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:

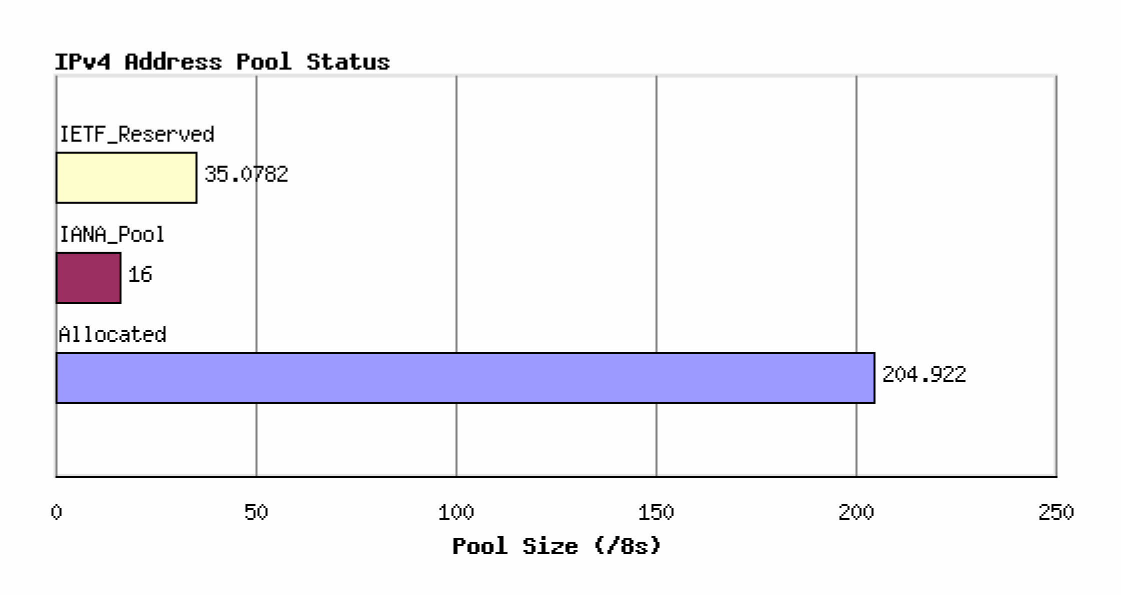
  `11000000 10101000 00000001 00001010`
- 2^32 total addresses
  - 4 billion
- Are you kidding? There are 7 billion people, they each need iPads, cell phones, Google brain chip implants, etc…

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

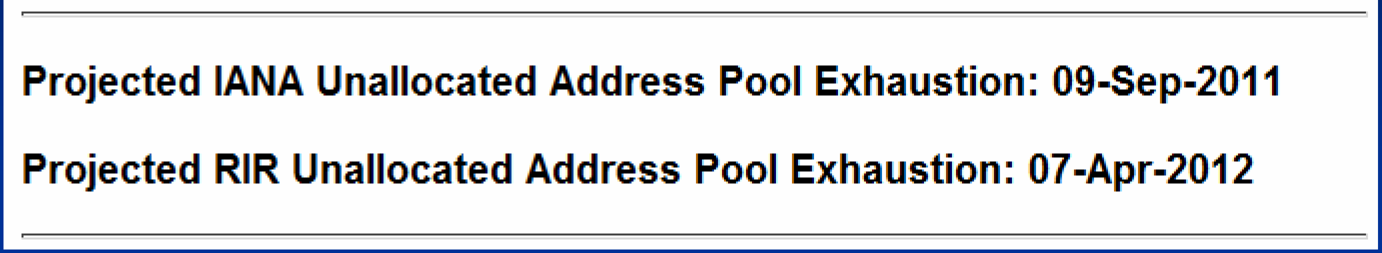
IPv4 Exhaustion

- 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



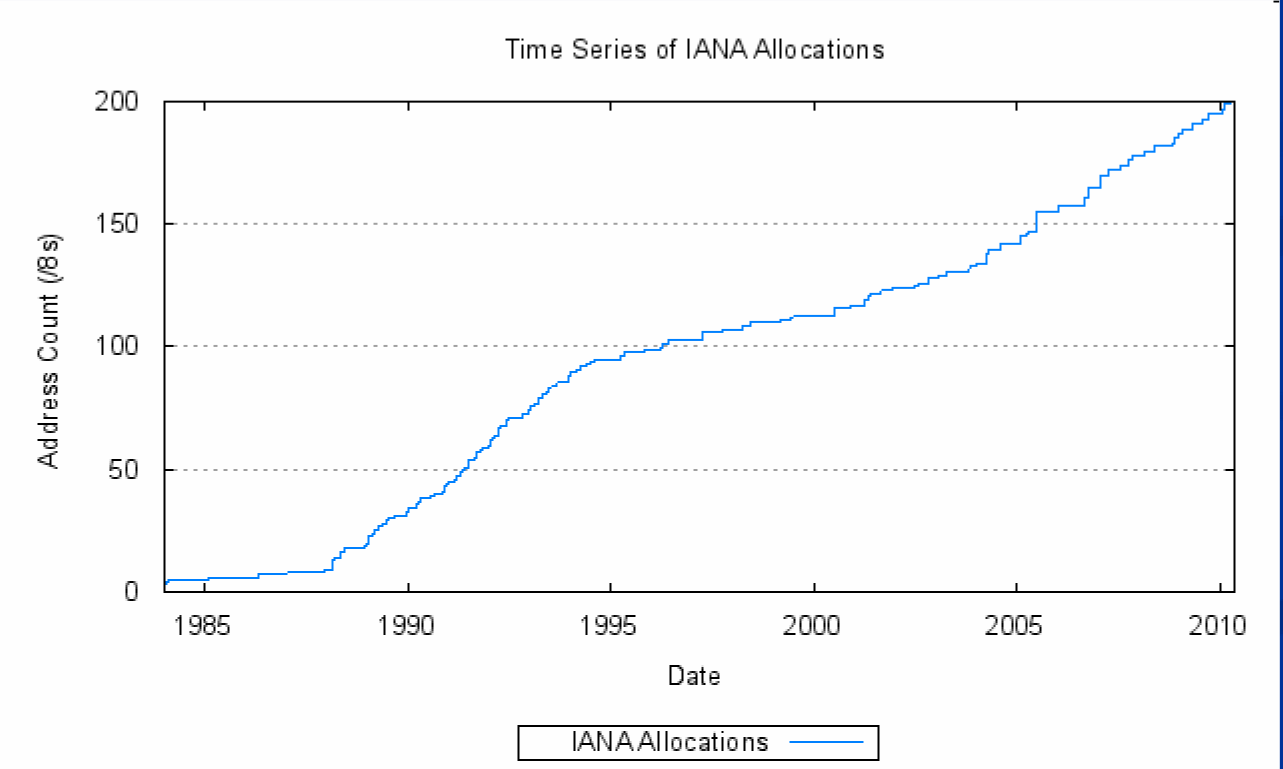
From link Defcon-talk 3

The End is Near



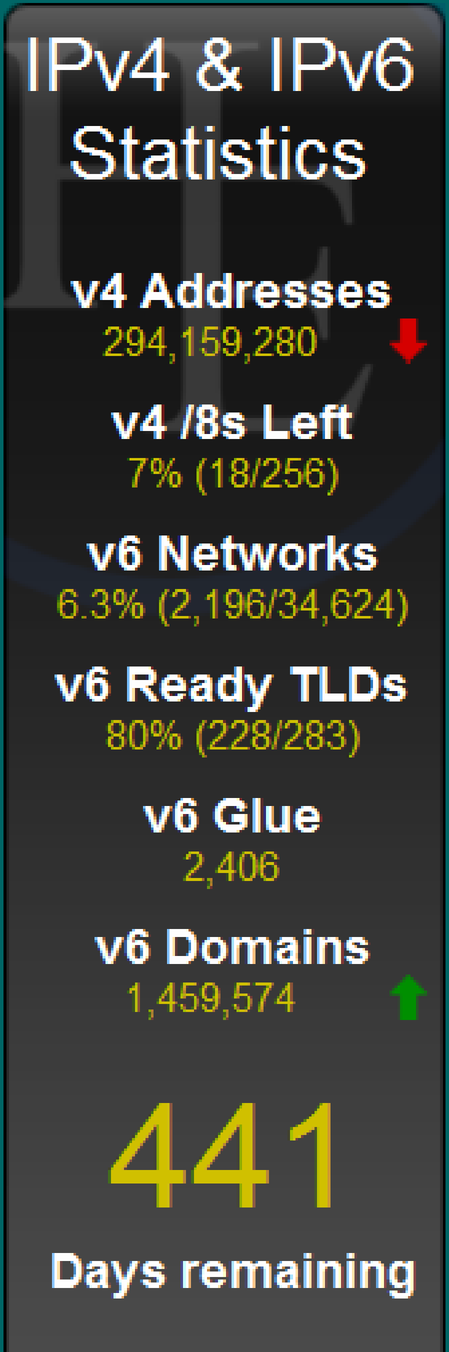
Projected IANA Unallocated Address Pool Exhaustion: 09-Sep-2011

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



IPv4 & IPv6 Statistics

v4 Addresses
294,159,280 ↓

v4 /8s Left
7% (18/256)

v6 Networks
6.3% (2,196/34,624)

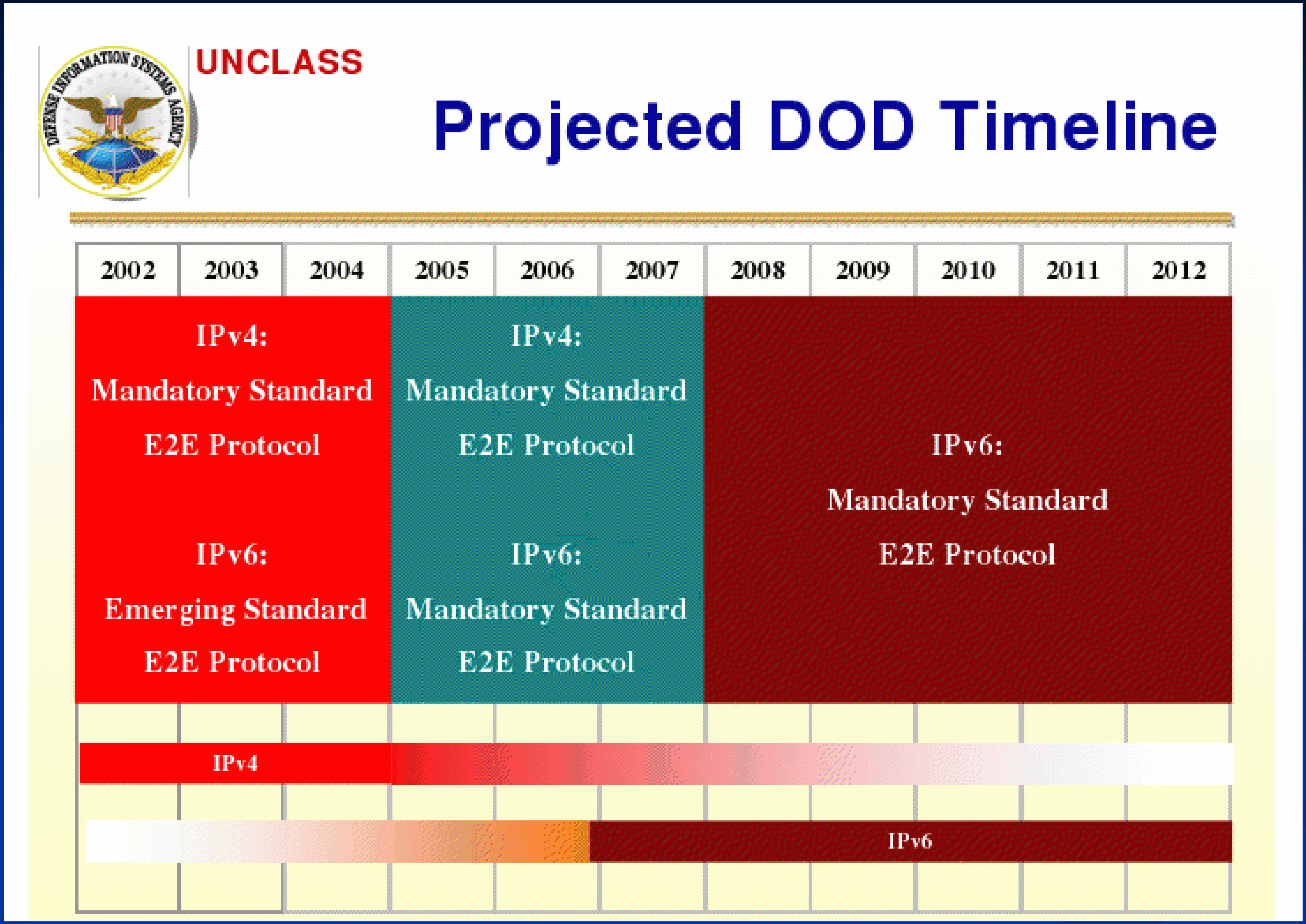
v6 Ready TLDs
80% (228/283)

v6 Glue
2,406

v6 Domains
1,459,574 ↑

441

Days remaining



UNCLASS

Projected DOD Timeline

2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012

2002–2004:

IPv4:
Mandatory Standard
E2E Protocol

IPv6:
Emerging Standard
E2E Protocol

2005–2007:

IPv4:
Mandatory Standard
E2E Protocol

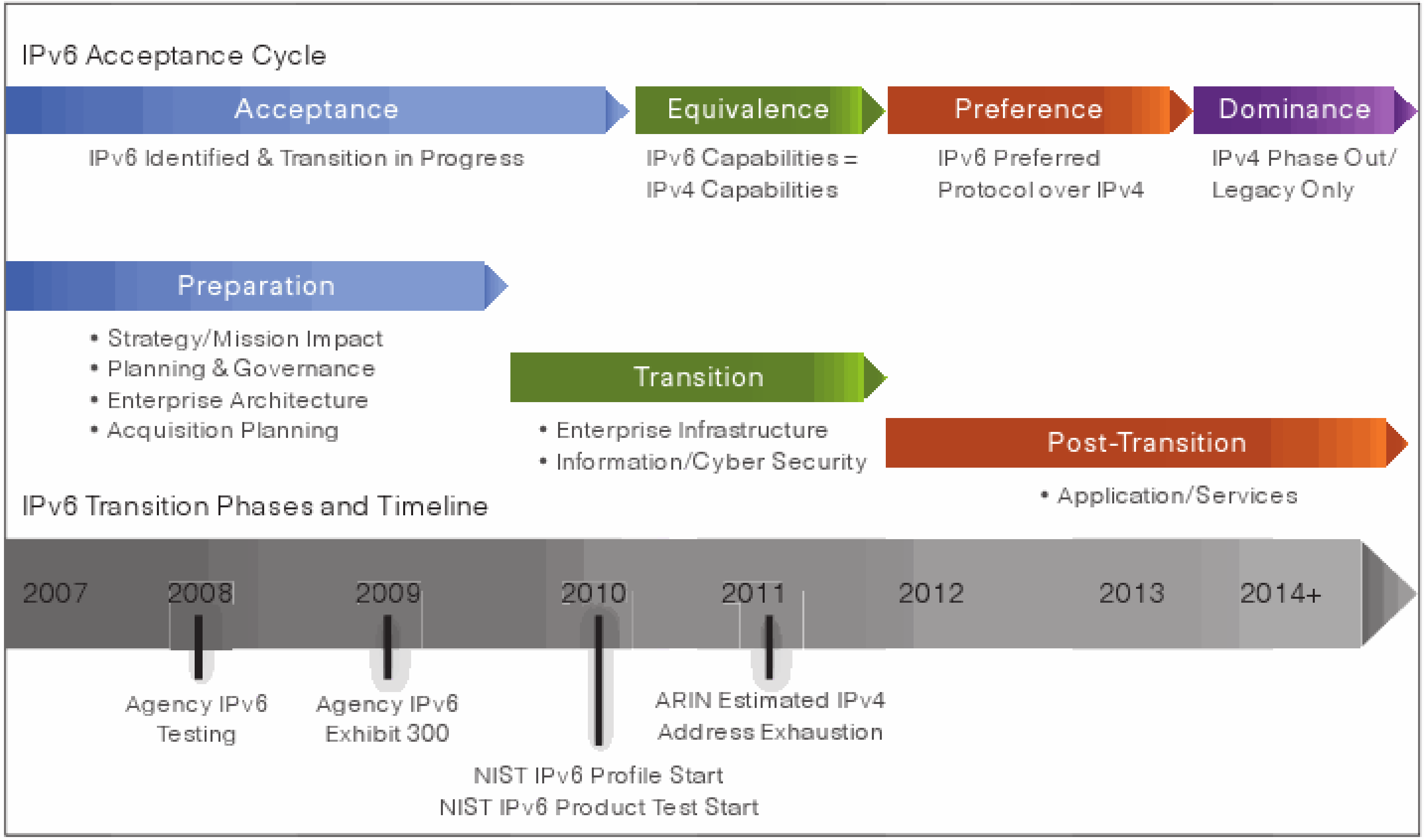
IPv6:
Mandatory Standard
E2E Protocol

2008–2012:

IPv6:
Mandatory Standard
E2E Protocol

- 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 2008 2009 2010 2011 2012 2013 2014+

Agency IPv6 Testing

Agency IPv6 Exhibit 300

NIST IPv6 Profile Start
NIST IPv6 Product Test Start

ARIN Estimated IPv4 Address Exhaustion

Figure 2: Federal IPv6 Transition Phases and Timelines

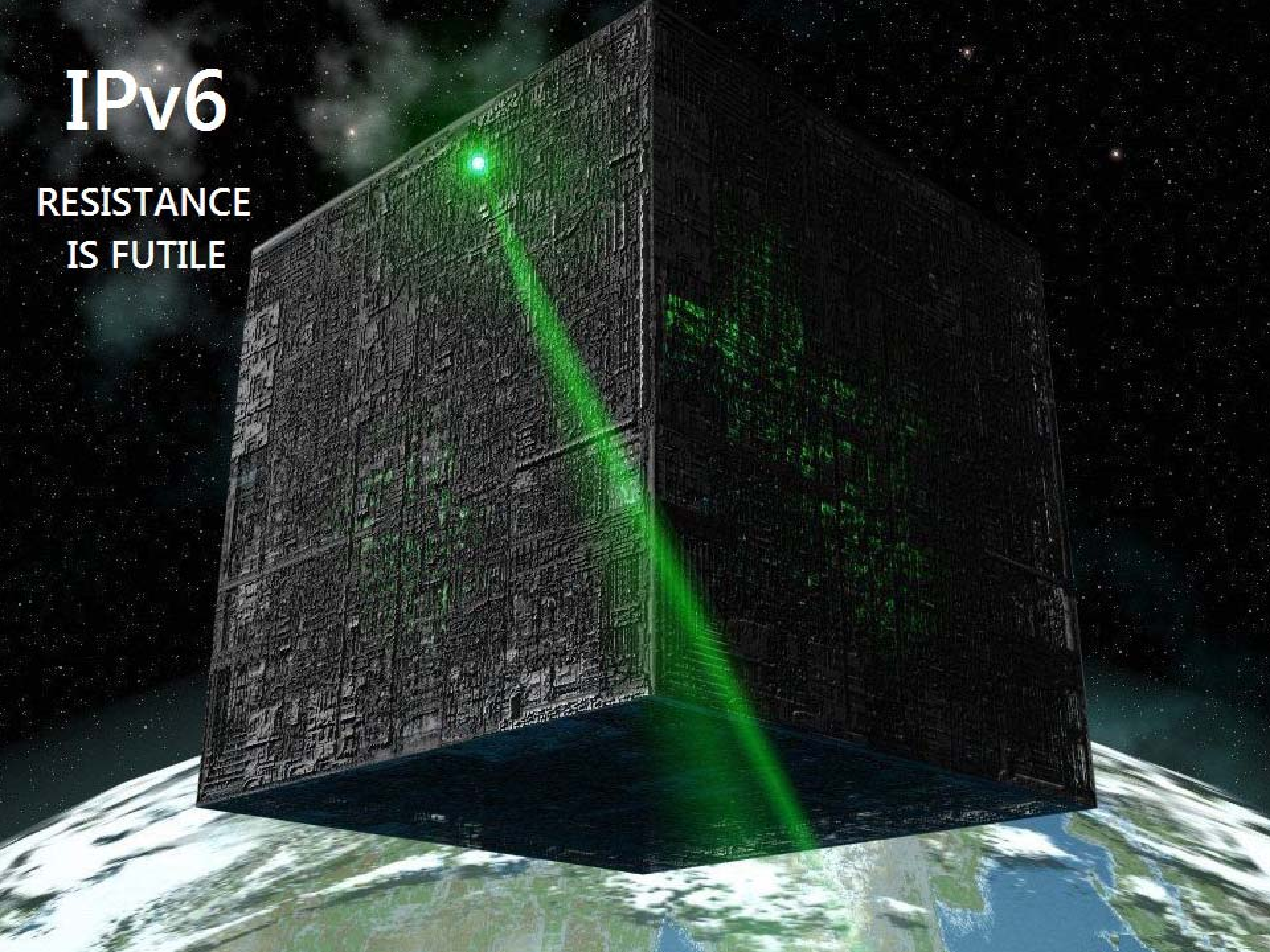
- From Cisco (link Defcon-talk 2)

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

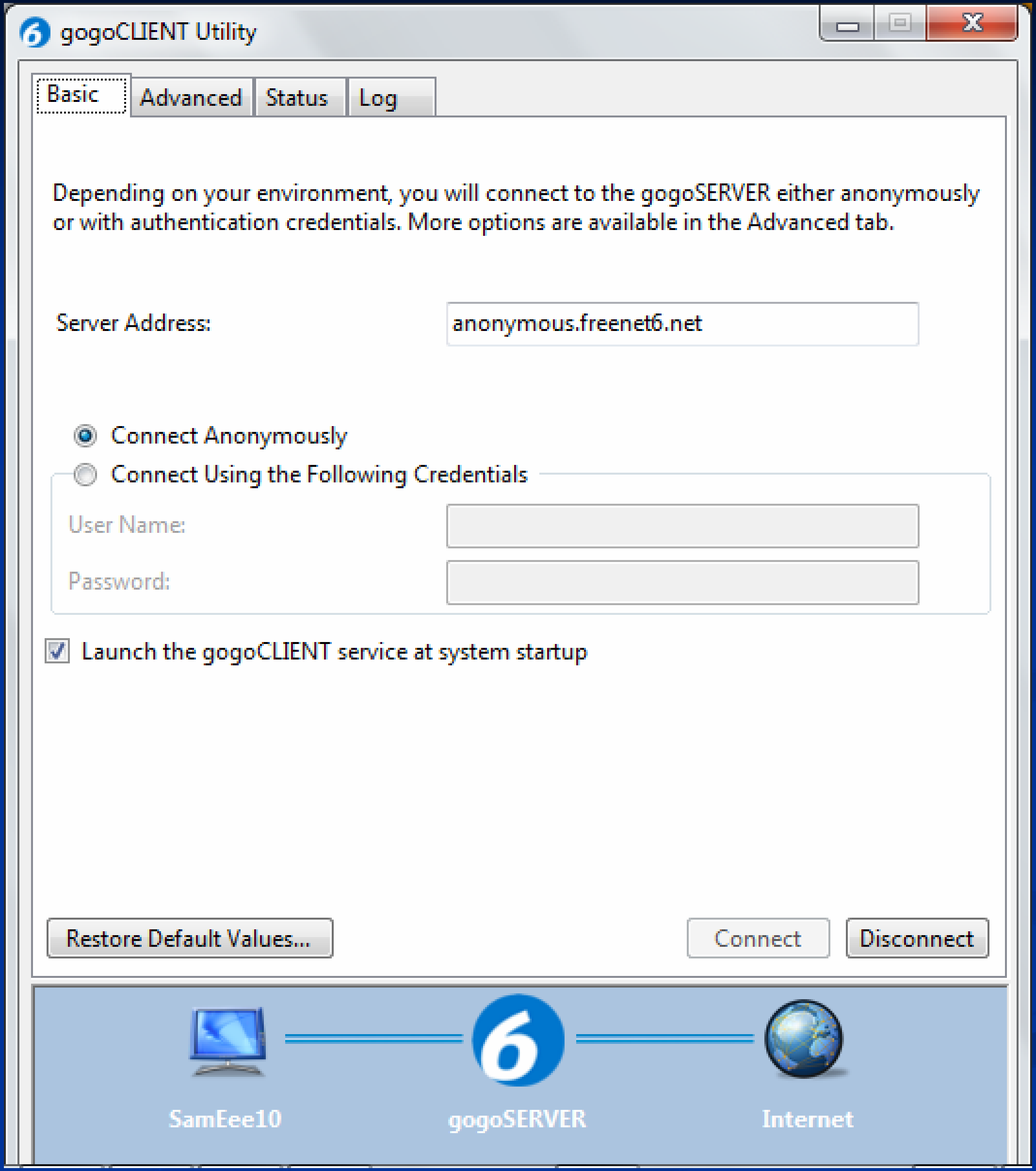
- **Ignore** IPv6: Stay on IPv4-only
- **Gateways**: Devices that convert IPv6 to IPv4
- **Tunnel** IPv6 over IPv4
- **Dual-Stack**: IPv4 and IPv6 together
- **Nirvana**: IPv6-only

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



gogoCLIENT Utility

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

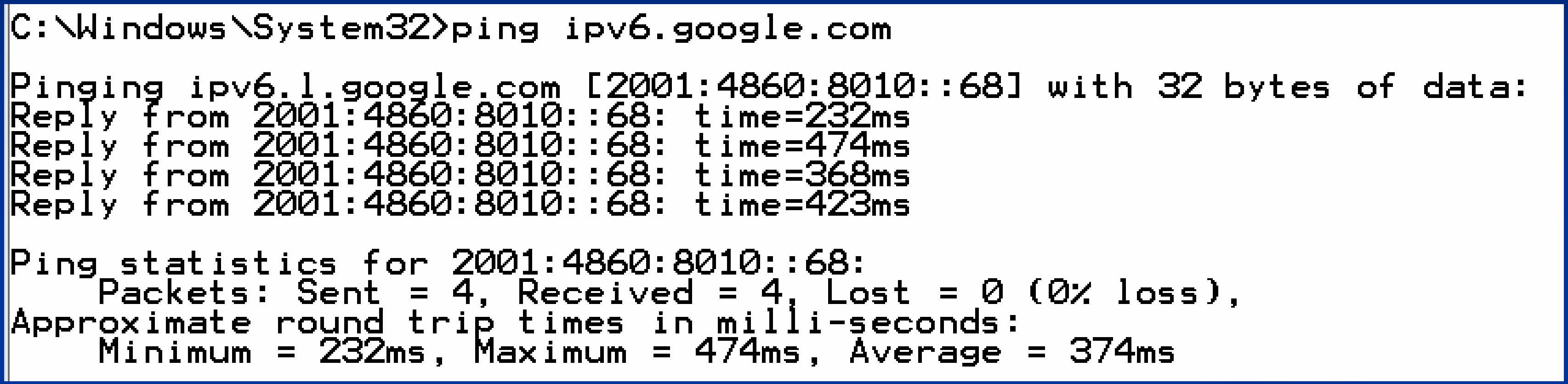
○ Connect Using the Following Credentials

User Name:

Password:

☑ Launch the gogoCLIENT service at system startup

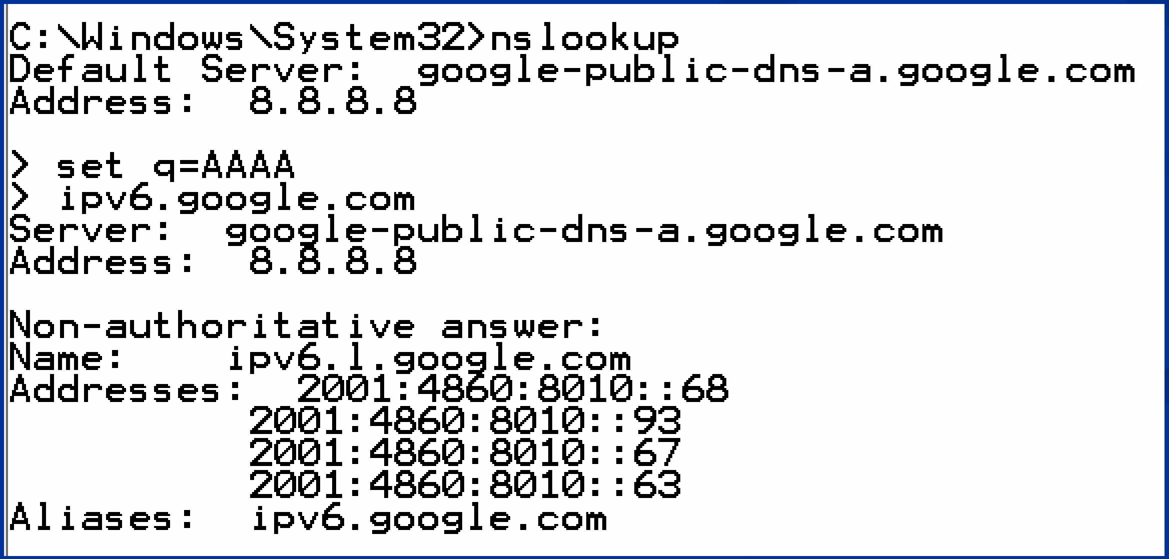
Demonstration



```
C:\Windows\System32>ping ipv6.google.com

Pinging ipv6.l.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
```



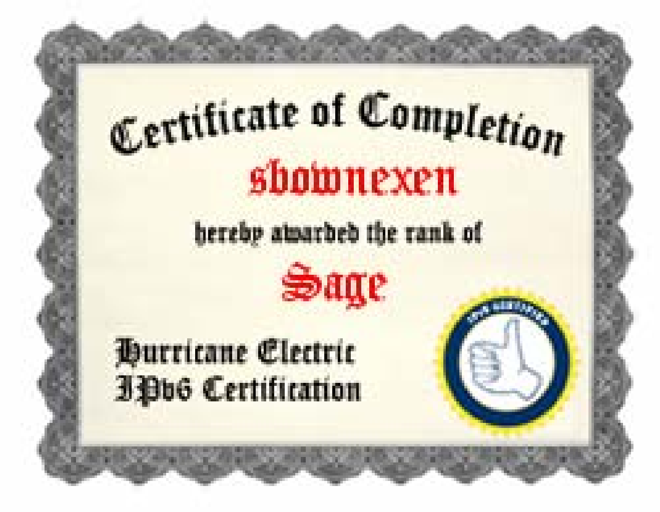
```
C:\Windows\System32>nslookup
Default Server:  google-public-dns-a.google.com
Address:  8.8.8.8

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

Non-authoritative answer:
Name:    ipv6.l.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



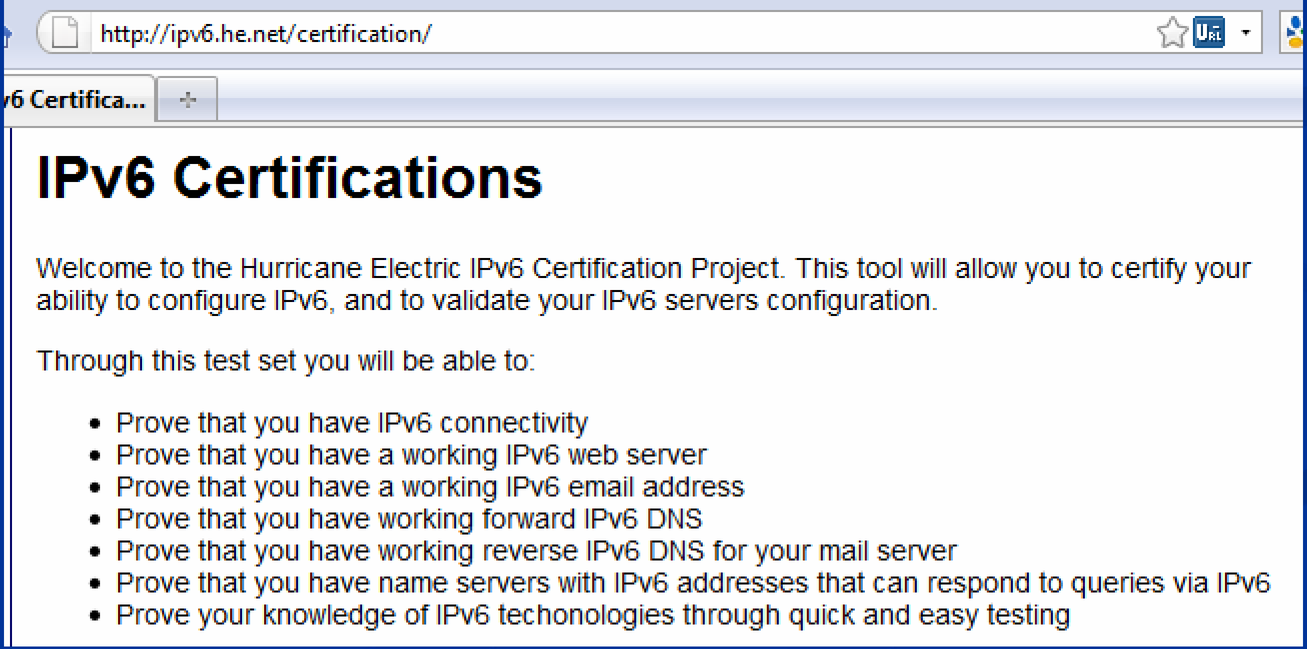
Certificate of Completion

shownexen

hereby awarded the rank of

Sage

Hurricane Electric
IPv6 Certification



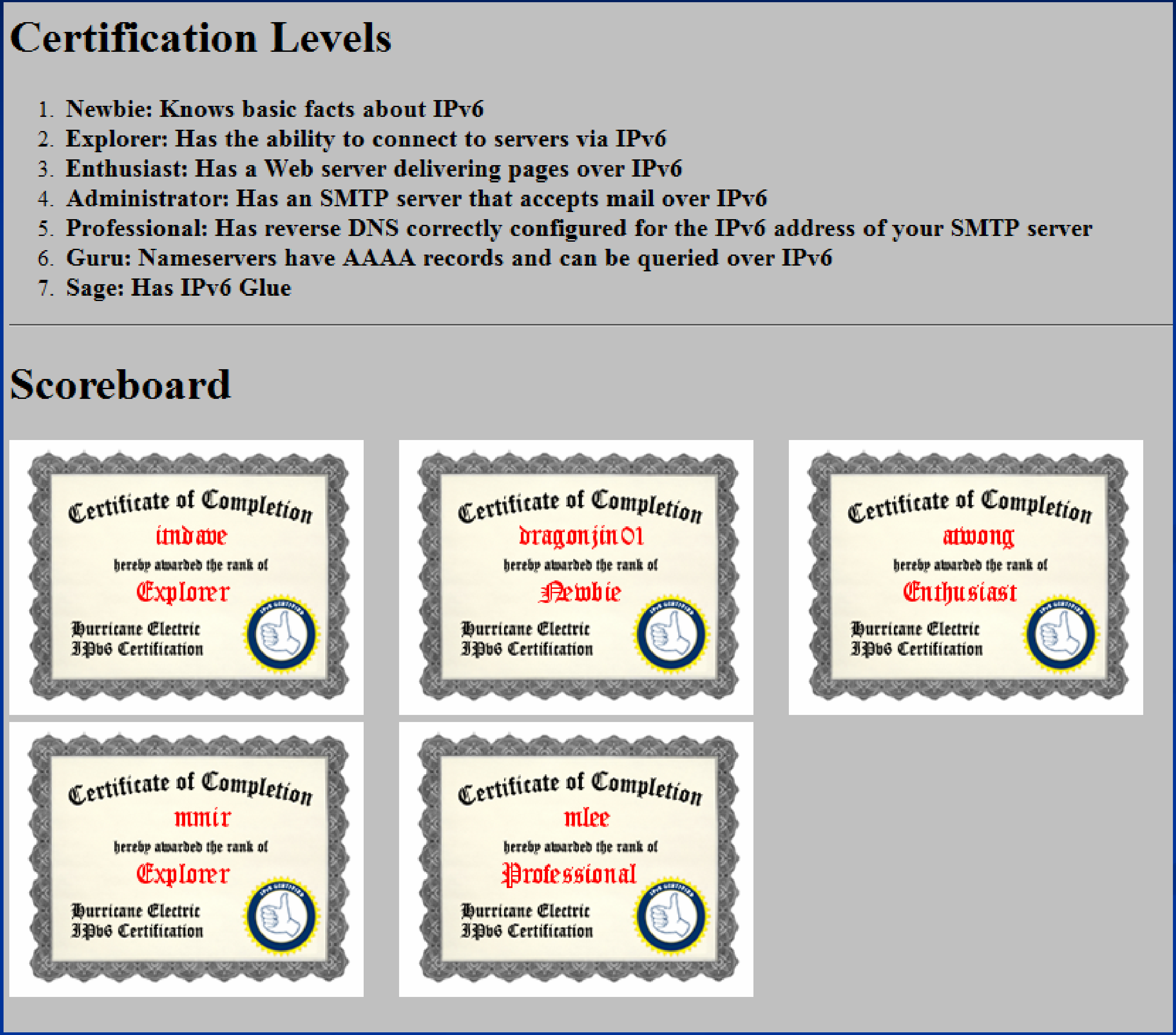
IPv6 Certifications

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 techonologies 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 AAAA records and can be queried over IPv6
7. Sage: Has IPv6 Glue

Scoreboard

Certificate of Completion
itmdave
hereby awarded the rank of
Explorer
Hurricane Electric
IPv6 Certification

Certificate of Completion
dragonjin01
hereby awarded the rank of
Newbie
Hurricane Electric
IPv6 Certification

Certificate of Completion
atwong
hereby awarded the rank of
Enthusiast
Hurricane Electric
IPv6 Certification

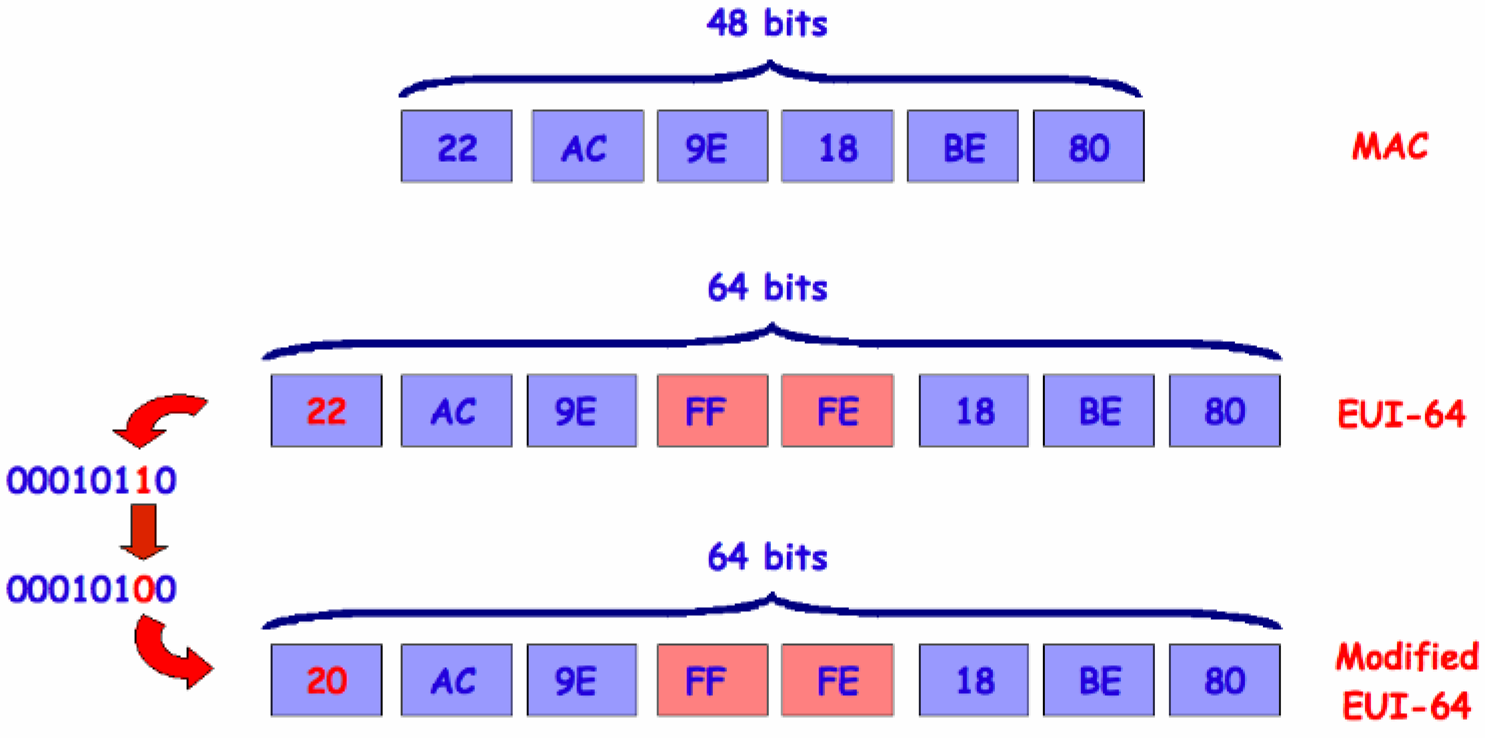
Certificate of Completion
mmir
hereby awarded the rank of
Explorer
Hurricane Electric
IPv6 Certification

Certificate of Completion
mlee
hereby awarded the rank of
Professional
Hurricane Electric
IPv6 Certification

Part III

Security Problems

Extended Unique Identifier EUI-64



48 bits

22	AC	9E	18	BE	80	MAC

64 bits

22	AC	9E	FF	FE	18	BE	80	EUI-64

00010110

00010100

64 bits

20	AC	9E	FF	FE	18	BE	80	Modified EUI-64

- Used by Ethernet

Privacy Risk

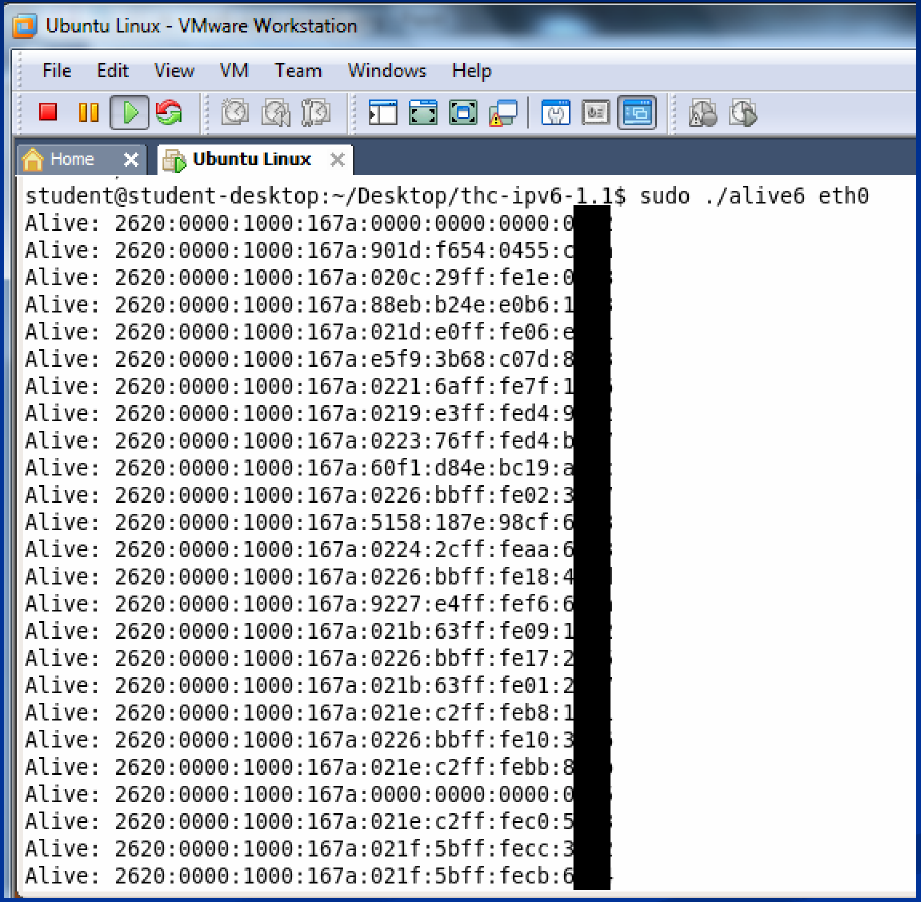
- Anyone who has your IP address also has your MAC address!
- There is a "Privacy Extensions" technique to avoid this, enabled by default in Vista and Windows 7

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



```
student@student-desktop:~/Desktop/thc-ipv6-1.1$ sudo ./alive6 eth0
Alive: 2620:0000:1000:167a:0000:0000:0000:[redacted]
Alive: 2620:0000:1000:167a:901d:f654:0455:
Alive: 2620:0000:1000:167a:020c:29ff:fe1e:
Alive: 2620:0000:1000:167a:88eb:b24e:e0b6:
Alive: 2620:0000:1000:167a:021d:e0ff:fe06:
Alive: 2620:0000:1000:167a:e5f9:3b68:c07d:
Alive: 2620:0000:1000:167a:0221:6aff:fe7f:
Alive: 2620:0000:1000:167a:0219:e3ff:fed4:
Alive: 2620:0000:1000:167a:0223:76ff:fed4:
Alive: 2620:0000:1000:167a:60f1:d84e:bc19:
Alive: 2620:0000:1000:167a:0226:bbff:fe02:
Alive: 2620:0000:1000:167a:5158:187e:98cf:
Alive: 2620:0000:1000:167a:0224:2cff:feaa:
Alive: 2620:0000:1000:167a:0226:bbff:fe18:
Alive: 2620:0000:1000:167a:9227:e4ff:fef6:
Alive: 2620:0000:1000:167a:021b:63ff:fe09:
Alive: 2620:0000:1000:167a:0226:bbff:fe17:
Alive: 2620:0000:1000:167a:021b:63ff:fe01:
Alive: 2620:0000:1000:167a:021e:c2ff:feb8:
Alive: 2620:0000:1000:167a:0226:bbff:fe10:
Alive: 2620:0000:1000:167a:021e:c2ff:febb:
Alive: 2620:0000:1000:167a:0000:0000:0000:
Alive: 2620:0000:1000:167a:021e:c2ff:fec0:
Alive: 2620:0000:1000:167a:021f:5bff:fecc:
Alive: 2620:0000:1000:167a:021f:5bff:fecb:
```

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"