IPv6 Security

Eric Vyncke, Distinguished Engineer, evyncke@cisco.com

A Foreword…

Ratio of IPv4 and IPv… | CARE DDTS | Directory | EDCS | Lab | LeSoir | http://www.vyncke… | Stocks | FXConverter – 164 … | Famille Vyncke-Deh… | Aut…

IPv6 Deployment Aggregated Status

As of 2011-11-06 and limited to the top-50 per Top Level Domain extracted from the Alexa list. See the bottom of this page for more information on the tests.
Click on a country to see specific statistics about top sites within this country or click on a flag:

Country	Sample	Green	Orange
Slovenia	50	22.0% (11)	0.0% (0)
Netherlands	50	16.0% (8)	2.0% (1)

Country	Sample	Green	Orange
Slovenia	50	22.0% (11)	0.0% (0)
Netherlands	50	16.0% (8)	2.0% (1)
Moldova	50	14.0% (7)	0.0% (0)
Switzerland	50	12.0% (6)	4.0% (2)

Country	Sample	Green	Orange
Netherlands	50	16.0% (8)	0.0% (0)
Norway	50	10.0% (5)	2.0% (1)
Moldova	50	10.0% (5)	0.0% (0)
Seychelles	50	8.0% (4)	0.0% (0)

DNS

Country	Sample	Green	Orange
Tunisia	50	78.0% (39)	0.0% (0)
Finland	50	44.0% (22)	2.0% (1)
Poland	50	40.0% (20)	0.0% (0)
Czech Republic	50	38.0% (19)	2.0% (1)

Source: http://www.vyncke.org/ipv6status

Agenda

- Security Myths of IPv6

IPv6 Myths: Better, Faster, More Secure

1995: RFC 1883

2011: IPv6

Is IPv6 (a teenager) really 'better and more secure'?
Eric: a father of two teenagers (16 & 19)…

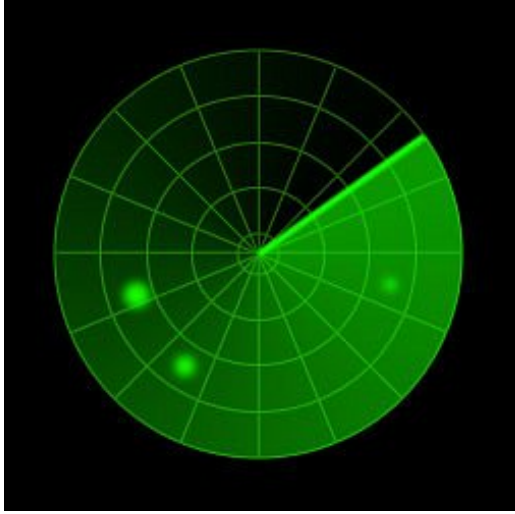
The Absence of Reconnaissance Myth

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

  10 Mpps = more than 50 000 years

- NMAP doesn't even support ping sweeps on
  IPv6 networks (but let's wait)

Reconnaissance in IPv6
Scanning Methods Are Likely to Change



- 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 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

Viruses and Worms in IPv6

- Viruses and email, IM worms: IPv6 brings no change
- Other worms:

  IPv4: reliance on network scanning

  IPv6: not so easy (see reconnaissance) => will use alternative techniques

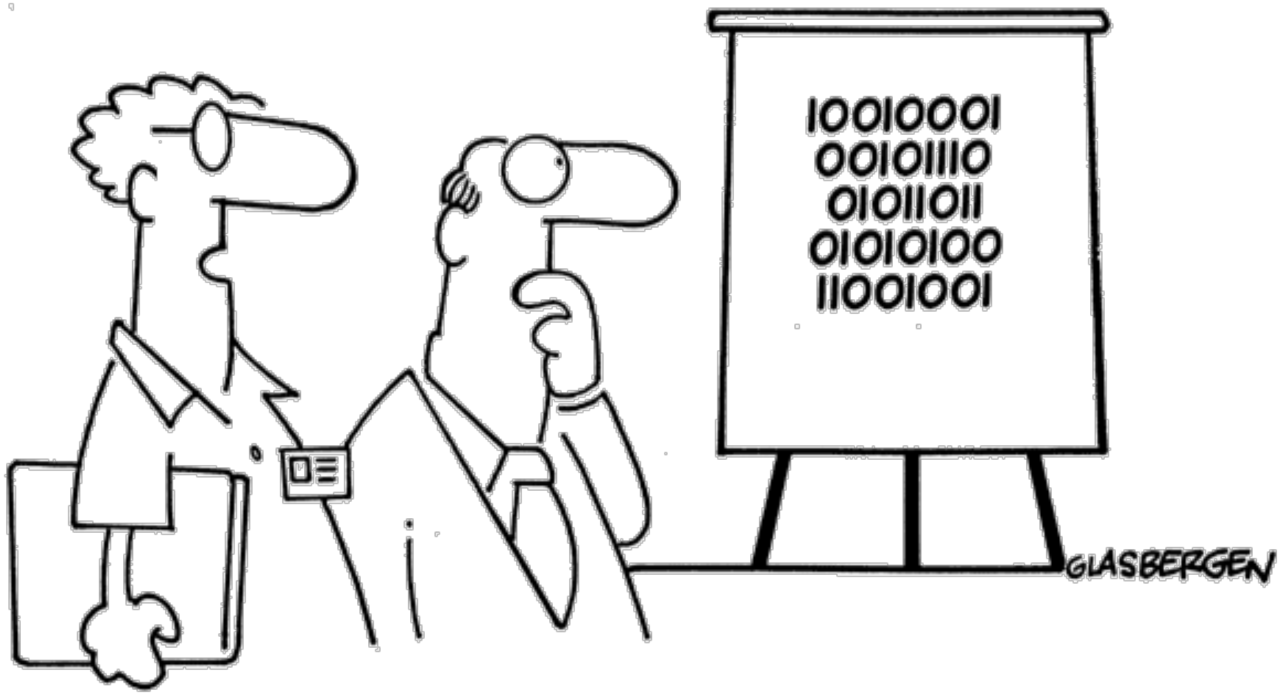
- Worm developers will adapt to IPv6
- IPv4 best practices around worm detection and mitigation remain valid

Scanning Made Bad for CPU

- Potential router CPU attacks if aggressive scanning
  - Router will do Neighbor Discovery... And waste CPU and memory
  - (Cisco) Built-in rate limiter but no option to tune it
- Using a /64 on **point-to-point links** => a lot of addresses to scan!
  - Using /127 could help (RFC 6164)
- **Internet edge/presence**: a target of choice
  - Ingress ACL permitting traffic to specific statically configured (virtual) IPv6 addresses only
- Using infrastructure ACL prevents this scanning
  - iACL: edge ACL denying packets addressed to your routers
  - Easy with IPv6 because new addressing scheme can be done ☺

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

- IPv6 mandates the implementation of IPsec
- Some organizations believe that IPsec should be used to secure all flows…



"We've devised a new security encryption code. Each digit is printed upside down."

The IPsec Reality: IPsec End-to-End will Not Save the World

- IPv6 mandates the implementation of IPsec (IETF 6MAN WG working change it)
- IPv6 does not require the use of IPsec
- Some organizations 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
  - Network **telemetry is blinded**: NetFlow/IPFIX 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.

The No Amplification Attack Myth
IPv6 and Broadcasts

- There are no broadcast addresses in IPv6
- Broadcast address functionality is replaced with appropriate link local multicast addresses
  - Link Local All Nodes Multicast—FF02::1
  - Link Local All Routers Multicast—FF02::2
  - Link Local All mDNS Multicast—FF02::FB

Note: anti-spoofing also blocks amplification attacks because a remote attacker cannot masquerade as his victim

http://iana.org/assignments/ipv6-multicast-addresses/

IPv6 and Other Amplification Vectors

- RFC 4443 ICMPv6

  No ping-pong on a physical point-to-point link Section 3.1

  *No ICMP **error** message should be generated in response to a packet with a multicast destination address Section 2.4 (e.3)*

  Exceptions for Section 2.4 (e.3)

  – *packet too big message*

  – *the parameter problem message*

  *ICMP **information** message (echo reply) should be generated even if destination is multicast*

•Rate Limit egress ICMP Packets

•Rate limit ICMP messages generation

•Secure the multicast network (source specific multicast)

•Note: Implement Ingress Filtering of Packets with IPv6 Multicast Source Addresses

IPv6 Attacks with Strong IPv4 Similarities

- Sniffing
  - IPv6 is no more or less likely to fall victim to a sniffing attack than IPv4
- Application layer attacks
  - 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 strong mutual authentication, any attacks utilizing MITM will have the same likelihood in IPv6 as in IPv4
- Flooding
  - Flooding attacks are identical between IPv4 and IPv6

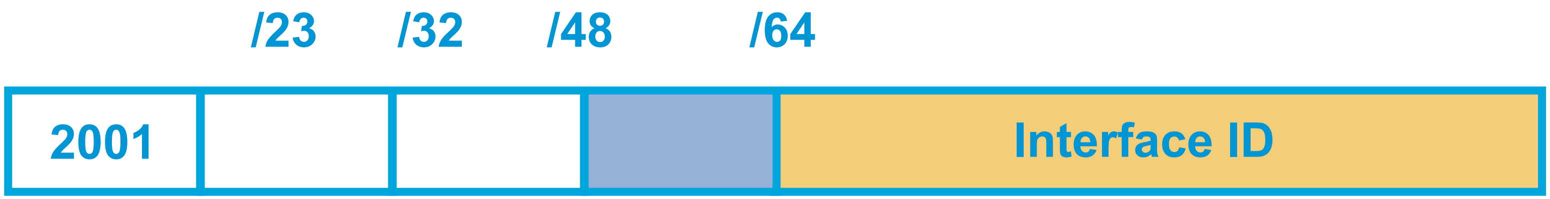
IPv6 Stack Vulnerabilities

- IPv6 stacks were new and could be buggy
- Some examples

CVE-2009-2208	Jun 2009	FreeBSD OpenBSD NetBSD and others	Local users can disable IPv6 without privileges
CVE-2010-1188	Mar 2010	Linux	DoS for socket() manipulation
CVE-2010-4684	Jan 2011	IOS	IPv6 TFTP crashes when debugging
CVE-2008-1576	Jun 2008	Apple Mac OS X	Buffer overflow in Mail over IPv6
CVE-2010-4669	Jan 2011	Microsoft	Flood of forged RA DoS

Specific IPv6 Issues

IPv6 Privacy Extensions (RFC 3041)

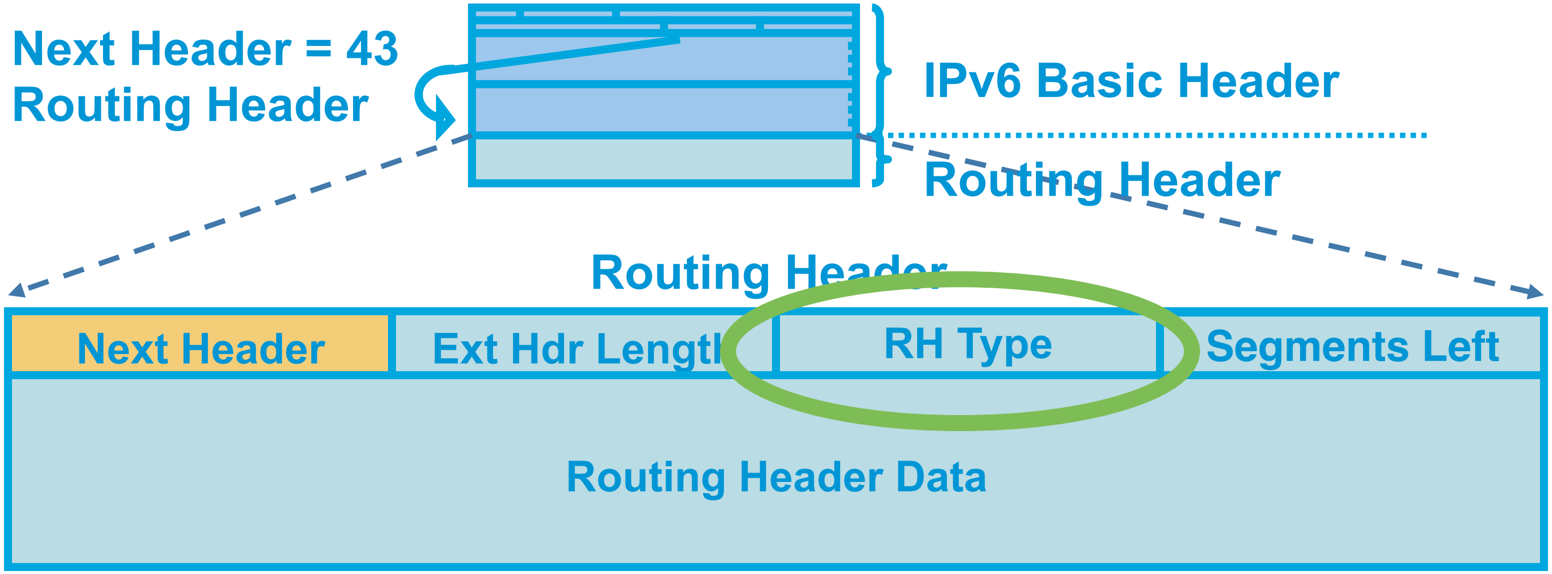


- Temporary addresses for IPv6 host client application, e.g. web browser
  - Inhibit device/user tracking
  - Random 64 bit interface ID, then run Duplicate Address Detection before using it
  - Rate of change based on local policy

Recommendation: Use Privacy Extensions for External Communication but not for Internal Networks (Troubleshooting and Attack Trace Back)

IPv6 Routing Header

- An extension header
- Processed by the listed intermediate routers
- Two types
  - Type 0: similar to IPv4 source routing (multiple intermediate routers)
  - Type 2: used for mobile IPv6

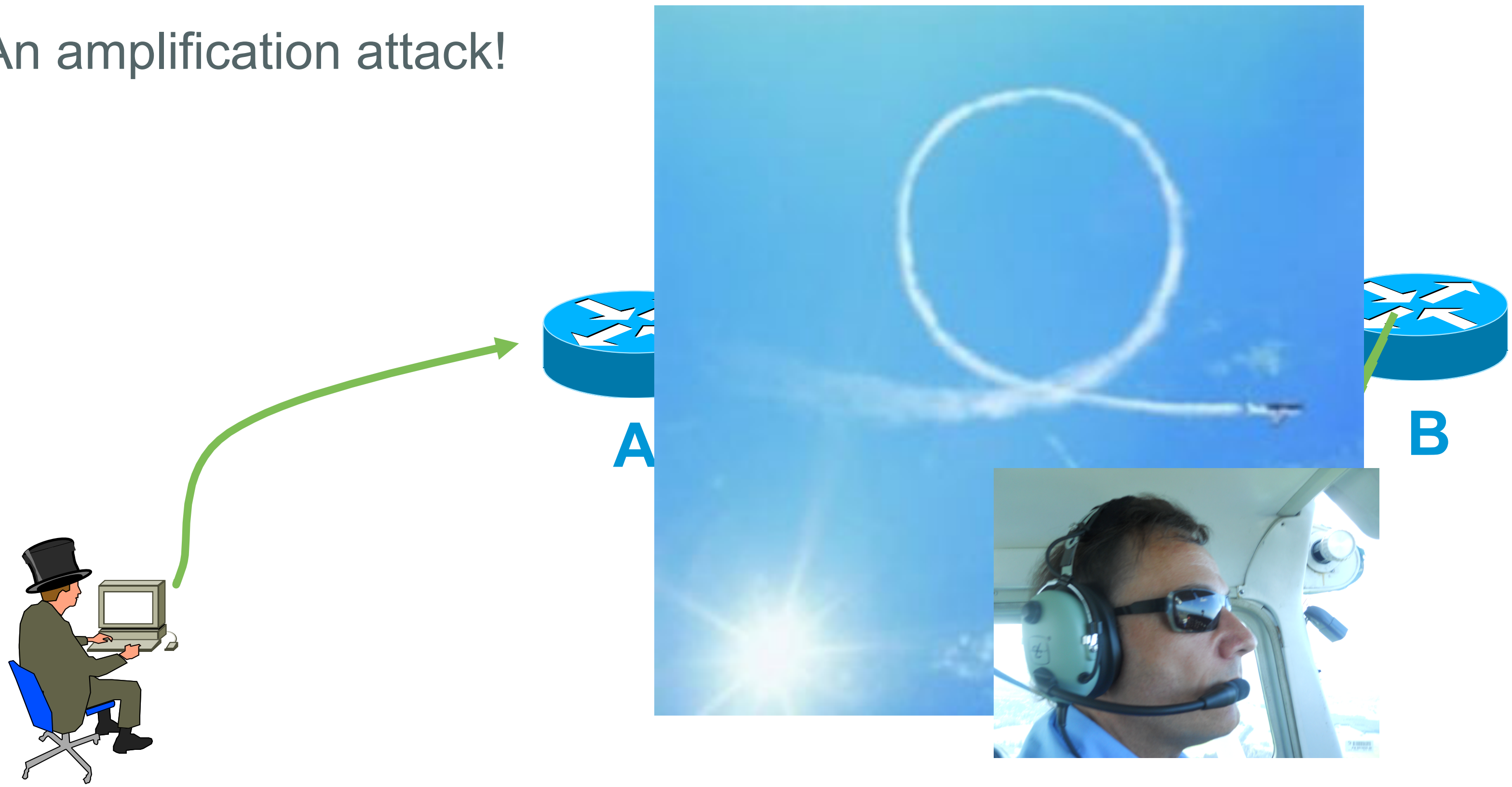


Type 0 Routing Header Amplification Attack

- 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 A-B
- An amplification attack!



Preventing Routing Header Attacks

- Apply same policy for IPv6 as for Ipv4:
  - Block Routing Header type 0
- Prevent processing at the intermediate nodes
  - ***no ipv6 source-route***
  - Windows, Linux, Mac OS: default setting
  - IOS-XR before 4.0: a bug prevented the processing of RH0
  - IOS before 12.4(15)T: by default RH0 were processed
- At the edge
  - With an ACL blocking routing header
- RFC 5095 (Dec 2007) RH0 is deprecated
  - Default changed in IOS 12.4(15)T and IOS-XR 4.0 to ignore and drop RH0

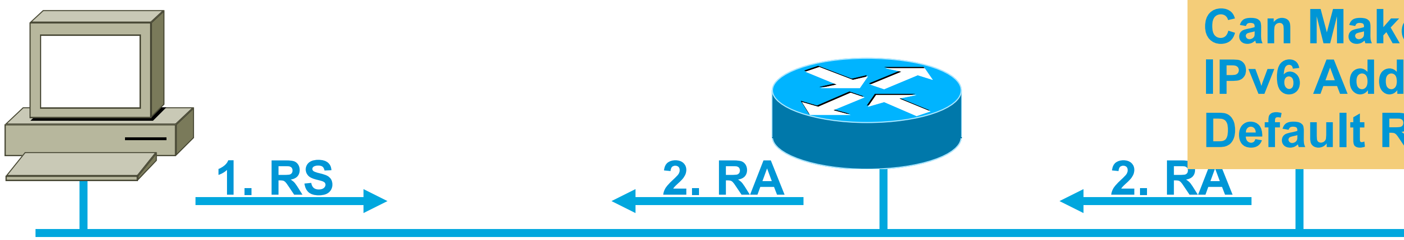
Neighbor Discovery Issue#1 Stateless Autoconfiguration

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

Neighbor Discovery Issue#2
Neighbor Solicitation

Security Mechanisms Built into Discovery Protocol = None

=> Very similar to ARP

Src = A
Dst = Solicited-node multicast of B
ICMP type = 135
Data = link-layer address of A
Query: what is your link address?

Src = B
Dst = A
ICMP type = 136
Data = link-layer address of B

A and B Can Now Exchange Packets on This Link

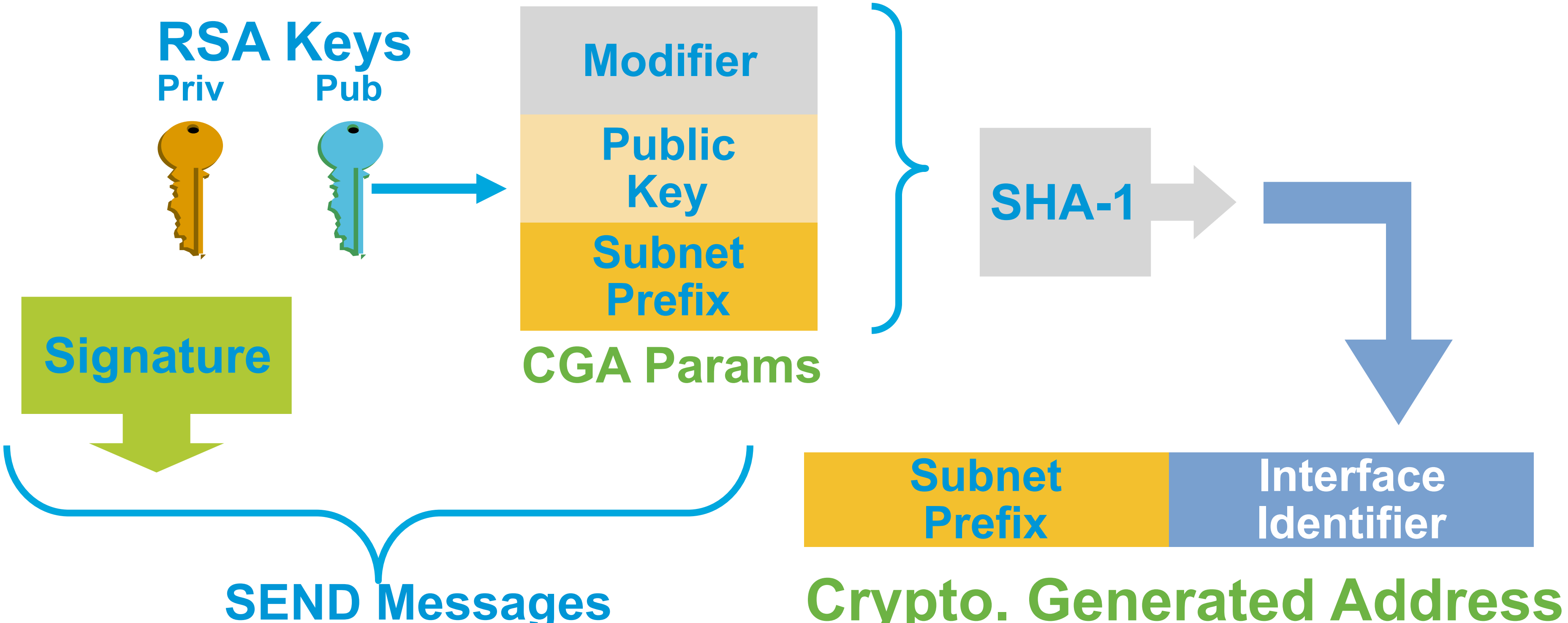
Attack Tool: **Parasite6**
Answer to all NS, Claiming to Be All Systems in the LAN...

ARP Spoofing is now NDP Spoofing: Mitigation

- **SEMI-BAD NEWS**: nothing yet like dynamic ARP inspection for IPv6
  - First phase (Port ACL & RA Guard) available since Summer 2010
  - Second phase (NDP & DHCP snooping) starting to be available since Summer 2011
  - http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-first_hop_security.html
- **GOOD NEWS**: Secure Neighbor Discovery
  - SEND = NDP + crypto
  - IOS 12.4(24)T
  - But not in Windows Vista, 2008 and 7, Mac OS/X, iOS, Android
  - Crypto means slower...
- Other **GOOD NEWS**:
  - Private VLAN works with IPv6
  - Port security works with IPv6
  - 801.x works with IPv6 (except downloadable ACL)

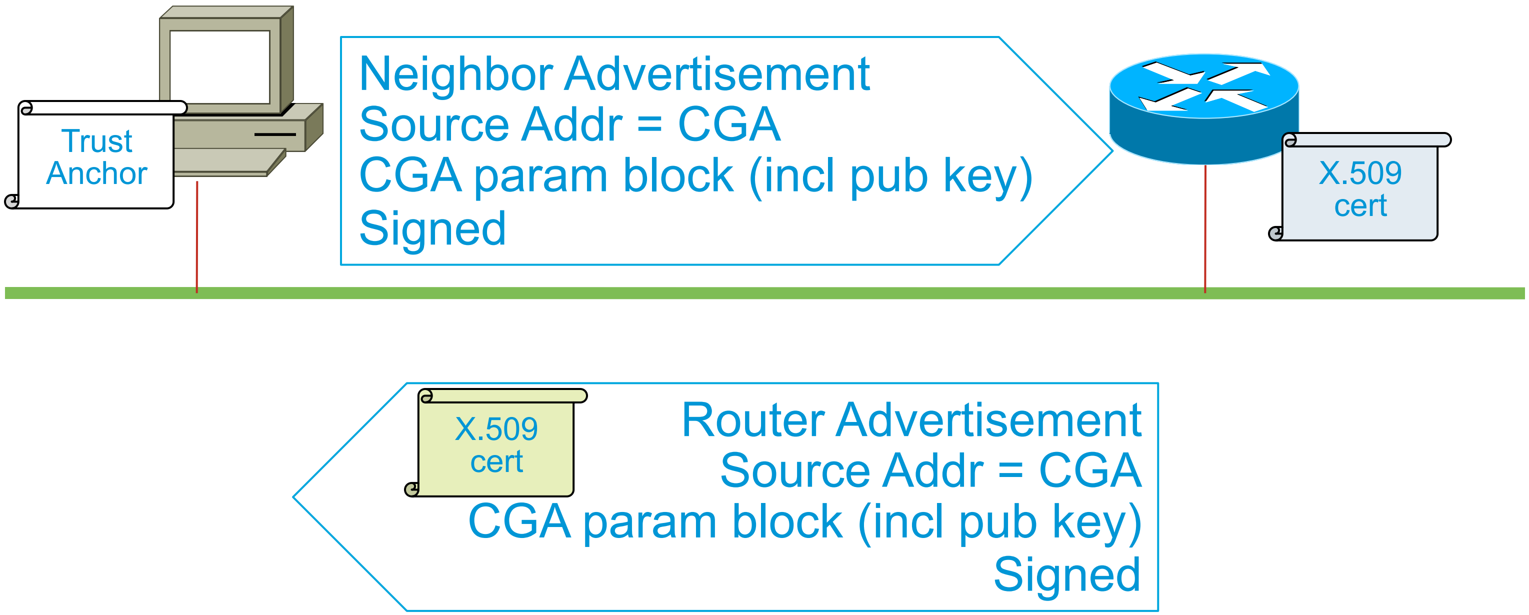
Cryptographically Generated Addresses CGA RFC 3972 (Simplified)

- Each devices has a RSA key pair (no need for cert)
- Ultra light check for validity
- Prevent spoofing a valid CGA address



Securing Neighbor and Router Advertisements with SEND

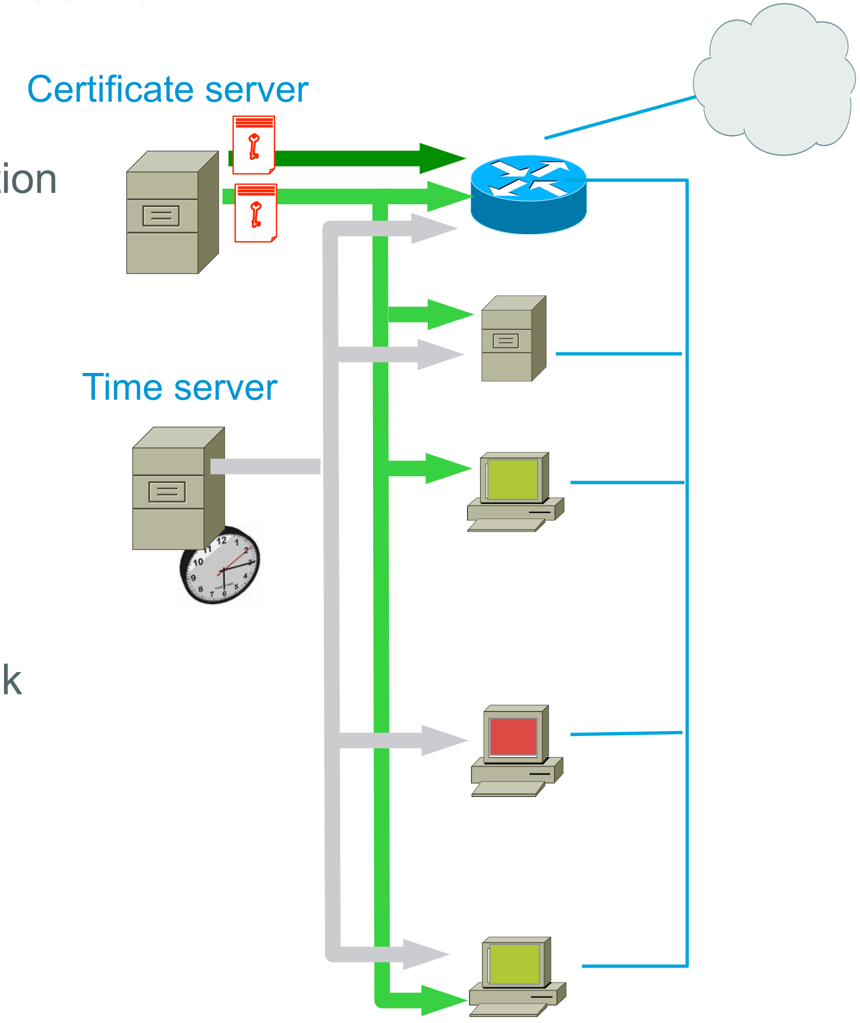
- Adding a X.509 certificate to RA
- Subject Name contains the list of authorized IPv6 prefixes



Securing Link Operations: on Nodes as per Original Specification ?

- **Advantages**
  - No central administration, no central operation
  - No bottleneck, no single-point of failure
  - Intrinsic part of the link-operations
  - Efficient for threats coming from the link

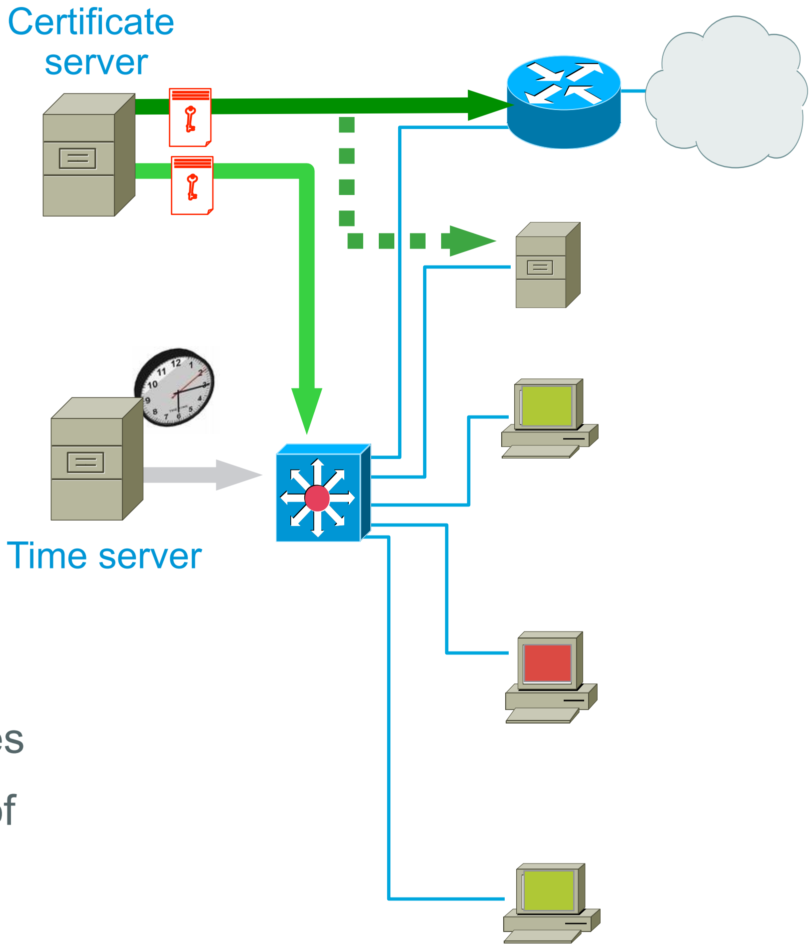
- **Disadvantages**
  - Heavy provisioning of end-nodes
  - Poor for threats coming from outside the link
  - Bootstrapping issue
  - Complexity spread all over the domain.
  - Transitioning quite painful



Securing Link Operations: First Hop Trusted Device

Cisco Short Term Roadmap SAVI WG@IETF

- **Advantages**
  - central administration, central operation
  - Complexity limited to first hop
  - Transitioning lot easier
  - Efficient for threats coming from the link
  - Efficient for threats coming from outside
- **Disadvantages**
  - Applicable only to certain topologies
  - Requires first-hop to learn about end-nodes
  - First-hop is a bottleneck and single-point of failure

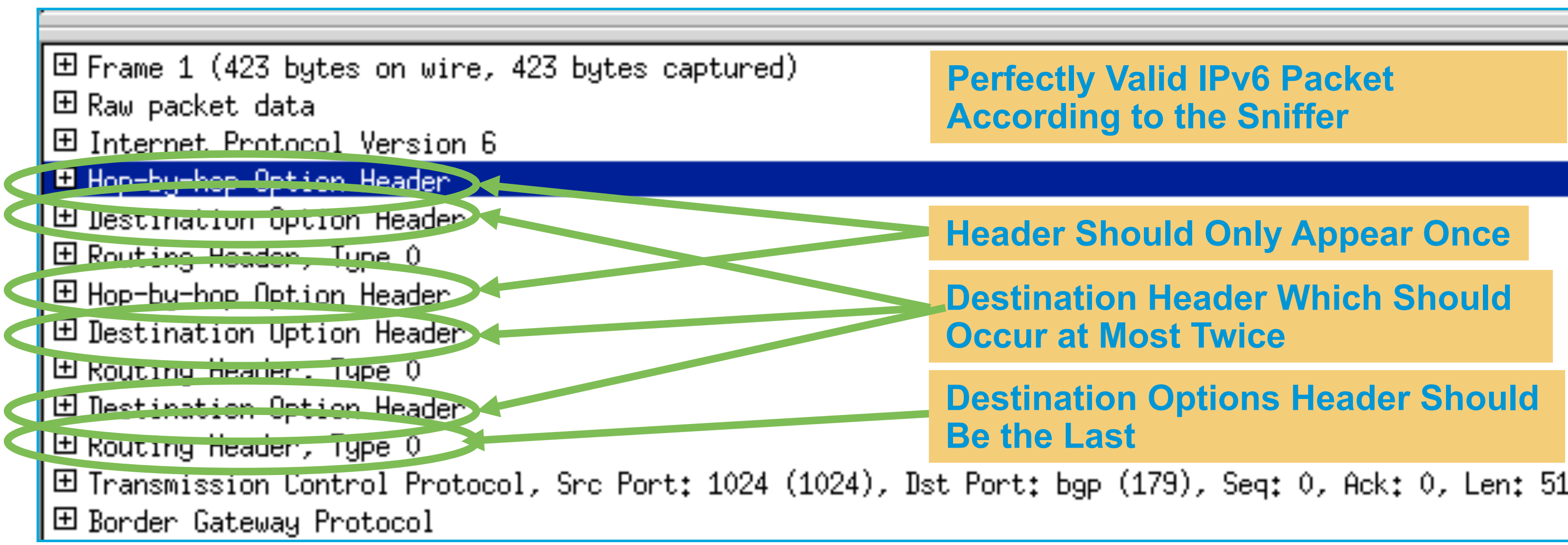


IPv6 Header Manipulation

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

  More boundary conditions to exploit

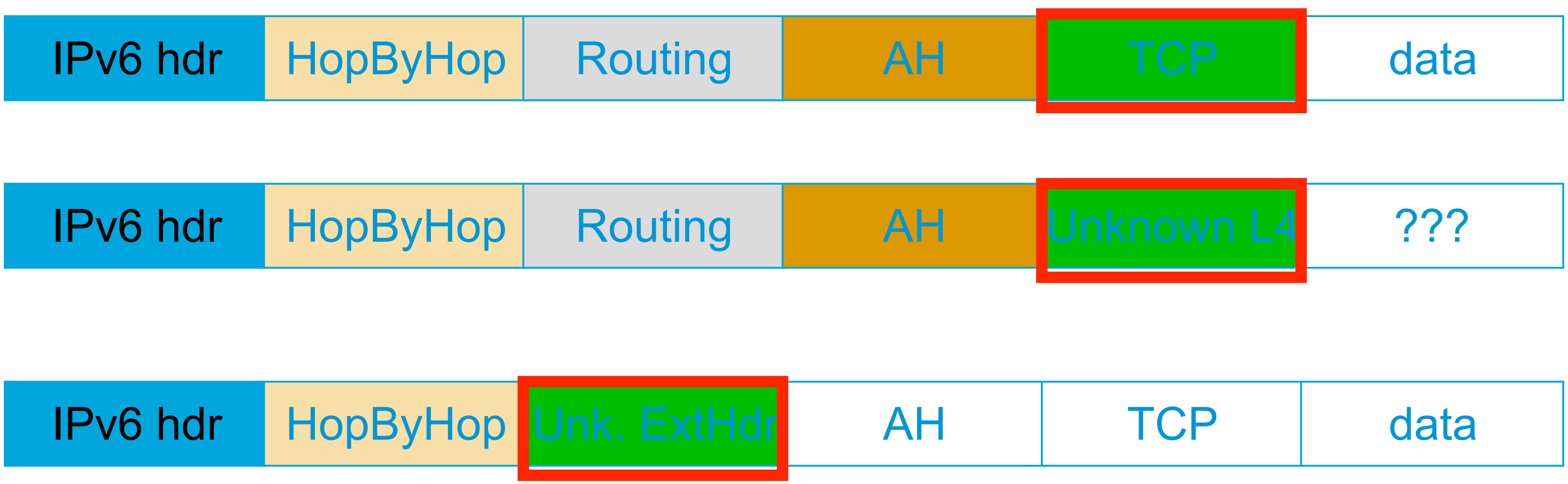
  Can I overrun buffers with a lot of extension headers?



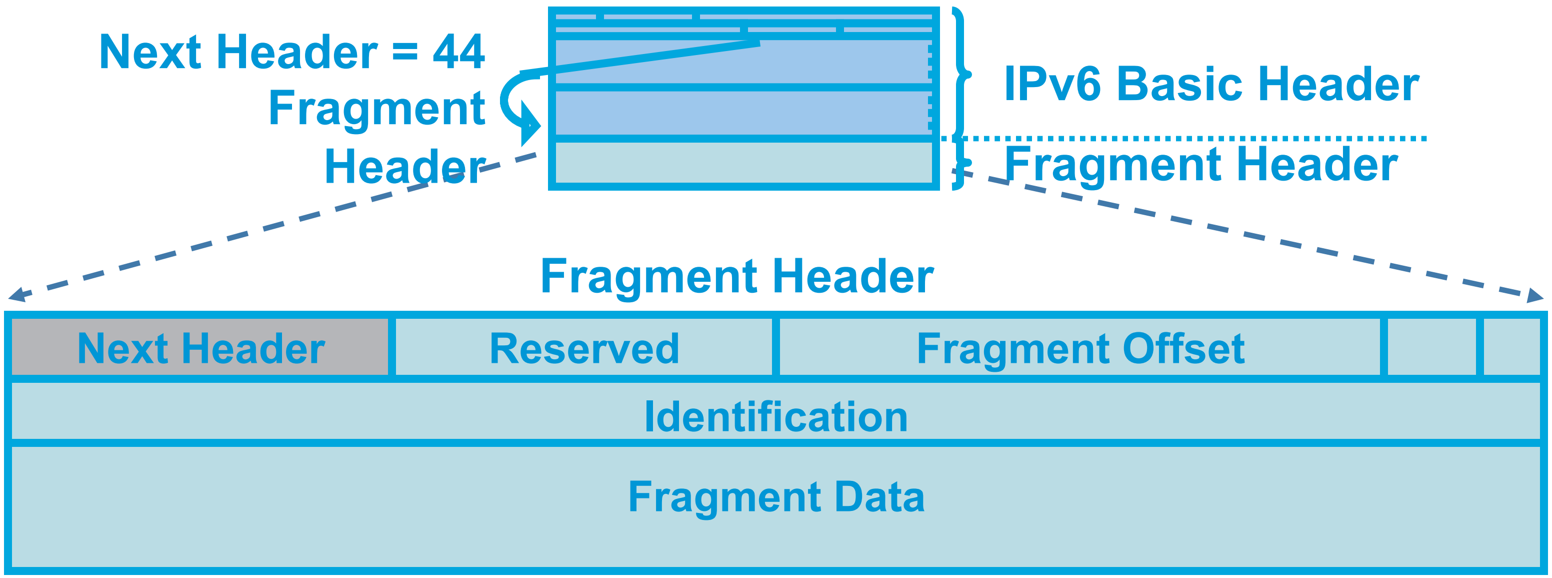
See also: http://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8054d37d.html

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**



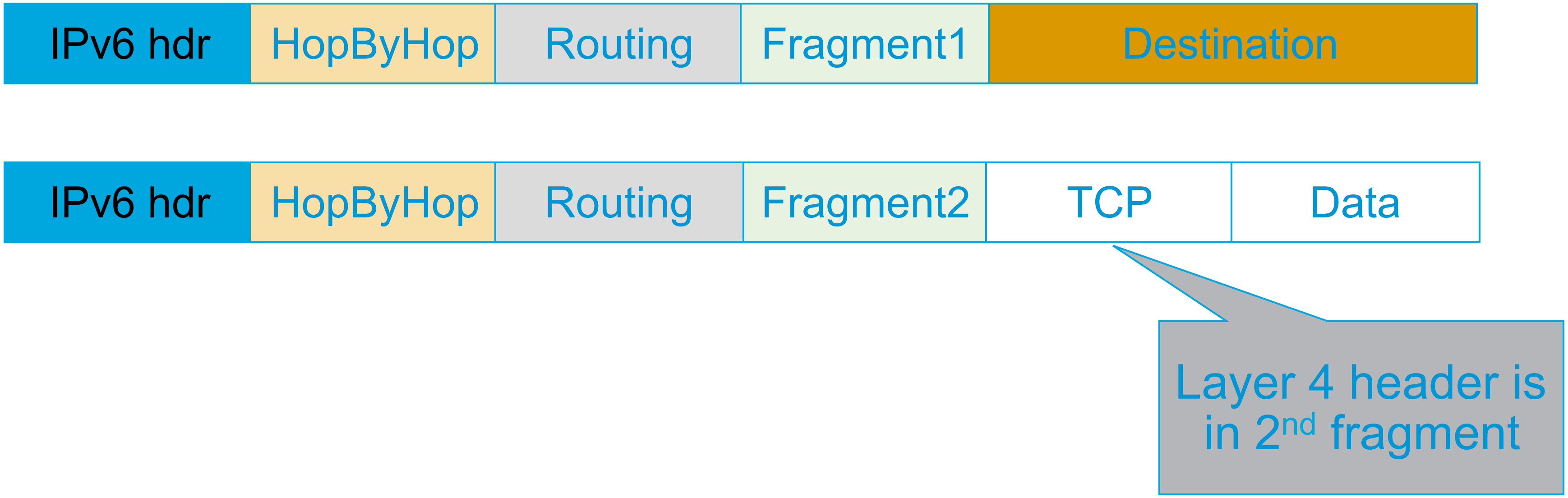
Fragment Header: IPv6



- In IPv6 fragmentation is done only by the end system
  - Tunnel end-points are end systems => Fragmentation / re-assembly can happy inside the network
- Reassembly done by end system like in IPv4
- RFC 5722: overlapping fragments => MUST drop the packet. Alas, not implemented by popular OS
- Attackers can still fragment in intermediate system on purpose
- ==> a great obfuscation tool

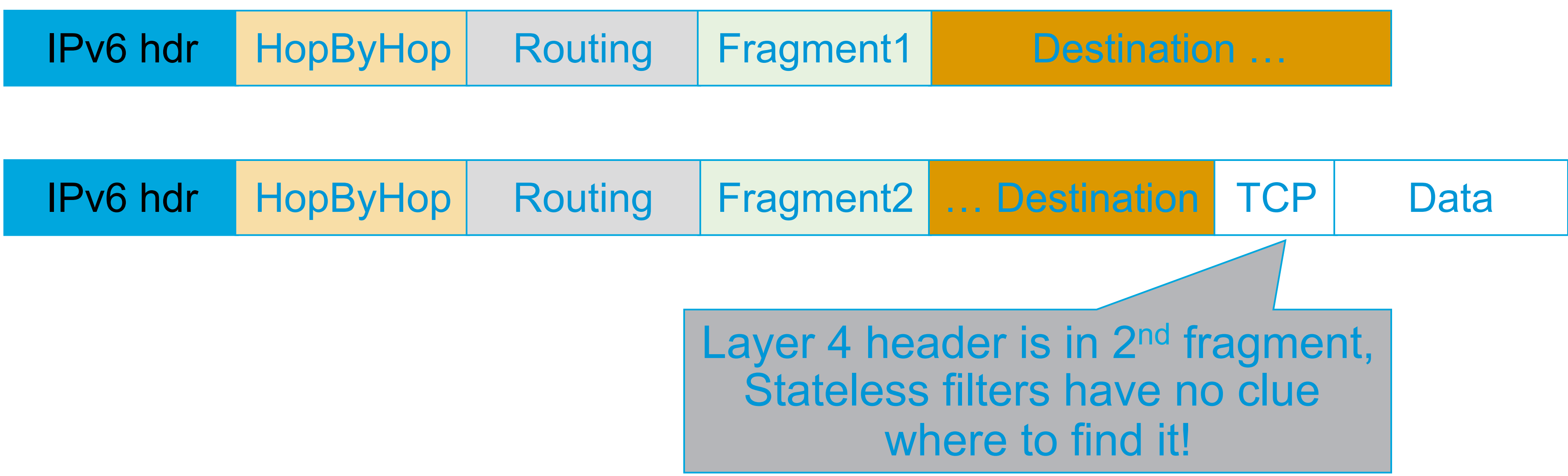
Parsing the Extension Header Chain Fragmentation Matters!

- Extension headers chain can be so large than it is 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

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

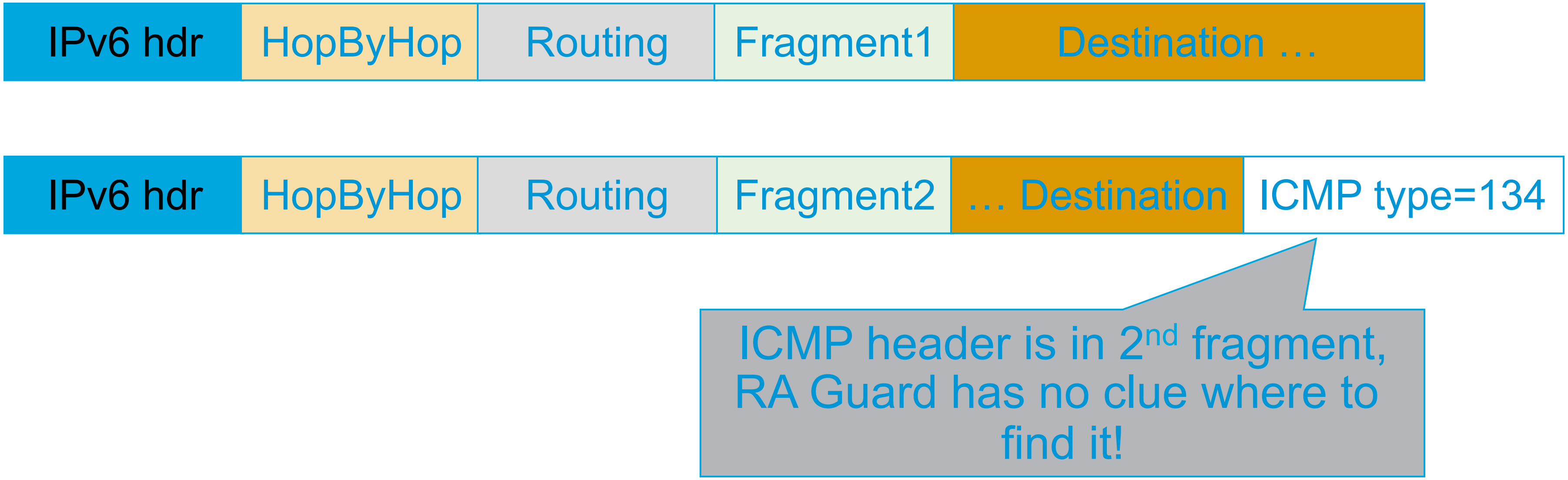


IPv6 Fragmentation & IOS ACL Fragment Keyword

- This makes matching against the first fragment non-deterministic:
  - layer 4 header might not be there but in a later fragment
  - ⇒Need for stateful inspection
- `fragment` keyword matches
  - Non-initial fragments (same as IPv4)
  - And the first fragment if the L4 protocol cannot be determined
- `undertermined-transport` keyword matches
  - Only for deny ACE
  - first fragment if the L4 protocol cannot be determined

Parsing the Extension Header Chain
Fragments and Stateless Filters (RA Guard)

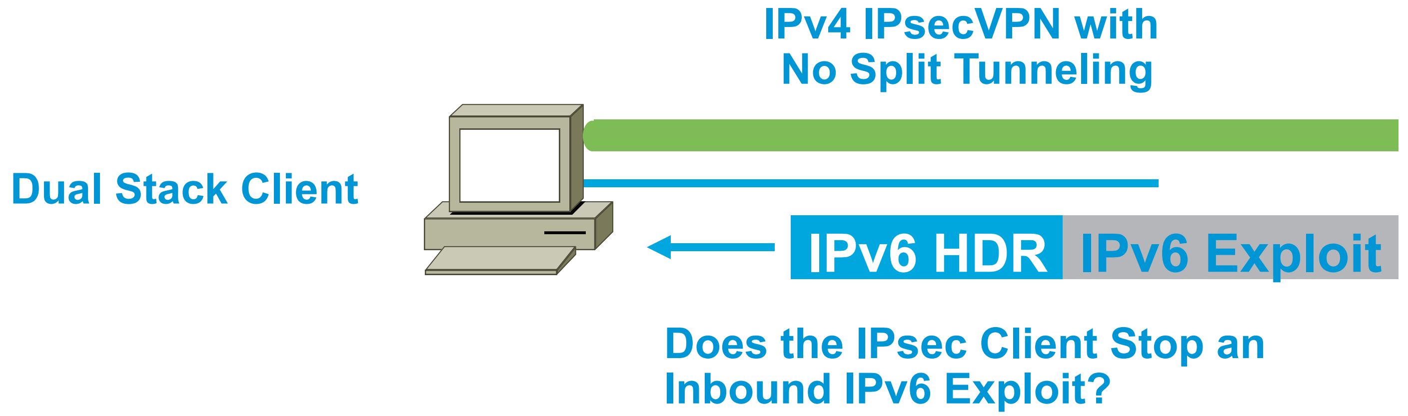
- RFC 3128 is not applicable to IPv6, extension header can be fragmented
- ICMP header could be in 2nd fragment after a fragmented extension header
- RA Guard works like a stateless ACL filtering ICMP type 134
- THC **`fake_router6 -FD`** implements this attack which bypasses RA Guard
- Partial work-around: block all fragments sent to ff02::1



Transition to IPv6 Issues

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.



Getting Bored at the BRU Airport…

Santé ! Gezonheid ! Cheers!

But a glass longs only 10 minutes

Bored again…

Still Bored at BRU Airport

```
$ ifconfig en1
en1: flags=8863<UP,BROADCAS                              TICAST> mtu 1500
        ether 00:26:bb:
        inet6 fe80::226:                              4 scopeid 0x6
        inet 10.19.19.11                             cast 10.19.19.255
        media: autoselect
        status: active
```

Humm…
Is there an
IPv6 Network?

```
$ ping6 -I en1 ff02::1%en1
PING6(56=40+8+8 bytes) fe80::226:bb                    ff02::1
16 bytes from fe80::226:                               =64 time=0.140 ms
. . .
16 bytes from fe80::ca                                 m=64 time=402.112 ms
^C
--- ff02::1%en1 ping6 statistics ---
4 packets transmitted, 4 packets received, +142 duplicates, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.140/316.721/2791.178/412.276 ms
```

Humm…
Are there any IPv6
peers?

```
$ ndp -an
Neigh                                                                  bs
200
. .
$ ndp
     64
```

Let's have some fun here… Configure
a tunnel, enable forwarding and
transmit RA

Dual Stack with Enabled IPv6 by Default

- Your host:
  - IPv4 is protected by your favorite personal firewall...
  - IPv6 is enabled by default (Vista, Linux, Mac OS/X, ...)
- 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

Looping Attack Between 2 ISATAP routers

1. Spoofed IPv6 packet
S: 2001:db8:2::200:5efe:c000:201
D: 2001:db8:1::200:5efe:c000:202

ISATAP router 1
Prefix 2001:db8:1::/64
192.0.2.1

ISATAP router 2
Prefix 2001:db8:2::/64
192.0.2.2

2. IPv4 ISATAP packet to 192.0.0.2 containing
S: 2001:db8:2::200:5efe:c000:201
D: 2001:db8:1::200:5efe:c000:202

3 IPv6 packet
S: 2001:db8:2::200:5efe:c000:201
D: 2001:db8:1::200:5efe:c000:202

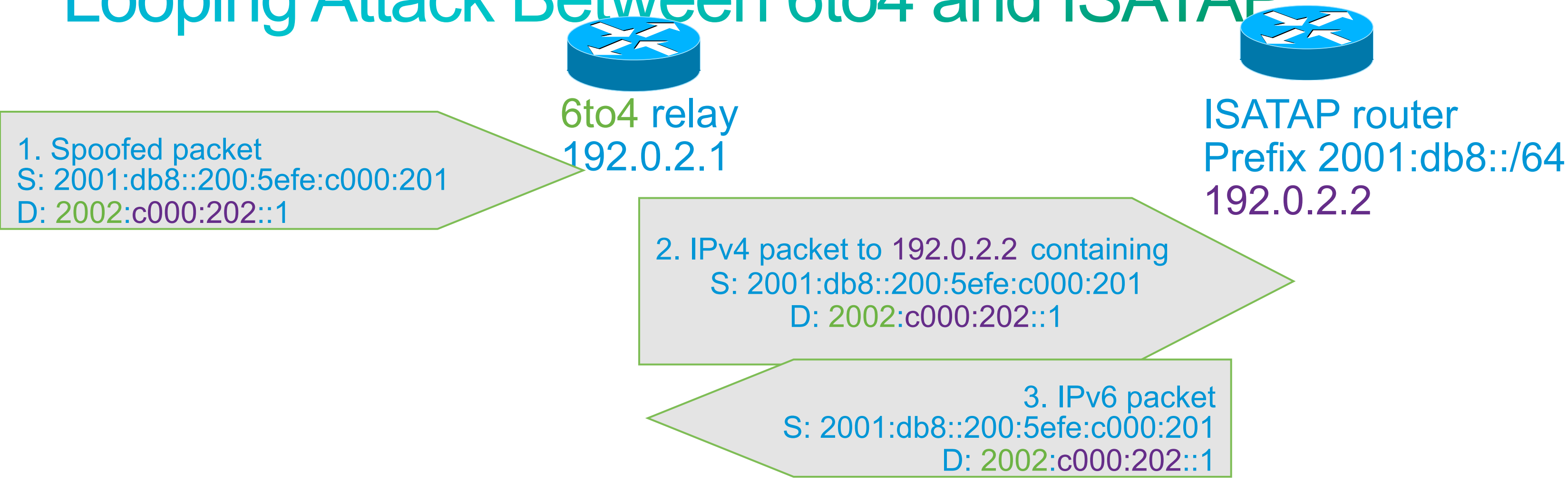
Repeat until Hop Limit == 0

- Root cause
  - ISATAP routers ignore each other
- ISATAP router:
  - accepts native IPv6 packets
  - forwards it inside its ISATAP tunnel
  - Other ISATAP router decaps and forward as native IPv6

Mitigation:
- IPv6 anti-spoofing everywhere
- ACL on ISATAP routers accepting IPv4 from valid clients only
- Within an enterprise, block IPv4 ISATAP traffic between ISATAP routers
- Within an enterprise block IPv6 packets between ISATAP routers

http://www.usenix.org/events/woot09/tech/full_papers/nakibly.pdf

Looping Attack Between 6to4 and ISATAP



Repeat until Hop Limit == 0

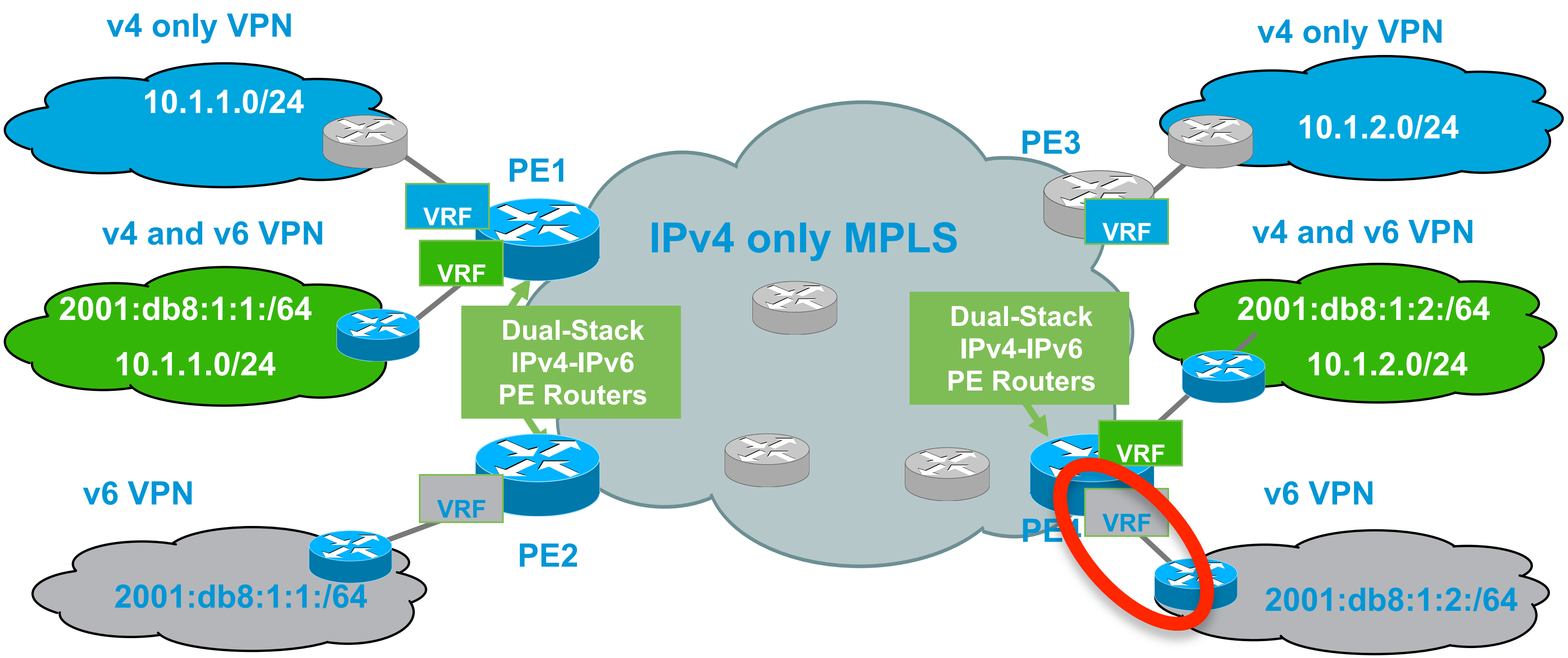
- Root cause
  - Same IPv4 encapsulation (protocol 41)
  - Different ways to embed IPv4 address in the IPv6 address
- ISATAP router:
  - accepts 6to4 IPv4 packets
  - Can forward the inside IPv6 packet back to 6to4 relay
- Symmetric looping attack exists

Mitigation:
•Easy on ISATAP routers: deny packets whose IPv6 is its 6to4
•Less easy on 6to4 relay: block all ISATAP-like local address?
•Enterprise block all protocol 41 at the edge which are not known tunnels
•Good news: not so many open ISATAP routers on the Internet

http://www.usenix.org/events/woot09/tech/full_papers/nakibly.pdf

SP Transition Mechanism: 6VPE

- 6VPE: the MPLS-VPN extension to also transport IPv6 traffic over a MPLS cloud and IPv4 BGP sessions



6VPE Security

- 6PE (dual stack without VPN) is a simple case
- Security is identical to IPv4 MPLS-VPN, see RFC 4381
- Security depends on correct operation and implementation
  - QoS prevent flooding attack from one VPN to another one
  - PE routers must be secured: AAA, iACL, CoPP …
- MPLS backbones can be more secure than “normal” IP backbones
  - Core not accessible from outside
  - Separate control and data planes
- PE security
  - Advantage: Only PE-CE interfaces accessible from outside
  - Makes security easier than in “normal” networks
  - **IPv6 advantage: PE-CE interfaces can use link-local for routing**
    - **=> completely unreachable from remote (better than IPv4)**

Security Controls DO Exist in 2011!
For Example Summary of Cisco IPv6 Security Products

- ASA Firewall
  - Since version 7.0 (released 2005)
  - Flexibility: Dual stack, IPv6 only, IPv4 only
  - SSL VPN for IPv6 (ASA 8.0)
  - Stateful-Failover (ASA 8.2.2)
  - Extension header filtering and inspection (ASA 8.4.2)
- FWSM
  - IPv6 in software... 80 Mbps … Not an option (put an IPv6-only ASA in parallel or migrate to ASA-SM)
- IOS Firewall
  - IOS 12.3(7)T (released 2005)
  - Zone-based firewall on IOS-XE 3.6 (2012)
- IPS
  - Since 6.2 (released 2008), management over IPv6: Q1 2012
- Email Security Appliance (ESA) under beta testing early 2010, shipping Q4 2011
- Web Security Appliance (WSA) Q1 2012
- ScanSafe Q1 2012

Security Controls DO Exist in 2011! Secure IPv6 over IPv4/6 Public Internet

- No traffic sniffing
- No traffic injection
- No service theft

Public Network	Site 2 Site	Remote Access
IPv4	▪6in4/GRE Tunnels Protected by IPsec ▪DMVPN 12.4(20)T	▪ ISATAP Protected by RA IPsec ▪ SSL VPN Client AnyConnect
IPv6	•IPsec VTI 12.4(6)T •*DMVPN 15.2(1)T*	*Any Connect H1 2012*

Best Common Practices

Candidate Best Practices

For Your Reference

- **Train your network operators and security managers on IPv6**
- **Selectively filter ICMP** (RFC 4890)
- Implement RFC 2827-like filtering
- Block Type 0 Routing Header at the edge
- Determine what extension headers will be allowed through the access control device
- Use traditional authentication mechanisms on BGP and IS-IS
- Use IPsec to secure protocols such as OSPFv3 and RIPng
- Document procedures for last-hop traceback

Candidate Best Practices (Cont.)

For Your Reference

- Implement privacy extensions carefully
- Filter internal-use IPv6 addresses & ULA at the border routers
- Filter unneeded services at the firewall
- Maintain host and application security
- Use cryptographic protections where critical
- Implement ingress filtering of packets with IPv6 multicast source addresses
- Use static tunneling rather than dynamic tunneling
- Implement outbound filtering on firewall devices to allow only authorized tunneling endpoints

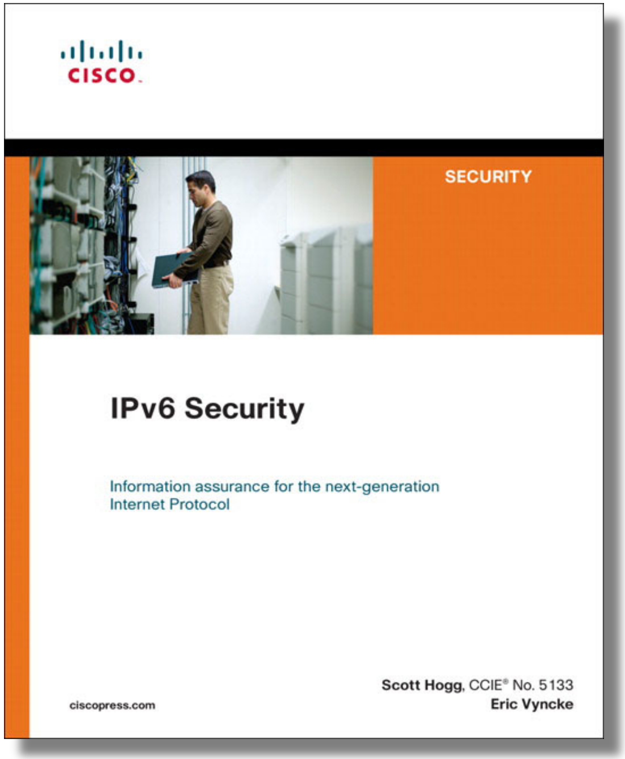
Summary

Key Take Away

- So, nothing really new in IPv6
  - Reconnaissance: address enumeration replaced by DNS enumeration
  - Spoofing & bogons: uRPF is our IP-agnostic friend
  - NDP spoofing: RA guard and more feature coming
  - Extension headers: firewall & ACL can process them
  - Amplification attacks by multicast mostly impossible
  - Potential loops between tunnel endpoints: ACL must be used
- Lack of operation experience may hinder security for a while: **training is required**
- Security enforcement is possible
  - Control your IPv6 traffic as you do for IPv4
- Leverage IPsec to secure IPv6 when suitable

Questions and Answers?

Recommended Reading



Source: Cisco Press

Congratulations!

I am trusting you that those sites are 99.99% secure…

Thank you.