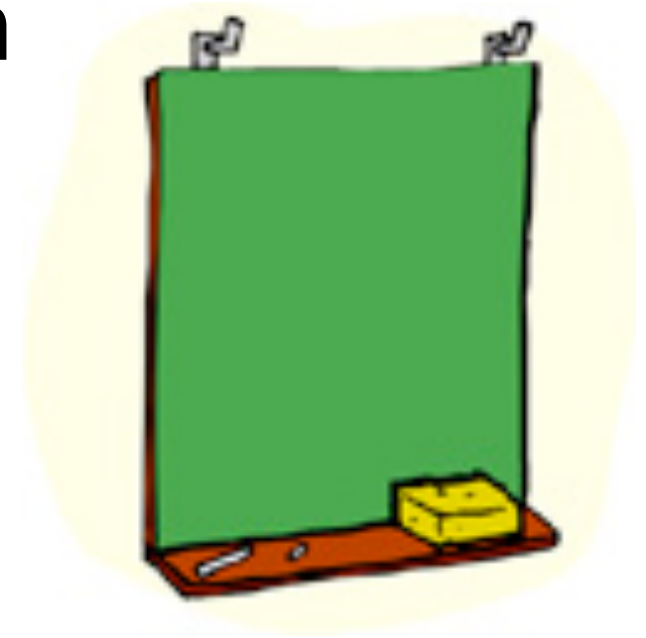

IPv6: The Friend you never knew you had

Johannes B. Ullrich, Ph.D.
SANS Technology Institute
jullrich@sans.edu

Outline

- Quick IPv6 Introduction
- IPv6 Autoconfiguration
- Tunnels
- Attack Tools
- Conclusion



History

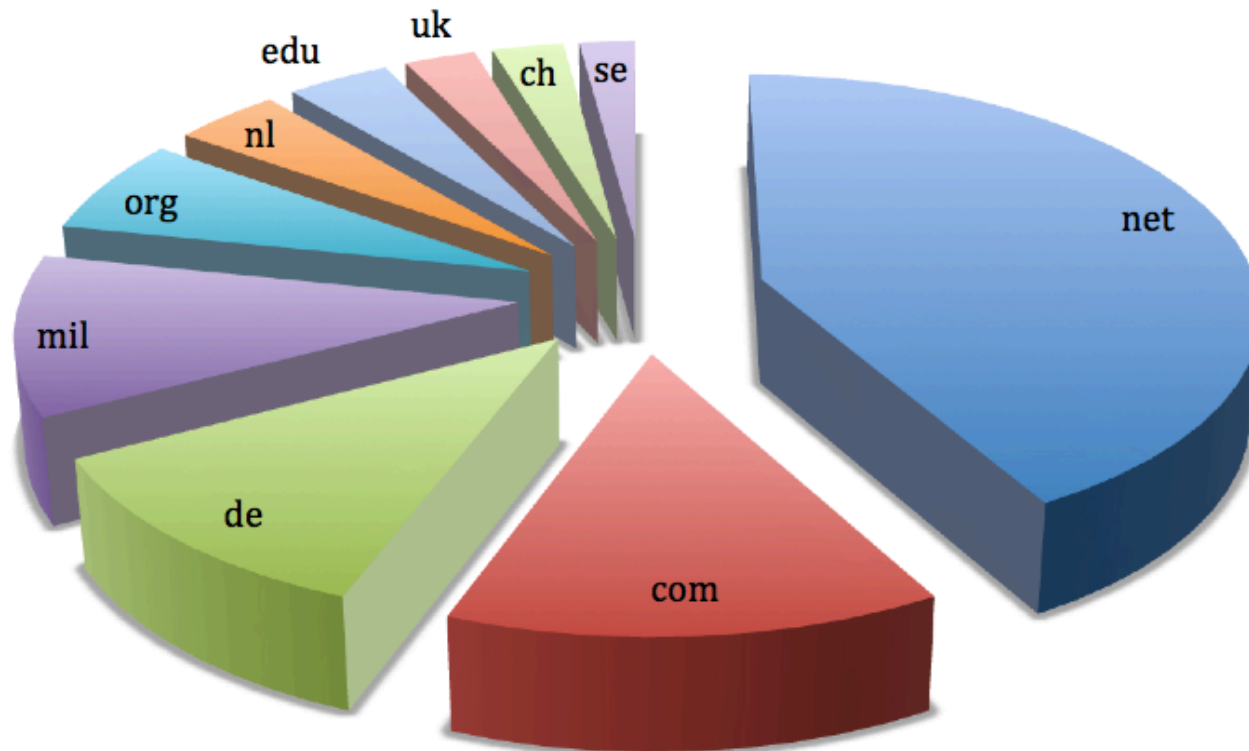
- IPv4: Developed in the 70s. IPv4 standard in 1981
- 2000/2001: About 400 Million users
- Today: 2 Billion users
- IPv6 development started mid 90s
- Why not IPv5?

IPv6 Penetration

- 235 out of 288 TLDs
- About 1 Million .com domains (out of 89 Million)
- 2402 Networks (AS) out of 35255
- 1477 out of top 1 Million websites have an IPv6 Address

IPv6 Usage

Top 10 TLDs for IPv6

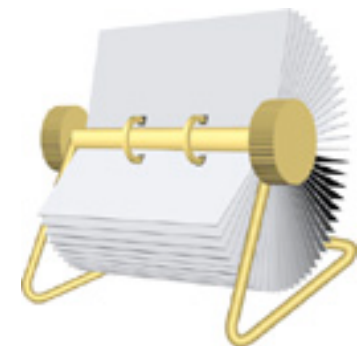


IPv6 Design Goals

- Make routing easier (less fragmented address space)
- Work well with modern hardware (64/128 Bit CPUs, more memory, high speed networks)
- Large “flat” networks

IPv6 Addresses

- 128 Bits (vs. 32 Bits for IPv4)
- Not because we need so many devices. But because it makes routing easier
- Matches modern 64/128 Bit hardware



IPv6 Routing

AAAA:BBBB:CCCC:DDDD:1111:2222:3333:4444

AAAA:BBBB -> Assigned by RIR to ISP (/32)

AAAA:BBBB:CCCC -> Assigned to "site" (/48)

AAAA:BBBB:CCCC:DDDD -> Assigned to subnet (/64)
(or home user). (DDDD = Subnet ID)

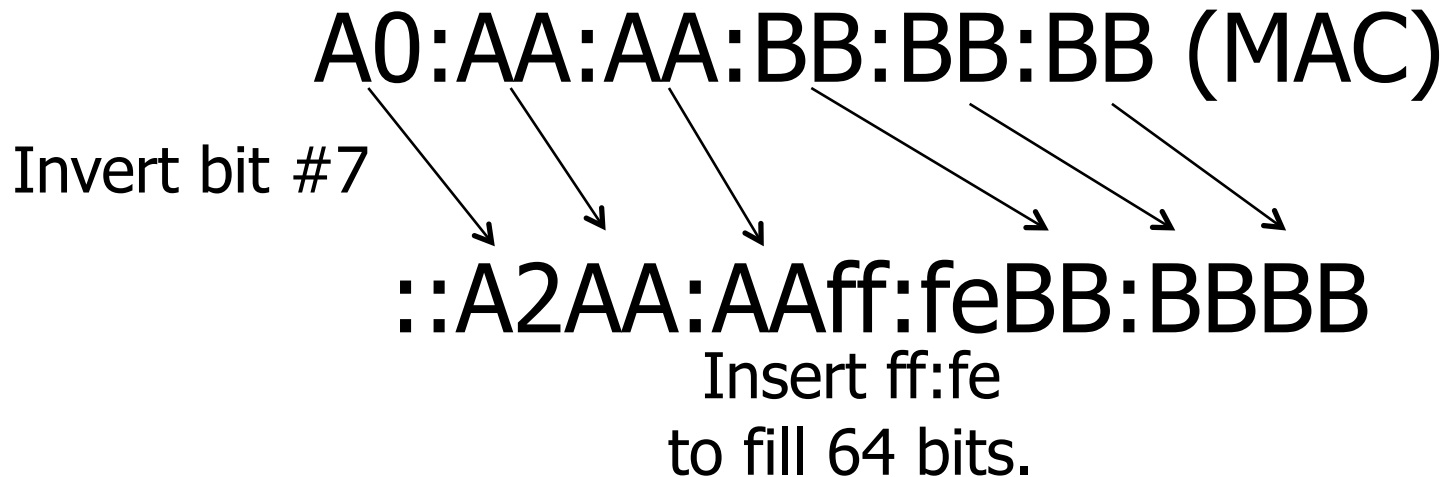
1111:2222:3333:4444 -> interface ID . Selected
by device if auto configuration is used.

Interface ID

- Various schemes to create last 64 bits:
 - Derived from MAC Address
 - Random (privacy enhanced)
 - DHCP
 - Cryptographically Generated (CGA)
 - Manually assigned

EUI-64

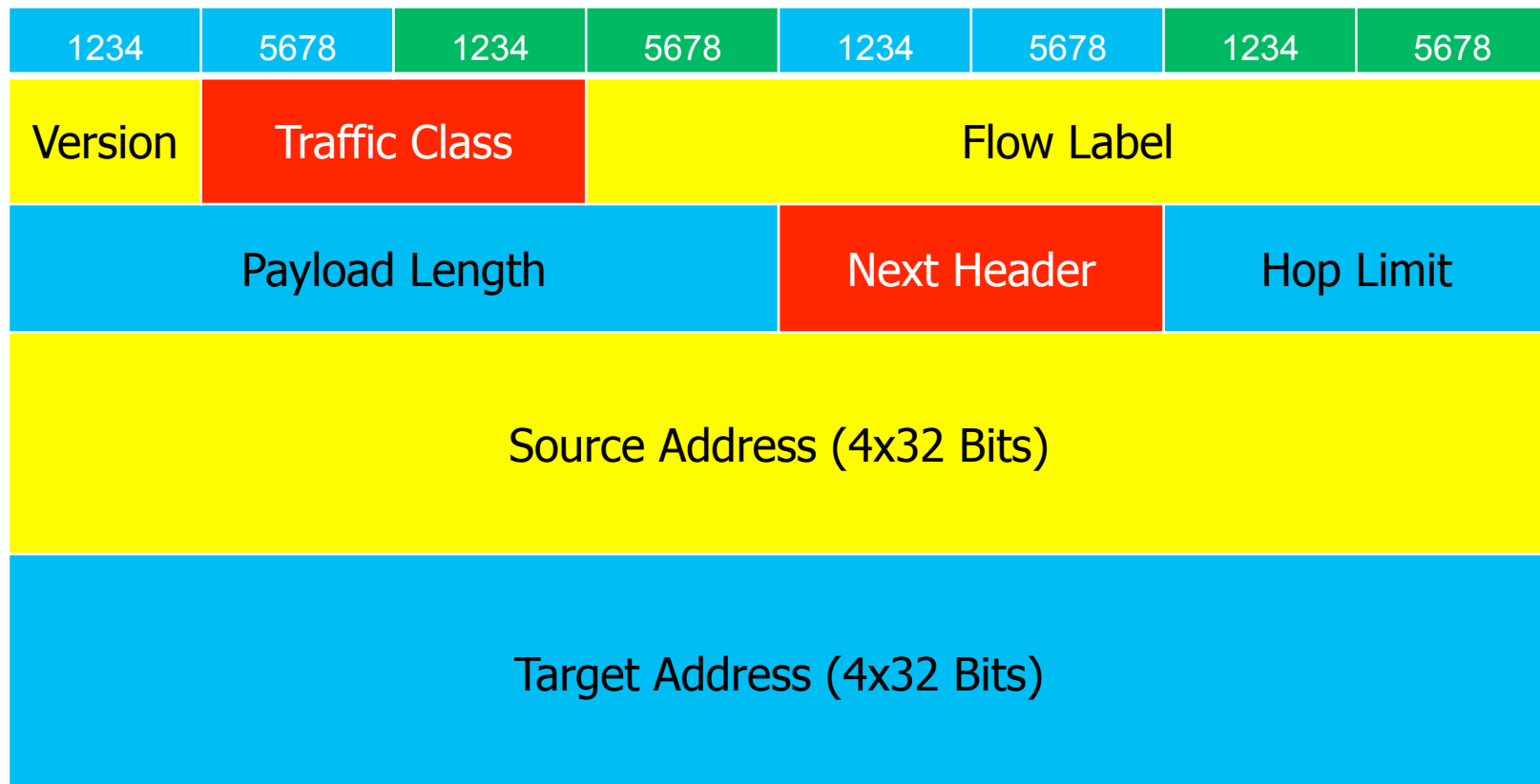
- Interface ID (64 Bits) derived from MAC Address (48 Bits).



Special Addresses

- IPv6 hosts typically hold multiple addresses:
- FE80:/16 – link local address
- 2000:/3 – globally routable
- FF00:/8 – multicast
- ::1 – localhost

IPv6 Header



Header Features

- Fixed Length (40 Bytes).
- No Options.
- No flags (Fragmentation).
- First 4 bits: 0110 (Version 6).
- 64 Bit alignment

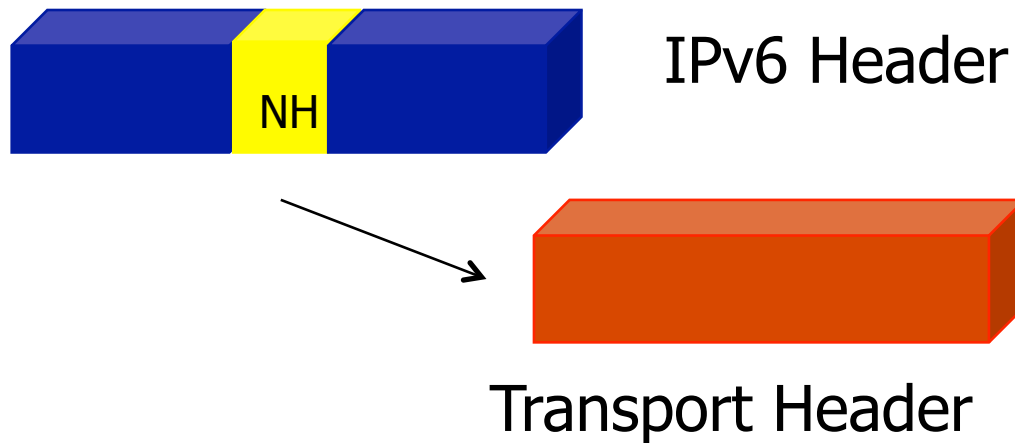
Extension Headers

- Some functions that are found in the IPv4 header are moved to extension headers
- “Next Header” may be an extension header, not a transport layer header

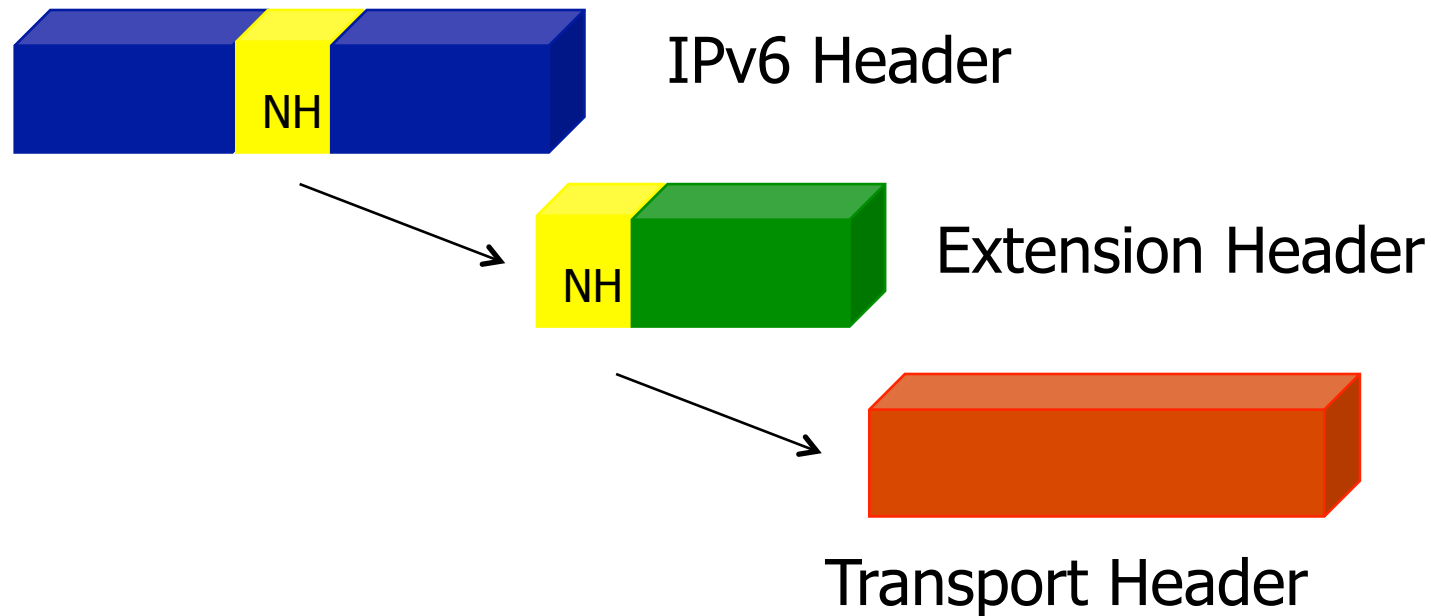
Extension Header Types

- Destination header
- Hop-By-Hop Header
- Routing Header
- Fragmentation Header
- IPSec (AH, ESP)

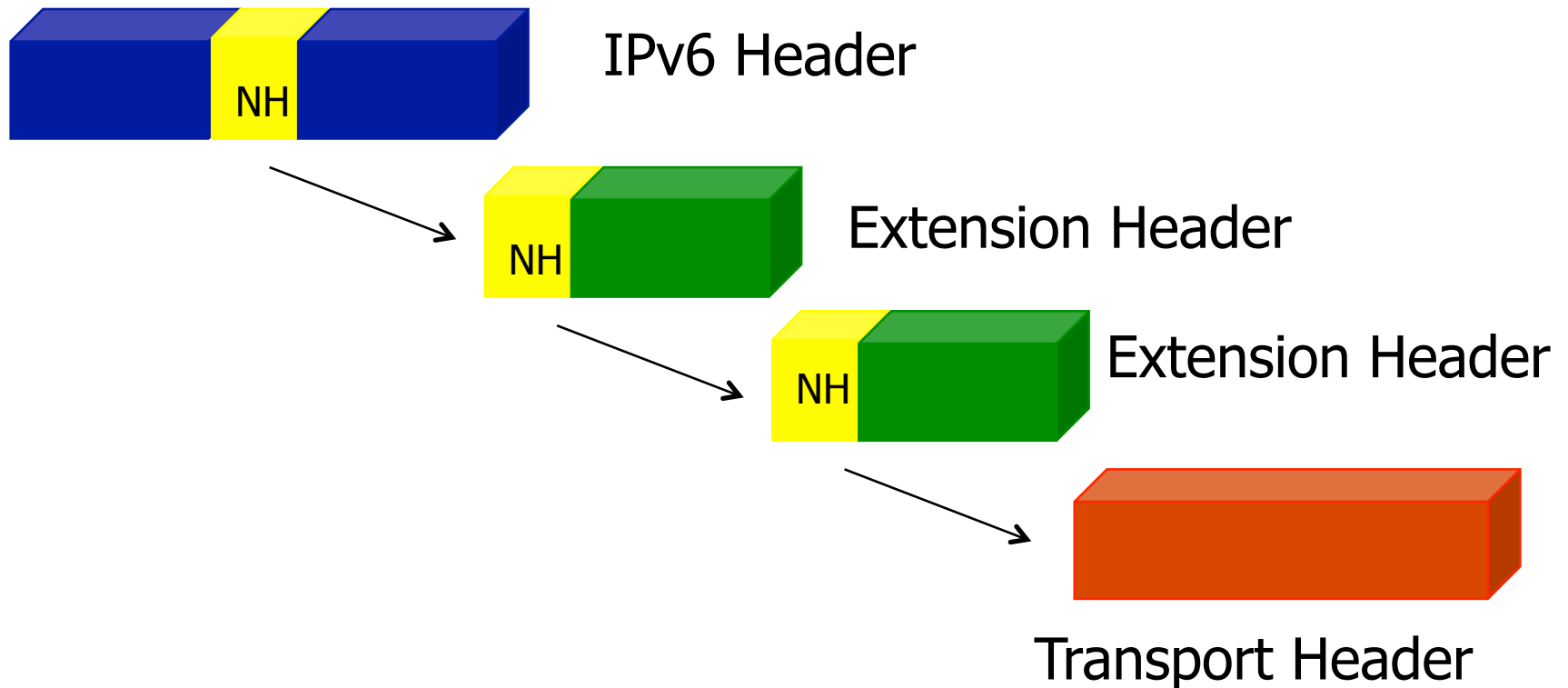
Extension Headers "stack"



Extension Headers "stack"



Extension Headers "stack"



IPv6 Routing Headers

- Source Routing for IPv6 (it didn't work in IPv4: Lets do it again... wrong)
- Source may specify some routers along the way
- May be used to reach internal networks

ARP and IPv6

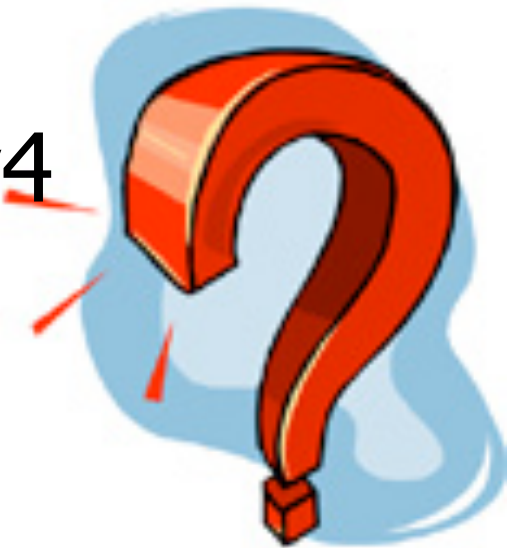
- No more ARP in IPv6
- Instead: ICMPv6 Multicast
- Very similar to ARP
- “Neighbor Discovery Protocol”
- Possibility to use “SEND” (Secure Neighbor Discovery)

Security Effects

- You got 2^{64} possible hosts in each subnet
- egress/ingress filtering may be easier
- layer 2 defenses may need rethinking (ARP Spoofing, DHCP?)

But why do we care?

- Do you use IPv6?
- Do you have a plan to implement it?
- Are you running out of IPv4 addresses?



You probably already use it!

- Most modern operating systems implement IPv6 support by default:
- Windows XP, Vista, Windows 7
- Windows 2003, 2008...
- OS X
- Linux

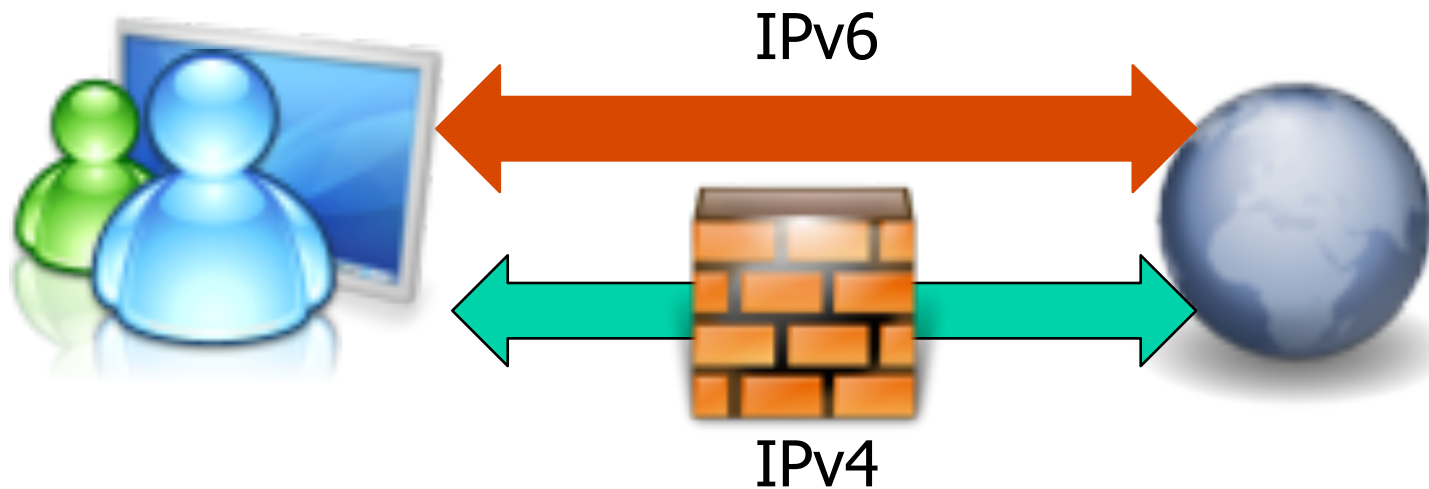
Dual Stack

- IPv4 and IPv6 is used at the same time
- IPv6 used locally even if no gateway
- IPv6 is preferred over IPv4 (if there is a route)

Autoconfiguration

- Router Advertisements
- Include network address
- Host picks interface ID
- DNS done via multicast

Dual Stack – Dual Firewalls?



IPv6 Firewalls

Forward IPv6 Traffic	30%
IPv6 Routing	24%
Static IPv6 Packet Filtering	29%
Stateful IPv6 Inspection	24%
Application level inspection (IPv6 payload)	17%
IDS/IPS Functions	14%
Tunneling (6to4 and 4to6)	29% and 14%

But what if I don't route IPv6?

- You still have to worry about local IPv6 traffic
- Tunnels. Some auto configure in default OS installs

Tunnel: IPv4

- IPv6 (in|over) IPv4
- Attach an IPv4 header in front of the IPv6 header
- Various schemes to do this. But easily detected via IP protocol field:
- GRE: 47 IPv6: 41

6to4

- Auto configure
- Anycast tunnel brokers:
192.88.99.1
- IPv6 address: 2002:[ipv4]:
[interfaceid]
- Requires routable IPv4 address

6to4 Security

- Easily blocked on firewall (protocol 41, 47)
- Requires routable IPv4 address to work
- But auto configured by Win2008 R2 and other modern OS.

Tunnels: UDP

- Teredo (Miredo)
- Introduced by Microsoft
- Now an open standard
- First deployed in Windows Vista
- Enabled by default in Windows 7
- Basic “trick” NAT gateways try to maintain UDP “connections”

Teredo Server

- Various public teredo servers are available: Microsoft, remlab ... more
- It is possible to stand up your own teredo server
- Teredo server will hand connection to Teredo Relay

Teredo Process

- Client connects to teredo server
- Handshake procedure establishes NAT parameters, defines address
- “STUN” like protocol
- Once connection is established, bubble packets will be used to maintain it

Teredo Addresses

- 2001:0000 Prefix
- AABB:CCDD Teredo Server IPv4
- eeee flags (12 bit “random”)
- ffff UDP port
- 1111:2222 client public IPv4

Finding IPv6 Hosts

- Dual Stack: Can be found easily locally
- 6to4 tunnels: IPv6 address predictable based on IPv4 address
- Teredo: IPv6 address somewhat predictable

6to4

- Use of multicast “ping” to all hosts (ff02::1)
- Passively by listening for ND messages
- Various tools

6to4

- IPv6 address is derived from IPv4:
- IPv6 = 2002:[IPv4]::[IPv4]
- Or IPv6 = 2002:[IPv4]::[MAC]

Teredo

- Not easy to “guess” full address.
- 16 bits of port and 12 bits of “flags” that are not easily predicted
- 268,435,456 possible addresses if you know the client and server IPv4 address

Finding Clients

- Force IPv6 content:
 - include IPv6 image in web site
 - include image in e-mail address
 - link via IM

Result: we get your IPv6 address

Attack Scenario: Rogue RA

- Router Advertisements (RA) are usually not authenticated
- Can be used just like DHCP to assign IPv6 addresses
- A rogue “router” will be able to assign IPv6 addresses

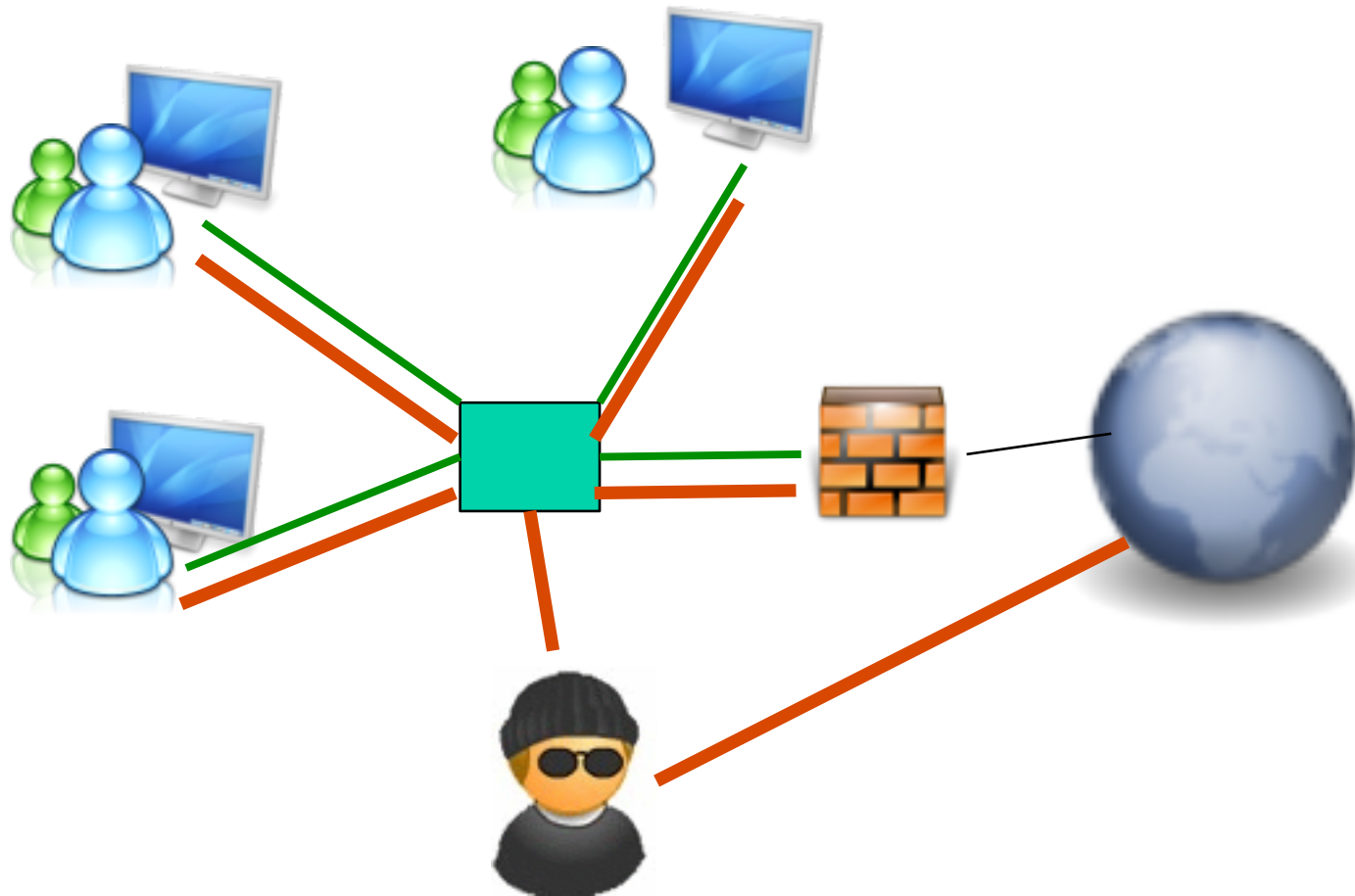
But what can it do?

- The IPv6 router can now play MiM, IF IPv6 connections are established
- IPv4 connections will be routed “as before”
- Only few resources are offered via IPv6

Advanced Attack: mDNS

- Modern operating systems tend to enable mDNS (Multicast DNS)
- mDNS is a core part of IPv6 auto configuration
- A mDNS server can either respond, or advertise additional DNS servers

Attack Sketch



IPv6 Attack Tools

- Scapy6: Allows crafting IPv6 packets at will
- THC IPv6 Attack Suite: basic library to create IPv6 packets plus good number of tools

alive6

- Useful to find hosts on local network
- Multicast ping
- Also tries IPv6 packet with unknown header and fragments
- Can be send to remote networks (RH... requires bad implementation)

Abusing regular IPv6 Tools

- radvd: Standard Unix implementation of router advertisement daemon
- Turns system into an IPv6 router
- all you have to do now is forward (or mess with) packets

Random Additional Reading

- NIST Publications (search nist.gov)
- Hurricane Electric Tunnel broker:
www.tunnelbroker.net
- Joe Klein's site:
<http://sites.google.com/site/ipv6security>
- ISC: <http://isc.sans.edu/tools/ipv6.html>

Conclusion

- Even if you don't plan on using IPv6, you may already use it
- Half of the connections to our test bed use auto configured IPv6
- Don't let it become the dark alley on your network
- Plan, test and implement controls