Who Cares About IPv6?

Sam Bowne
City College San Francisco
Part I

Who Cares?
IPv4 Addresses: 32 Bits

- IPv4 address: 192.168.1.10
  - Four bytes
- In Binary:
  11000000 10101000 00000001 00001010
- $2^{32}$ total addresses
  - 4 billion
- Are you kidding? There are 7 billion people, they each need iPads, cell phones, Google brain chip implants, etc…
IPv6 Addresses: 128 Bits

- **IPv6 address**
- `2001:05c0:1000:000b:0000:0000:0000:66fb`
  - Omitting unnecessary zeroes;
- `2001:5c0:1000:b::66fb`
  - Eight fields, each 16 bits long
    - 4 hexadecimal characters
- **2^128 total addresses**
  - 256 billion billion billion billion
  - Enough for a while
IPv4 Exhaustion

As of 6-30-2010, 16 "/8 address ranges" remain
- Each /8 has 16.8 Million Addresses
- 205 /8s already allocated
- 35 Reserved for special uses

From link Defcon-talk 3
The End is Near

Projected IANA Unallocated Address Pool Exhaustion: 09-Sep-2011
Projected RIR Unallocated Address Pool Exhaustion: 07-Apr-2012
The End of the World

- No Reprieve
  - IANA will not re-purpose class D or E addresses for general use
- People who ask for IPv4 addresses after exhaustion will not get them
  - Hoarding, scalping, and simple direct sale of IPv4 addresses will begin soon
## Projected DOD Timeline

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2003</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2004</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2005</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2006</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2007</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2008</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2009</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2010</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2011</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **From link Defcon-talk 4**
Federal IPv6 Transition Timeline

- **IPv6 Acceptance Cycle**
  - **Acceptance**: IPv6 Identified & Transition in Progress
  - **Equivalence**: IPv6 Capabilities = IPv4 Capabilities
  - **Preference**: IPv6 Preferred Protocol over IPv4
  - **Dominance**: IPv4 Phase Out/Legacy Only

- **Preparation**
  - Strategy/Mission Impact
  - Planning & Governance
  - Enterprise Architecture
  - Acquisition Planning

- **Transition**
  - Enterprise Infrastructure
  - Information/Cyber Security

- **Post-Transition**
  - Application/Services

- **IPv6 Transition Phases and Timeline**
  - 2007: Agency IPv6 Testing
  - 2008: Agency IPv6 Exhibit 300
  - 2009: ARIN Estimated IPv4 Address Exhaustion
  - 2010: NIST IPv6 Profile Start
  - 2011: NIST IPv6 Product Test Start
  - 2012
  - 2013
  - 2014+

*From Cisco (link Defcon-talk 2)*
Summary of Part I
IPv4 is Full

Image from zinyaw.files.wordpress.com
IPv6

RESISTANCE IS FUTILE
Part II

What Now?
Methods of IPv6 Migration

- **Ignore IPv6**: Stay on IPv4-only
- **Gateways**: Devices that convert IPv6 to IPv4
- **Tunnel**: IPv6 over IPv4
- **Dual-Stack**: IPv4 and IPv6 together
- **Nirvana**: IPv6-only
IPv6 Tunnels

- Fast and easy to set up—best for n00bs
- Not the best for security or performance
- Free IPv4-to-IPv6 Tunnels
  - Gogo6.com
  - Sixxs.net
  - Tunnelbroker.com
    - Links Defcon-talk 5-7
GoGo6

- Easiest

Depending on your environment, you will connect to the gogoSERVER either anonymously or with authentication credentials. More options are available in the Advanced tab.

Server Address: anonymous.freenet6.net

- Connect Anonymously
- Connect Using the Following Credentials

User Name:
Password:

Launch the gogoCLIENT service at system startup

Restore Default Values...  Connect  Disconnect

SamEee10  gogoSERVER  Internet
Demonstration

C:\Windows\System32>ping ipv6.google.com
Pinging ipv6.1.google.com [2001:4860:8010::68] with 32 bytes of data:
Reply from 2001:4860:8010::68: time=232ms
Reply from 2001:4860:8010::68: time=474ms
Reply from 2001:4860:8010::68: time=368ms
Reply from 2001:4860:8010::68: time=423ms

Ping statistics for 2001:4860:8010::68:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 232ms, Maximum = 474ms, Average = 374ms

C:\Windows\System32>nslookup
Default Server: google-public-dns-a.google.com
Address: 8.8.8.8

> set q=AAAA
> ipv6.google.com
Server: google-public-dns-a.google.com
Address: 8.8.8.8

Non-authoritative answer:
Name: ipv6.1.google.com
Addresses: 2001:4860:8010::68
          2001:4860:8010::93
          2001:4860:8010::67
          2001:4860:8010::63
Aliases: ipv6.google.com
IPv6 Certifications

- Fun, realistic projects
- He.net
- Link Defcon-talk 12

Welcome to the Hurricane Electric IPv6 Certification Project. This tool will allow you to certify your ability to configure IPv6, and to validate your IPv6 servers configuration.

Through this test set you will be able to:

- Prove that you have IPv6 connectivity
- Prove that you have a working IPv6 web server
- Prove that you have a working IPv6 email address
- Prove that you have working forward IPv6 DNS
- Prove that you have working reverse IPv6 DNS for your mail server
- Prove that you have name servers with IPv6 addresses that can respond to queries via IPv6
- Prove your knowledge of IPv6 technologies through quick and easy testing
IPv6 Certifications

Certification Levels

1. Newbie: Knows basic facts about IPv6
2. Explorer: Has the ability to connect to servers via IPv6
3. Enthusiast: Has a Web server delivering pages over IPv6
4. Administrator: Has an SMTP server that accepts mail over IPv6
5. Professional: Has reverse DNS correctly configured for the IPv6 address of your SMTP server
6. Guru: Nameservers have AAAAA records and can be queried over IPv6
7. Sage: Has IPv6 glue

Scoreboard
Part III

Security Problems
Privacy Risk

- Anyone who has your IP address also has your MAC address!
- There is a "Privacy Extensions" technique to avoid this, enabled by default in Vista and Windows 7
ICMPv6

- Required for all networks
- Cannot be blocked
- Replaces ARP
- "Neighbor Discovery" is trivial
THC-IPv6

- Hacker's Toolkit
- Runs fine on Ubuntu, even in VMware on Windows 7
- Instructions: link Defcon-talk 8
Other Risks

- Many security appliances are not ready for IPv6, so it often bypasses them
  - Torrents run over IPv6
    - Link Defcon-talk 9
  - Some VPN appliances are not ready, so IPv6 connections must bypass them

- Packet Amplification Attacks
  - Routing Header Zero
  - Ping-pong
    - Links Defcon-talk 10 and 11
Contact

- Sam Bowne
- Computer Networking and Information Technology, City College San Francisco
- Email: sbowne@ccsf.edu
- Twitter: @sambowne

This whole talk and all the referenced links are on my Web site: samsclass.info

- Click "Defcon Materials"