Introduction to IPv6 and its Security

Agenda

- What is IPv6?
- Shared Issues by IPv4 and IPv6
- Specific Issues for IPv6
  - IPsec everywhere, dual-stack, tunnels
- Enforcing a Security Policy in IPv6
  - ACL, Firewalls and Host IPS
- Wrap-up

What is IPv6

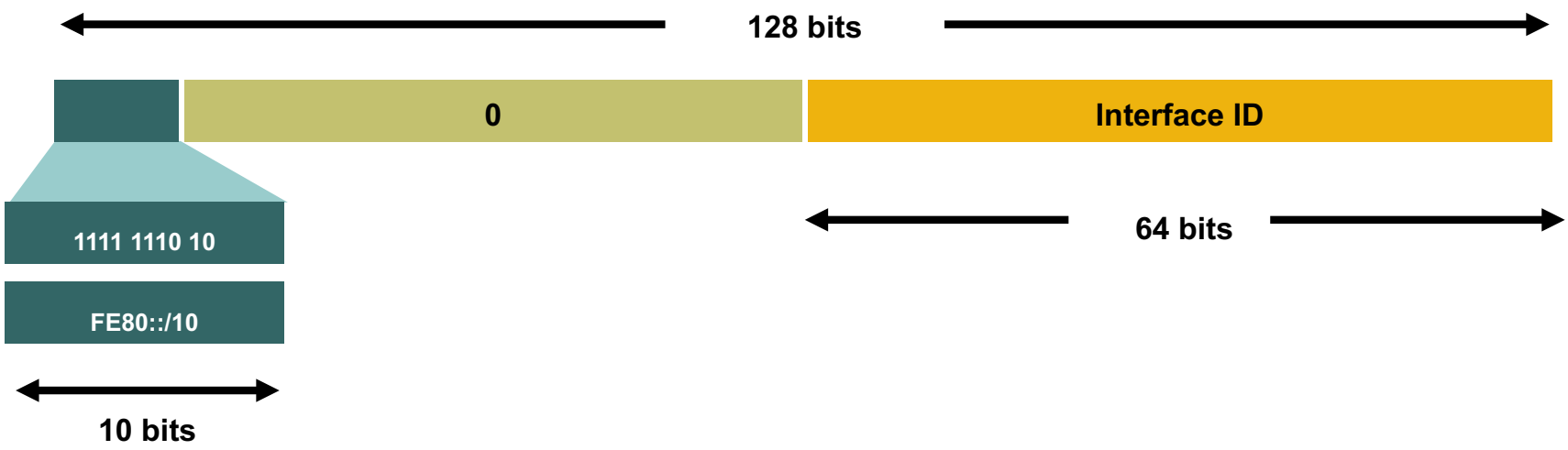
What is actually IPv6?

How can we deploy IPv6?

IPv6 in One Slide

- IPv6 is IPv4 with larger addresses
  - 128 bits vs. 32 bits
- Data-link layer unchanged: Ethernet, xDSL, …
- Transport layer unchanged: UDP, TCP, …

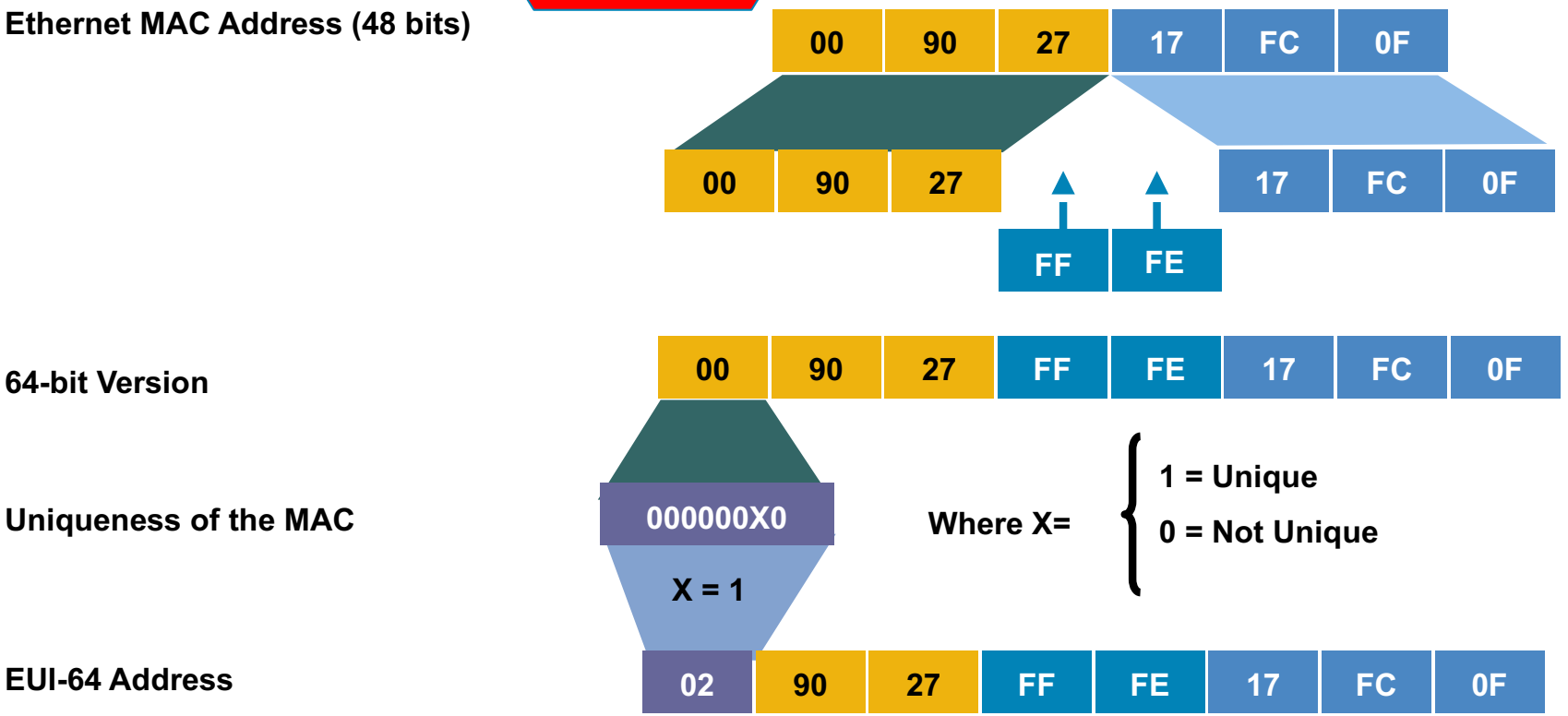
Link-Local



- Link-local addresses:
  - Have a limited scope of the link
  - Are automatically configured with the interface ID

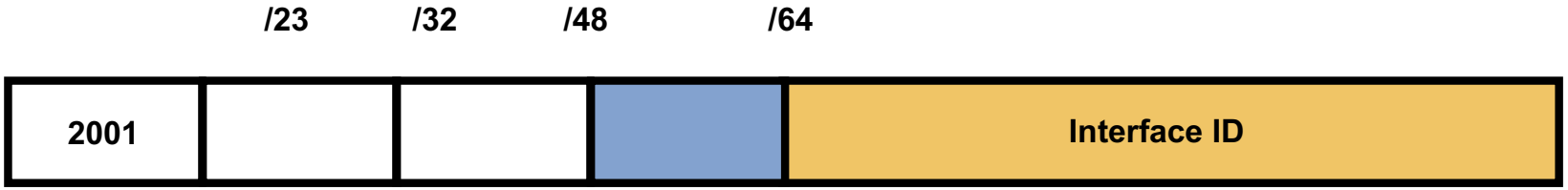
EUI-64

No more used Except for IoT



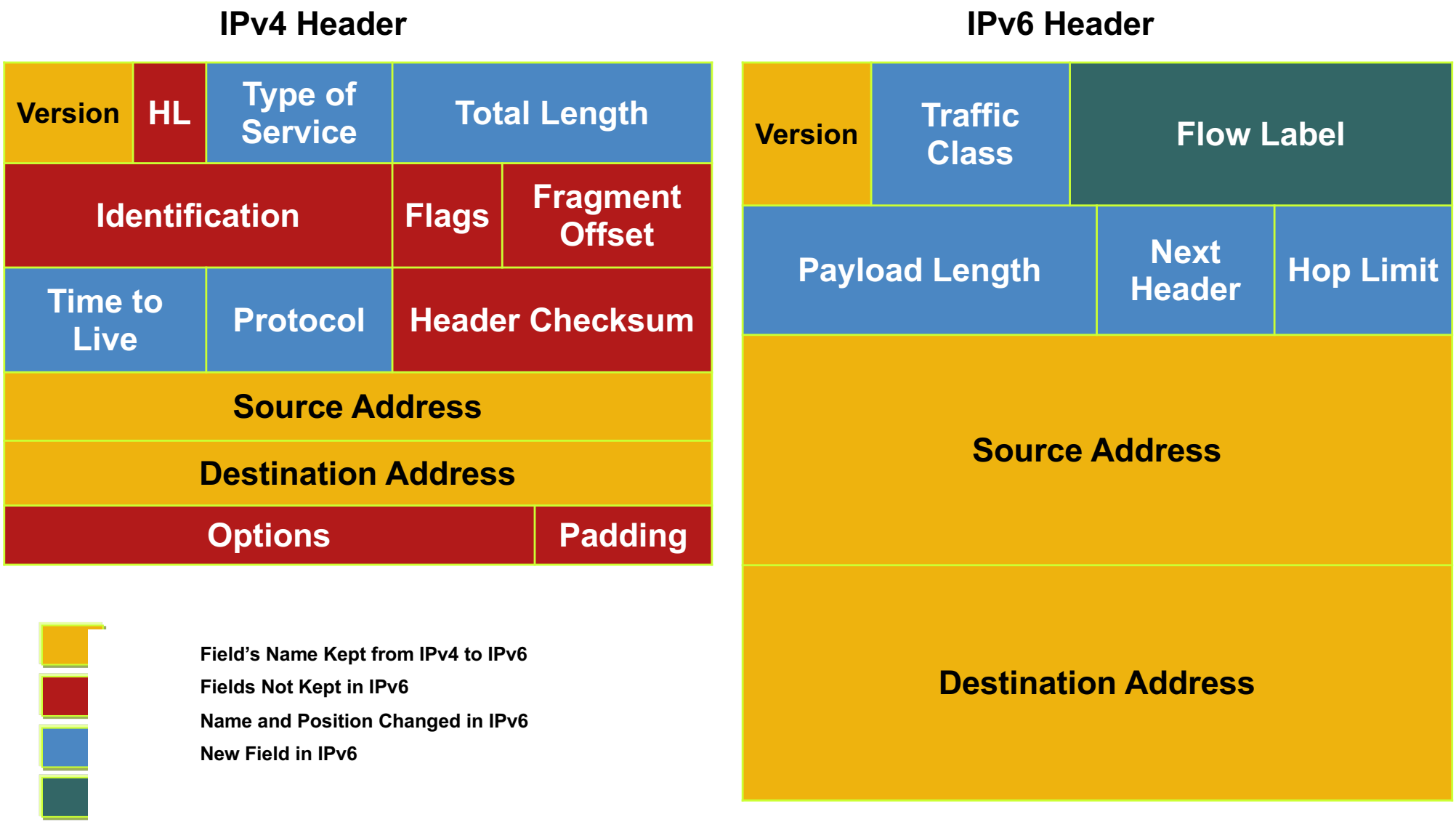
- EUI-64 address is formed by inserting "FFFE" and ORing a bit identifying the uniqueness of the MAC address
- MAC address is unique and stable => part of IPv6 can be used to identify a user ☹
- IETF may deprecate this use (under discussion)

IPv6 Privacy Extensions (RFC 4941)



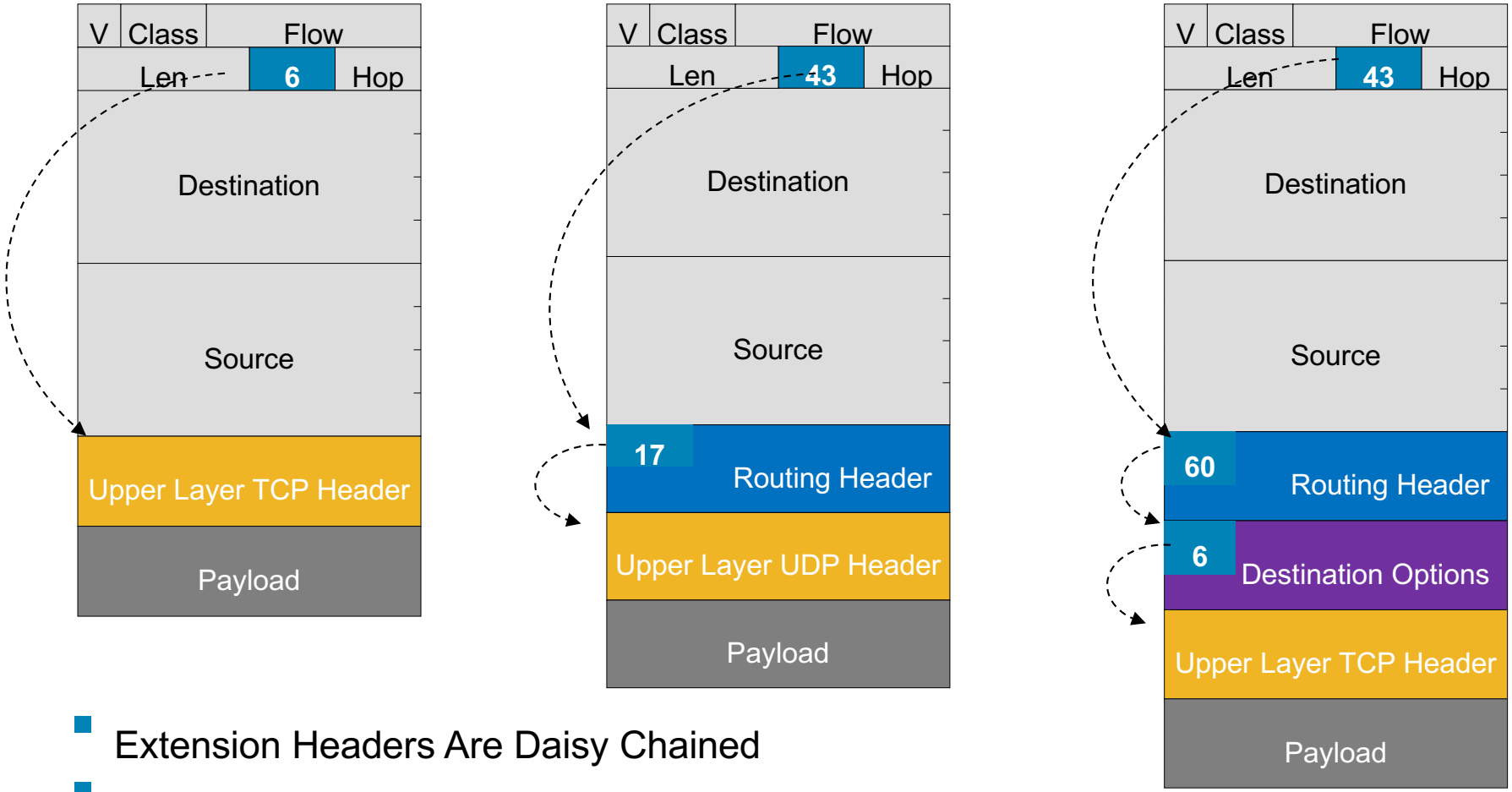
- Temporary addresses for IPv6 host client application, e.g. web browser
  - Inhibit device/user tracking
  - Random 64 bit interface ID, then run Duplicate Address Detection before using it
  - Rate of change based on local policy
- Enabled by default in Windows, Android, iOS 4.3, Mac OS/X 10.7

IPv4 and IPv6 Header Comparison



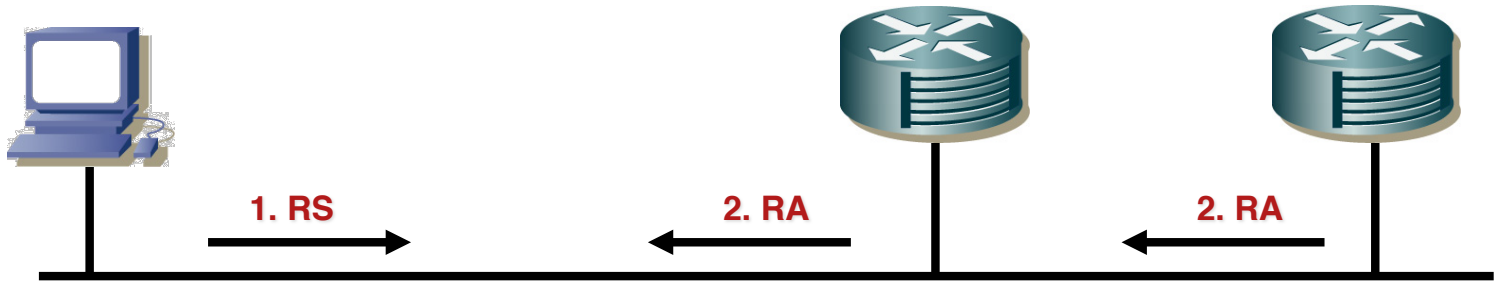
Extension Headers

More options...
More difficult to parse
⇒ More bugs
⇒ More security issue



- Extension Headers Are Daisy Chained
- Upper Layer Headers, must be last, following extension headers

StateLess Address AutoConfiguration (SLAAC)




```
1. RS:
ICMP Type = 133

Src = ::
Dst = All-Routers multicast Address
query= please send RA
```

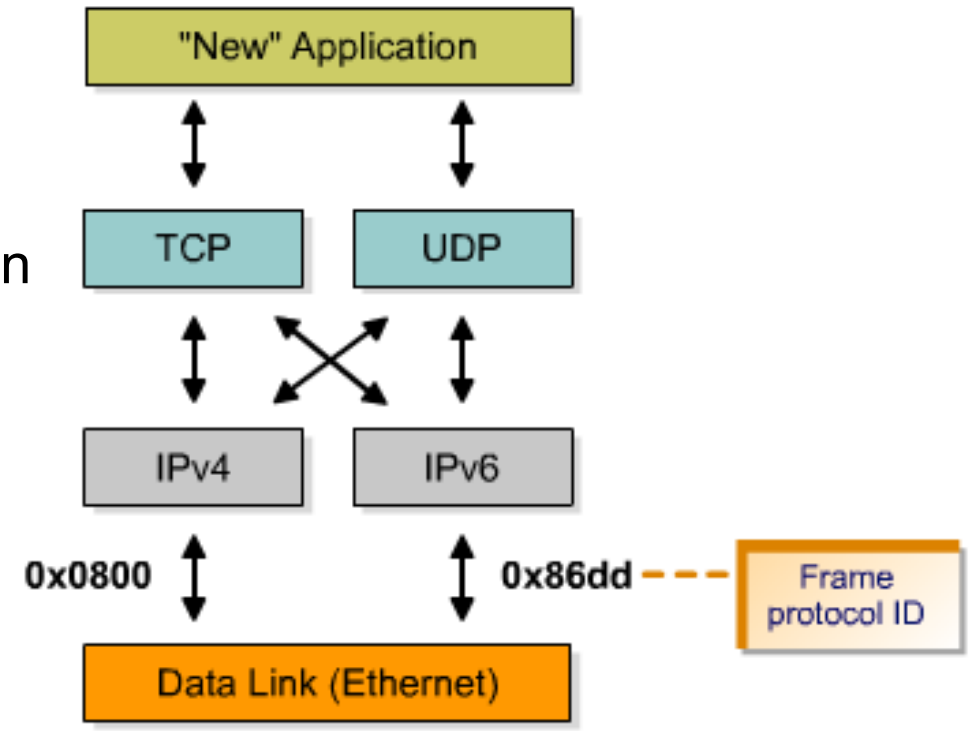
```
2. RA:
ICMP Type = 134

Src = Router Link-local Address
Dst = All-nodes multicast address
Data= options, prefix(es), lifetime,  autoconfig
flag (no managed flag)
```

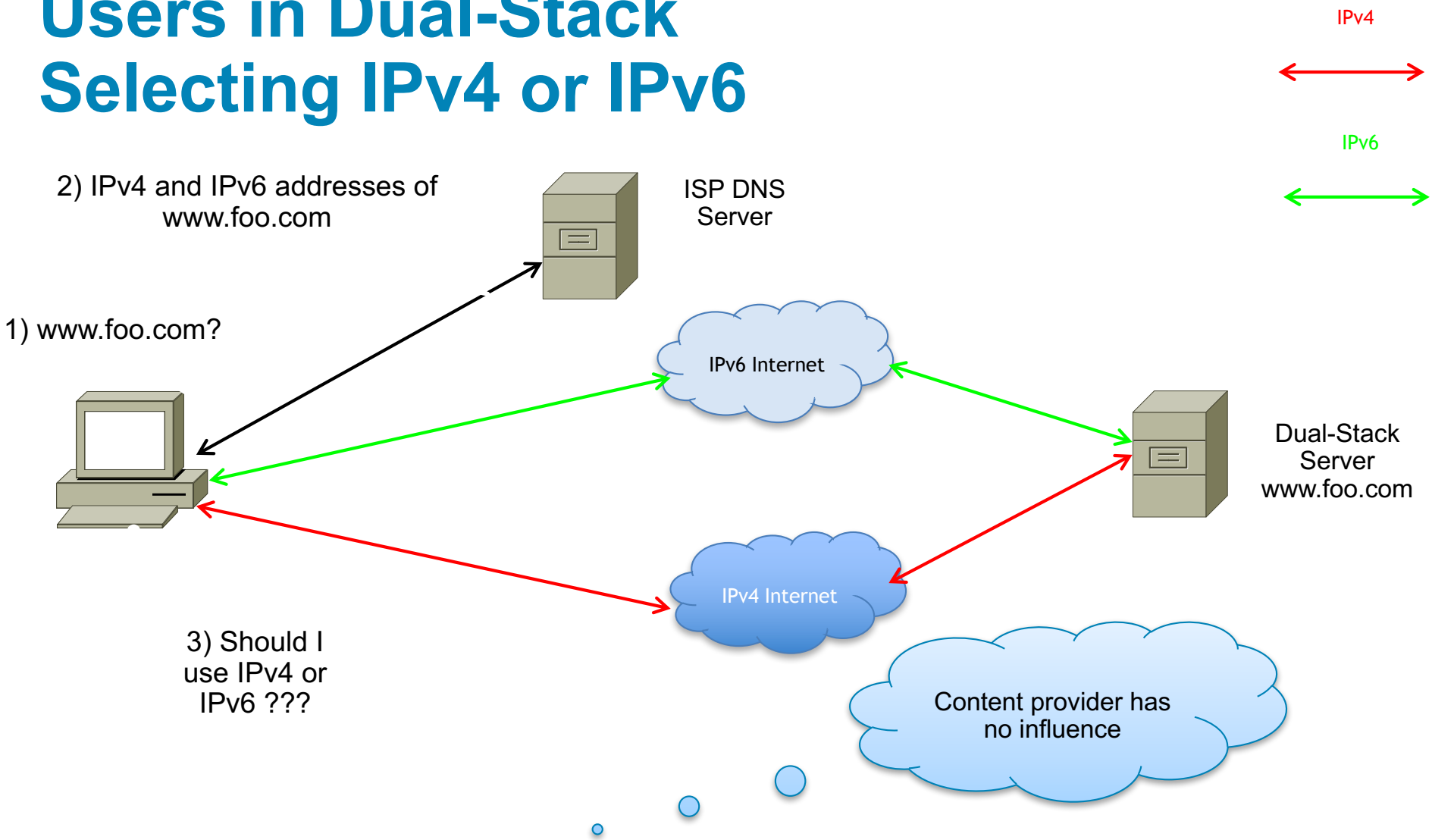
- **Router solicitations are sent by booting nodes to request RAs for configuring the interfaces.**

Dual Stack

- Both IPv4 and IPv6 stacks are enabled.
- Applications can talk to both.
- Choice of the IP version is based on name lookup and application preference.



Users in Dual-Stack Selecting IPv4 or IPv6



Decision by the USER/INITIATOR:

- RFC 6555: Happy Eyeball, try both and keep the fastest
- RFC 6724: local policy, usually IPv6 is preferred

Shared Security Issues

Security Issues Shared by IPv4 and IPv6

IPv6 Myths: Better, Faster, More Secure

Sometimes, newer means better and more secure

Sometimes, experience IS better and safer!

The IPsec Myth: IPsec End-to-End will Save the World

- IPv6 originally mandated the implementation of IPsec (but not its use)
- Now, RFC 6434 "*IPsec SHOULD be supported by all IPv6 nodes*"
- Some organizations still believe that IPsec should be used to secure all flows...

  Interesting **scalability** issue (n^2 issue with IPsec)

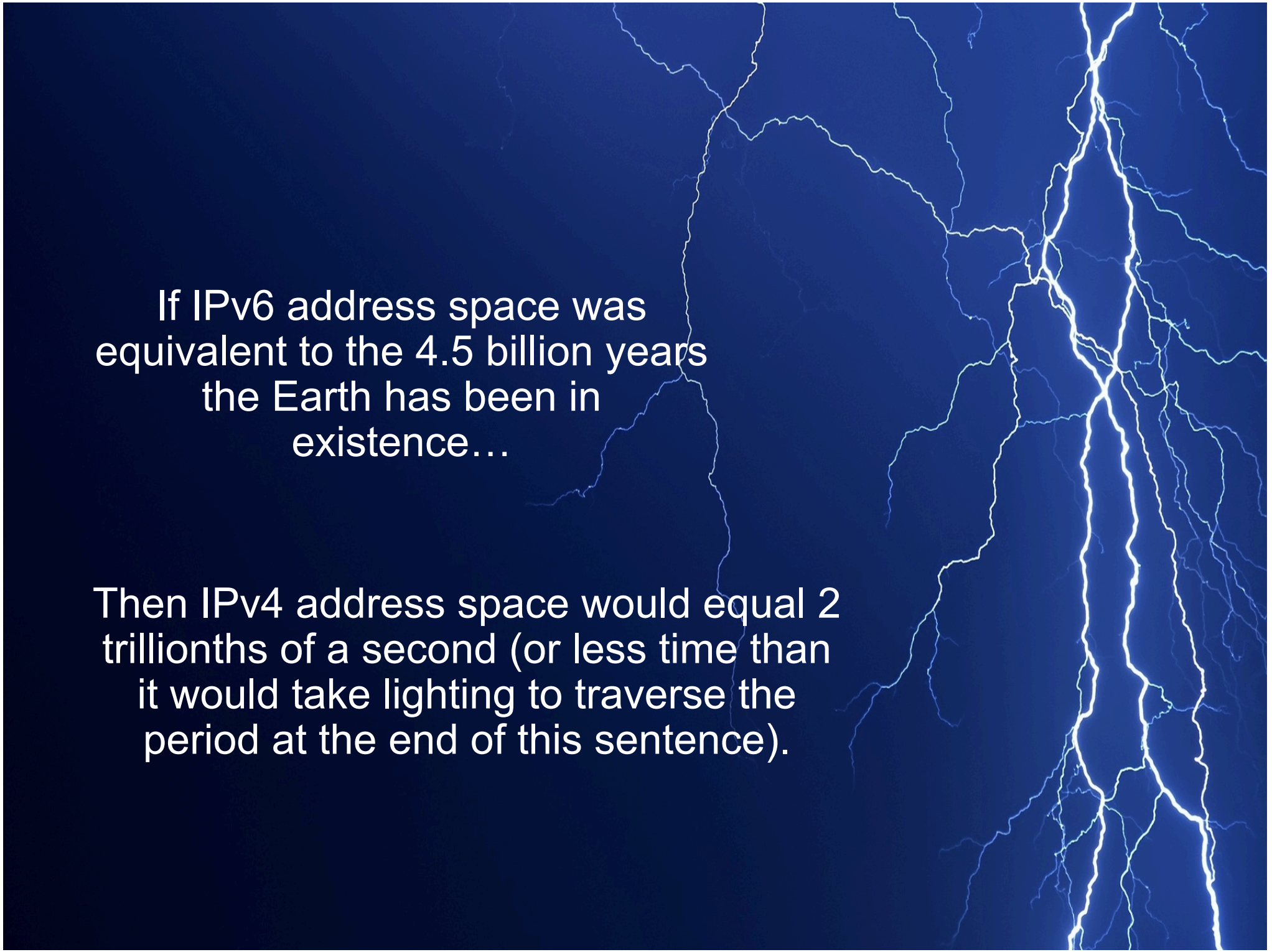
  Need to **trust endpoints and end-users** because the network cannot secure the traffic: no IPS, no ACL, no firewall

    IOS 12.4(20)T can parse the AH

  Network **telemetry is blinded**: NetFlow of little use

  Network **services hindered**: what about QoS?

Recommendation: do not use IPsec end to end within an administrative domain.
Suggestion: Reserve IPsec for residential or hostile environment or high profile targets EXACTLY as for IPv4

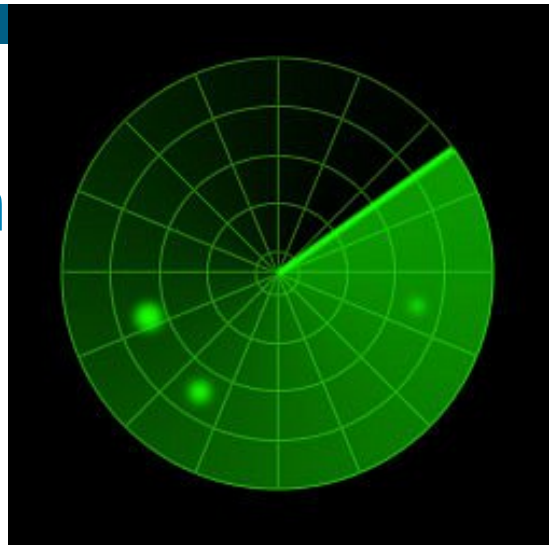

If IPv6 address space was equivalent to the 4.5 billion years the Earth has been in existence…
Then IPv4 address space would equal 2 trillionths of a second (or less time than it would take lighting to traverse the period at the end of this sentence).

Reconnaissance in IPv6
Subnet Size Difference

- Default subnets in IPv6 have 2^{64} addresses

  10 Mpps = more than 50 000 years

Reconnaissance in IPv6
Scanning Methods Are Likely to Ch



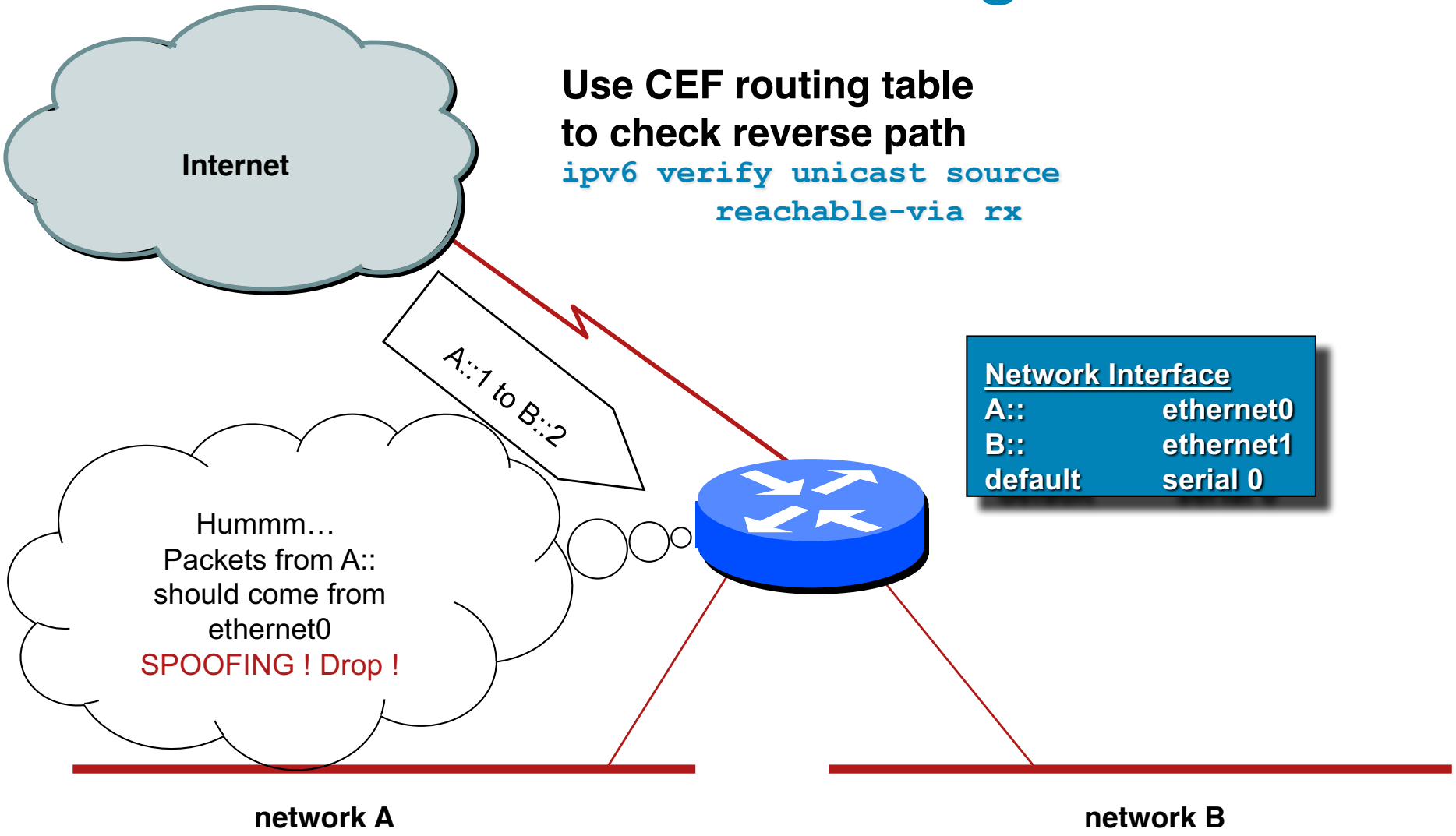
- Public servers will still need to be DNS reachable

  ⇒More information collected by Google...
- Increased deployment/reliance on dynamic DNS

  ⇒More information will be in DNS
- Using peer-to-peer clients gives IPv6 addresses of peers
- Administrators may adopt easy-to-remember addresses (::10,::20,::F00D, ::C5C0, :ABBA:BABE or simply IPv4 last octet for dual stack)
- By compromising hosts in a network, an attacker can learn new addresses to scan
- Transition techniques (see further) derive IPv6 address from IPv4 address

  ⇒ can scan again

IPv6 Address Spoofing
=>Reverse Path Forwarding Check



ICMPv4 vs. ICMPv6

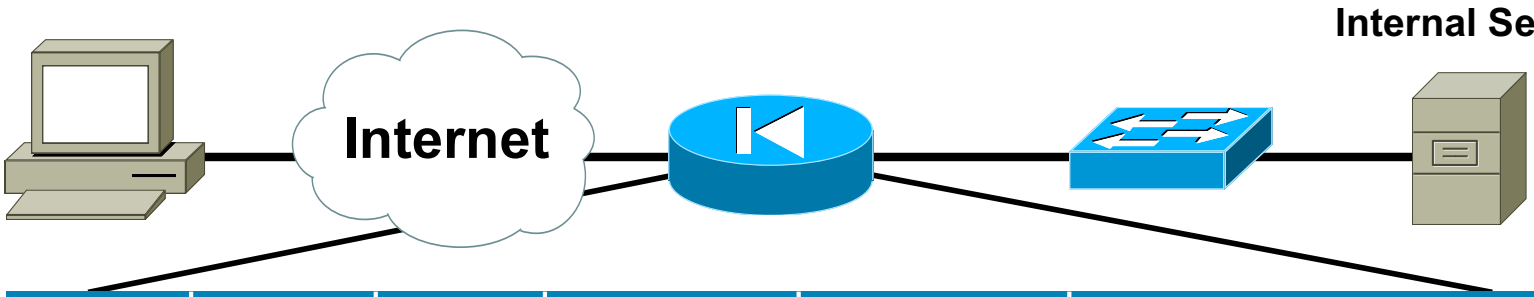
- Significant changes
- More relied upon

ICMP Message Type	ICMPv4	ICMPv6
Connectivity Checks	X	X
Informational/Error Messaging	X	X
Fragmentation Needed Notification	X	X
Address Assignment		X
Address Resolution		X
Multicast Group Management		X
Mobile IPv6 Support		X

- => ICMP policy on firewalls needs to change

Equivalent ICMPv6 Border Firewall Policy*

For Your Reference

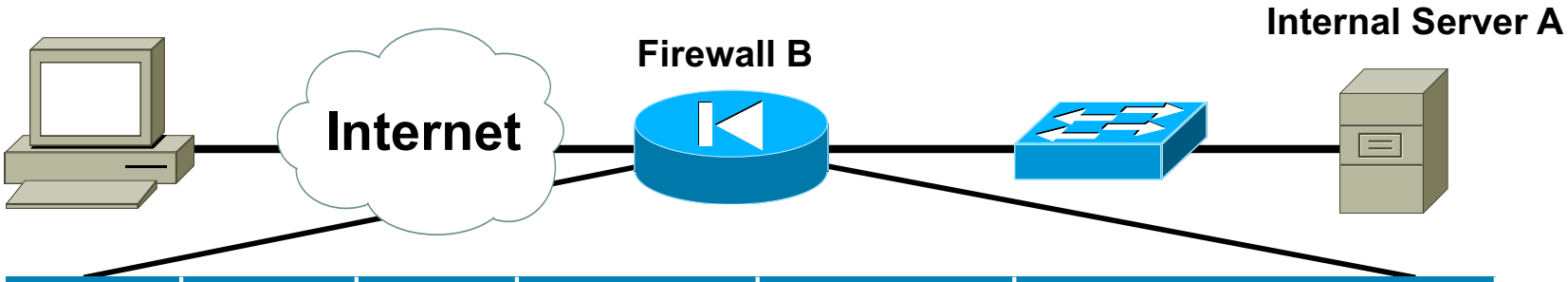


Action	Src	Dst	ICMPv6 Type	ICMPv6 Code	Name
Permit	Any	A	128	0	Echo Reply
Permit	Any	A	129	0	Echo Request
Permit	Any	A	1	0	No Route to Dst.
Permit	Any	A	2	0	Packet Too Big
Permit	Any	A	3	0	Time Exceeded—TTL Exceeded

*RFC 4890

Potential Additional ICMPv6 Border Firewall Policy*

For Your Reference



Action	Src	Dst	ICMPv6 Type	ICMPv6 Code	Name
Permit	Any	A	4	0	Parameter Problem
Permit	Any	B	2	0	Packet too Big
Permit	Any	B	130–132	0	Multicast Listener
Permit	Any	B	135/136	0	Neighbor Solicitation and Advertisement
Permit	Any	B	4	0	Parameter Problem

*RFC 4890

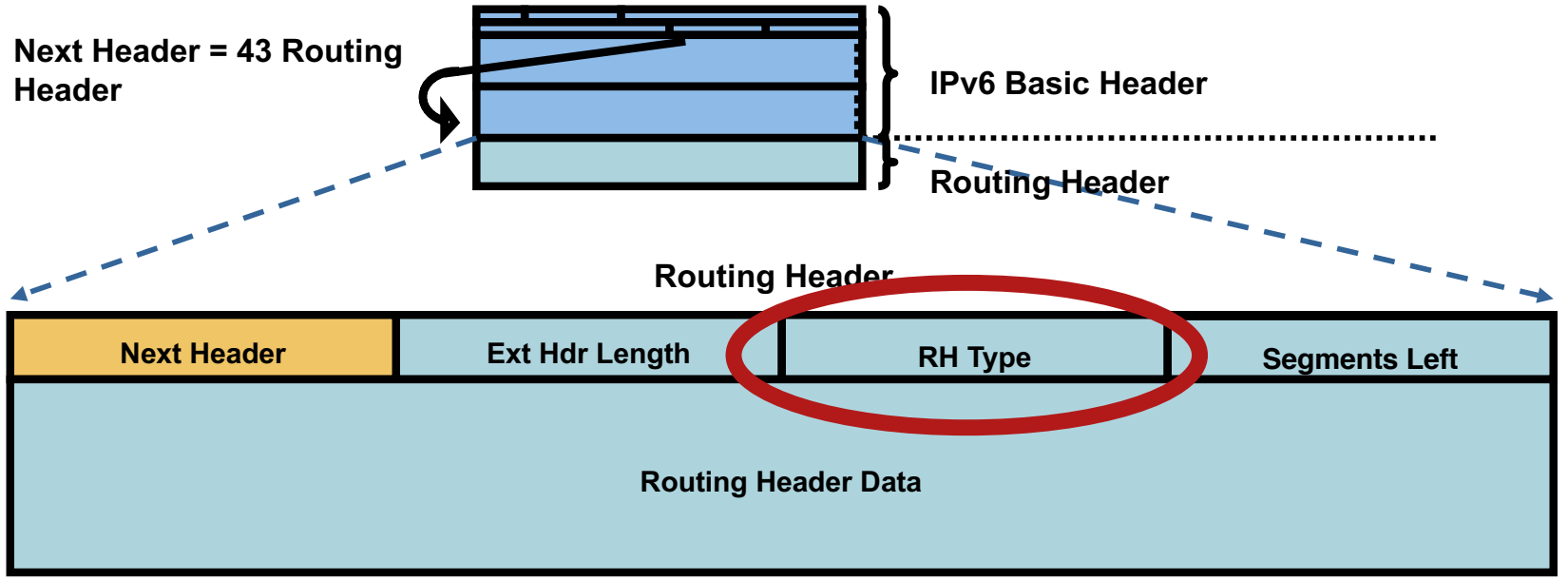
IPv6 Routing Header

- An extension header, processed by intermediate routers
- Three types

  Type 0: similar to IPv4 source routing (multiple intermediate routers)

  Type 2: used for mobile IPv6

  Type 3: RPL (Routing Protocol for Low-Power and Lossy Networks)

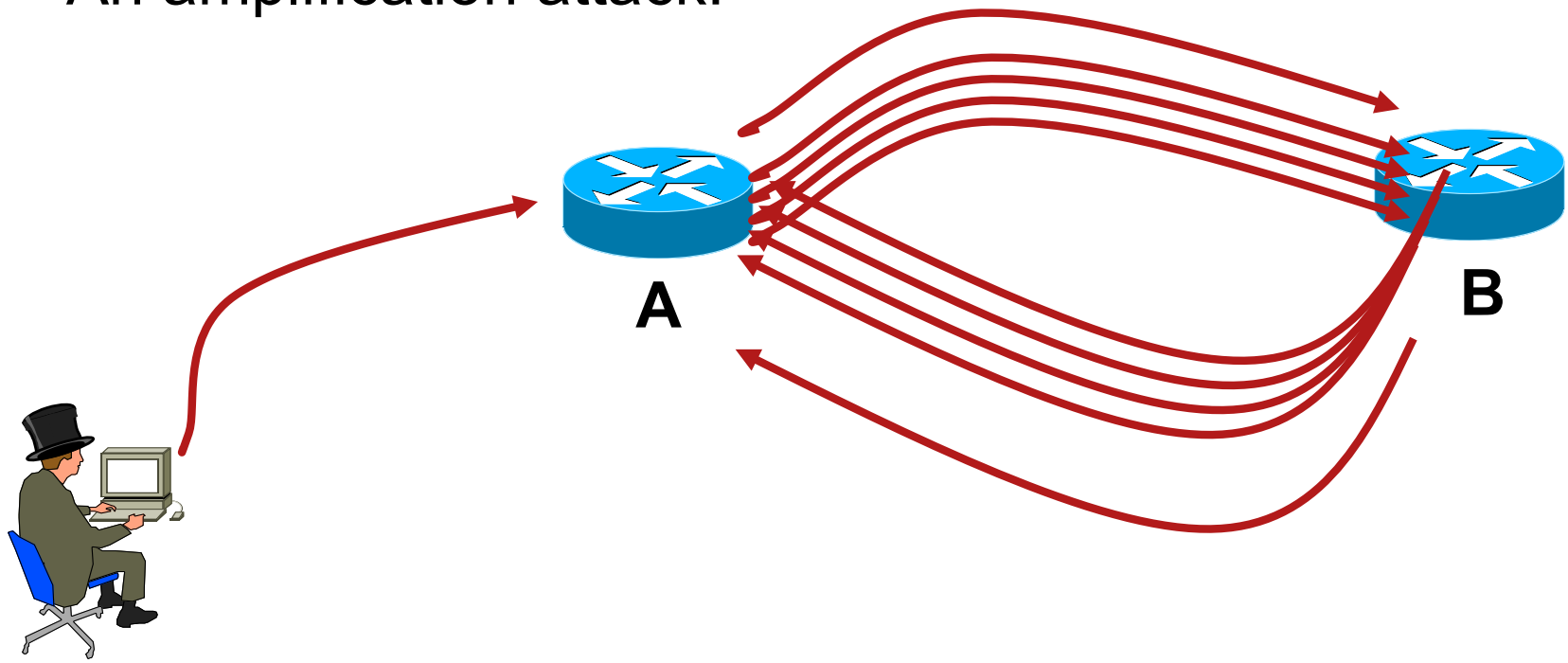


Type 0 Routing Header Issue #2: Amplification Attack

- What if attacker sends a packet with RH containing

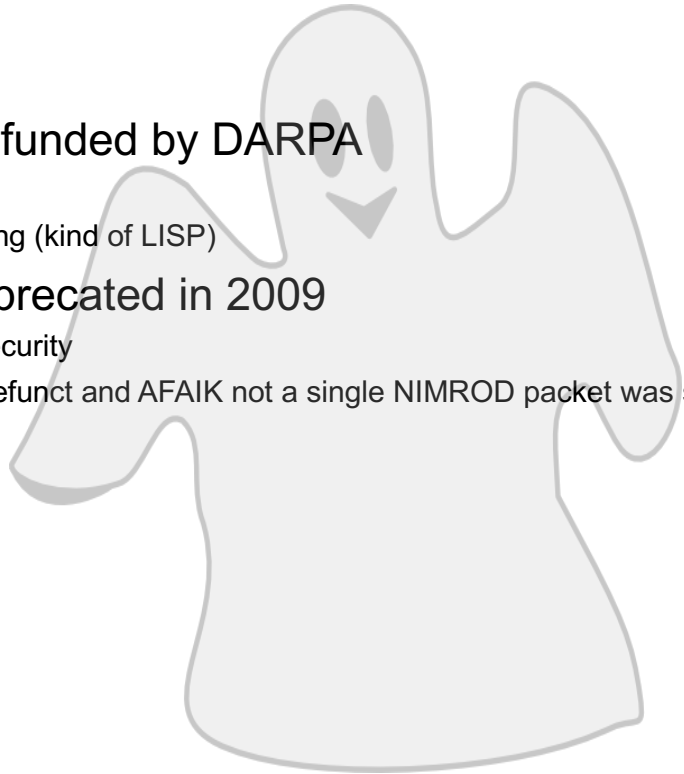
  A -> B -> A -> B -> A -> B -> A -> B -> A ....

- Packet will loop multiple time on the link R1-R2
- An amplification attack!



Routing Header Type 1: NIMROD

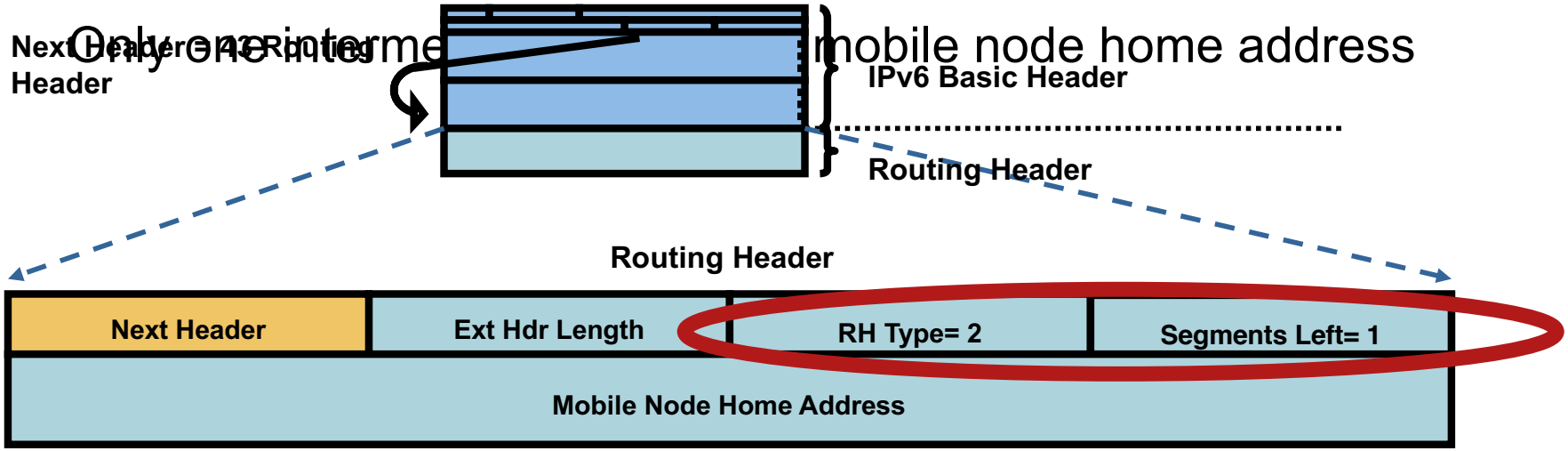
- A 1994 project funded by DARPA
  - Mobility
  - Hierarchy of routing (kind of LISP)
- Type 1 was deprecated in 2009
  - not because of security
  - but project was defunct and AFAIK not a single NIMROD packet was sent over IPv6...



Source: Clipartpanda.com

Routing Header Type 2 for Mobile IPv6 is OK

- Required by mobile IPv6
- Rebound/amplification attacks impossible



Only one intermediate mobile node home address

BRK SEC-3200

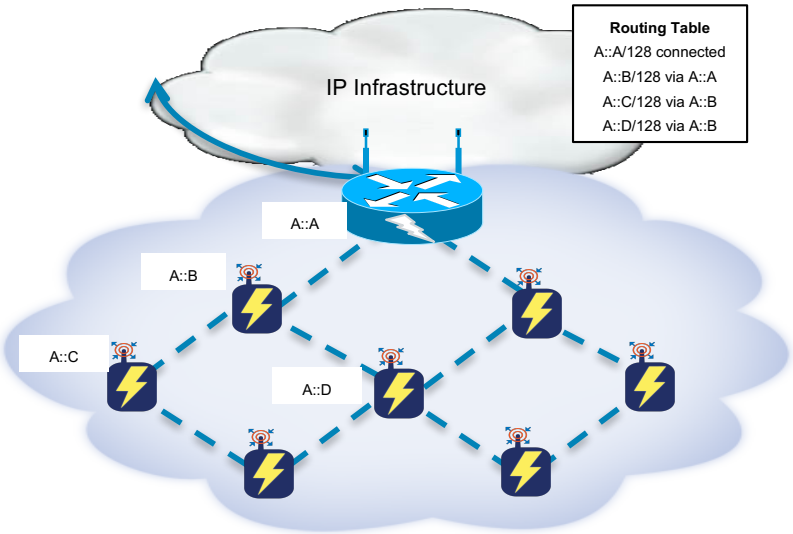
Routing Header Type 3 for RPL is OK

For Your Reference

- Used by Routing Protocol for Low-Power and Lossy Networks
- But only within a single trusted network (strong authentication of node), never over a public untrusted network

  Damage is limited to this RPL network

  If attacker is inside the RPL network, then he/she could do more damage anyway



BRK SEC-3200

Preventing Routing Header Attacks

- Apply same policy for IPv6 as for IPv4:

  Block Routing Header type 0 & do not process them

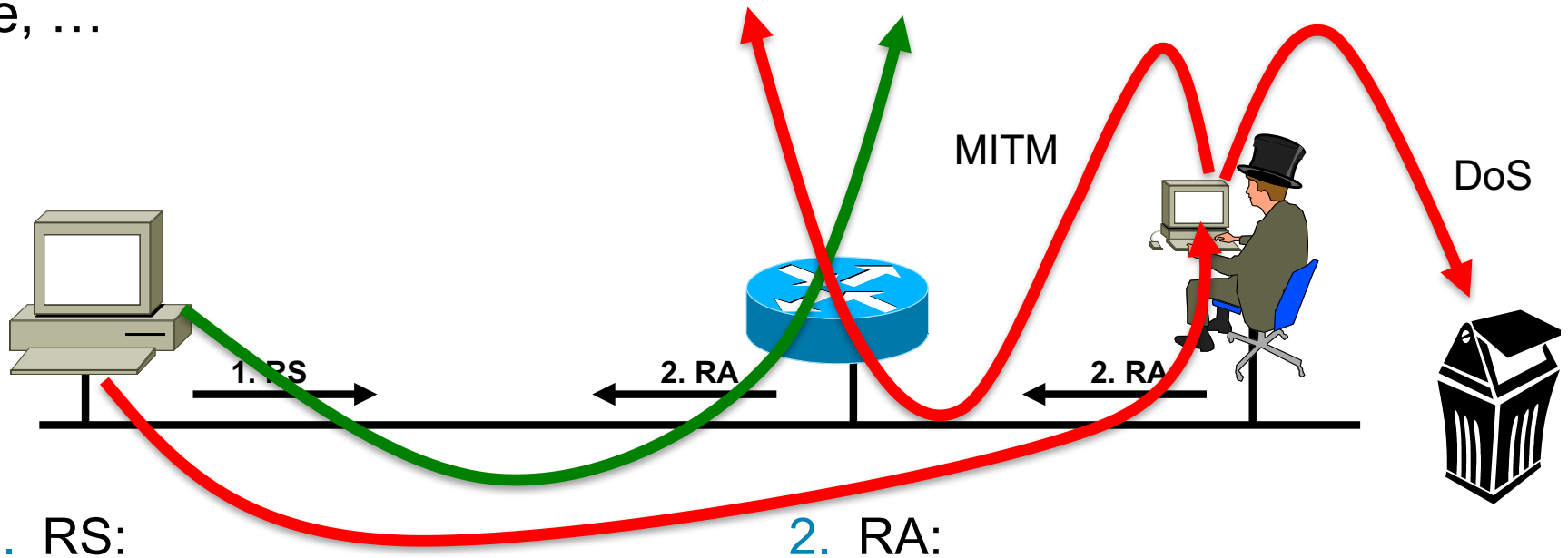
- RFC 5095 (Dec 2007) RH0 is deprecated

  No more a problem ☺

Rogue Router Advertisement

RA w/o Any Authentication Gives Exactly Same Level of Security as DHCPv4 (None)

Router Advertisements contains:
- Prefix to be used by hosts
- Data-link layer address of the router
- Miscellaneous options: MTU, DHCPv6 use, …



1. RS:

Data = Query: please send RA

2. RA:

Data= options, **prefix**, lifetime, A+M+O flags

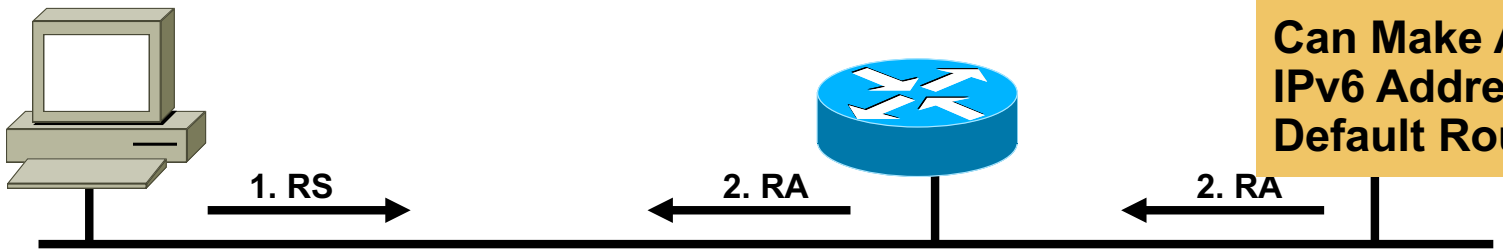
Neighbor Discovery Issue#1 Stateless Autoconfiguration

Router Solicitations Are Sent by Booting Nodes to Request Router Advertisements for Stateless Address Auto-Configuring

RA/RS w/o Any Authentication Gives Exactly Same Level of Security as ARP for IPv4 (None)

Attack Tool:
fake_router6

Can Make Any IPv6 Address the Default Router



1. RS:
   - Src = ::
   - Dst = All-Routers multicast Address
   - ICMP Type = 133
   - Data = Query: please send RA

2. RA:
   - Src = Router Link-local Address
   - Dst = All-nodes multicast address
   - ICMP Type = 134
   - Data= options, prefix, lifetime, autoconfig flag

Effect of Rogue Router Advertisements

- Devastating:

  Denial of service: all traffic sent to a black hole

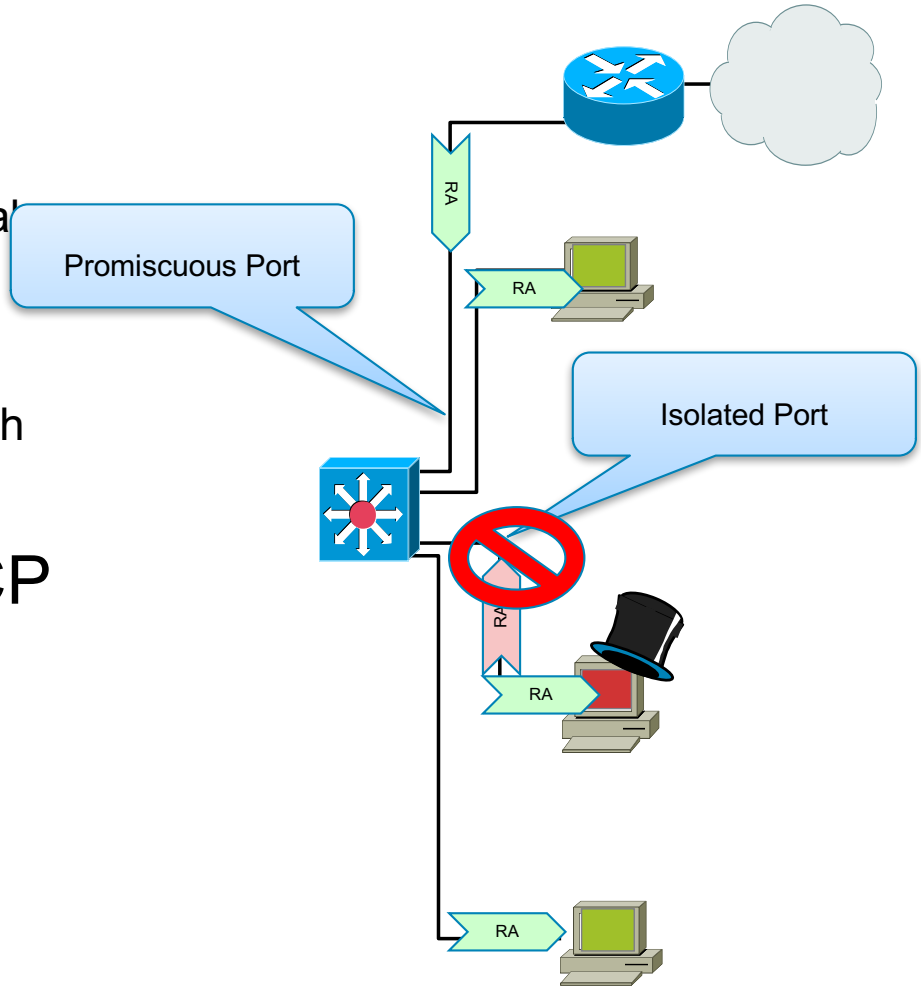
  Man in the Middle attack: attacker can intercept, listen, modify unprotected data

- Also affects legacy IPv4-only network with IPv6-enabled hosts
- Most of the time from non-malicious users
- Requires layer-2 adjacency (some relief…)

- The major blocking factor for enterprise IPv6 deployment

Mitigating Rogue RA: Host Isolation

- Prevent Node-Node Layer-2 communication by using:
  - Private VLANs (PVLAN) where nodes (isolated port) can only contact the official router (promiscuous port)
  - WLAN in ‘AP Isolation Mode’
  - 1 VLAN per host (SP access network with Broadband Network Gateway)
- Link-local multicast (RA, DHCP request, etc) sent only to the local official router: no harm
  - But Duplicate Address Detection does not work anymore...



Mitigating Rogue RA: RFC 6105

- **Port ACL** blocks all ICMPv6 RA from hosts

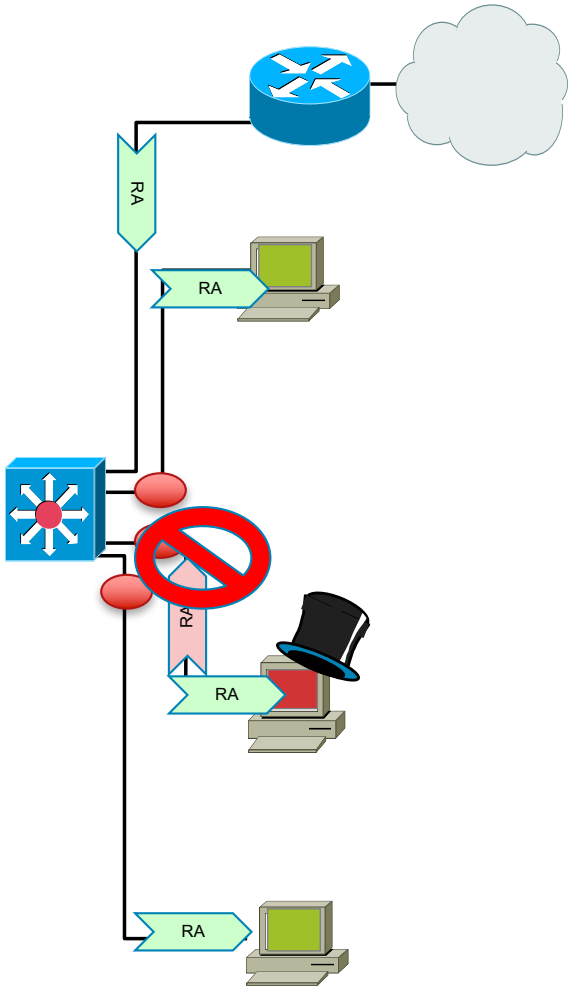
```
interface FastEthernet0/2
  ipv6 traffic-filter ACCESS_PORT in
  access-group mode prefer port
```

- **RA-guard lite** (12.2(33)SXI4 & 12.2(54)SG): also dropping all RA received on this port

```
interface FastEthernet0/2
  ipv6 nd raguard
  access-group mode prefer port
```

- **RA-guard** (12.2(50)SY)

```
ipv6 nd raguard policy HOST device-role host
ipv6 nd raguard policy ROUTER device-role
router
ipv6 nd raguard attach-policy HOST vlan 100
interface FastEthernet0/0
  ipv6 nd raguard attach-policy ROUTER
```



IPv6 Attacks with Strong IPv4 Similarities

- Sniffing

  Without IPSec, IPv6 is no more or less likely to fall victim to a sniffing attack than IPv4

- Application layer attacks

  Even with IPSec, the majority of vulnerabilities on the Internet today are at the application layer, something that IPSec will do nothing to prevent

- Rogue devices

  Rogue devices will be as easy to insert into an IPv6 network as in IPv4

- Man-in-the-Middle Attacks (MITM)

  Without IPSec, any attacks utilizing MITM will have the same likelihood in IPv6 as in IPv4

- Flooding

  Flooding attacks are identical between IPv4 and IPv6

Specific IPv6 Issues

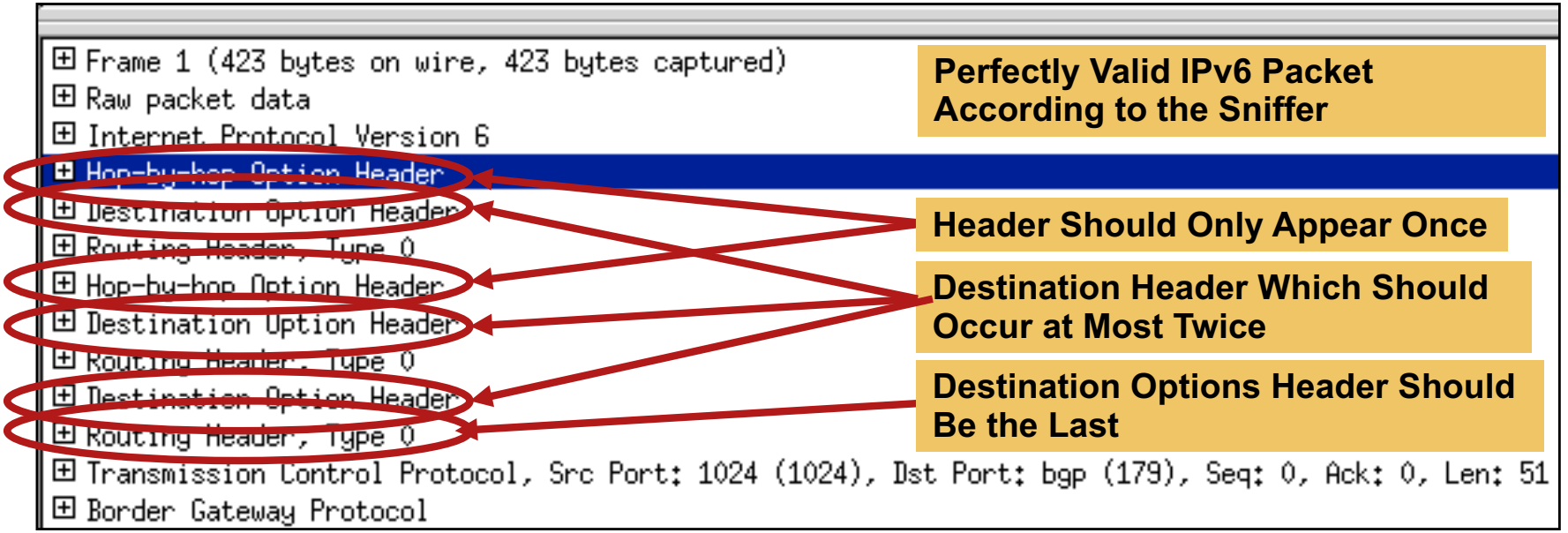
Issues Applicable only to IPv6

IPv6 Header Manipulation

- Unlimited size of header chain (spec-wise) can make filtering difficult
- Potential DoS with poor IPv6 stack implementations

  More boundary conditions to exploit

  Can I overrun buffers with a lot of extension headers?



Extension Header Security Policy

- White list approach for your traffic

  Only allow the REQUIRED extension headers (and types), for example:

  Fragmentation header

  Routing header type 2 & destination option (when using mobile IPv6)

  IPsec ☺ AH and ESP

  And layer 4: ICMPv6, UDP, TCP, GRE, ...

  If your firewall is capable:

  Drop 1st fragment without layer-4 header

  Drop routing header type 0

  Drop/ignore hop-by-hop

Source: Tony Webster, Flickr

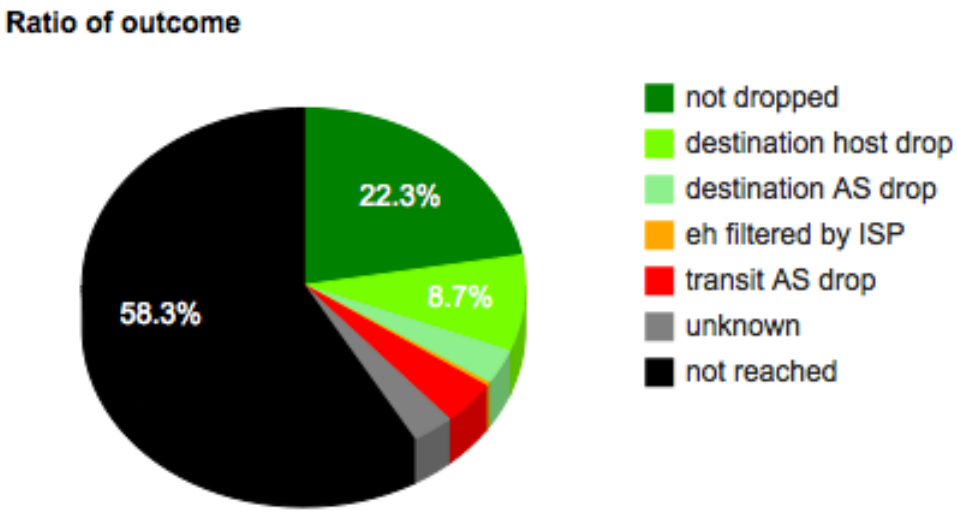
Extension Header Loss over the Internet

- End users SHOULD filter packets with extension headers
- But, what are your ISP and its transit provider doing to your packets?

Source: Paul Townsend, Flickr

- RFC 7872
  - About 20-40% of packets with Ext Hdr are dropped over the Internet

Things Keeps Improving Though



- Current research by Polytechnique Paris (Mehdi Kouhen) and Cisco (Eric Vyncke)

  And VM provided by Sander Steffann

- http://btv6.vyncke.org/exthdr/index.php?ds=bgp&t=fh (work in progress!)

IPv4 to IPv6 Transition Challenges

- 16+ methods, possibly in combination
  - IP spoofing
- Dual stack
  - Consider security for both protocols
  - Cross v4/v6 abuse
  - Resiliency (shared resources)
- Tunnels
  - Bypass firewalls (protocol 41 or UDP)

Dual Stack Host Considerations

- Host security on a dual-stack device

  Applications can be subject to attack on both IPv6 and IPv4

  Fate sharing: as secure as the least secure stack...

- Host security controls should block and inspect traffic from both IP versions

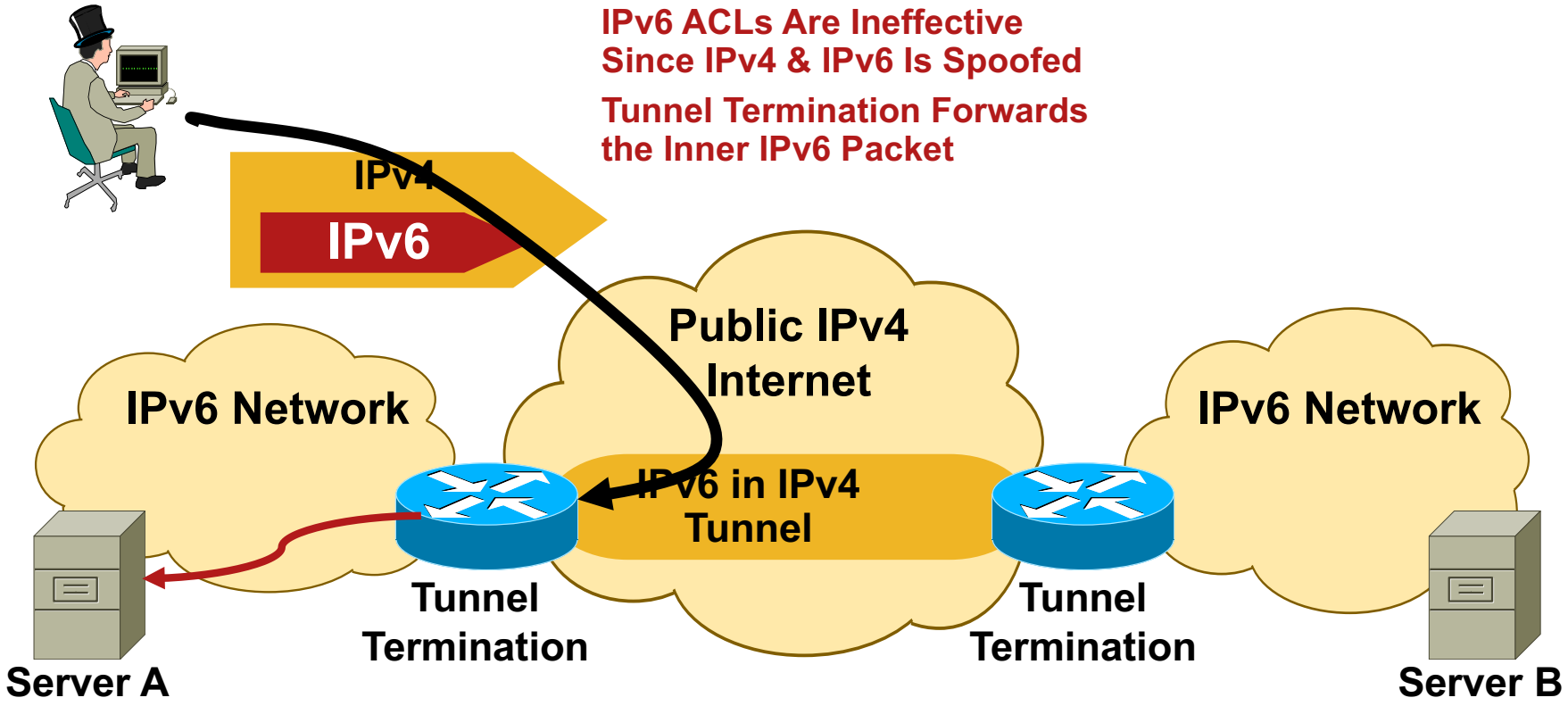
  Host intrusion prevention, personal firewalls, VPN clients, etc.

Dual Stack with Enabled IPv6 by Default

- Your host:
  - IPv4 is protected by your favorite personal firewall...
  - IPv6 is enabled by default (Vista, Linux, MacOS, ...)
- Your network:
  - Does not run IPv6
- Your assumption:
  - I'm safe
- Reality
  - You are **not** safe
  - Attacker sends Router Advertisements
  - Your host configures silently to IPv6
  - You are now under IPv6 attack
- => Probably time to think about IPv6 in your network

L3-L4 Spoofing in IPv6 When Using IPv6 over IPv4 Tunnels

- Most IPv4/IPv6 transition mechanisms have no authentication built in
- => an IPv4 attacker can inject traffic if spoofing on IPv4 and IPv6 addresses



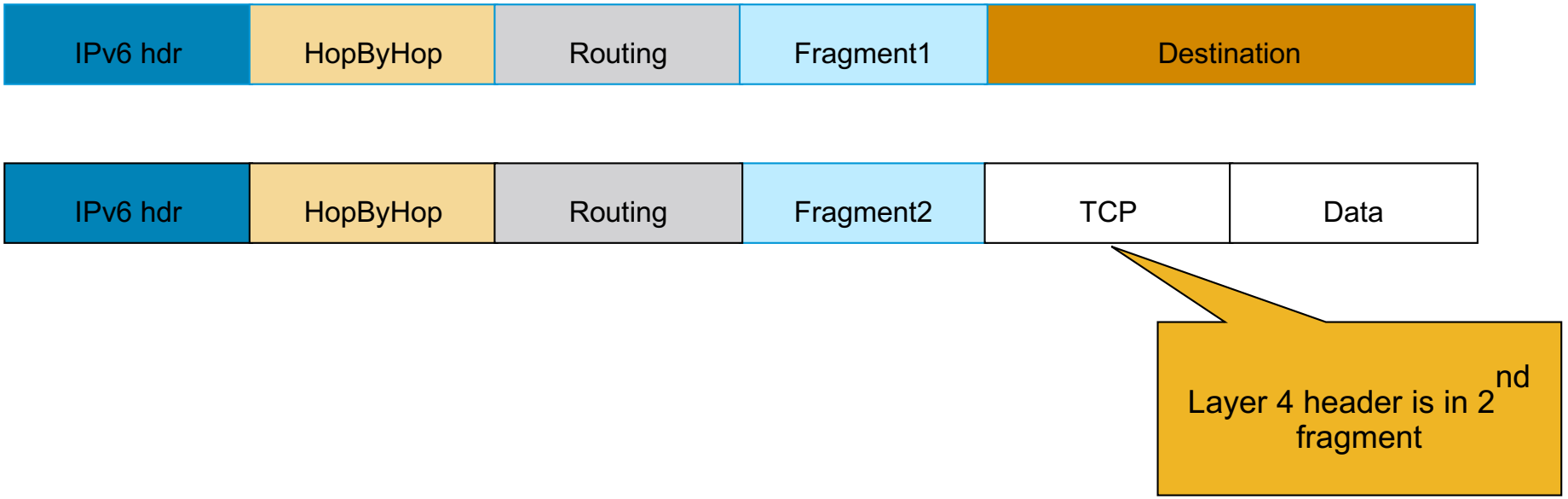
Enforcing a Security Policy

Parsing the Extension Header Chain

- Finding the layer 4 information is not trivial in IPv6
  - Skip all known extension header
  - Until either known layer 4 header found => **SUCCESS**
  - Or unknown extension header/layer 4 header found... => **FAILURE**

Parsing the Extension Header Chain Fragmentation Matters!

- Extension headers chain can be so large than it must be fragmented!
- RFC 3128 is not applicable to IPv6
- Layer 4 information could be in 2nd fragment

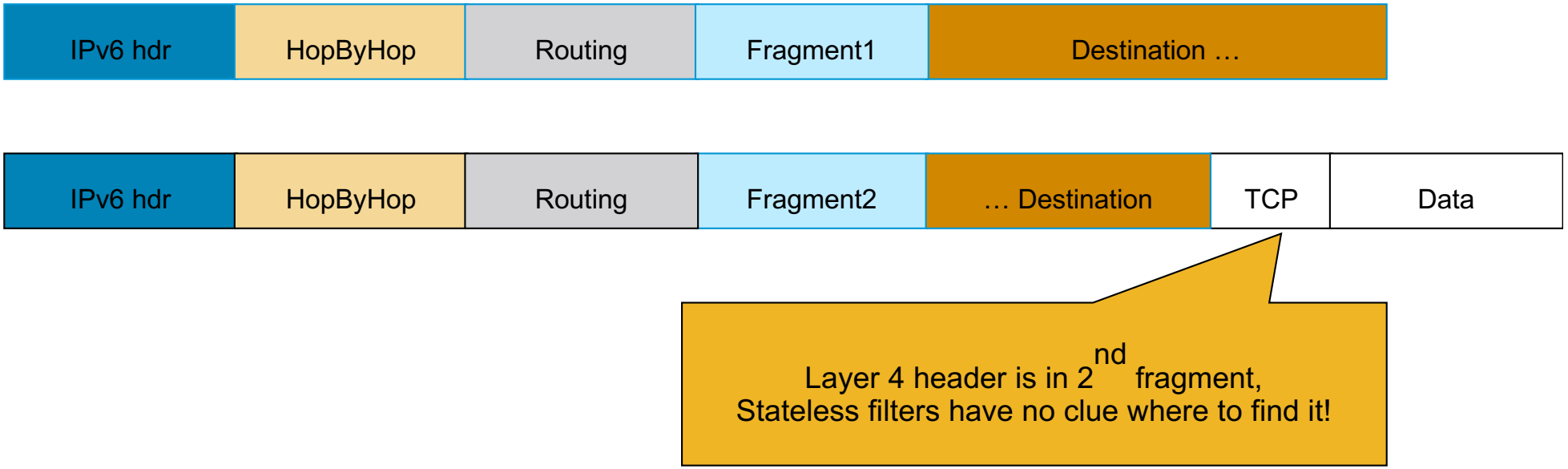


Parsing the Extension Header Chain Fragments and Stateless Filters

- Layer 4 information could be in 2nd fragment
- But, stateless firewalls could not find it if a previous extension header is fragmented
- RFC 3128 is not applicable to IPv6 but

  RFC 6980 ‘nodes MUST silently ignore NDP ... if packets include a fragmentation header’ ;-)

  RFC 7112 ‘A host that receives a First Fragment that does not satisfy ... SHOULD discard the packet’ ;-)



Some Recent IPv6 Security News

IETF Mail Servers under Spam Attack

"A rather widespread spam attack is currently underway, and the IETF server is amongst its targets.

…

On a positive note, the IETF will at least be pleased to know that more than 10,000 of those 26,000 hosts are using IPV6. Hooray for our side."

Glen Barney, IT Director, IETF Secretariat, 4 August 2017

NAT does not Protect IoT

"Early 2017, a multi-stage Windows Trojan containing code to scan for vulnerable IoT devices and inject them with Mirai bot code was discovered. The number of IoT devices which were previously safely hidden inside corporate perimeters, vastly exceeds those directly accessible from the Internet, allowing for the creation of botnets with unprecedented reach and scale."

"The call is coming from inside the house! Are you ready for the next evolution in DDoS attacks?" Steinthor Bjanarson, Arbor Networks, DEFCON 25

Europol LEA: CGN Are Painful, IPv6 is THE solution

HOME › NEWSROOM › ARE YOU SHARING THE SAME IP ADDRESS AS A CRIMINAL? LAW ENFORCEMENT CALL FOR THE END OF CARRIER GRADE NAT (CGN) TO INCREASE AC...

ARE YOU SHARING THE SAME IP ADDRESS AS A CRIMINAL? LAW ENFORCEMENT CALL FOR THE END OF CARRIER GRADE NAT (CGN) TO INCREASE ACCOUNTABILITY ONLINE

17 October 2017

Press Release

This was supposed to be a temporary solution until the transition to IPv6 was completed but for some operators it has become a substitute for the IPv6 transition. Despite IPv6 being available for more than 5 years the internet access industry increasingly uses CGN technologies (90% for mobile internet and 50% for fixed line) instead of adopting the new standard.

Some Nuggets Heard at Europol

- About CGN sharing ratio
  - Some mobile providers has a sharing ratio of 1:30.000
  - Another ISP in Baltic countries shares 1 public to 100.000 subscribers!
  - Law Enforcement Agencies knows about the 5-tuple with client port and destination address
  - Big content providers do not log the source port / destination address (in case of CDN)
- Big ISP Infosec: IPv6 is more secure than IPv4 because IPsec is always used...

Conclusion

Key Take Away

- So, nothing really new in IPv6

  Lack of operation experience may hinder security for a while

- Security enforcement is possible

  Control your IPv6 traffic as you do for IPv4

- Leverage IPsec to secure IPv6 when possible

- Beware of the IPv6 latent threat: your network may be vulnerable to IPv6 attacks