IPv6
From an Application Layer Perspective

Patrik Fältström
Area Director, Applications Area, IETF
Consulting Engineer, Cisco Systems
Agenda

- What are Applications?
- Why is end-to-end so important?
- What is IPv6 solving for Applications?

- Summary...
Contrary to traditional communication, we have three layers on the Internet:

- Application
- Transmission
Contrary to traditional communication, we have three layers on the Internet:

- Application
- Internet (IP)
- Transmission
Why is this so important?

- With three layers, the application layer ends up being independent from the transmission.
- As soon as you have IP connectivity, you can run any application using IP.
- Previously, you had to change application if transmission changes.
How does this work?

- Create a packet
- Include your (sender) information
- Add address of destination
- Send on your local interface
- Packet will reach destination
- Or you will be told otherwise
Addressing

Absolutely fundamental is the existence of the 5-tuple which identifies a connection!
Simple "fetch"

- A simple fetch in a TCP-based protocol is more than one exchange of packets.
- HTTP 1.1 spec. is 176 pages long!
A simple network

- Two hosts connected to the same cable
The Internet

- Routing is introduced
In some cases, firewalls are used. People mix up firewalls with NAT.
Firewall

- Security can also be inside endnode
Firewall

- As part of the connection to Internet
It is possible to open a connection towards the Internet through a firewall.
Firewall

- But, from the Internet, connections are blocked
One address

- The NAT box remembers a connection
## One connection

<table>
<thead>
<tr>
<th>Outside</th>
<th>Inside</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source: 130.237.72.201:3212</td>
<td>Source: 192.168.1.1:6712</td>
</tr>
<tr>
<td>Destination: 67.32.12.3:25</td>
<td>Destination: 67.32.12.3:25</td>
</tr>
</tbody>
</table>

Protocol: TCP
This sort of works

- When connecting to servers
- A strict client-server relationship
Can host X connect to host A?
Mapping

- “If connection is initiated towards outside port 80, forward to 192.168.1.2 on inside, port 80”

- This makes it possible to connect to host A, but not host B
Protocols

- Both SIP and FTP (as two examples) have two channels
  - Control channel
    - Negotiation of data channel, commands and other signaling
  - Data channel
    - Where data is transferred
What IP address and port number is to be used for the actual call?
NAT is not fun!

- The problem is that the client doesn’t know what IP address and port number to use
- Those values are allocated in the NAT
- Network configuration is uglier and uglier
What about IPv6

- Some people claim IPv6 will solve
  - Routing issues
  - Security issues
  - Quality of service issues
  - Addressing issues

- Is that true?
What about IPv6?

- We will have many, many addresses
- In IPv6 world, we don’t need NAT
- IPv6 give an opportunity for new applications
- Applications have to be changed
- Contrary to what many people think
With public IP addresses and no NAT, this ends up being so simple.
Why not more IPv6?

- It’s a Catch-22:
  - People are not asking for it
  - Vendors and ISP’s are not implementing
  - It is not deployed
Problems

- IPv6 is nothing extra for the end user
- “ping” is not that exciting
- ISP can not charge for introduction
- Still, it cost an ISP money to deploy
- Real IP addresses is THE new thing!
- Consumer might understand...
Solution:

- Interested parties must start using IPv6
- The European Commission and governments by requiring it on all IP connections they buy
  - http://europa.eu.int over IPv6?
- Applications will help (and need) IPv6 deployment via non-NAT networks
Questions?

Patrik Fältström

Email: paf@cisco.com