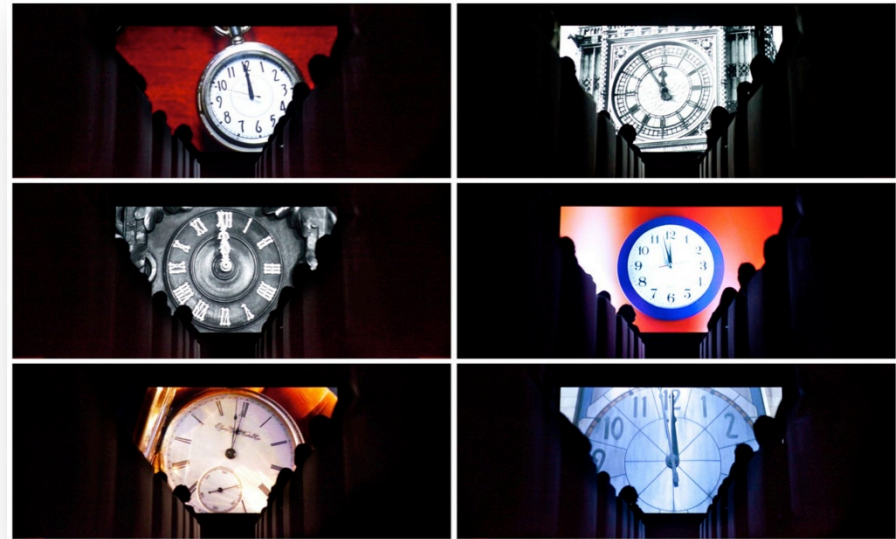


IPv6

Security & Fun With Very Big Numbers...

Agenda

- A little history
- Similarities/Differences between IPv4 and IPv6
 - It's not that bad, really...
- Security Concerns for IPv6 & Transition Strategies
- Demo/Conclusion






Per-Country IPv6 adoption



[World](#) | [Africa](#) | [Asia](#) | [Europe](#) | [Oceania](#) | [North America](#) | [Central America](#) | [South America](#)

The chart above shows the availability of IPv6 connectivity around the world.




-  Regions where IPv6 is more widely deployed (the darker the green, the greater the deployment) and users experience infrequent issues connecting to IPv6-enabled websites.
-  Regions where IPv6 is more widely deployed but users still experience significant reliability or latency issues connecting to IPv6-enabled websites.
-  Regions where IPv6 is not widely deployed and users experience significant reliability or latency issues connecting to IPv6-enabled websites.

Per-Country IPv6 adoption



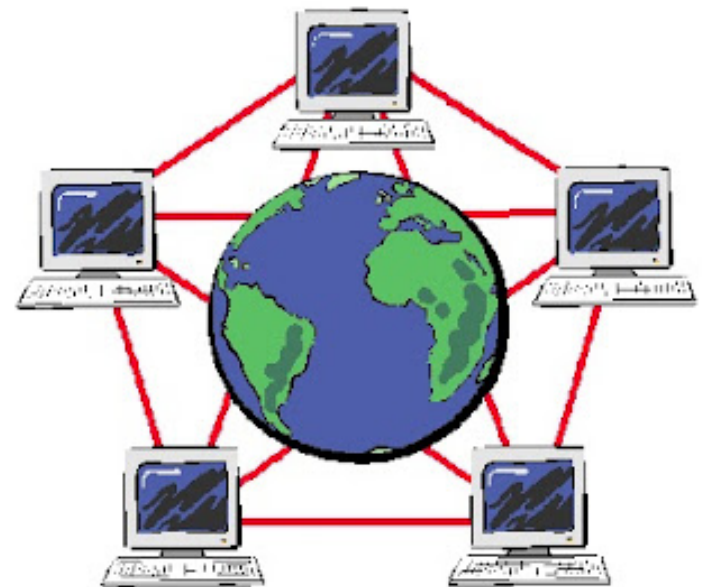
[World](#) | [Africa](#) | [Asia](#) | [Europe](#) | [Oceania](#) | [North America](#) | [Central America](#) | [South America](#)

The chart above shows the availability of IPv6 connectivity around the world.

-  Regions where IPv6 is more widely deployed (the darker the green, the greater the deployment) and users experience infrequent issues connecting to IPv6-enabled websites.
-  Regions where IPv6 is more widely deployed but users still experience significant reliability or latency issues connecting to IPv6-enabled websites.
-  Regions where IPv6 is not widely deployed and users experience significant reliability or latency issues connecting to IPv6-enabled websites.

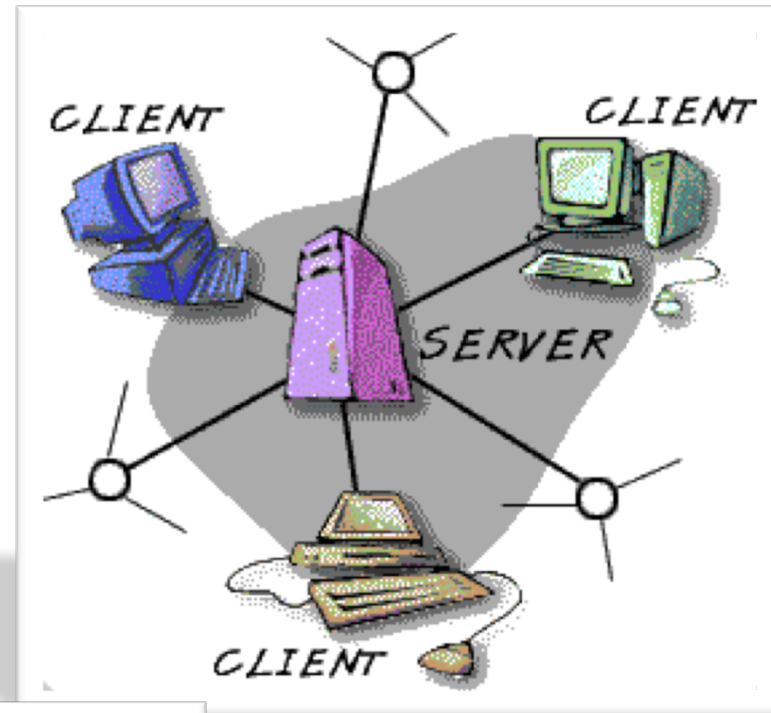
History Lesson – How did we Get here?

- Internet originally allowed for peer-to-peer connectivity
 - Only a few thousand machines on the network
 - Everybody trusted everybody – network consisted of governments, universities (until Mr. Morris in 1988)
- As more people were added...
 - “trust model” disintegrated – witness the first Internet Gateway from Digital Equipment in the early 1990s
 - IP address space began to dwindle
 - IP addresses became assets – A Class B 134.141.*.* address space worth 6-7 figures now
 - IP addresses began to be shared
 - SPs with small allocations began to ‘rotate’ public addresses or NAT entire networks
- Big impact – “peer to peer” became “client server”



Client Server? Really?

- NAT (many clients sharing same public IP address) invented to prolong V4's lifetime
- Client/server paradigm OK for Web, email, etc... But...
 - Why can't I have a camera to watch my kids whilst at work?
 - Online Gaming, peer-to-peer file transfer, peer-to-peer communications (voice/video) all broken or made needlessly complex
- NAT complicates many protocols!
 - Especially those which offer services on "fixed ports"
 - Requires complex work-arounds
- Enter double & triple NAT...



It was quite unfair, really...

Country	Addresses (Millions)	Population (Millions)	Addresses/person
USA	1,536	312	4.923
UK	68	62	1.097
Japan	82	128	0.640
Korea	19	50	0.380
China	222	1,334	0.166
India	2	1,241	0.002

Free Pool of IPv4 Address Space Depleted

IPv6 adoption at critical phase

Montevideo, 3 February 2011 – The Number Resource Organization (NRO) announced today that the free pool of available IPv4 addresses is now fully depleted. On Monday, January 31, the Internet Assigned Numbers Authority (IANA) allocated two blocks of IPv4 address space to APNIC, the Regional Internet Registry (RIR) for the Asia Pacific region, which triggered a global policy to allocate the remaining IANA pool equally between the five RIRs. Today IANA allocated those blocks. This means that there are no longer any IPv4 addresses available for allocation from the IANA to the five RIRs.

IANA assigns IPv4 addresses to the RIRs in blocks that equate to 1/256th of the entire IPv4 address space. Each block is referred to as a “/8” or “slash-8”. A global policy agreed on by all five RIR communities and ratified in 2009 by ICANN, the international body responsible for the IANA function, dictated that when the IANA IPv4 free pool reached five remaining /8 blocks, these blocks were to be simultaneously and equally distributed to the five RIRs.

“This is an historic day in the history of the Internet, and one we have been anticipating for quite some time,” states Raúl Echeberría, Chairman of the Number Resource Organization (NRO), the official representative of the five RIRs. “The future of the Internet is in IPv6. All Internet stakeholders must now take definitive action to deploy IPv6.”

Each block = 16.7 million addresses;

2 blocks = 33.5 million addresses;

$33.5\text{M} / 2753\text{M} = .012$ addresses per person

83.3 people must share each address.

People, not devices!!

IPv6 Address Space

(A.K.A. fun with numbers subject)

- 340,282,366,920,938,463,463,374,607,431,768,211,456
 - 3.4×10^{38} ! Means 340 undecillion addresses, where 1 undecillion = a billion billion billion
 - Enough for each person (assuming 10B people) to have 3,400,000,000,000,000,000,000,000,000 (3.4×10^{27}) addresses
 - Enough for each square CM of earth to have 667,000,000,000,000,000,000 (6.67×10^{20}) addresses (*46 Million times more than entire IPv4 Address Space of 4,294,967,296*)



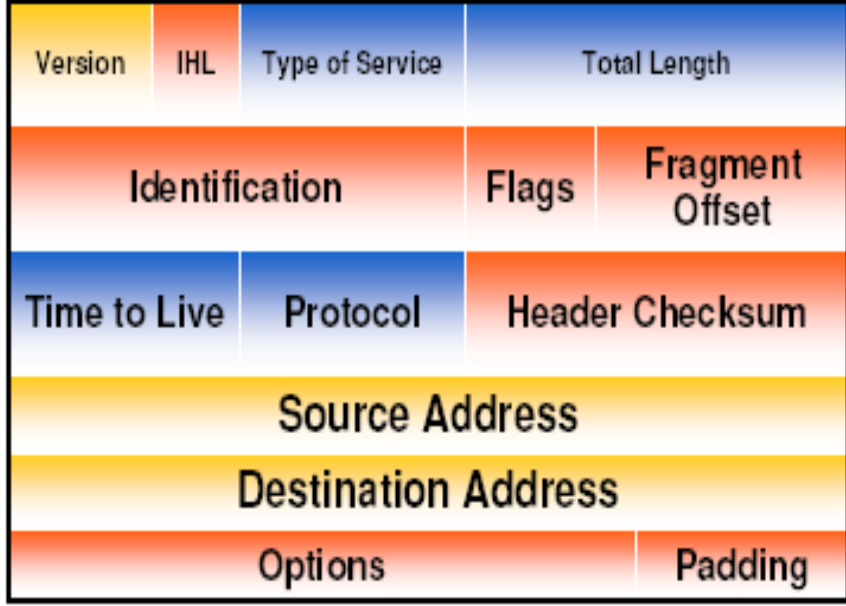
This space (1 CM²) 46 million times more addresses than all of IPv4

- Allows universal addressability
 - Eliminates need for NAT and all of its problems
 - Enables universal “network of things, including stuff inside your network
 - Increases need for strong authentication
- Increases need for security policies that address “perimeter perforation”

A look at IPv6 and some Plusses and Minuses...

Musical Chairs – different places, same meaning

IPv4 Header



IPv6 Header



- 3 fields same
- 4 with new names but same meaning
- 1 new field
- 7 deleted

Legend

- field's name kept from IPv4 to IPv6

- fields not kept in IPv6

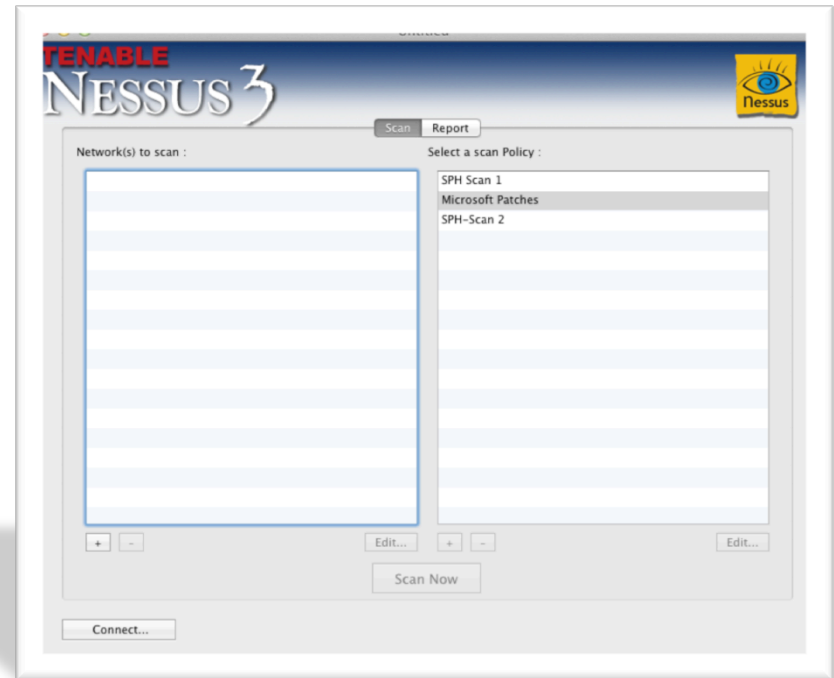
- Name & position changed in IPv6

- New field in IPv6

Destination Address

Large Address Space & Scanning

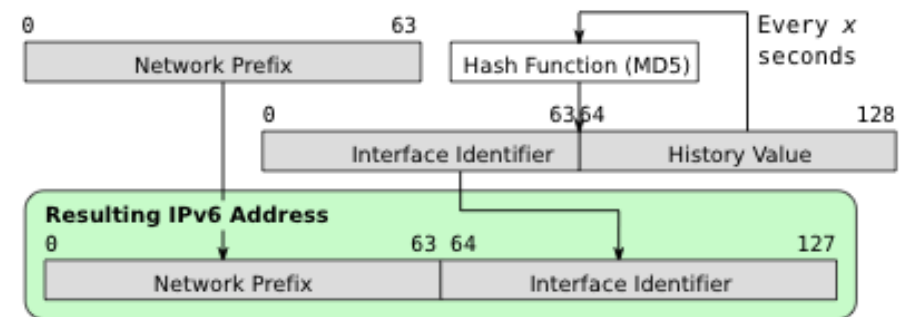
- “Scanning” is one way hackers and automated software such as worms and viruses look for victims
 - In IPv4, one “subnet” might contain as many as 256 computers (class c) and is dense
 - In IPv6, one subnet contains 18 quintillion (1.8×10^{19}) addresses and they are sparse
- **IPv6 effectively “breaks” scanning**
 - If scanner were scanning one IPv6 subnet with 10,000 hosts at 1 million scans per second, it would take 28 years to find the first target!



- **Some tricks but much harder...**
 - Sniffing (requires physical access to LAN, WiFi access or compromised machine)
 - Multicast ping (requires physical access to LAN)

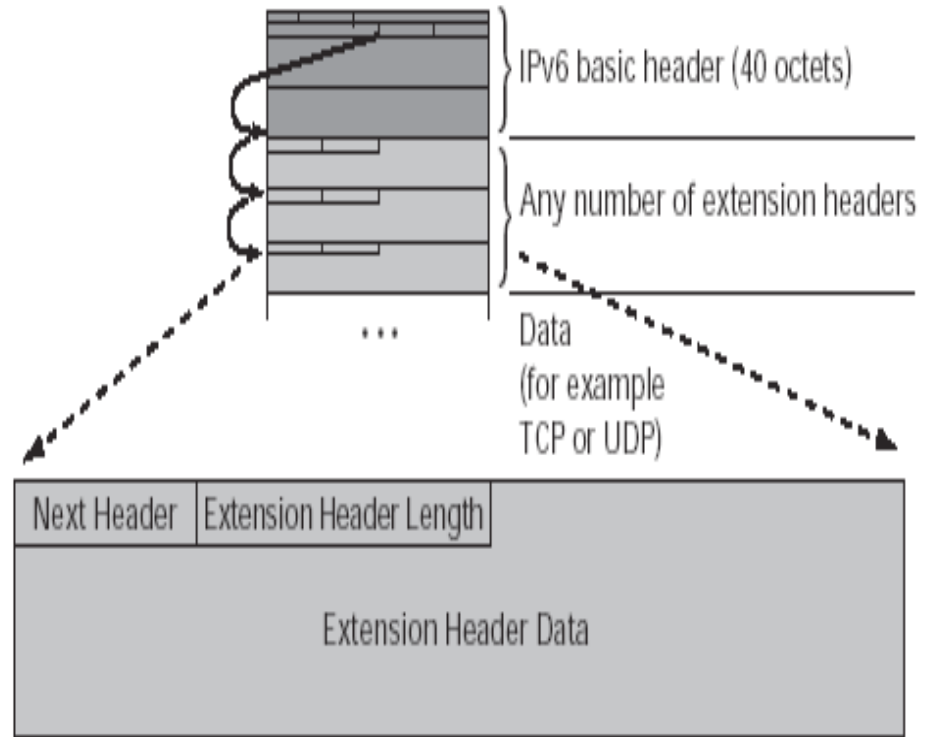
Privacy Concerns...

- **MAC addresses (layer 2 Ethernet) may form lower part of IPv6 address**
 - MAC address is globally unique, and can uniquely identify an end station
 - All L2 technologies (i.e. Bluetooth, 3G, 4G, WiFi) use MAC addresses
 - End station can be specifically tracked to individual device, with the associated privacy concerns
- IPv6 handles this with (***optional***) Privacy Extensions
 - Stateless auto-configuration uses periodically changing address that changes every X seconds, computed by client
 - Default is 24 hours, but configuration settable by network
 - Often **better** than IPv4 DHCP since frequently with v4 you get the same address over and over again!



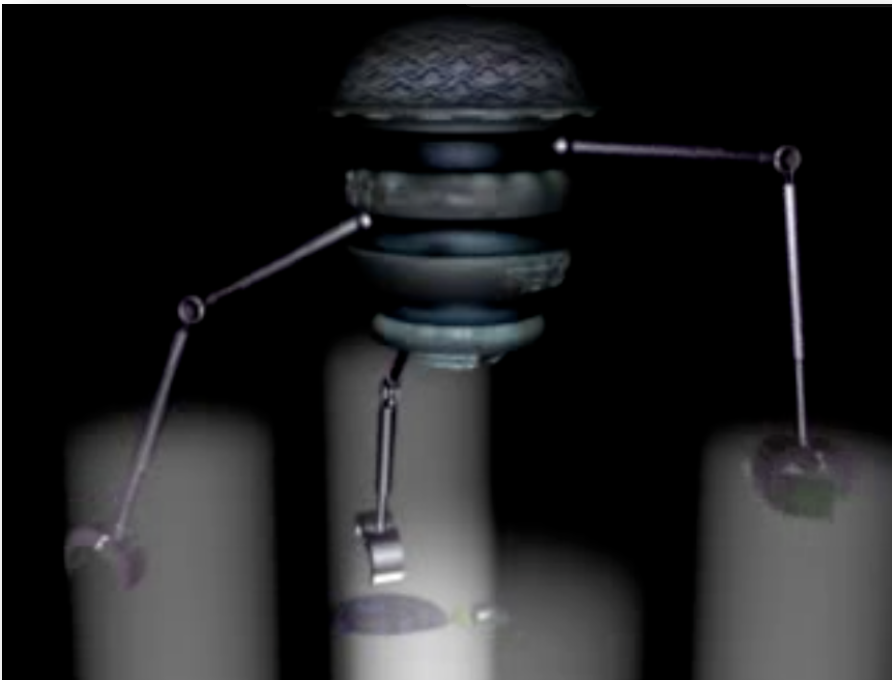
Extension Headers

- Next header field identifies the type of extension header
- Basic header is 40 Octets
- Subsequent headers are found by looking “extension header length” bytes past beginning of extension header
- Header types include:
 - Upper Layer Header (i.e. TCP, UDP)
 - Hop-by-Hop Options header
 - Destination Options Header
 - Routing Header
 - Fragment Header
 - Authentication Header (IPSec)



Extension Header Vulnerabilities

- Extension headers are variable length
 - Possible to craft packet with infinite number of headers – crashing devices in the path (DDoS vector)
 - Could make huge packets with many headers to force fragmentation and circumvent or DoS firewalls or IPSs in path
- Extension Header “fuzzing” attacks...
 - Uses **IP Stack Integrity Checker (ISIC)**, generates random data (fuzz) with the intention of performing bounds checking on receiving software
 - Common technique to crash or compromise end systems
- Risks can be mitigated by router rules
 - Just discard them!



The Transition & Associated Risks

The Transition...

- IPv4 will be around “**FOREVER**”...
 - Rarely does a new technology ever completely replace its predecessor; example: don’t we have **BOTH** wired Ethernet and Wireless LANs? Or both tablets and laptops?
- Two **must** coexist:
 - Systems must be in place to allow v6 to traverse v4 infrastructures
 - Systems must be in place to allow v4 to traverse v6 infrastructures
 - Systems must be in place to allow v4 nodes to communicate with v6 nodes, and v6 nodes to communicate with v4 nodes

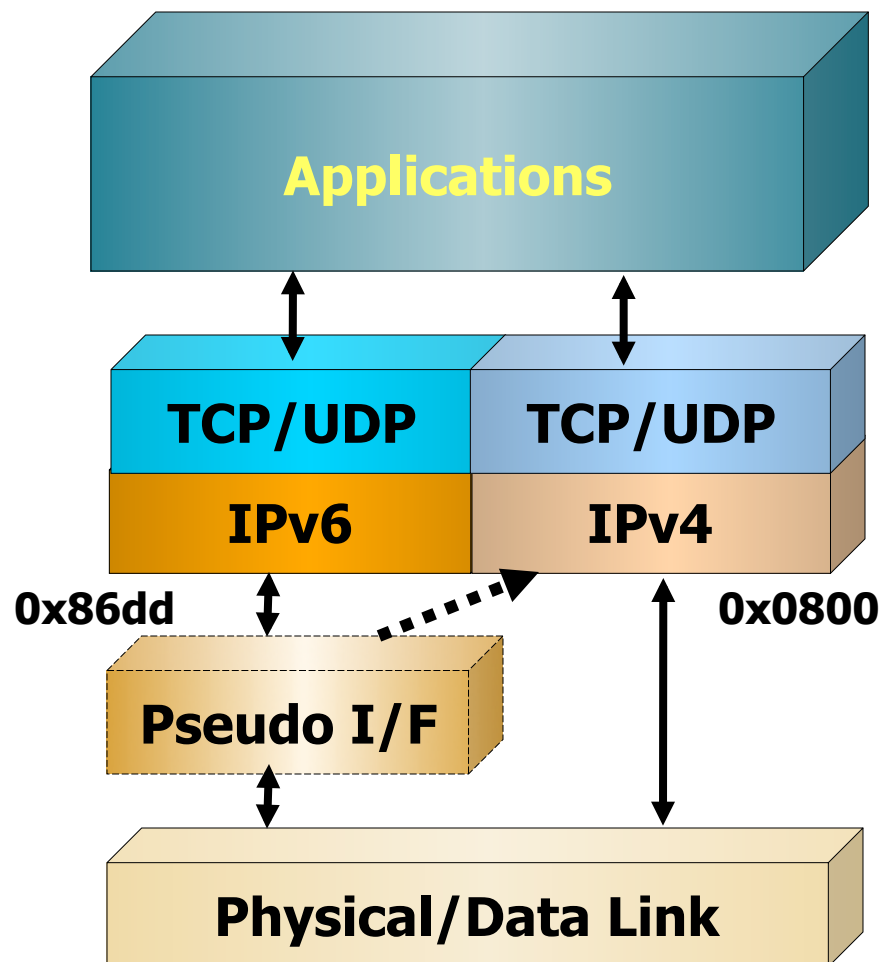


Dual Stack Strategy



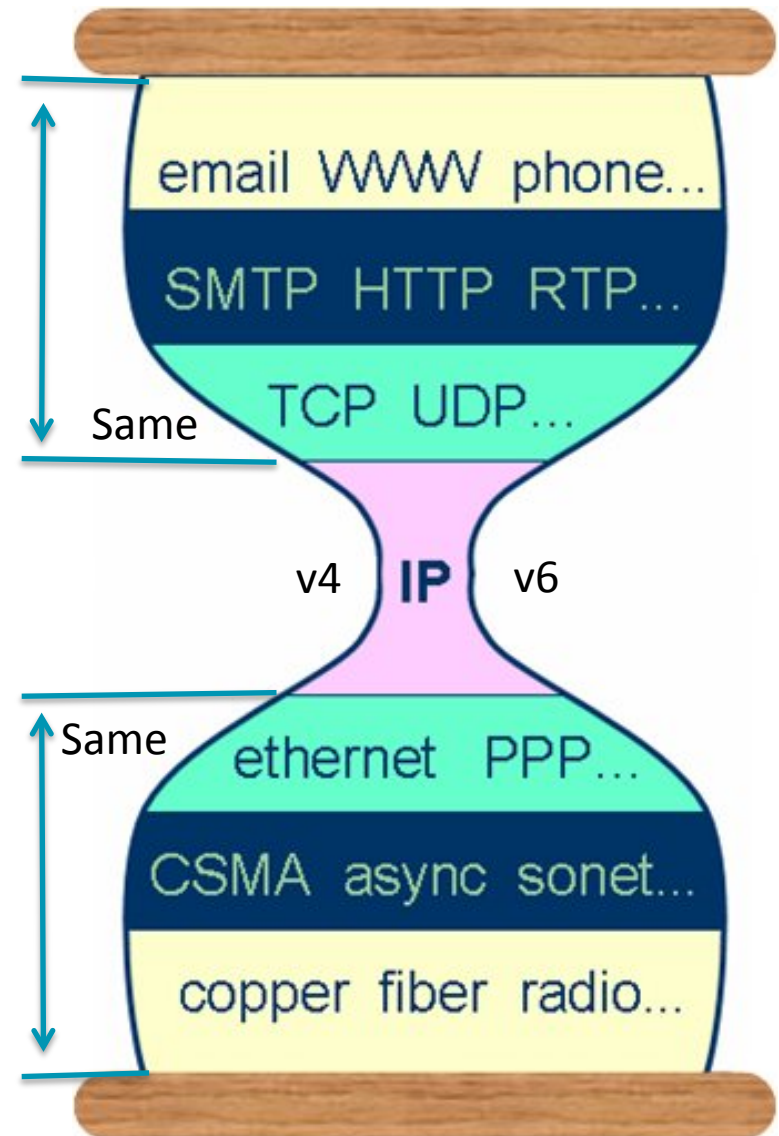
- Deploy 'dual stack' nodes

- **All** currently shipping client operating systems support IPv6 out of the box – and generally available since Windows XP in 2001!
- “Ships in the night”, v4 and v6 protocols operate independently of each other
- End stations speak v6 and v4 if infrastructure supports it (routers can handle v6 in v4 tunneling)
- Many operating systems try IPv6 first, then “downgrade” to IPv4



Dual Stack Risks...

- **TCP** and **UDP**, which runs **on top of IP**, are unaware of the protocol underneath that transports the data – **Security risks same between v4 and v6**
- Applications *generally* are unaware of protocols below, except for logging of remote IP addresses – **Security Risks approximately the same between v4 and v6**
- **IPv6 does not have as much “mileage” as IPv4**
 - Risks of unknown bugs in network equipment
 - Risks of unknown attack tools
 - Risk of inadvertent activation of IPv6 (see next slide...)

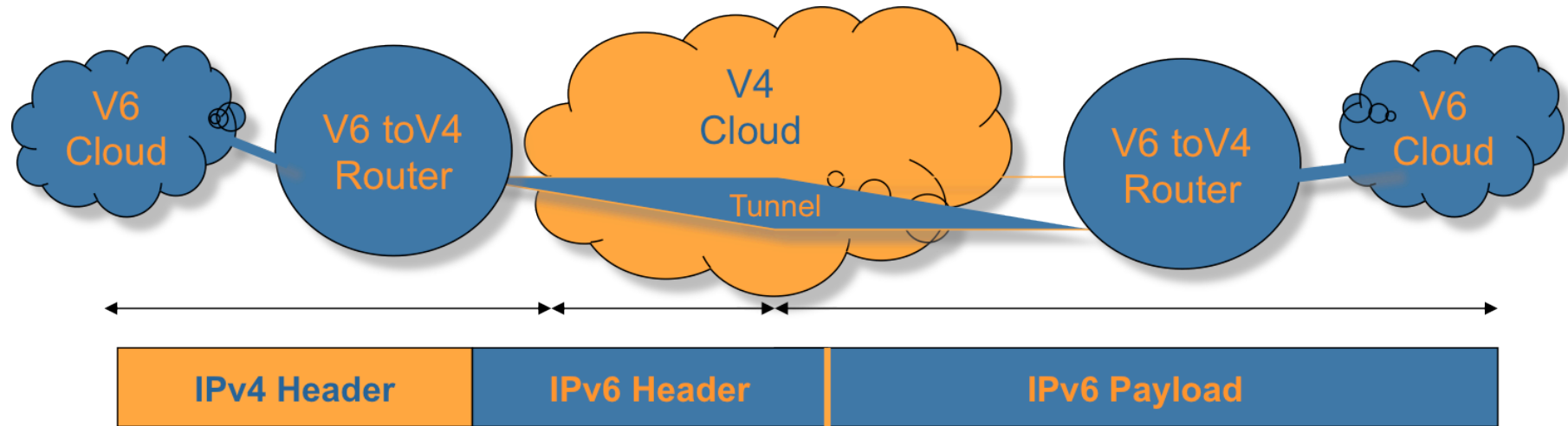


Some Facts to Consider...

- **All** currently shipping client operating systems support IPv6 – so it's there even if you are not ready!
- Many deployed network security tools do not support IPv6
- For devices that support v6, tools are often left in default configuration or misconfigured by inexperienced staff
- Most products supporting IPv6 are still relatively new, with potential vulnerabilities and bugs
- Vendor product support is often weak
- **MITIGATION STRATEGY – GET v6READY**
 - **Immediately – block IPv6 if you are not confident you are ready (firewall/personal firewall)**
 - Procure IPv6 capable security devices over the next upgrade cycle
 - Insist that penetration testing exercises include IPv6 testing

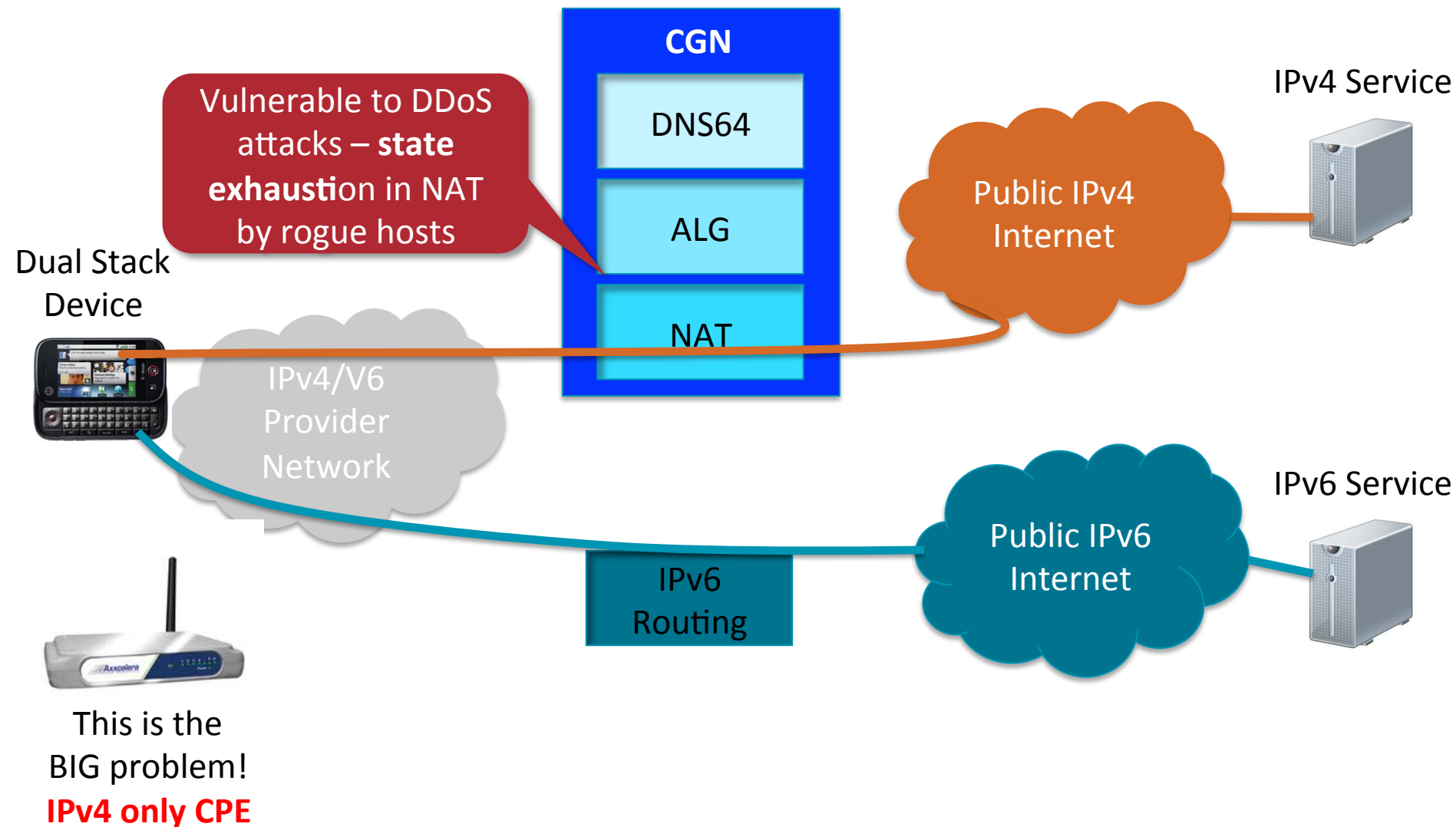


Tunneling Strategy: v6 over v4

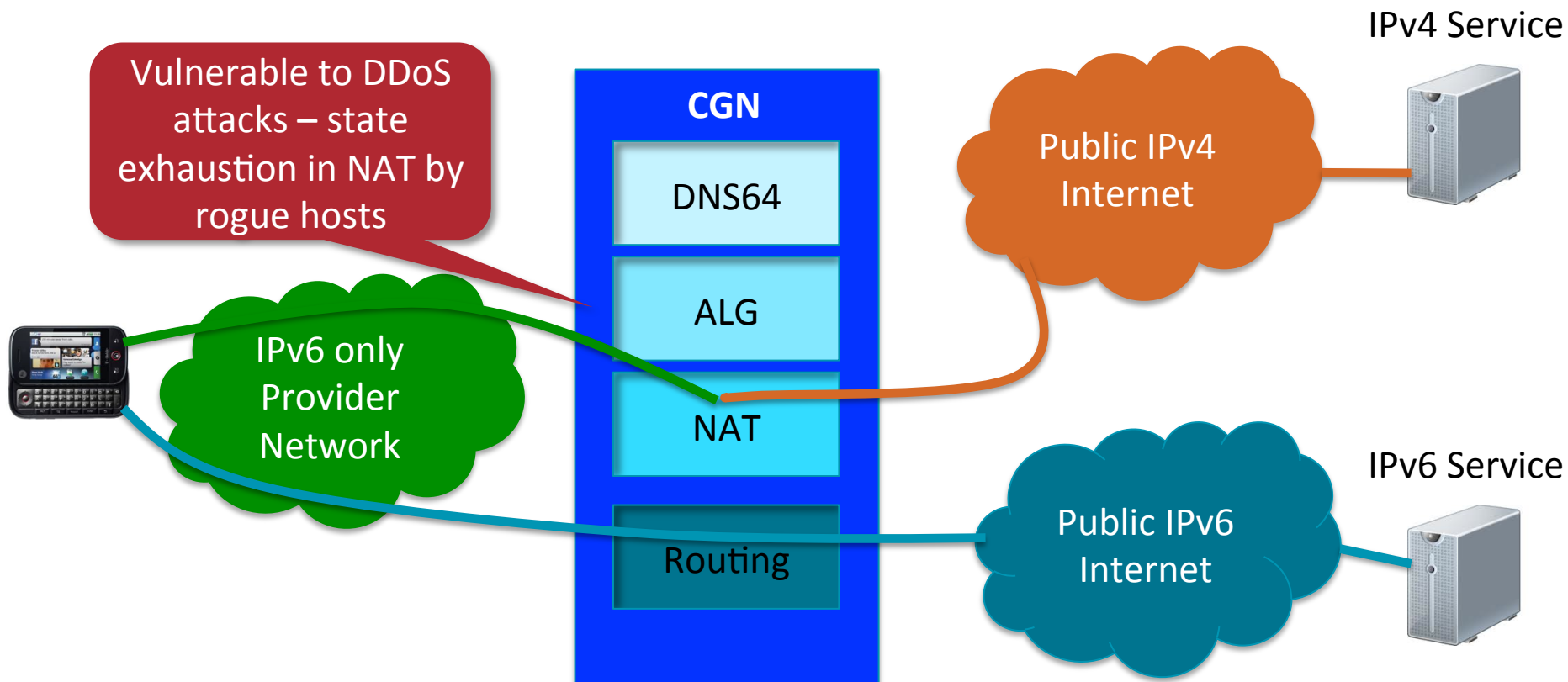


- Used to transmit IPv6 over existing IPv4 clouds (no native connectivity)
 - Site-to-site or remote access to IPv6 clouds
 - 6in4, cannot run through existing IPv4 NAT
 - MPLS
 - Teredo (client instigated, Microsoft, runs through NAT)
- No built-in security of any type
 - Vulnerable to tunnel injection and tunnel sniffing
 - Same vulnerabilities that exist with GRE tunnels in IPv4
- Easy to mitigate
 - Reject packets who's source address does not match any tunnel
 - Block Teredo tunnels from forming (potential backdoor to host)
 - Use IPSec
- Will probably not be used in production anyway – more for experimentation...

Ideal Scenario – ISP supports both

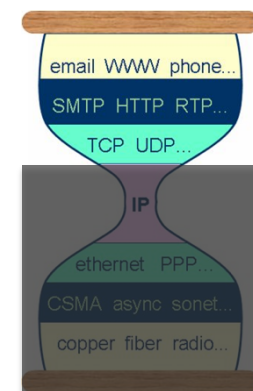


ISP Supports IPv6 Only



Threat Similarities between v4 & v6

- All our old friends are still here!!
 - IP spoofing
 - Buffer Overflows, Cross Site Scripting, SQL Injection
 - Email Vulnerabilities
 - Trojans, Viruses, Worms
 - DDoS Attacks
 - Spyware...
 - Chat, P2P
 - Physical Security
 - Social Engineering
- Why? Because most attacks work at upper layers, not at the protocol layer itself!



Attack
vectors are
here!

Slight Differences between v4 & V6

- LAN based attacks
- Attacks against DHCPv6
- DoS or DDoS attacks against routers
- Fragmentation attacks (in IPv6 done by host instead of routers)
- Multicast “Packet Amplification” attacks

- Reconnaissance & scanning worms
- Attacks against ICMPv6
- Extension Header Attacks
- Auto configuration Attacks (NDP)
- Attacks on Transition Mechanisms (DDoS)
- Attacks against the IPv6 protocol stack itself

IPv6 Attack Tools Scarce but Available

- Even hackers need time to transition!!
 - SCAPY6
 - Hackers Choice IPv6 Toolkit
 - IP Stack Integrity Checker
- Brief and surprisingly effective Demo of Hackers Choice to follow...

```
student@ubuntu: ~  
File Edit View Terminal Help  
student@ubuntu:~$ sudo scapy  
INFO: Can't import python gnuplot wrapper . Won't be able to plot.  
INFO: Can't import PyX. Won't be able to use psdump() or pdfdump().  
Welcome to Scapy (2.0.1)  
>>> i = IP()  
>>> i.display()  
### IP ###  
version= 4  
ttl= none  
tos= 0x0  
len= none  
id= 1  
flags=  
frag= 0  
ttl= 64  
proto= ip  
checksum= 0x0  
src= 127.0.0.1  
dst= 127.0.0.1  
options= '  
>>>
```



The Hacker's Choice

[0x03] The Included Tools

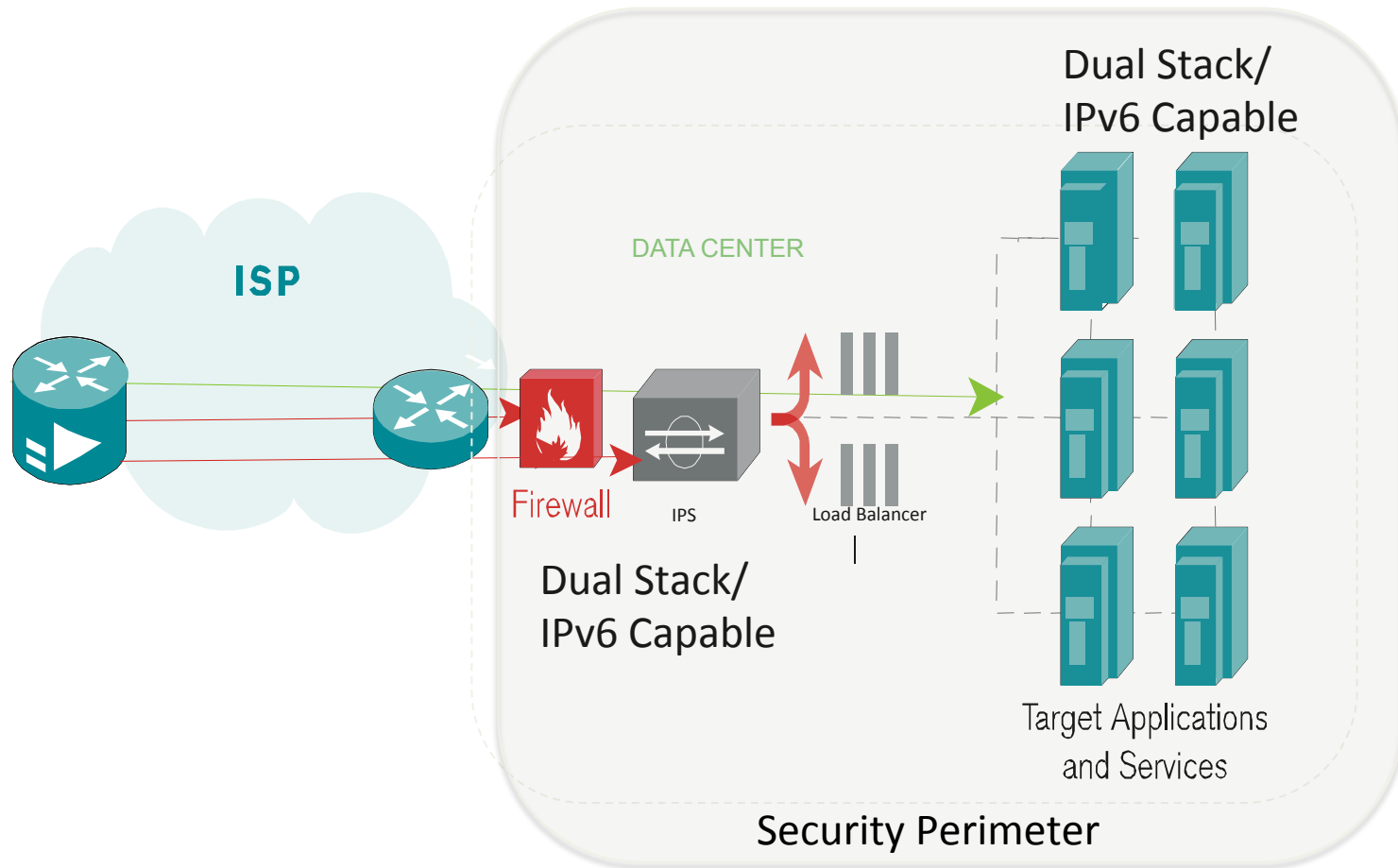
- parasite6: icmp neighbor solitication/advertisement spoofer, puts you as man-in-the-middle, same as ARP mitm (and parasite)
 - alive6: an effective alive scanning, which will detect all systems listening to this address
 - dnsdict6: parallized dns ipv6 dictionary bruteforcer
 - fake_router6: announce yourself as a router on the network, with the highest priority
 - redir6: redirect traffic to you intelligently (man-in-the-middle) with a clever icmp6 redirect spoofer
 - toobig6: mtu decreaser with the same intelligence as redir6
 - detect-new-ip6: detect new ip6 devices which join the network, you can run a script to automatically scan these systems etc.
 - dos-new-ip6: detect new ip6 devices and tell them that their chosen IP collides on the network (DOS).
 - trace6: very fast traceroute6 with supports ICMP6 echo request and TCP-SYN
 - flood_router6: flood a target with random router advertisements
 - flood_advertise6: flood a target with random neighbor advertisements
 - exploit6: known ipv6 vulnerabilities to test against a target
 - denial6: a collection of denial-of-service tests againsts a target
 - fuzz_ip6: fuzzer for ipv6
 - implementation6: performs various implementation checks on ipv6
 - implementation6d: listen daemon for implementation6 to check behind a fw
 - fake_mld6: announce yourself in a multicast group of your choice on the net
 - fake_mld26: same but for MLDv2
 - fake_mldrout6: fake MLD router messages
 - fake_mip6: steal a mobile IP to yours if IPSEC is not needed for authentication
 - fake_advertiser6: announce yourself on the network
 - smurf6: local smurfer
 - rsmurf6: remote smurfer, known to work only against linux at the moment
 - sendpees6: a tool by willdamn(ad)gmail.com, which generates a neighbor solicitation requests with a lot of CGAs (crypto stuff ;-)) to keep the CPU busy. nice.
 - thcping6: sends a hand crafted ping6 packet
- [and about 20 more tools for you to discover]

The Security Perimeter with IPv6

- Initially security perimeter will remain the same – remember protocol hourglass
 - Will remain client-server and existing architectures will remain unchanged
- Perimeter **may** become perforated over time
 - IPv6 encourages peer-to-peer communications rather than client-server
 - IPSec is part of IPv6 rather than a bolt-on so more peer-to-peer secure tunnels will exist
- Extent of “perforation” depends on IPv6 security policy
- Firewalls, IPSs and APSs will remain key components of security with IPv6



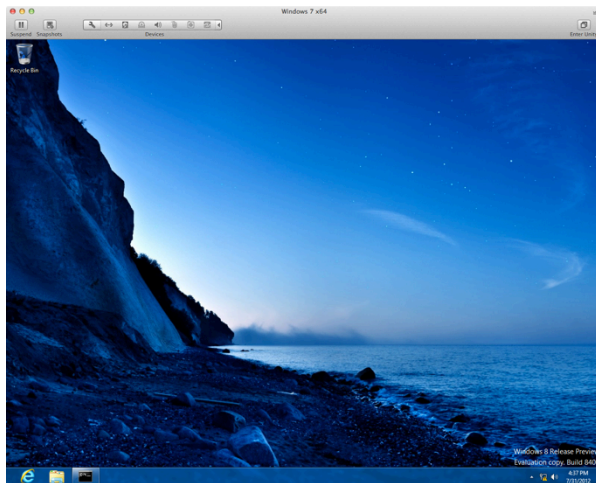
Before and After Security Perimeter



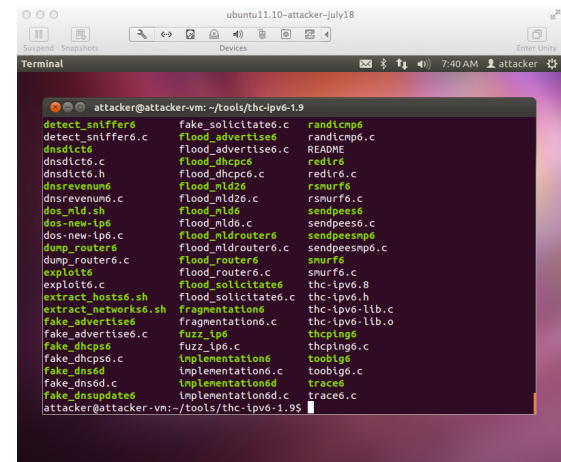
DoS State Attack Demo...

Flood Router Advertisements on LAN segment
 Victim will create new virtual interface for each “new” router
 Victim will die
 All versions of windows since XP are vulnerable to this

Windows 8 Victim



Linux Attacker
 thc-ipv6 attack tool suite



LAN Segment

Router Advertisement Floods

Conclusions

- All that you know is **still** relevant:
 - IPv6 Infrastructures generally have the same topology as IPv4 infrastructures – and same security principles apply
 - Existing network topologies can continue to exist
 - Existing Network Perimeter design can remain the same – may change as peer-to-peer models emerge
- But...
 - Must ensure security equipment and software supports IPv6
 - Must guard against specific v6 vulnerabilities
 - Must be careful against accidental deployments of IPv6 – wait until ready!
- You still have time to plan carefully
 - But the clock is ticking – **IPv6 WILL HAPPEN, and NOTHING CAN STOP IT!**





Thank You