPv6 peering
IPv6 BGP
IPv6 DNS TLD

"Who was first?"
The transition to IPv6 must happen everywhere

User equipment

Access networks / ISPs

Internet

Servers / Content providers

Google

Facebook
Modern operating systems are Dual Stack (DS)

IPv4-only Internet

Application
TCP
UDP
IPv4
Link layer
IPv4 stack

Dual-Stack Internet

Application
TCP
UDP
IPv4
IPv6
Link layer
Dual Stack (Vista, Linux, OS X,...)

IPv6-only Internet

Application
TCP
UDP
IPv6
Link layer
Native IPv6

Frame protocol ID = 0x86dd
Frame protocol ID = 0x0800
Applications can now be written transparently

- For older OSes (e.g. XP) applications must handle sockets for IPv4 and IPv6 separately
  - New OSes: Applications use one IPv6 socket
    - Sockets are normally by default `IPV6_V6ONLY=1` (except in Linux)
    - Use `setsockopt()` to set `IPV6_V6ONLY=0` for dual stack usage (i.e. allows for IPv4 usage)
  - The socket accepts connections from both IPv4 and IPv6 clients on a specific port
  - IPv4 addresses can be used over that socket
    - IPv4-mapped-IPv6 address (RFC 4291)
      - `192:0:2:128` -> `::ffff:192:0:2:128`
      - `getsockname()` and `getpeername()` will return an IPv4 address in this format

- All modern OSes for both PC and mobile phones have IPv6 *installed* by default. Most of these also have full support for DHCPv6
- Does not mean that IPv6 will be used (... see next slide ...)

![Diagram showing application levels and link layer with TCP and UDP sockets connected to IPv4 and IPv6]
The transition to IPv6 must happen everywhere
IPv6 at Google (2010)

- The "IPv6 brokenness" problem:
  - Dual stack or tunneled solutions with bogus IPv6 connectivity, will time out (4secs – 3 mins) before IPv4 is attempted
    - Especially older versions of Mac OS X
    - Problem for about 0.06% of the users (about 1 out of 2000 users)

- Google search available over IPv6 since 2008: ipv6.google.com

- DNS Whitelisting of www.google.com on a per-ISP basis:

  Default behavior:

  IP source address prefix of resolver is whitelisted (i.e. the ISP proven to provide IPv6 to its customers):
World IPv6 Day, June 8th 2011

Content over IPv6 offered for a 24-hour "test flight" by many content providers

- E.g. at [www.google.com](http://www.google.com) (i.e. without using specific URL ipv6.google.com)
- DNS AAAA record requests for [www.google.com](http://www.google.com) is resolved to an IPv6 address
- Experience: No big problems reported. Brokenness was insignificant.
World IPv6 launch 2012

• This time, IPv6 was not turned off after 24 hrs
The most popular web-sites are now IPv6 enabled

Popular sites using IPv6
- google.com
- facebook.com
- youtube.com
- yahoo.com
- wikipedia.org
- google.co.in
- linkedin.com
- yandex.ru
- google.co.jp
- vk.com

In terms of number of web-sites, IPv6 deployment is increasing only slowly (2013/14):

Source: http://w3techs.com/technologies/details/ce-ipv6/all/all
The most popular web-sites are now IPv6 enabled

However, in terms of number of web-sites, IPv6 deployment is increasing still only slowly (2015):

Source: http://w3techs.com/technologies/details/ce-ipv6/all/all
The most popular web-sites are now IPv6 enabled

In terms of number of web-sites, IPv6 deployment is increasing only slowly (2015/16):

- google.com
- facebook.com
- youtube.com
- yahoo.com
- wikipedia.org
- google.co.in
- linkedin.com
- yandex.ru
- google.co.jp
- vk.com

Source: http://w3techs.com/technologies/details/ce-ipv6/all/all
The transition to IPv6 must happen everywhere
Is IPv6 native on all backbones globally?

- Peering in nearly all countries
  - Hurricane reported > 122 countries in 2011
- IPv6 peering at all major peering points in US, Europe and Asia
- Peering at 10GBps or higher
- Classic backbones got native IPv6 ~ year 2010
- DNS: 96.7% of all Top Level Domains (TLDs) have IPv6 name servers (2015)

⇒ There exists an "IPv6 Internet"
Tier 1: A network that can reach every other network on the Internet without purchasing IP transit or paying settlements. (A transit-free network that peers with every other tier-1 network. No alternative routes. But not all transit-free networks are tier 1 networks. It is possible to become transit-free by paying for peering or agreeing to settlements.)

Tier 2: A network that peers with some networks, but still purchases IP transit or pays settlements to reach at least some portion of the Internet. Some are larger than the tier-1 networks, and do massive peering, i.e. have often better connectivity and are often closer to the end user than a tier-1 network.

Tier 3: A network that solely purchases transit from other networks to reach the Internet. Pure resellers of Internet connectivity.
Growing amount of IPv6 routing in BGP - I

Growing amount of IPv6 routing in BGP - II

IPv6 Prefixes Originated (1000 Days)

Announcements from more than 150 countries

ASN's with IPv6 Announcements (1000 Days)

Compare:
IPv6 2015: 9944 ASNs
IPv4 2015: 50679 ASNs

Source: http://bgp.he.net/report/prefixes
A growing number of IPv6-enabled ASes emerging in BGP

Source: http://v6asns.ripe.net/

Lacking v6 growth in Africa, due to no IPv4-scarcity there?
Norway is definitely not lagging behind

Norway ahead (2016): 149 out of 222 ASes

Source: http://v6asns.ripe.net/
The transition to IPv6 must happen everywhere.
ISPs are about to grasp the "business case for IPv6"...

• ISPs and Operators
  – Often IPv6 capable routers
    • Simply to "turn on IPv6" (dual-stack)?
    • All systems/servers must work for IPv6
    • Operational experience, training

• The "killer app for IPv6" is simply connectivity
  – Sales of IPv6 connectivity?
  – Interested customers come when the IPv4 address space dry out
Transition mechanisms: v4+v6
(resolving chicken&egg problem?)

EXAMPLE:
NAT64 transition mechanism (to access IPv4 content over IPv6):

- Enables an IPv6 UE to initiate communication with an IPv4 host or server.
- Translation details:
  - UE performs a DNS query for the server and gets an AAAA record that contains the IPv6 with a prefix Pref64::/96 that associated with the NAT64 device and the server’s IPv4 address in the lowest 32 bits.
  - The host sends an IPv6 packet destined to the server via the NAT64 device that does the mapping:
    - Source IPv4 address and transport number are from the address and port number pool maintained by the NAT64 device, respectively.
    - Destination IPv4 address is extracted from the lowest 32 bits of the destination IPv6 address. The destination port number is extracted from the destination IPv6 port number.
  - Translating the packet headers according to SIIT RFC2765
  - Requires the NAT64 device to maintain translation state

NAT64 replaces former NAT-PT
Telenor example: A number of transition mechanisms identified, but only a few considered of practical use

• Dual Stack 😊
  – Supporting IPv4 and IPv6 in parallel
  – This is the preferred solution if the IPv4 address pool can sustain customer growth

• Translation 😞
  – NAT64 translates from IPv6 clients to IPv4 servers. Often used together with DNS64. Same drawbacks as NAT44 and will not scale if the public IPv4 address pool is too small.
  – IPv6-to-IPv4 through a load balancer. Well suited for a datacenter solution that wants to expose IPv4 services to IPv6 clients.
  – 464XLAT: Client-side SIIT translator, plus NAT64. (E.g. used in Android and T-Mobile is USA)

• Tunneling
  – Manual tunnels (i.e. IPv6 over IPv4 using GRE) 😊
  – 6PE (IPv6 over MPLS) (works well in core) 😊
  – Automatic tunneling
    • 6to4 (moved to historical, i.e. should not be supported) 😞
    • 6RD, improvement over 6to4. Well suited for an ISP with access network not supporting IPv6. 😞
    • Teredo (IPv6 tunneling over UDP/w FW traversal. This is a client solution) 😞

• Others
  – DS-lite (Dual-Stack Lite). Tunnels IPv4 traffic over an IPv6 access network to a Large Scale NAT (LSN). Does not scale if the public IPv4 address pool is too small. Requires software support at the client. 😞
  – MAP: Cisco’s tunneling/translation solution
Mobile industry is important for the development

• Germany: Deutsche Telekom announced start of IPv6 in their mobile network in Q2 2015.
• Poland: Mobile operator Orange Polska launched IPv6 Internet access in 2013. (Sept. 2013 Sony Xperia Z1 becomes first ipv6 compliant device available in Orange Poland).
• USA: T-Mobile made in 2013 IPv6 its default phone configuration for all new Android 4.3+ devices using 464XLAT / RFC6877. As of December 2013, phones configured by default for IPv6 / 464XLAT include the Samsung Galaxy Note 3, Galaxy Light, MetroPCS Samsung Mega, and the Google Nexus 5
• …and many more examples of initiatives in the industry
Migration of the mobile networks

• 3GPP release > 7: v4v6 pdp context, implies using only one radio bearer for both
  – However, Telenor has already migrated to Rel. 8 (LTE) and 9
  – Actually, Telenor supports pure v6 PDP Context in existing Rel. 7 networks

• Terminal support: Where are the mobile phones?
  – Some Nokia phones has supported IPv6 for years
  – Symbian, Windows Mobile, Android and IPhone 4.0 supports IPv6
    • However, most chipsets support only Rel. 7 and only IPv4 PDP-Context
    • Often no IPv6 over 3G, only possible over WLAN

• Migrating operator requires also:
  – HSS/HLR upgrade (2 bits to set user capabilities: v4, v6, DS)
  – Upgrade billing system to support v6 or DS CDRs (Call Detail Records)
  – Update Deep Packet Inspection (DPI)
  – ... Generally not a complex issue to migrate, according to Ericsson
Something is about to happen!

Percentage of worldwide hits at Google that are IPv6

Source: Google

USA and Europe are driving the development worldwide (2015)

Percentage of worldwide hits at Google that are IPv6

Source: Google

USA
2015: 14.6%
(2014: 7.0 %)
USA and Europe are driving the development worldwide (2016)

Percentage of worldwide hits at Google that are IPv6

Per-Country IPv6 adoption

USA
- 2016: 23.4 %
- 2015: 14.6 %
- 2014: 7.0 %

Japan (10.1 %)

China (1.5 %)

India (0.6 %)

Brazil (7.1 %)

Source: Google
Some European countries are in the forefront worldwide (2015)

Percentage of European hits at Google that are IPv6

- **France**: 5.4% (2014: 17%)
- **Belgium**: 33% (2014: 17%)
- **Germany**: 14.7% (2014: 8.3%)
- **Switzerland**: 9.3%
- **Norway**: 7.4% (2014: 2.4%)
- **Romania**: 7.1% (2014: 6.0%)
- **Greece**: 8.1%
- **Estonia**: 5.3%
- **Portugal**: 7.7%

Source: Google

Some European countries are in the forefront worldwide (2016)

Percentage of European hits at Google that are IPv6

Per-Country IPv6 adoption

- **Norway**: 7.9% (2015: 7.4%; 2014: 2.4%)
- **Germany**: 21.6% (2015: 14.7%; 2014: 8.3%)
- **Greece**: 20.8% (2015: 8.1%)
- **Belgium**: 41% (2015: 33%; 2014: 17%)
- **France**: 6.9% (2015: 5.4%)
- **Portugal**: 24.0% (2015: 7.7%)
- **Switzerland**: 26.4% (2015: 9.3%)
- **Estonia**: 9.5% (2015: 5.3%)
- **Norway**: 7.9% (2015: 7.4%; 2014: 2.4%)
- **Finland**: 7.7%
- **Sweden**: 2.7%
- **Czech**: 9.7%
- **Romania**: 7.1% (2014: 6.0%)
- **Portugal**: 24.0% (2015: 7.7%)

Source: Google
Are there other benefits of IPv6, apart from pure connectivity?

Larger address space, enables:
- Global reachability (no NATs)
- Flexibility
- Aggregation
- Multi-homing
- “Plug and Play” and Renumbering
- Auto-configuration

Simpler header, enables:
- Less unnecessary overhead
- Routing efficiency
- Performance and forwarding rate scalability

Mandatory support and enhancements
- Security
- Mobility
- Better QoS support
- Better multicast
- Other stuff (Optional)
Various types of IPv6 addresses give a lot of flexibility

- **Global**: Prefix: 2000::/3 (i.e. "001") (Like IPv4 unicast)
- **ULA**: Prefix: FC00::/7 (i.e. "1111 110") (Like RFC1918/private)
- **Link local**: Prefix: fe80::/10 (Like 169.254.0.0/16)
- **Multicast**: Prefix: ff00::/8
- **Anycast addresses**: No distinction vs. unicast addresses
  - Can have several alternative routes to a router
- **Other reserved addresses**
  - unspecified (::/128), loop back (::1/128), IPv4-mapped (::ffff/96)
  - teredo addresses, 6to4 addresses, etc...
Aggregation of global addresses

In default-free zone

For the topology of an organization

Where

FP = Format Prefix (001)
Site multihoming problematic with IPv4

- Advertisement of prefix not good for router table size
- Stub-network advertises prefixes for better resilience
  - The hierarchic address aggregation is undermined
  - BGP router size explodes
Multihoming is better with IPv6

- Several IPv6 addresses assigned to each interface and to the network
  - Site managers use “Router renumbering” to add (/remove) router prefix automatically
  - Host receive router advertisements and create additional global address with the new prefix
- Plug and play!
IPv6 Address Auto-Configuration

• Stateful
  – DHCPv6

• Stateless
  – Host starts forming link-local IPv6 address
    • Predefined link-local prefix + 64-bits interface ID
  – Duplicate Address Detection (DAD)
    • Neighbor Discovery to ensure no address collision on same subnet
  – Neighbor Discovery i RFC2461 (replace ARP and RA/RS)
    • Host discovers prefix from routers on the same subnet
  – Host generates address from discovered prefix
    • E.g. Discovered prefix + MAC-address as Interface ID

• Securing Neighbor Discovery (SeND)
  – Certificate-information is hashed into the interface ID
  – Used to secure the Neighbor Discovery
Other benefits of IPv6

• Larger address space, enables:
  – Global reachability (no NATs)
  – Flexibility
  – Aggregation
  – Multi-homing
  – “Plug and Play” and Renumbering
  – Auto-configuration

Simpler header, enables:
  – Less unnecessary overhead
  – Routing efficiency
  – Performance and forwarding rate scalability

• Mandatory support and enhancements
  – Security
  – Mobility
  – Better QoS support
  – Better multicast
  – Other stuff (Optional)
**Simplified IPv6 header**

<table>
<thead>
<tr>
<th>IPv6 (40 bytes)</th>
<th>Version (4 bits)</th>
<th>Traffic Class (8 bits)</th>
<th>Flow Label (20 bits)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payload Length</td>
<td>16 bits</td>
<td>Next Header (8 bits)</td>
<td>Hop Limit (8 bits)</td>
</tr>
<tr>
<td>Source Address</td>
<td>128 bits</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Destination Address</td>
<td>128 bits</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IPv4 (20 bytes)</th>
<th>Vers = 4</th>
<th>IHL</th>
<th>Type of Service</th>
<th>Total Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identification</td>
<td></td>
<td></td>
<td>Flags</td>
<td>Fragment Offset</td>
</tr>
<tr>
<td>Time to Live</td>
<td></td>
<td></td>
<td>Protocol</td>
<td>Header Checksum</td>
</tr>
<tr>
<td>Source Address</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Destination Address</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Options</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Changes to simplify router treatment
  - No header checksum: Link layer does this anyway
  - No hop-by-hop fragmentation: MTU discovery if needed
  - Flow-label simplifies QoS treatment of a "flow"
IPv6 Extension Headers

• Option field of IPv4 is replaced by extension headers
  – Reducing overhead: For special usage
  – Only treated by the destination (except hop-by-hop e.h.)
  – Extension headers linked efficiently together
  – 64-bits alignment, for efficient router processing
  – Option extensibility: No limit on options (IPv4 max length is 40 bytes)
IPv6 Header Types and order

- **Header Types**
  - Hop-by-Hop Opt. Header = 0
  - Destination Opt. Header
  - Routing Header = 43
  - Fragment Header = 44
  - Authentication Header = 51
  - Encrypted Payload = 52
  - Destination Opt. Header
  - TCP = 6 or UDP = 17
  - Alternatively: “No-next-header” = 59

**Extension headers**
- Info that every router must handle
- Must only be handled by dest.
  (With a code per action if option is unknown)
- For e.g., source-routing
  For end-to-end fragmentation

**Must be checked by the ultimate destination** (after other options have been checked)
Other benefits of IPv6

• Larger address space, enables:
  – Global reachability (no NATs)
  – Flexibility
  – Aggregation
  – Multi-homing
  – “Plug and Play” and Renumbering
  – Auto-configuration

• Simpler header, enables:
  – Less unnecessary overhead
  – Routing efficiency
  – Performance and forwarding rate scalability

Mandatory support and enhancements
  – Security
  – Mobility
  – Better QoS support
  – Better multicast
  – Other stuff (Optional)

Comes included!
Other enhancements with IPv6

• Security:
  – Mandatory support for IPsec headers

• Mobility:
  – Mandatory support for Mobil IPv6 with route optimisation

• Multicast
  – replaces IPv4 broadcast

• A number of new IPv6 features/initiatives
  – Jumbograms, HIP, Shim6, ...

• Support for all IPv4 mechanisms
  – IPsec – diffserv – QoS features – osv....
That's all Folks!
BACKUP SLIDES
Annet stoff som man bør kjenne (ikke foreleste)

- Reuse of IP addresses / NATing
- IPv6 address auto-configuration
  - 64-bits Interface ID
- More details about some IPv6 address types
  - Link-locale addresses
  - Unique Local Addresses (ULA)
  - Multicast addresses
Gjenbruk av globale IPv4 adresser

1. I utgangspunktet hadde vi statiske globale adresser
2. Dynamiske adresser vha DHCP
   – IP adresse kun til aktive brukere (Gjenbruk)
3. Private adresser vha “Basic NAT”
   – Globale IP-adresser forbrukes kun av brukere som aktivt kommuniserer med Internett (Gjenbruk)
     • NAT-boksen oversetter mellom privat og global adresse (se neste slide)
4. NAT med port-translation (“NAPT”)
   – Brukere som aktivt kommuniserer over Internett, deler den samme IP-adressen (Gjenbruk)
     • NAT-boksen multiplekser ulike bruker-sesjoner på samme globale IPv4 adresse, men på ulike TCP-/UDP- port nummer
     • Teoretisk kan 1 global adresse brukes til $2^{16} = ca 65000$ ulike sesjoner.
"Basic NAT" – Eksempel

NAT ADRESSE-POOL:

<table>
<thead>
<tr>
<th>Global IPv4 adresse</th>
<th>Privat adr.</th>
<th>Global adr.</th>
<th>Timeout</th>
</tr>
</thead>
<tbody>
<tr>
<td>144.4.4.40</td>
<td>10.0.0.10</td>
<td>144.4.4.42</td>
<td>12:10:15</td>
</tr>
<tr>
<td>144.4.4.41</td>
<td>10.0.0.11</td>
<td>144.4.4.41</td>
<td>12:10:34</td>
</tr>
<tr>
<td>144.4.4.42</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

IP-pakke:
Src addr = 175.35.4.133
Dst addr = 10.0.0.10 (!)

IP-pakke:
Src addr = 175.35.4.133
Dst addr = 144.4.4.42 (!)

IP-pakke:
Src addr = 144.4.4.42 (!)
Dst addr = 175.35.4.133

IP-pakke:
Src addr = 175.35.4.133
Dst addr = 10.0.0.10 (!)

Private IPv4 adresser

Global IPv4 adresse

NAT TABELL:
"NAPT" – Eksempel

NAPT ADRESSE:

| 144.4.4.40 |

NAT TABELL:

<table>
<thead>
<tr>
<th>Privat</th>
<th>Global</th>
<th>Timeout</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.10:5555</td>
<td>144.4.4.40:6666</td>
<td>12:26:09</td>
</tr>
<tr>
<td>10.0.0.11:8080</td>
<td>144.4.4.40:7777</td>
<td>12:17:15</td>
</tr>
</tbody>
</table>
Ulike Typer NAT bokser (I)

• NAT kan altså karakteriseres etter hvordan den mapper ut-trafikk
  – NAT uten eller med port-translation
    • I.e. ”Basic NAT” vs. NAPT, som vi så på foregående slides

• NAT kan også karakteriseres etter hvordan den ”filtrerer” retur-trafikk fra Internet
  – f.eks. kan returpakken komme fra hvilken som helst node, eller må source-adressen i pakken være lik destination-adressen til den opprinnelige pakken
  – La oss se litt nærmere på dette på neste slide...
### Ulike typer NAT-bokser (II)

- Hvis A sender en port-x pakke til E, kan en returpakke komme fra en annen node (F) og/eller fra en annen applikasjon?
  - Dette avhenger av NAT-typen:

<table>
<thead>
<tr>
<th>NAT type</th>
<th>Permitted source IP addr. of return traffic:</th>
<th>Permitted source port number of return traffic:</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;Full Cone” NAT</td>
<td>Any (also from F)</td>
<td>Any (also from any applic.)</td>
</tr>
<tr>
<td>(Address-) &quot;Restricted Cone” NAT</td>
<td>1 (only from E)</td>
<td>Any (also from any applic.)</td>
</tr>
<tr>
<td>&quot;Port-Restricted Cone” NAT</td>
<td>Any (also from F)</td>
<td>1 (only from same port)</td>
</tr>
<tr>
<td>&quot;Symmetric” NAT</td>
<td>1 (only from E)</td>
<td>1 (only from same port)</td>
</tr>
</tbody>
</table>
Problemer med NAT* ) (I)

• Applikasjoner som bærer en IP-adresse eller portnummer i IP-payloaden vil slutte å fungere
  • F.eks. FTP, SIP, etc.
    – (Bryter med lagdelingen)
  • Inter-dependent flows (f.eks. H.323)

• NAT skaper problemer for ny lag-3 funksjonalitet
  • Mobilitet (Mobile IP)
  • Sikkerhet (IPSec/VPN)
  • IP-in-IP tunnelering
  • ...etc...

*) “NAT” = “Basic NAT” og “NAPT”
Problemer med NAT (II)

- Dynamisk NATing forutsetter klient/tjener-kommunikasjon
  - En server kan ikke nås fra Internett, når den står bak NATen
    - “Always-on” tjenester
    - Peer-to-peer- kommunikasjon umulig mellom to noder som begge står bak en NAT-boks
Problemer med NAT (III)

• Undergraver dynamisk ruting
  – Avhengig av ruting via NAT-boksen

• ”Fate-sharing”:
  – ”Sjebnen” til sesjonen er avhengig av ”sjebnen” til
    NAT-boksen

• Bryter ende-til-ende-prinsippet
  – En sesjon vil være avhengig av tilstandsinformasjon
    på en NAT-boks i nettet
  – ”Logikk i nettet”
64-bits Interface ID
(Bruker ofte globalt unik MAC adr.)

En 48 bit IEEE 802 MAC adresse:

+-----------------------------------------------+ (c = Company_ID
|ccccccccccccccccccccccccccccmmmmmmmmmmmmmm| m = Manufacturer-selected
+-----------------------------------------------+ Extension_ID)

...kan konverteres til en EUI-64 Identifier:

+-----------------------------------------------+ +-----------------------------------------------+
|cccccccccccccccccccccccccccccccccccccc111111|11111110mmmmmmmm|mmmmmmmmmmmmmmmm|
+-----------------------------------------------+ +-----------------------------------------------+

...som danner en globalt unik IPv6 Interface ID

+-----------------------------------------------+ +-----------------------------------------------+
|cccccccccccccccccccccccccccccccccccccccc|mmmmmmmmmmmmmmmm|mmmmmmmmmmmmmmmm|
+-----------------------------------------------+ +-----------------------------------------------+

‘u’-bitet som angir Universal (global unik!) / Local unikhet
Men man kan alternativt velge lokal unik Interface ID

- Setter i stedet \( u \)-bitet til 0
- Kan derfor alternativt velge random Interface ID
- F.eks. nyttig for å skule sin identitet:
  - Skifter periodisk til ny Interface ID (RFC3041)
  - Når man ikke ønsker å bli identifisert med en globalt unik Inteface ID når man kommuniserer
Link Lokale Adresseer

<table>
<thead>
<tr>
<th>1111 1110 10</th>
<th>0</th>
<th>Interface ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 bits</td>
<td>n bits</td>
<td>118-n bits</td>
</tr>
</tbody>
</table>

- Rutere sender ikke pakker til slike adresser utenfor linken
- Praktisk for lokal kommunikasjon på linken, f.eks. før en node har oppdaget en ruter
  - Brukes bl.a. i Neighbor Discovery
- I praksis er Interface ID oftest 64 bit
  - Alle unicast adresser som ikke starter med 000-prefix
Unique Local IPv6 Unicast Addr.

<table>
<thead>
<tr>
<th>Interface ID</th>
<th>Global ID</th>
<th>Subnet ID</th>
<th>7 bits</th>
<th>41 bits</th>
<th>16 bits</th>
<th>64 bits</th>
</tr>
</thead>
</table>

- Unique Local IPv6 Unicast Adresser ("Local IPv6 Addresses")
  - Foreløpig bare Internet Draft
  - erstatter de lite implementerte “Site-Local” adressene

- Lokale IP adresser skal ikke være rutbare på Internet
  - Kan brukes internt i en site
  - Hvis en pakke feilaktig rutes utenfor site, så oppdages feilen (pakken droppes) pga Global ID bits
  - (Dette var feilen med “Site-Local” addresser)
IPv6 – Multicast Addresses

<table>
<thead>
<tr>
<th>Flags</th>
<th>Scope</th>
<th>Group ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>1111 1111</td>
<td>8 bits</td>
<td>4 bits</td>
</tr>
</tbody>
</table>

• **Flag:** 000T
  – T=0 for permanent address (definert for alle mulige scopes)
  – T=1 for transient address (kun gyldig innen scope)

• **Definerte scope:**
  – Node-Lokal, Link-Lokal, Site-Lokal, Organisasjons-Lokal, Global

• **Merk at Broadcast er fullstending erstattet av Multicast i IPv6**
Work-in-progress slides
Improvements of slides

• Terminal support: Where are the mobile phones?
  – Nokia phones has supported IPv6 for years
  – Symbian, Windows Mobile, Android and IPhone 4.0 supports IPv6
    • Often only over WLAN (below) – support for higher release?
• 3GPP release > 7: v4v6 pdp context, implies using only one radio bearer for both
  – Timeline for migration?
• Migrating operator requires also:
  – HSS/HLR upgrade (2 bits to set user capabilities: v4, v6, DS)
  – Upgrade billing system to support v6 or DS CDRs (Call Detail Records)
• Check: NATing i BUer
DS-lite overview

- Assumptions /goals
  - IPv4 in homes with NAT on CPE
  - Wants to avoid the use of a global IPv4 address at the CPE
- Function
  - DS-lite: Instead the CPE tunnels IPv6 packet to a Carrier-Grade-NAT (CGN)
- Result
  - Thus, ISP network is IPv6 only
  - Also allows for IPv6 traffic behind the CPE
6to4 overview

• Assumptions/goals:
  – Connect an IPv6 island to other IPv6 islands or to the native IPv6 Internet
  – An IPv6 island has a global IPv4 address

• Function:
  – A 48bit 6to4 IPv6 prefix for use inside the IPv6 island, as 2002:<IPv4-address>::/48 is given
  – 6to4 router tunnels (6in4) IPv6 packets to other 6to4 routers over IPv4, using the IPv4-address as encoded in the destination 6to4 address as the endpoint of the tunnel
  – Otherwise, the traffic is tunneled to the IPv4 anycast address 192.88.99.1 to hit a 6to4 relay, injects inner IPv6 packet into native IPv6 Internet
  – 6to4 relays announces into the native IPv6 Internet availability (routes) to the 6to4 IPv6 anycast prefix 2002::/16, and tunnels this traffic over IPv4 back to the 6to4 router IPv4 address encoded in the 6to4 IPv6 address
The problems of 6to4 relates to the 6to4 relays

Brokenness
• 6to4 depends on the charity of an unknown third-party to operate the relays between the 6to4 cloud and the native IPv6 Internet.
• No customer-relationship, no way to know which relay is used and no support
• The placement of the relay can lead to increased latency, and in the case the relay is overloaded packet loss.
• 6to4 has no specified mechanism to handle the case where the protocol (41) is blocked in an intermediate firewalls (the 6in4 encapsulation)
• Relays can be mis-configured
• Brokenness rates measured to be of around 15%!

Security
• 6to4 relays can be used to anonymize traffic and inject attacks into IPv6 that are very difficult to trace.

6to4 has been moved to historic. Use 6rd (IPv6 Rapid Deployment) instead!
6RD (IPv6 Rapid Deployment)

• Assumption/Goals:
  – ISPs proved IPv6 connectivity to customers
  – Without having to upgrade access network to IPv6

• Function:
  – Like 6to4, but IPv4 internet is replaced by ISP’s IPv4 network
  – Relays (6RD GW) placed on the border between the ISPs network and the native IPv6 network
  – These are under control of the ISP, i.e. the known issues with the 6to4 relays are mitigated