Internet Storm Center

The Security Impact of IPv6

How I Learned to Stop Worrying and Love IPv6

Johannes B. Ullrich, Ph.D.

jullrich@sans.edu

acm Association for Computing Machinery

Advancing Computing as a Science & Profession

“Housekeeping”

- This presentation consists of slides and audio. If you are experiencing any problems/issues, please press the **F5** key on your keyboard if you’re using **Windows**, or **Command + R** if you’re on a **Mac**, to refresh your console, or close and re-launch the presentation. You can also view the Webcast Help Guide, by clicking on the “Help” widget in the bottom dock.

- To control volume, adjust the master volume on your computer.

- At the end of the presentation, you’ll see a **survey URL** on the final slide. Please take a minute to click on the link and fill it out to help us improve your next webinar experience.

- You can download a PDF of these slides by clicking on the **Resources** widget in the bottom dock.

- This presentation is being recorded and will be available for on-demand viewing in the next few days. You will receive an **automatic e-mail notification** when the recording is ready.

- If you think of a question during the presentation, please type it into the **Q&A** box and click on the submit button. You do not need to wait until the end of the presentation to begin submitting questions. You may also use the Q&A box (and the survey at the end) to suggest topics for future webinars of interest to you.

Association for Computing Machinery

Advancing Computing as a Science & Profession

ACM Learning Center

http://learning.acm.org

- 1,350+ trusted technical books and videos by leading publishers including O’Reilly, Morgan Kaufmann, others

- Online courses with assessments and certification-track mentoring, member discounts on tuition at partner institutions

- Learning Webinars on big topics (Cloud/Mobile Development, Cybersecurity, Big Data, Recommender Systems, SaaS, Agile, Natural Language Processing, Parallel Programming)

- ACM Tech Packs on top current computing topics: Annotated Bibliographies compiled by subject experts

- Popular video tutorials/keynotes from ACM Digital Library, A.M. Turing Centenary talks/panels

- Podcasts with industry leaders/award winners

Association for Computing Machinery

Advancing Computing as a Science & Profession

Talk Back

- Use the Facebook widget in the bottom panel to share this presentation with friends and colleagues

- Use Twitter widget to Tweet your favorite quotes from today's presentation with hashtag #ACMWebinarIPv6

- Submit questions and comments via Twitter to @acmeducation – we're reading them!

Why IPv6

Scalability

IPv4 vs. Reality

	IPv4 Design	Today’s Reality
Network Size	Million’s of Hosts	Billion’s
Network Speed	Kbit/MBit	GBit
RAM/System	MBytes	GBytes
Network Use	EDU/GOV	COM
Endpoints	Servers/Workstations	Mobile/Devices

When did we run out of Addresses

- We are out of IPv4 addresses since 1993 (RFC 1517)
- CIDR is a “hack” to extend the life of IPv4 address space
- Even with CIDR, IPv4 address space now exhausted

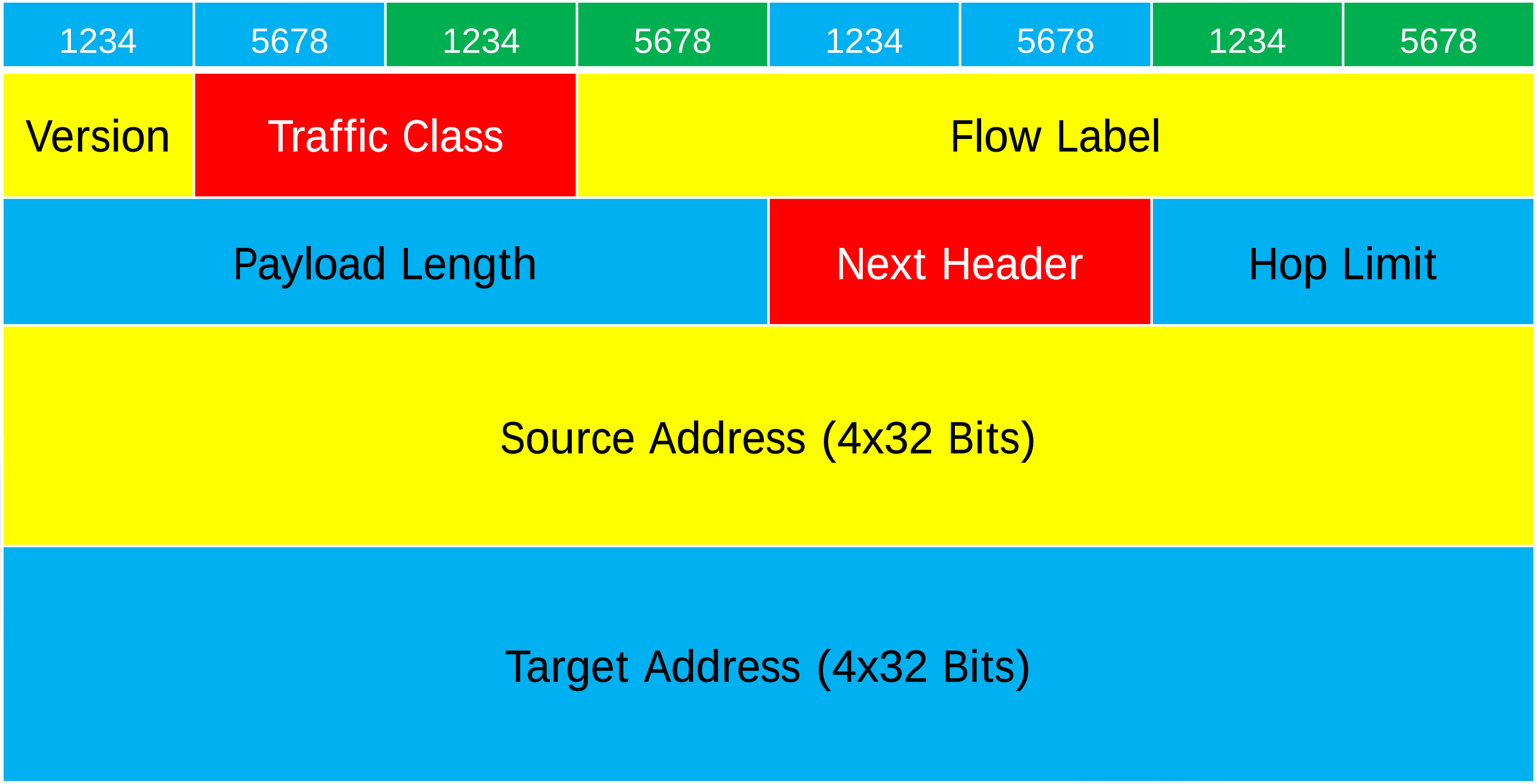
What is today’s Internet

- Internet of devices: Most IP endpoints are devices without a “user”
- Mobile Internet: Biggest (only?) growth area right now is mobile devices
- Security: Business transactions require more security

IPv6 Design Goals

- Scaling the Internet
  - More addresses
  - Simpler routing
- Adjusting to Modern Hardware
  - More memory
  - Larger address buses in CPUs
  - Mobility

IPv6 Header



<table>
<tr><td>1234</td><td>5678</td><td>1234</td><td>5678</td><td>1234</td><td>5678</td><td>1234</td><td>5678</td></tr>
<tr><td>Version</td><td colspan="2">Traffic Class</td><td colspan="5">Flow Label</td></tr>
<tr><td colspan="4">Payload Length</td><td colspan="2">Next Header</td><td colspan="2">Hop Limit</td></tr>
<tr><td colspan="8">Source Address (4x32 Bits)</td></tr>
<tr><td colspan="8">Target Address (4x32 Bits)</td></tr>
</table>

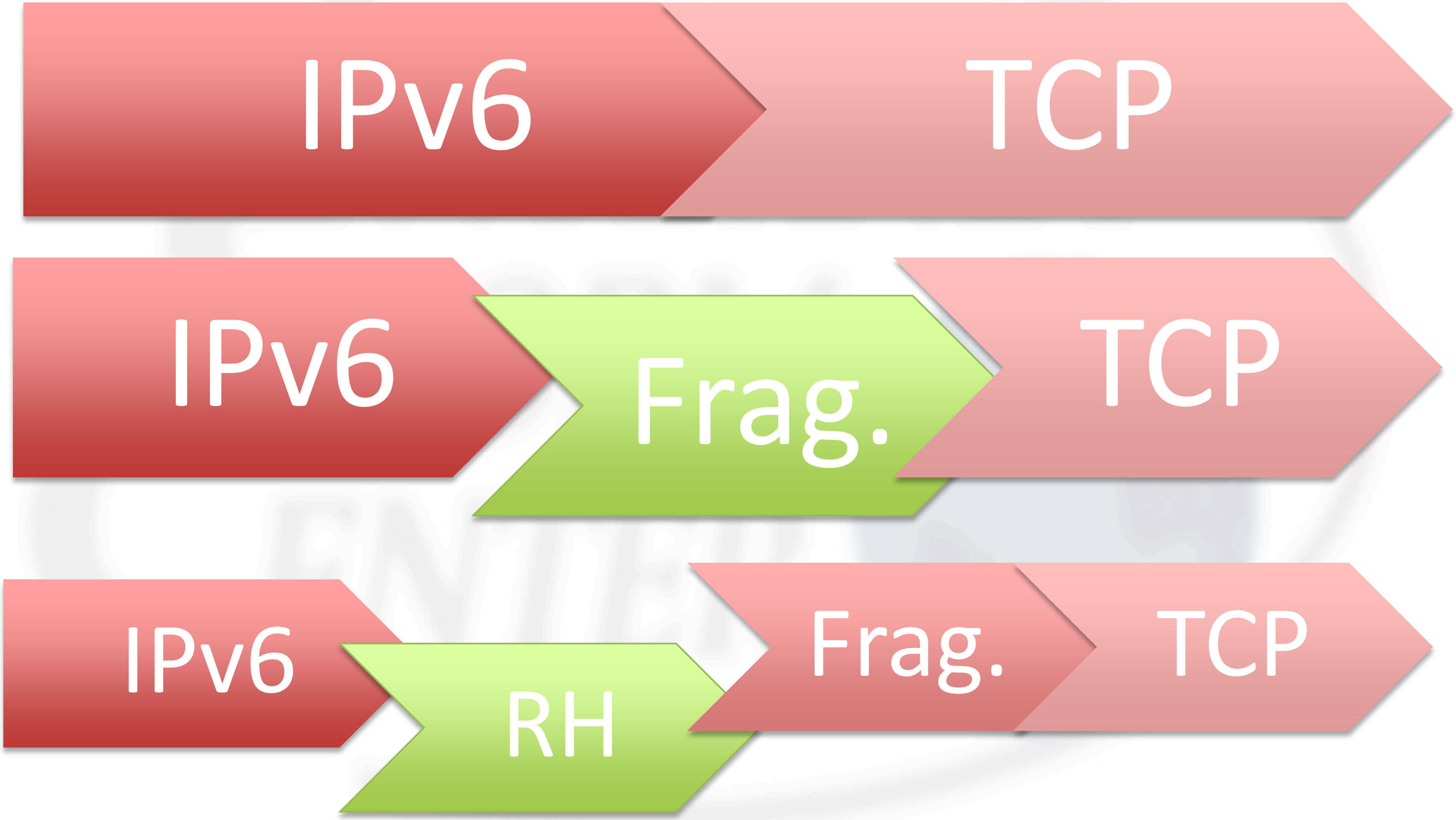
Compare to IPv4

1234	5678	1234	5678	1234	5678	1234	5678
Version	HL	TOS		Total Length			
IP ID				Fragmentation			
TTL		Protocol		Header Checksum			
Source Address							
Target Address							

Extension Headers

- Many of the complexities are moved to extension headers
- Extension headers are optional
- Order is recommended but not enforced
- Can make IPv6 much more complex than IPv4

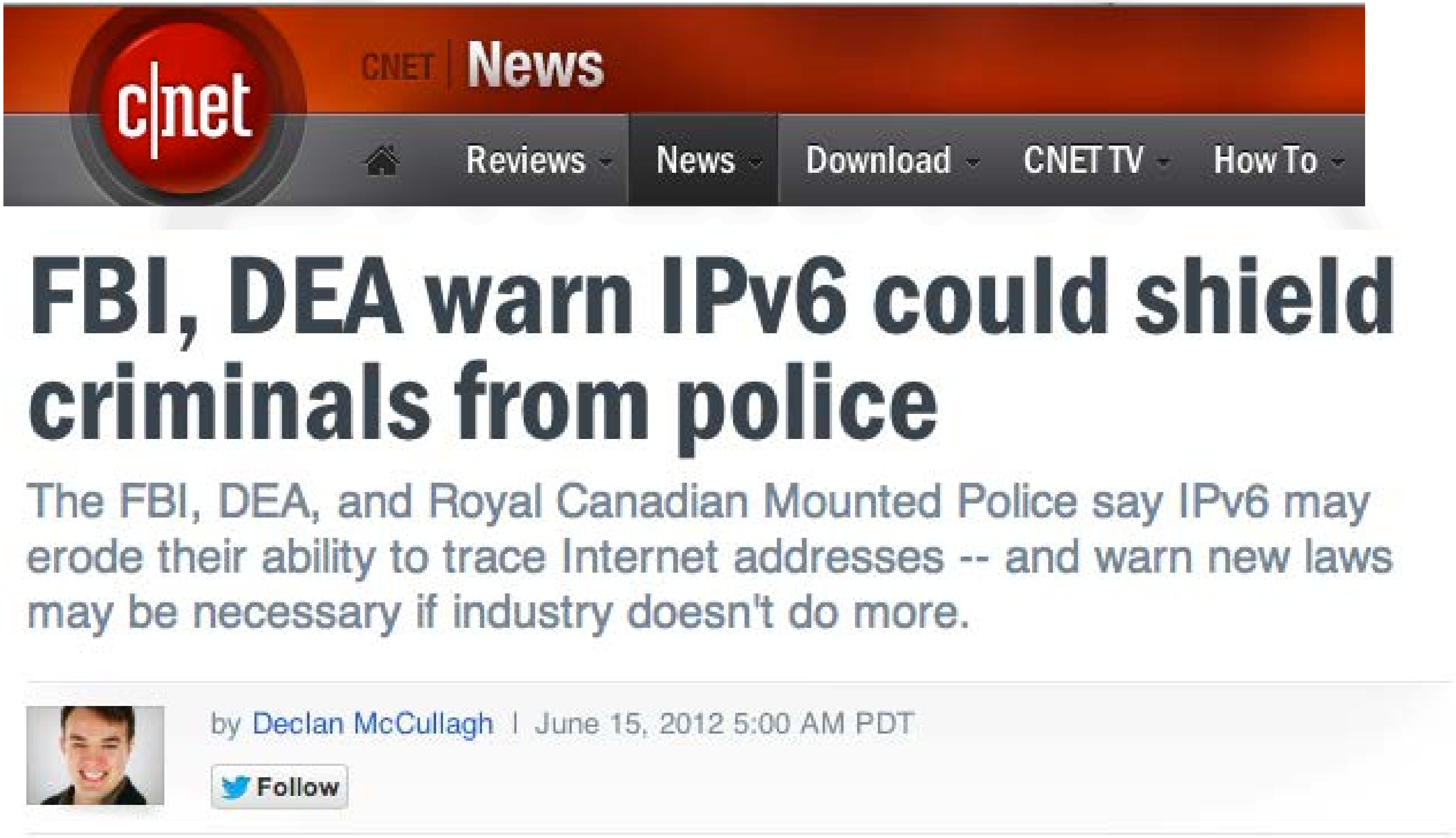
Extension Headers



Outline

- Privacy
- What happened to NAT?
- Fake Routers
- But I am not running IPv6! Why should I care?

IPv6 Privacy

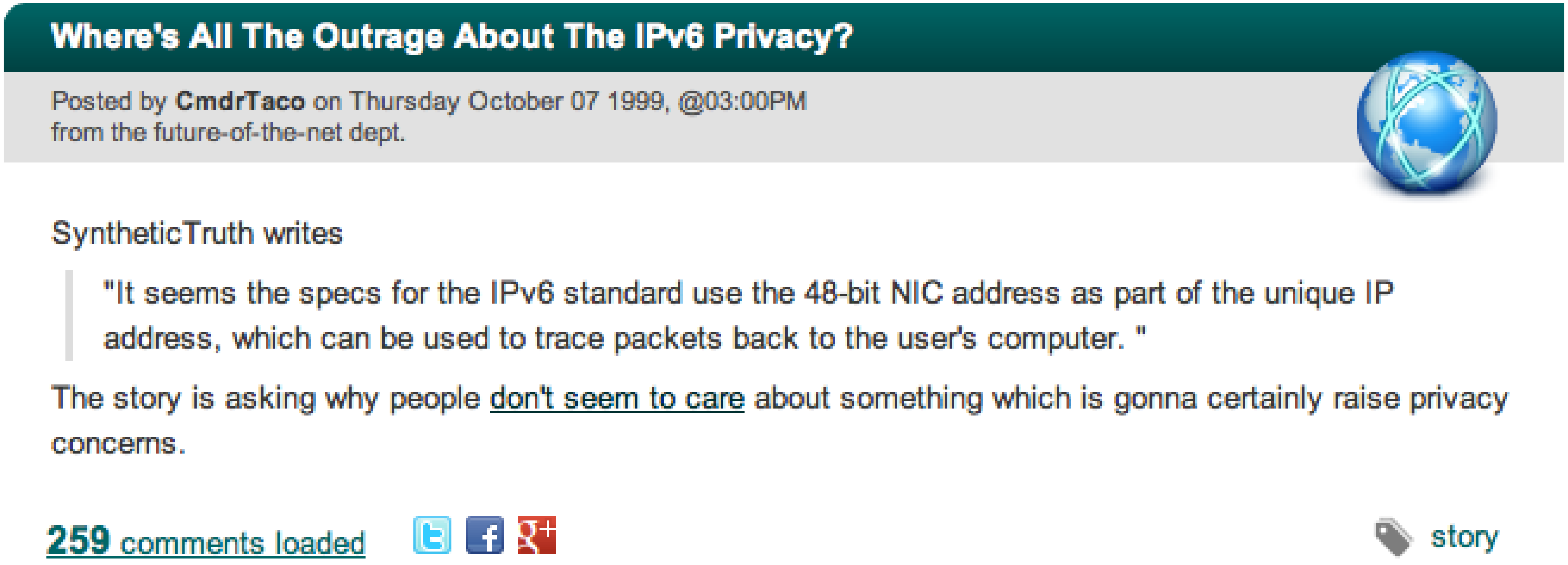


FBI, DEA warn IPv6 could shield criminals from police

The FBI, DEA, and Royal Canadian Mounted Police say IPv6 may erode their ability to trace Internet addresses -- and warn new laws may be necessary if industry doesn't do more.

by Declan McCullagh | June 15, 2012 5:00 AM PDT

IPv6 Privacy



Where's All The Outrage About The IPv6 Privacy?

Posted by **CmdrTaco** on Thursday October 07 1999, @03:00PM
from the future-of-the-net dept.

SyntheticTruth writes

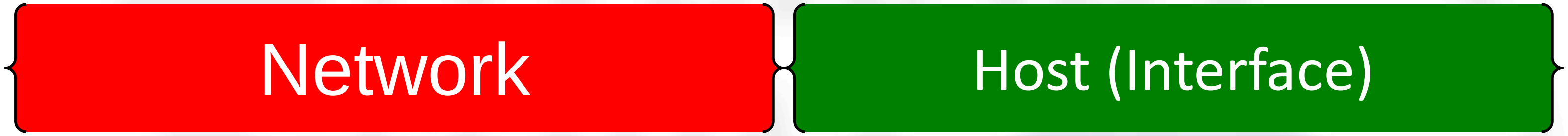
> "It seems the specs for the IPv6 standard use the 48-bit NIC address as part of the unique IP address, which can be used to trace packets back to the user's computer. "

The story is asking why people don't seem to care about something which is gonna certainly raise privacy concerns.

259 comments loaded

IPv6 Addresses

2001:DB8:ABCD:1234:abcd:efab:cdef:abcd



Network

Host (Interface)

- 64 Bit to identify network
  - ISP may assign you /48, /56 or /64
- 64 Bit to identify interface

Interface ID

- MAC Derived

  Privacy issues!

- Privacy Enhanced / Temporary

  Hard to manage

- DHCP

  Probably best “enterprise” solution.

- Static

Interface ID Recommendation

- Home users / small business: Privacy enhanced addresses
- Managed Networks: DHCP
- Servers: DHCP / Static

But What about NAT?

Who told you NAT is a security feature in the first place?

ULA Addresses

- fc00::/7 reserved address space
- Pick a random subnet

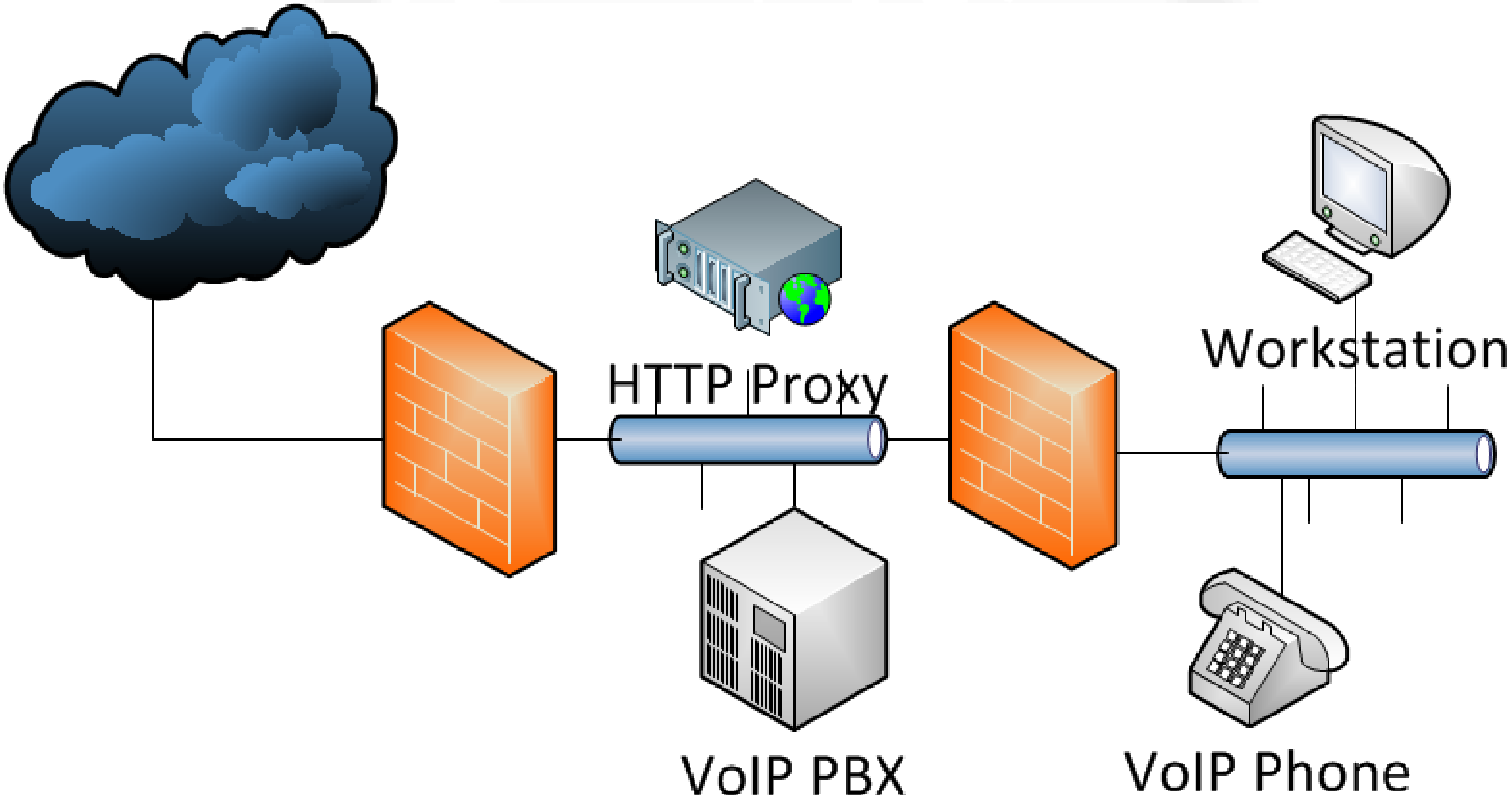
fdaa:bbcc:ddee::/48

If you really like NAT, you can still do it! (ask your Vendor)

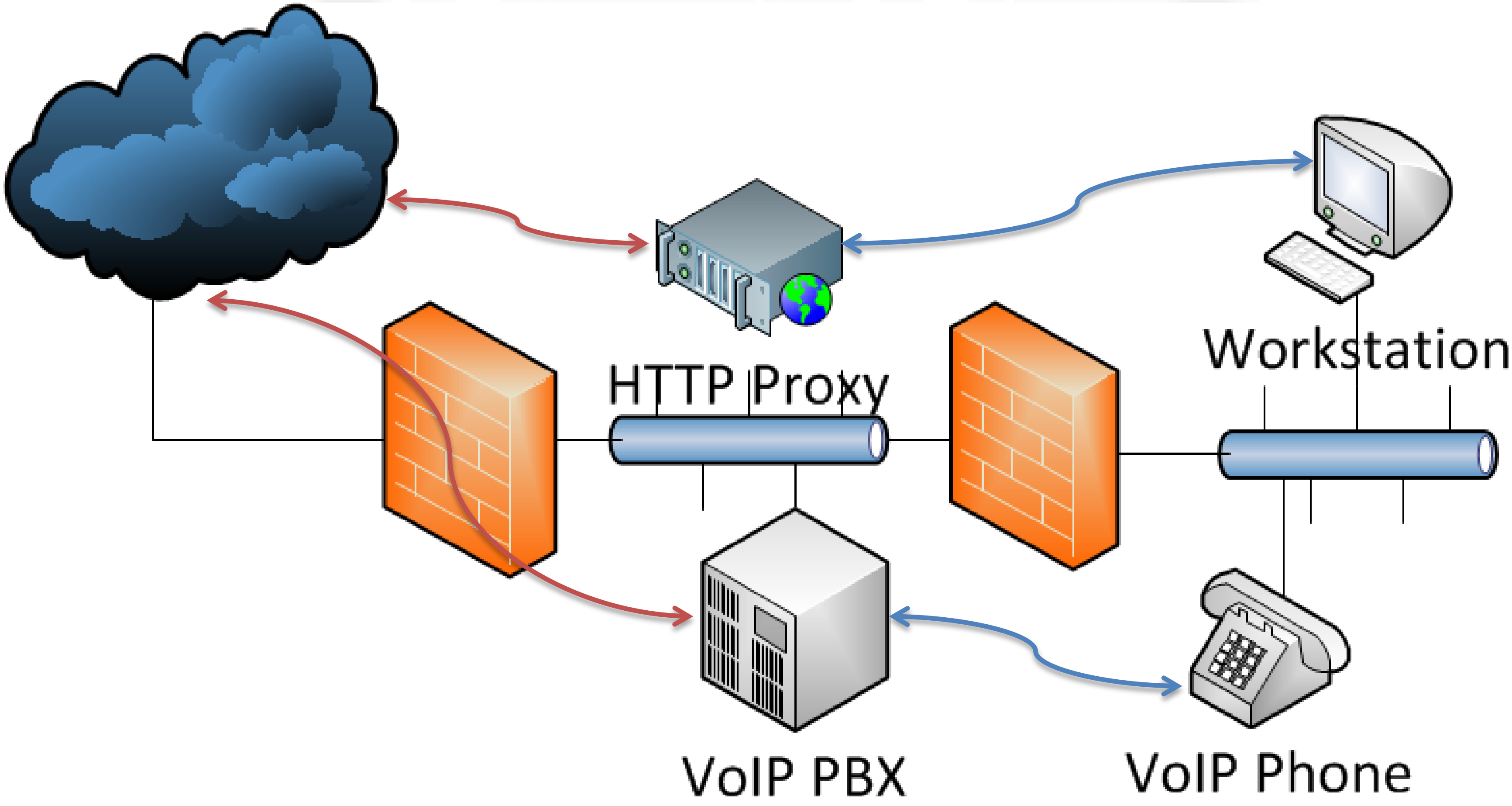
NAT and IPv6 (don’t tell your kids!)

- RFC 6296: IPv6-to-IPv6 Network Prefix Translation
- Cisco: NPTv6 (Network Prefix Translation)
- Juniper: basic-nat66
- ip6tables: -t nat66

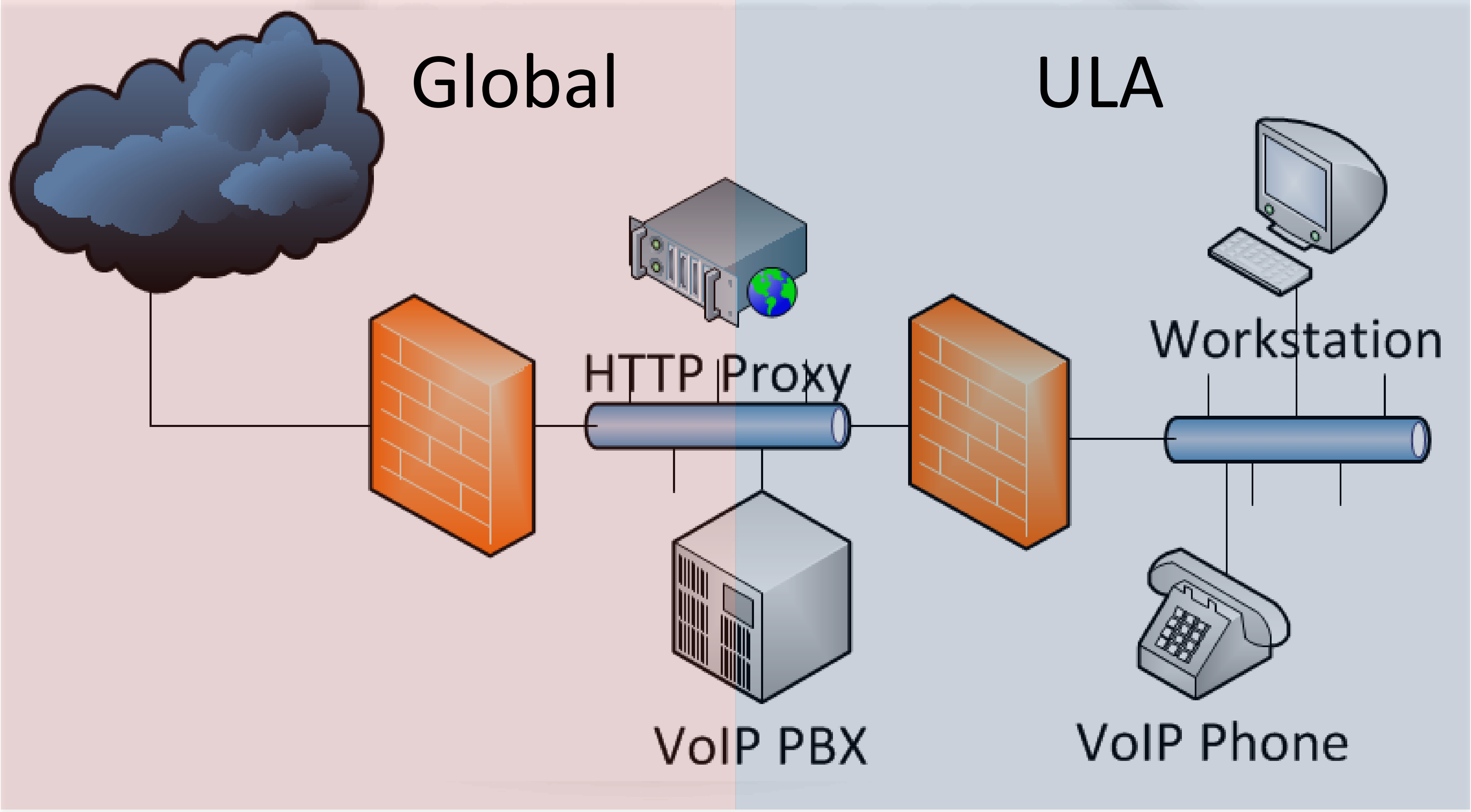
Sample Network



Sample Network



Sample Network



How is this different than IPv4?

- Sure you can do the same in IPv4
- But in IPv6, no NAT should be the standard
- Better vendor support?
- Easier Management?
- Maybe we should try to improve our networks?

Vendor Support

- IPv6 Firewalls have come a long way
- Not all Firewalls support IPv6 (so what?)
- Advanced features may be missing
  - – Deep packet inspection?
  - – Performance?

Router Advertisements

- “DHCP Lite”
- Used to configure IP address
- Router advertises first 64 bits, host picks the next 64 bits
- In some cases, a DNS server and other settings may be configured

Fake routers

- Just like a rogue DHCP server
- For DHCP we got DHCP Snooping in switches
- For Router Advertisements, we got “RAGuard” in a few switches

Router Advertisements

- Switch needs to detect router advertisements
- Sounds easy: “Next Header” is ICMPv6 and ICMPv6 Type is “Router Advertisement”

RAGuard

- Feature is some modern switches (few) to detect Router Advertisements and limit them to authorized ports.
- Not widely implemented (unlike DHCP Snooping)

RAGuard Bypass

- ICMPv6 packets may include extension headers
- “Next Header” field in IPv6 header may not indicate ICMPv6
- Switch has to look for last header

RAGuard Bypass

- ICMPv6 may be fragmented
- Switch has to reassemble fragments to figure out if packet is a RA
- Has to do it for all fragments where the NH is not a transport header

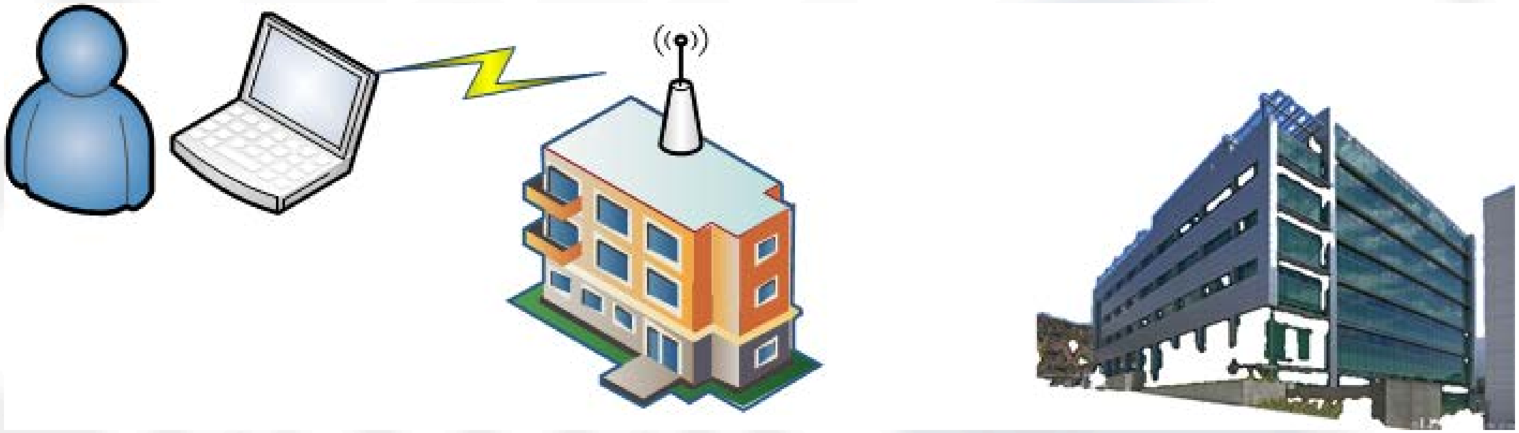
But what happens if...

- “I am not running IPv6”

(one of the top 10 networking lies like: “All my critical devices are air gapped”)

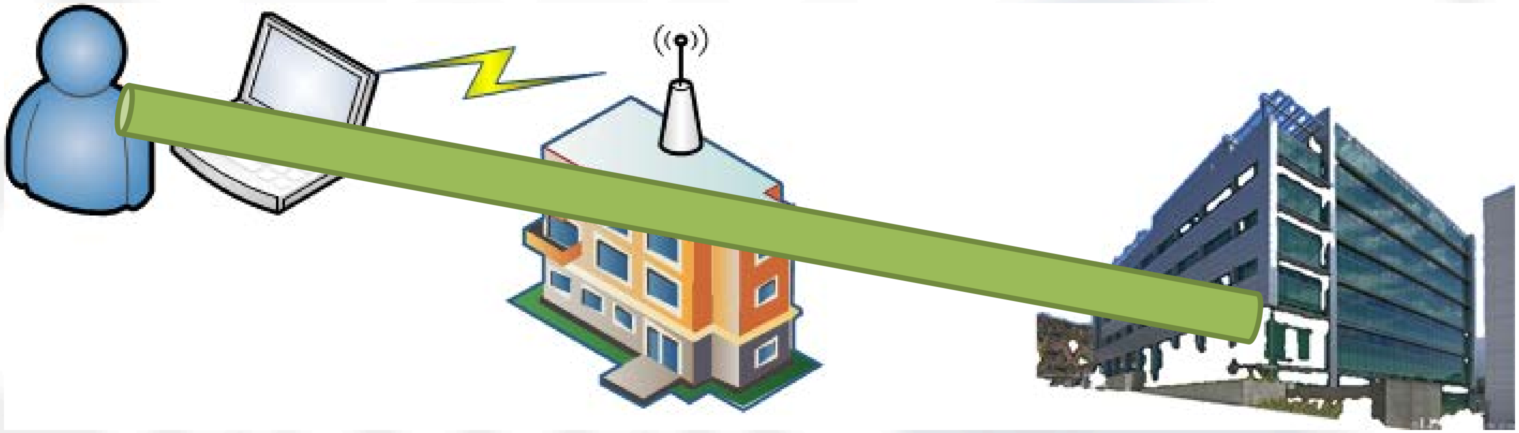
IPv6 VPN Exfiltration

User connecting from remote location back to an internal network



IPv6 VPN Exfiltration

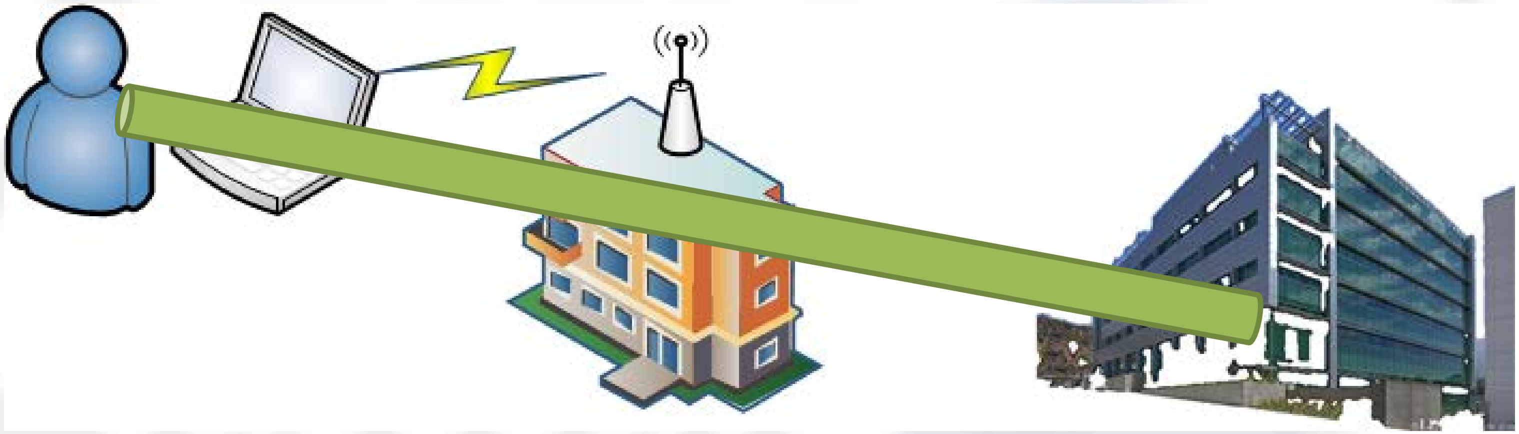
Standard Solution: IPSEC (or other) VPN:
All Traffic routed via VPN!



IPv6 VPN Exfiltration

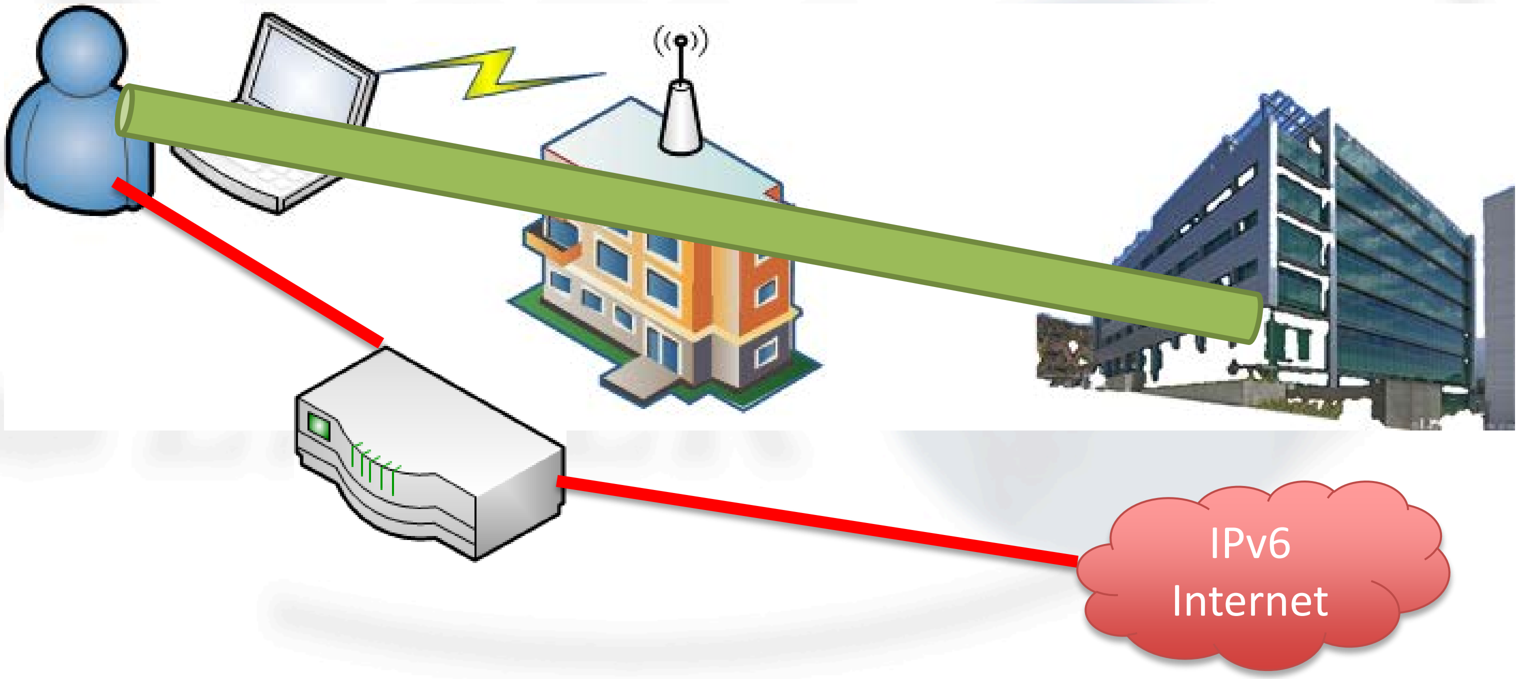
Standard Solution: IPSEC (or other) VPN:

All **IPv4** Traffic routed via VPN!



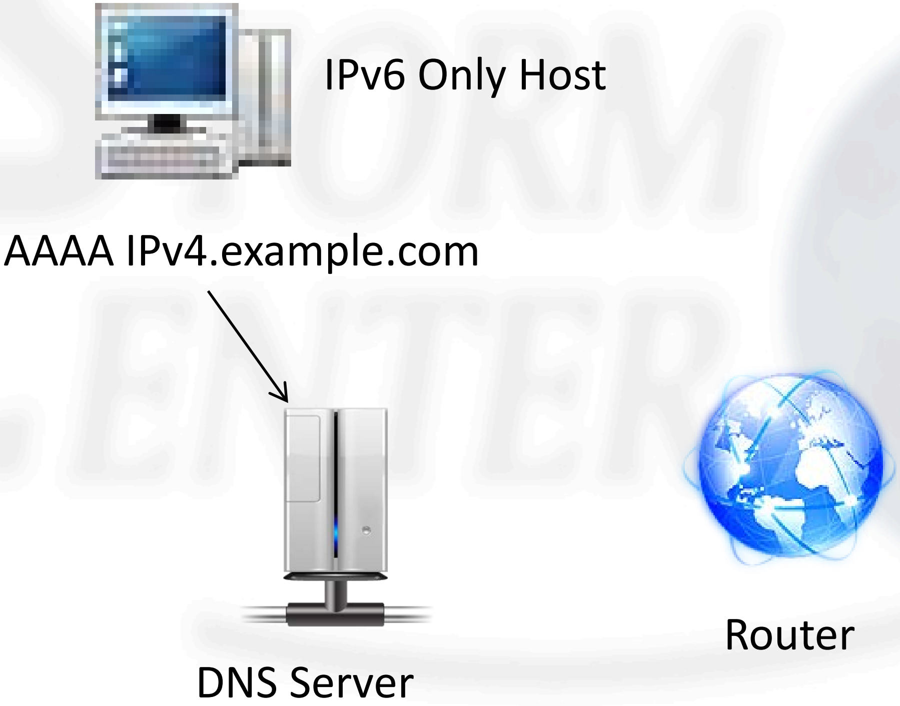
IPv6 VPN Exfiltration

Attacker inserts IPv6 router



Interlude: DNS64

Host attempts to connect to an IPv4 Server



IPv6 Only Host

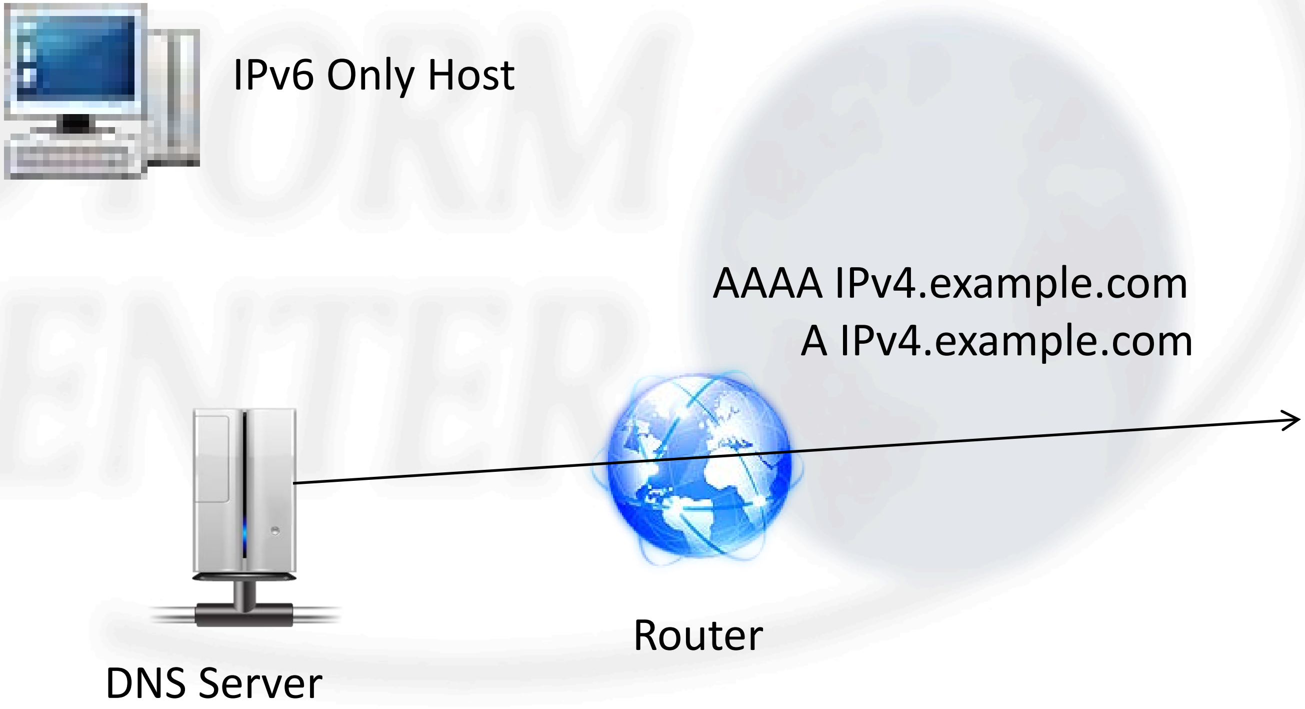
AAAA IPv4.example.com

DNS Server

Router

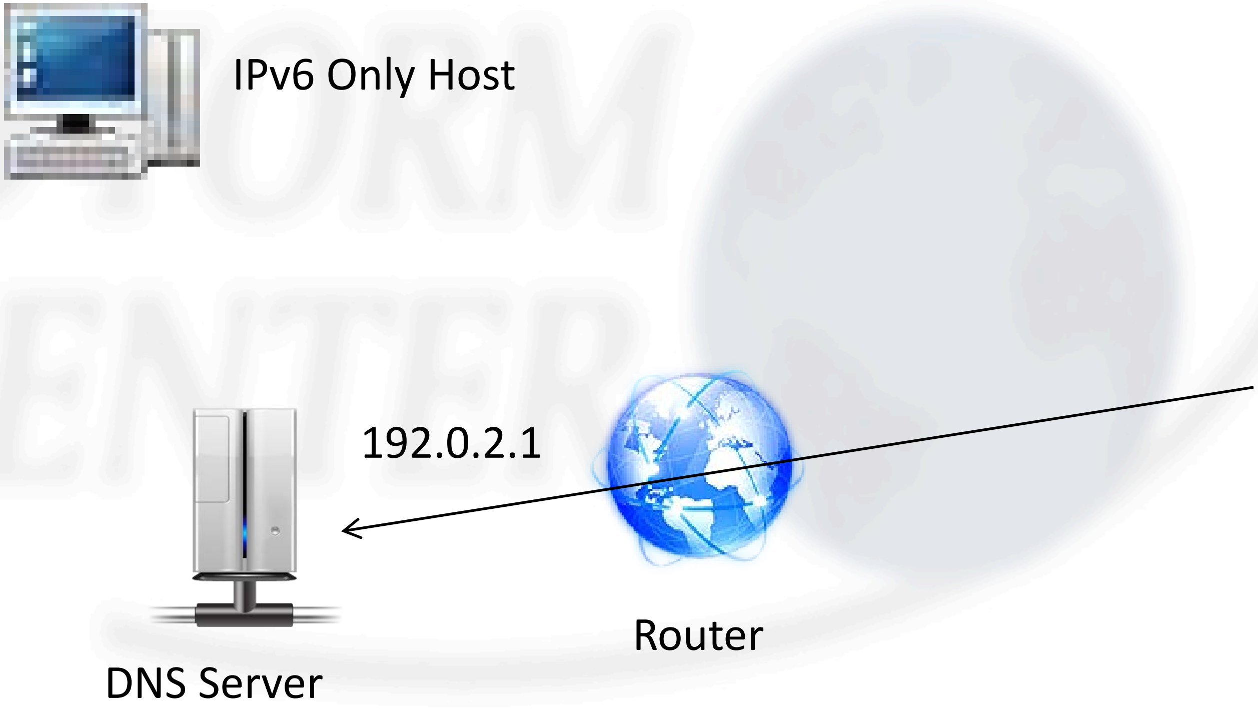
Interlude: DNS64

Host attempts to connect to an IPv4 Server



Interlude: DNS64

Host attempts to connect to an IPv4 Server



IPv6 Only Host

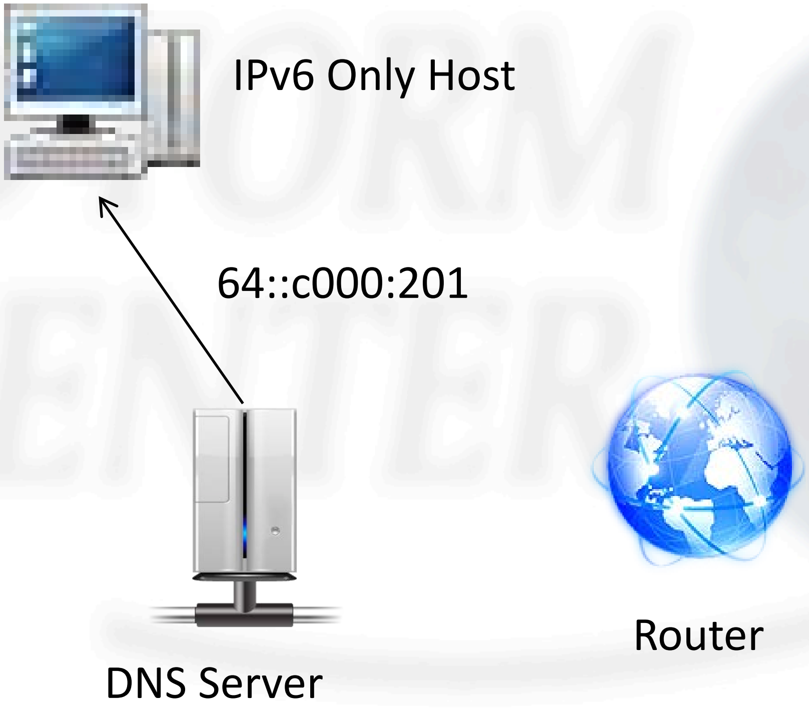
192.0.2.1

Router

DNS Server

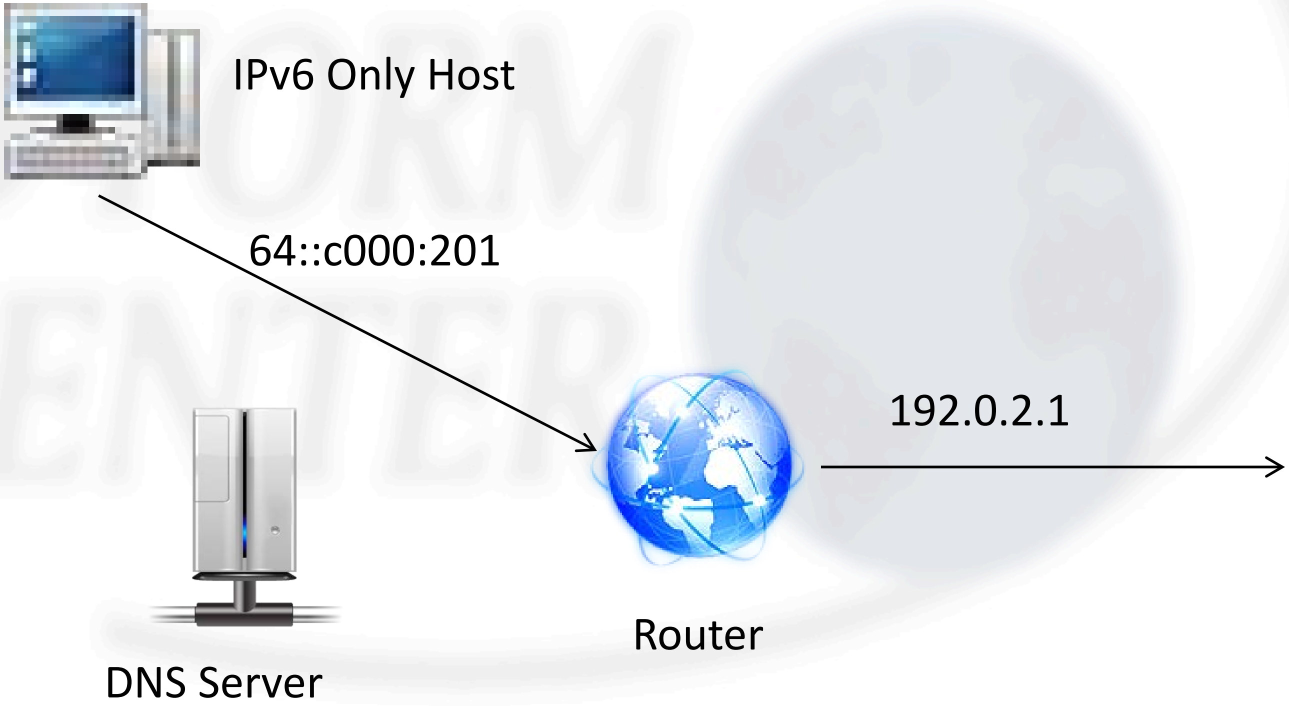
Interlude: DNS64

Host attempts to connect to an IPv4 Server



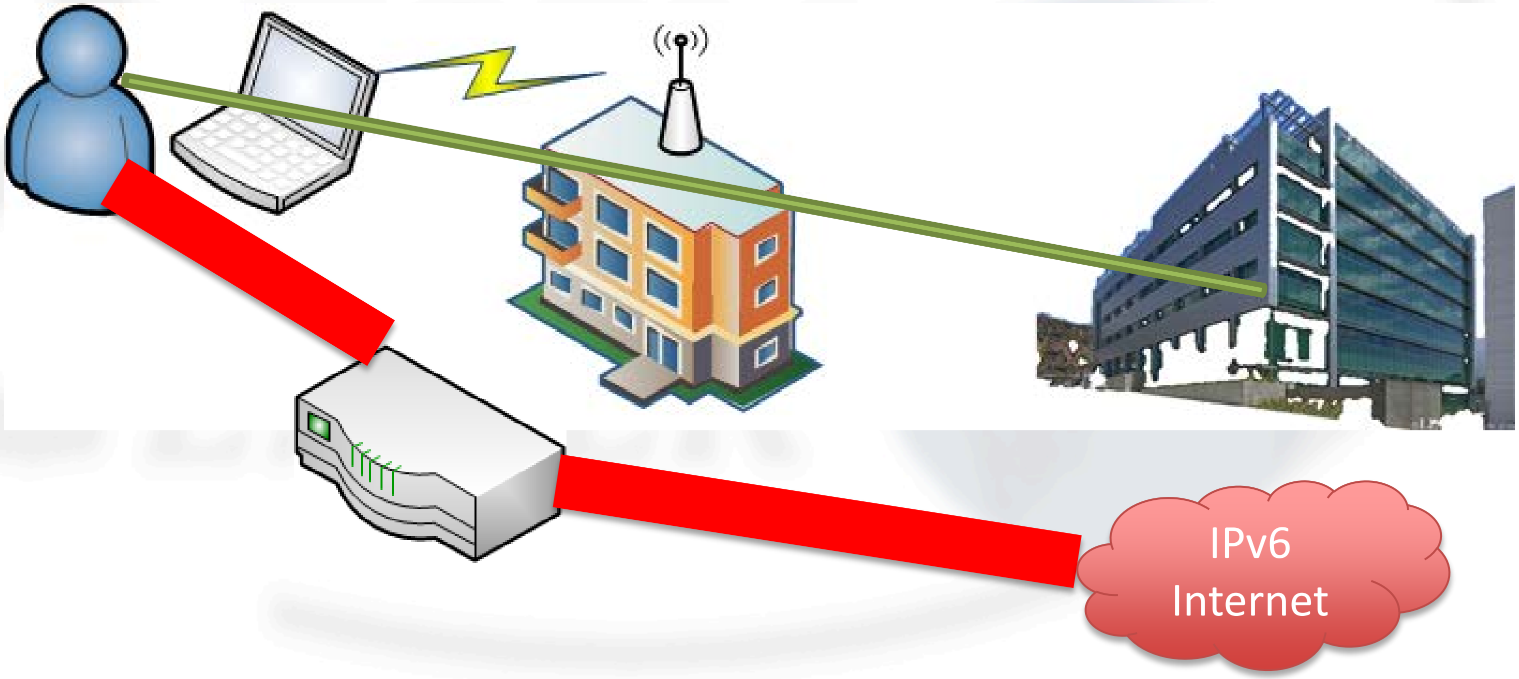
Interlude: DNS64

Host attempts to connect to an IPv4 Server



IPv6 VPN Exfiltration

Attacker inserts IPv6 router + DNS64!



Testing Results

- Still ongoing. Need to test various VPN/OS combinations
- Windows + IPSEC seems to be ok (uses VPN advertised DNS server only, does not request AAAA records if VPN is IPv4 only)

TCP Session Reassembly

- TCP uses “Sessions”: Establishes sequence of packets and allows receiver to detect missing packets
- TCP stream starts with random initial sequence number (SEQ1)
- Sequence number increments with number of bytes sent

Packet 1	Packet 2	Packet 3	Packet 4
⇧SEQ1	⇧SEQ1+len(Packet 1)		

TCP Session Reassembly Problems

- Designed to allow for error recovery
- If an error is detected, affected data is resent
- Intrusion Detection System (IDS) has to figure out which data is accepted and not accepted
- Not an easy problem even in IPv4

TCP Complications in IPv6

- Extension header may cause packet to be dropped by destination (or not)
- For example:
  - Unknown destination options
  - Routing headers
  - Unknown routing options

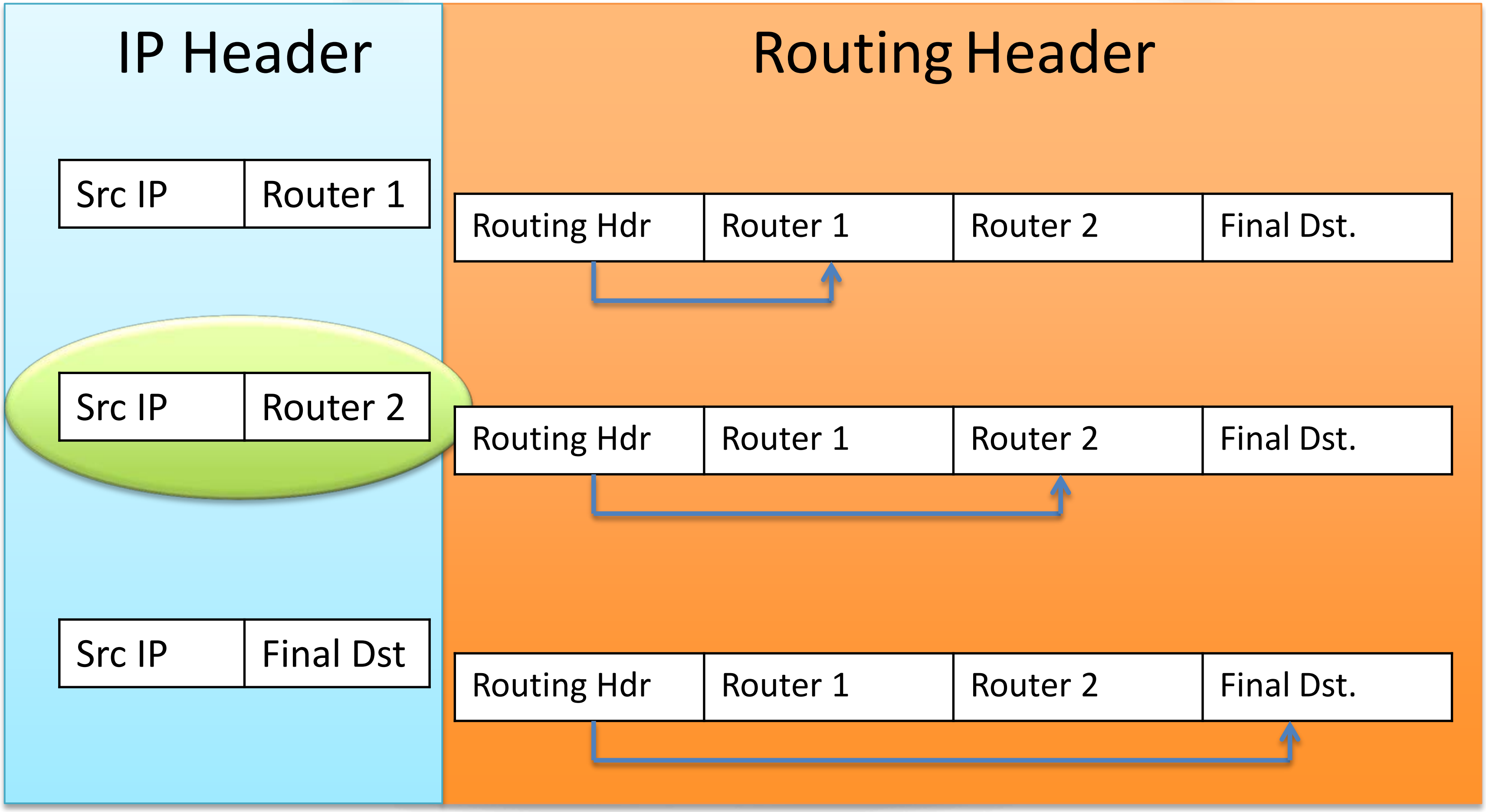
Common Issues

- Some operating systems prefer first copy of a sequence number, some prefer second copy
- timestamp (TCP Option) may matter
- Large packets may be dropped
- Packets with small TTL may be dropped after passing IDS

Example: Routing Header

- Routing header may be used to request specific routers to be used
- Result: IP header changes after each specified router is reached
- IDS may not recognize routing header
- Uses IP header destination as “final”

Example



IP Header

Routing Header

Src IP | Router 1

Routing Hdr | Router 1 | Router 2 | Final Dst.

Src IP | Router 2

Routing Hdr | Router 1 | Router 2 | Final Dst.

Src IP | Final Dst

Routing Hdr | Router 1 | Router 2 | Final Dst.

Summary

- Should I implement IPv6?
  - It is not just a security question, it’s a business question: Do you need it?
  - It is not really that different than IPv4
  - IPv6 offers new security options
  - We (YOU!) need operational experience
  - Learn and experiment NOW before it becomes an emergency

Help Us Help You

- If you see any odd IPv6 activity let us know:

https://isc.sans.edu/contact.html

We will try to keep an eye on IPv6 activity

Thank you!

jullrich@sans.edu

Twitter: johullrich

http://isc.sans.edu

Please Contribute

Daily Updates * Daily Podcast * Live Data Feeds

Resources

- RIPE IPv6 Page ipv6actnow.org
- IPv6 Test Site: test-ipv6.com
- Microsoft: http://technet.microsoft.com/en-us/network/bb530961.aspx
- Free IPv6 Tunnel: tunnelbroker.net
- Internet Society IPv6 page: http://www.internetsociety.org/deploy360/ipv6
- IPv6 Ready: ipv6ready.org

ACM: The Learning Continues…

- Questions about this webcast? learning@acm.org
- ACM Learning Webinars (including archives): http://learning.acm.org/webinar
- ACM Learning Center: http://learning.acm.org
- ACM Queue: http://queue.acm.org
- Tom Limoncelli's blog: http://EverythingSysadmin.com

Association for
Computing Machinery

Advancing Computing as a Science & Profession