IPv6 Security Threats and Mitigations

Andy Chien (錢小山)

Customer Solutions Architect

Cisco Systems

Nov-22-2012

Agenda

- Debunking IPv6 Myths
- Shared Security Issues by IPv4 and IPv6
- Specific Security Issues for IPv6
  - IPsec everywhere, dual-stack, tunnels and 6VPE
- Enforcing a Security Policy in IPv6
  - ACL, Firewalls and IPS
- Secure IPv6 Connectivity
  - Secure IPv6 transport over public network

IPv6 Myths

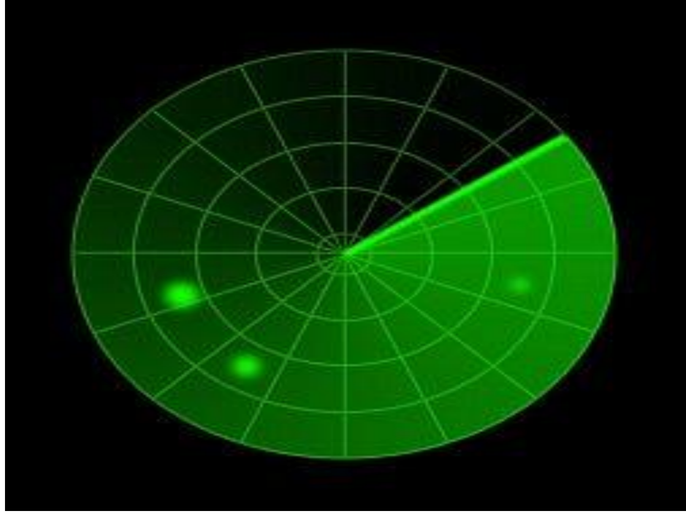
IPv6 Myths: Better, Faster, More Secure

1995: RFC 1883

2012: IPv6

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

Reconnaissance in IPv6
Scanning Methods Are Likely to Change



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

  10 Mpps = more than 50 000 years

- 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

Viruses and Worms in IPv6

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

  IPv4: reliance on network scanning

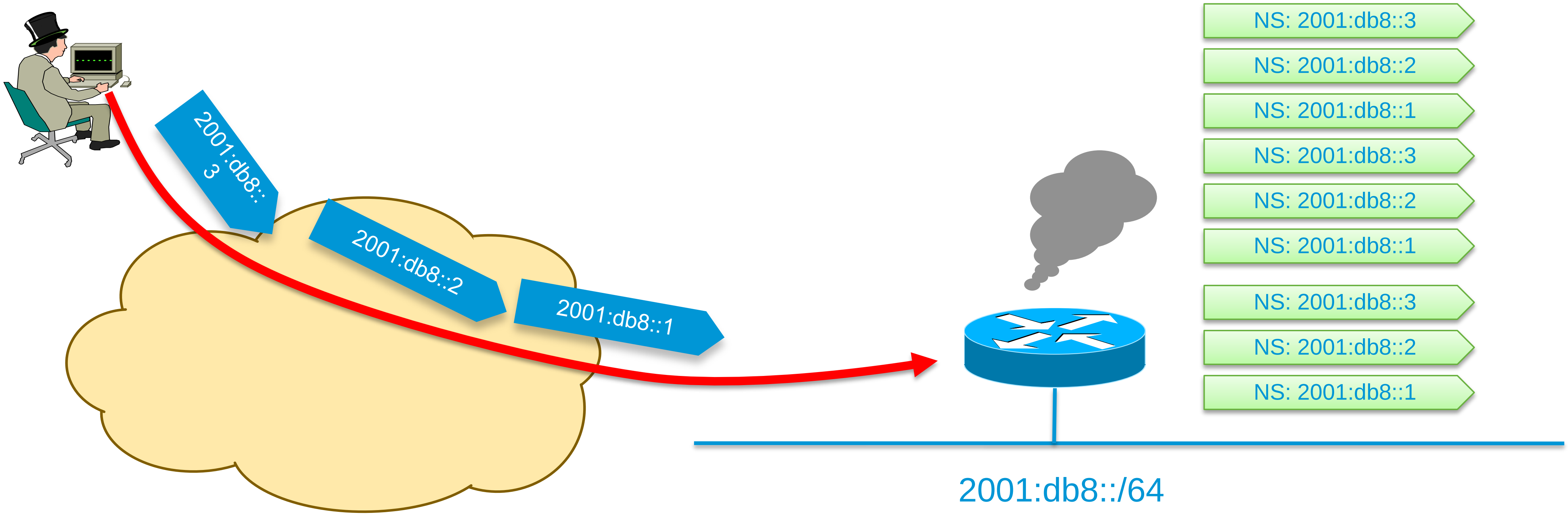
  IPv6: not so easy (see reconnaissance) => will use alternative techniques

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

Scanning Made Bad for CPU
Remote Neighbor Cache Exhaustion

- Potential router CPU/memory attacks if aggressive scanning

    Router will do Neighbor Discovery... And waste CPU and memory



Mitigating Remote Neighbor Cache Exhaustion

- **Built-in rate limiter** but no option to tune it
  - Since 15.1(3)T: `ipv6 nd cache interface-limit`
  - Or IOS-XE 2.6: `ipv6 nd resolution data limit`
  - Destination-guard is coming with First Hop Security phase 3
- 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 ☺

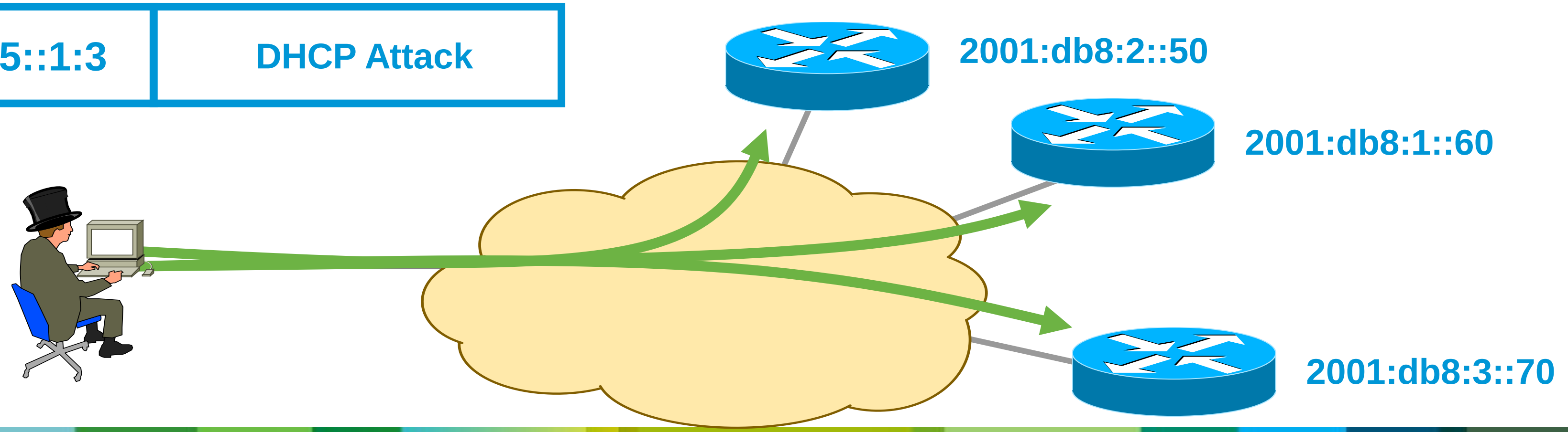
Reconnaissance in IPv6? Easy with Multicast!

- No need for reconnaissance anymore
- 3 site-local multicast addresses (not enabled by default)

  FF05::2 all-routers, FF05::FB mDNSv6, FF05::1:3 all DHCP servers
- Several link-local multicast addresses (enabled by default)

  FF02::1 all nodes, FF02::2 all routers, FF02::F all UPnP, …

Source	Destination	Payload
Attacker	FF05::1:3	DHCP Attack



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

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

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*

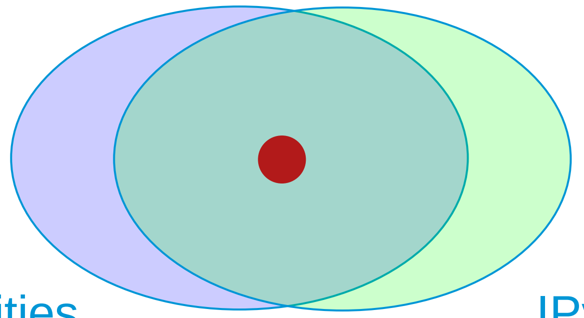
•Rate Limit egress ICMP Packets

•Rate limit ICMP messages generation

•Secure the multicast network (source specific multicast)

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

Shared Issues

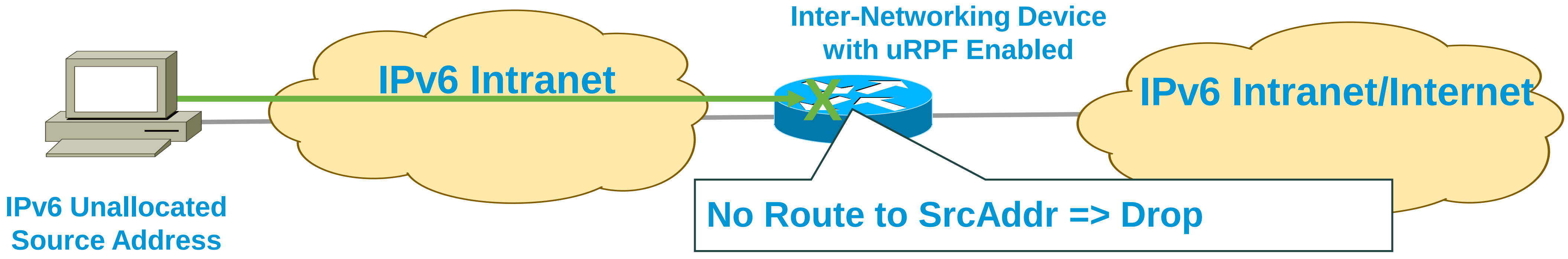


IPv4 Vulnerabilities.

IPv6 Vulnerabilities.

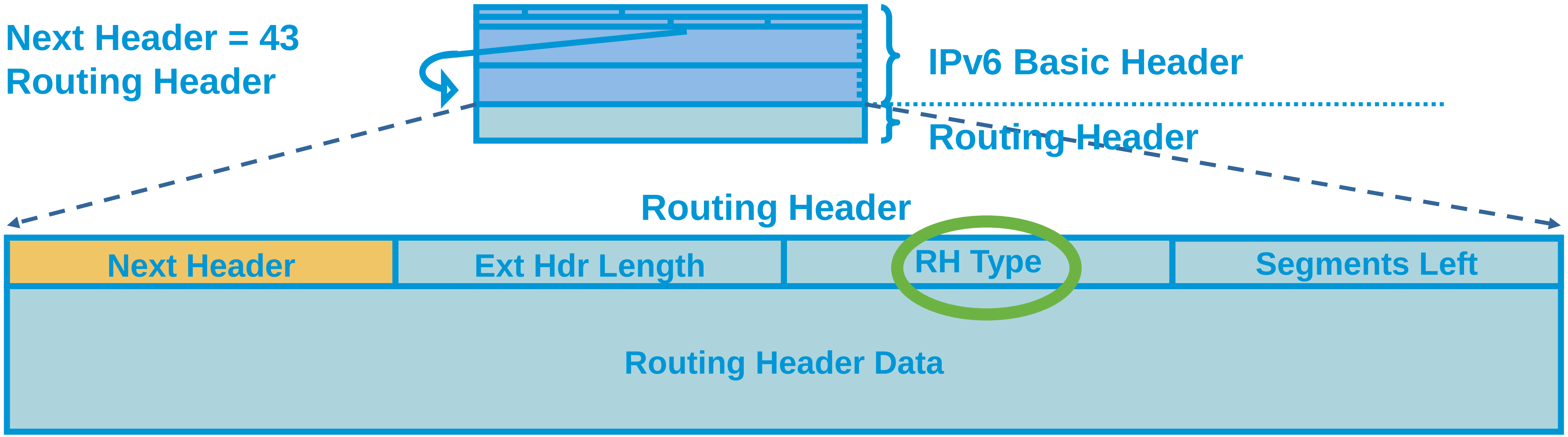
IPv6 Bogon and Anti-Spoofing Filtering

- Bogon filtering (data plane & BGP route-map): http://www.cymru.com/Bogons/ipv6.txt
- Anti-spoofing = uRPF



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



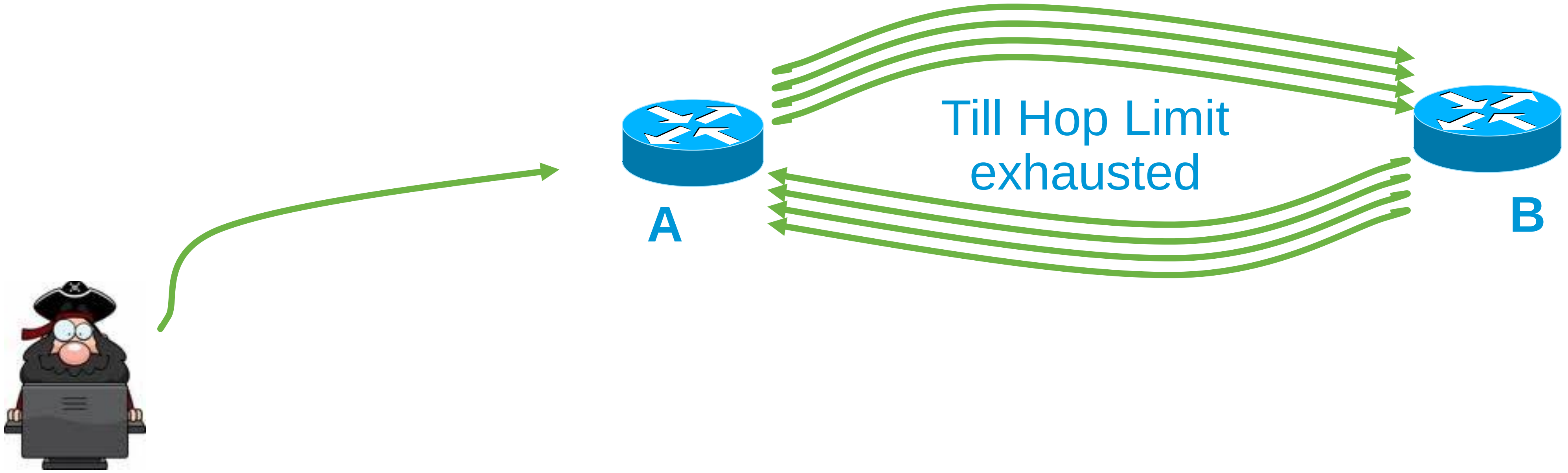
*: http://tools.ietf.org/html/draft-ietf-6man-rpl-routing-header (work in progress, should be OK for security)

Type 0 Routing Header
Issue: 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

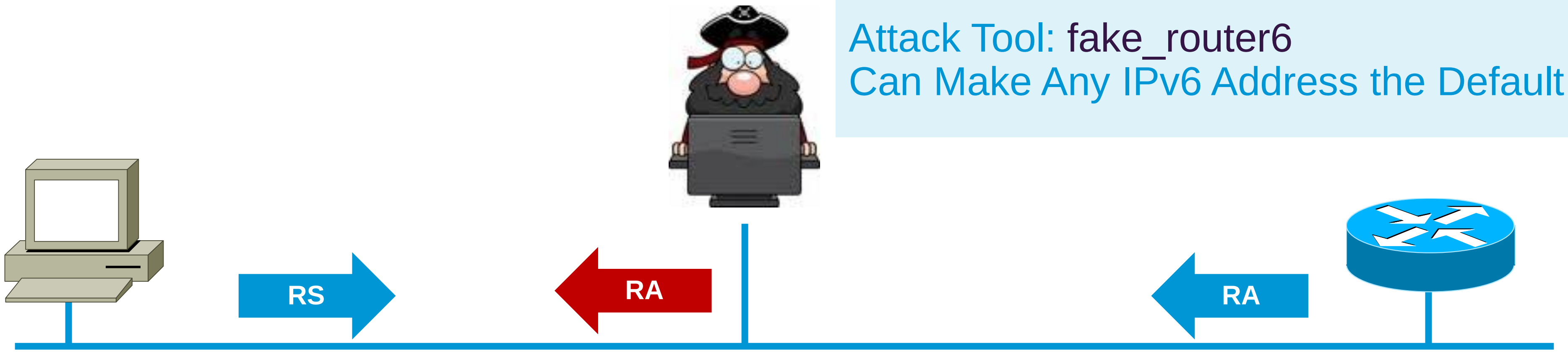
- Apply same policy for IPv6 as for Ipv4:
  - Block Routing Header type 0
- Prevent processing at the intermediate nodes
  - ***no ipv6 source-route***
  - Windows, Linux, Mac OS: default setting
  - IOS-XR before 4.0: a bug prevented the processing of RH0
  - IOS before 12.4(15)T: by default RH0 were 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



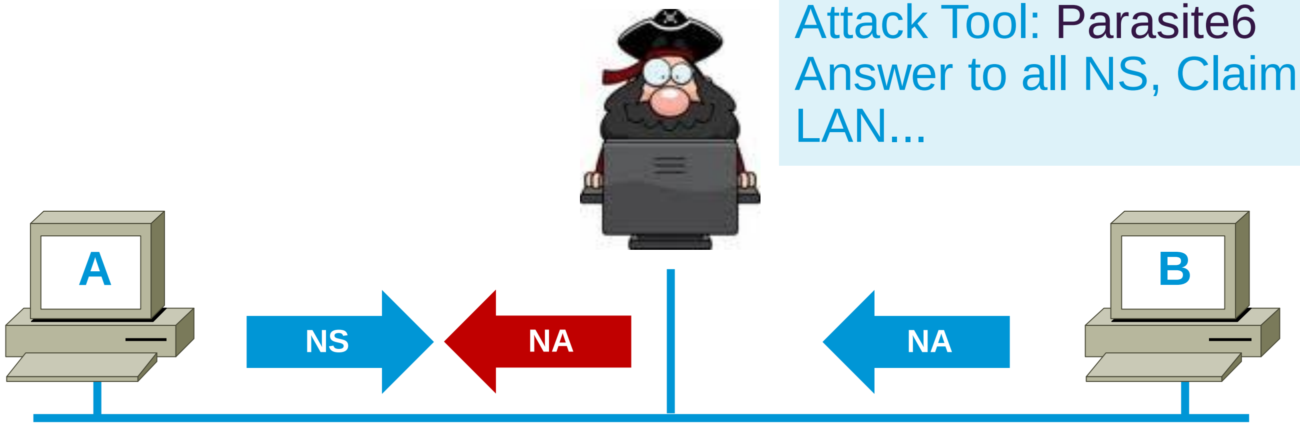
Router Solicitation	
ICMP Type	133
IPv6 Source	A Link Local (FE80::1)
IPv6 Destination	All Routers Multicast (FF02::2)
Query	Please send RA

Router Advertisement	
ICMP Type	134
IPv6 Source	A Link Local (FE80::2)
IPv6 Destination	All Nodes Multicast (FF02::1)
Data	Options, subnet prefix, lifetime, autoconfig flag

Neighbor Discovery Issue#2
Neighbor Solicitation

No Security Mechanisms Built into Discovery Protocol therefore very similar to ARP

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



Neighbour Solicitation	
ICMP Type	135
IPv6 Source	A Unicast
IPv6 Destination	B Solicited Node Multicast
Data	FE80:: address of A
Query	What is B link layer address?

Neighbour Advertisment	
ICMP Type	136
IPv6 Source	B Unicast
IPv6 Destination	A Unicast
Data	FE80:: address of B

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
  - IEEE 802.1X works with IPv6 (except downloadable ACL)

Secure Neighbor Discovery: Caveats

- Private/public key pair on all devices for CGA
- Overhead introduced

  Routers have to do many public/private key calculation (some may be done in advance of use)

  => Potential DoS target

  Routers need to keep more state

- Available:

  Unix (DoCoMo)

  Cisco IOS 12.4(24)T

- Microsoft:

  no support in Vista, Windows 2008 and Windows7

Secure Neighbor Discovery (SeND) RFC 3971

- Certification paths

  Anchored on trusted parties, expected to certify the authority of the routers on some prefixes

- Cryptographically Generated Addresses (CGA)

  IPv6 addresses whose interface identifiers are cryptographically generated

- RSA signature option

  Protect all messages relating to neighbor and router discovery

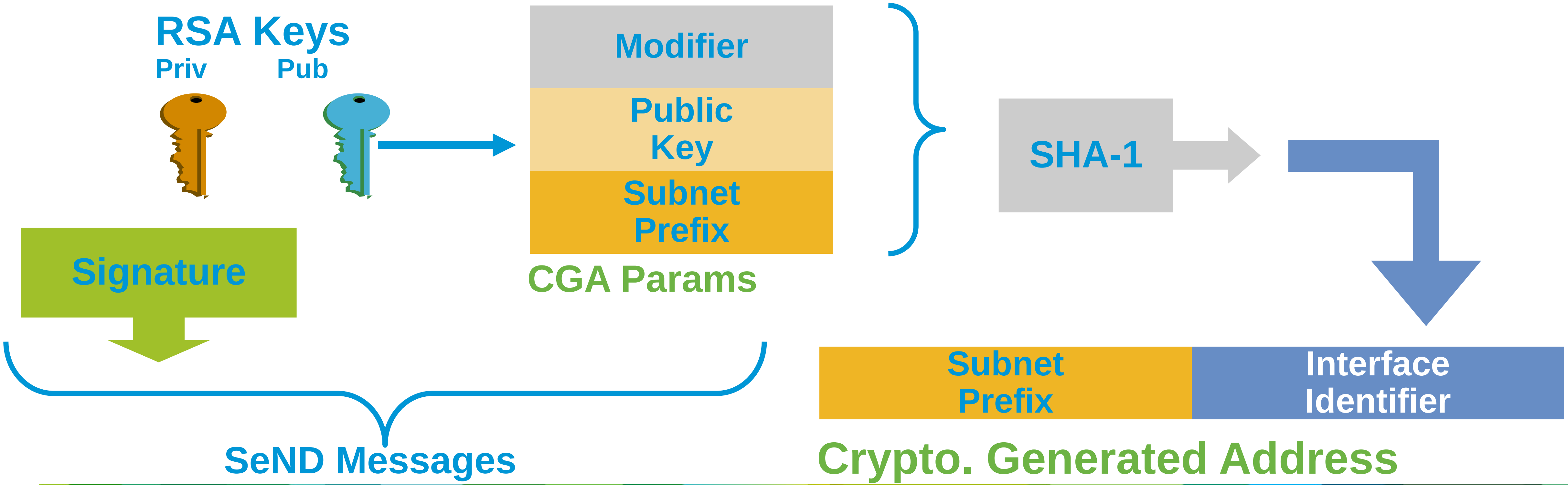
- Timestamp and nonce options

  Prevent replay attacks

- Requires IOS 12.4(24)T

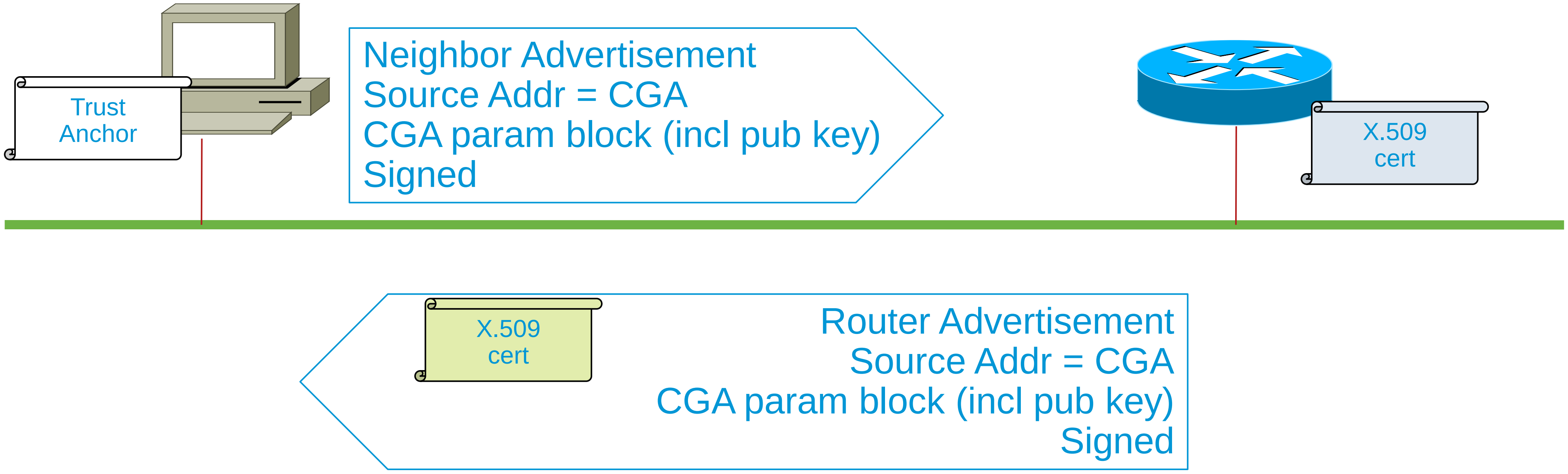
Cryptographically Generated Addresses CGA RFC 3972 (Simplified)

- 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

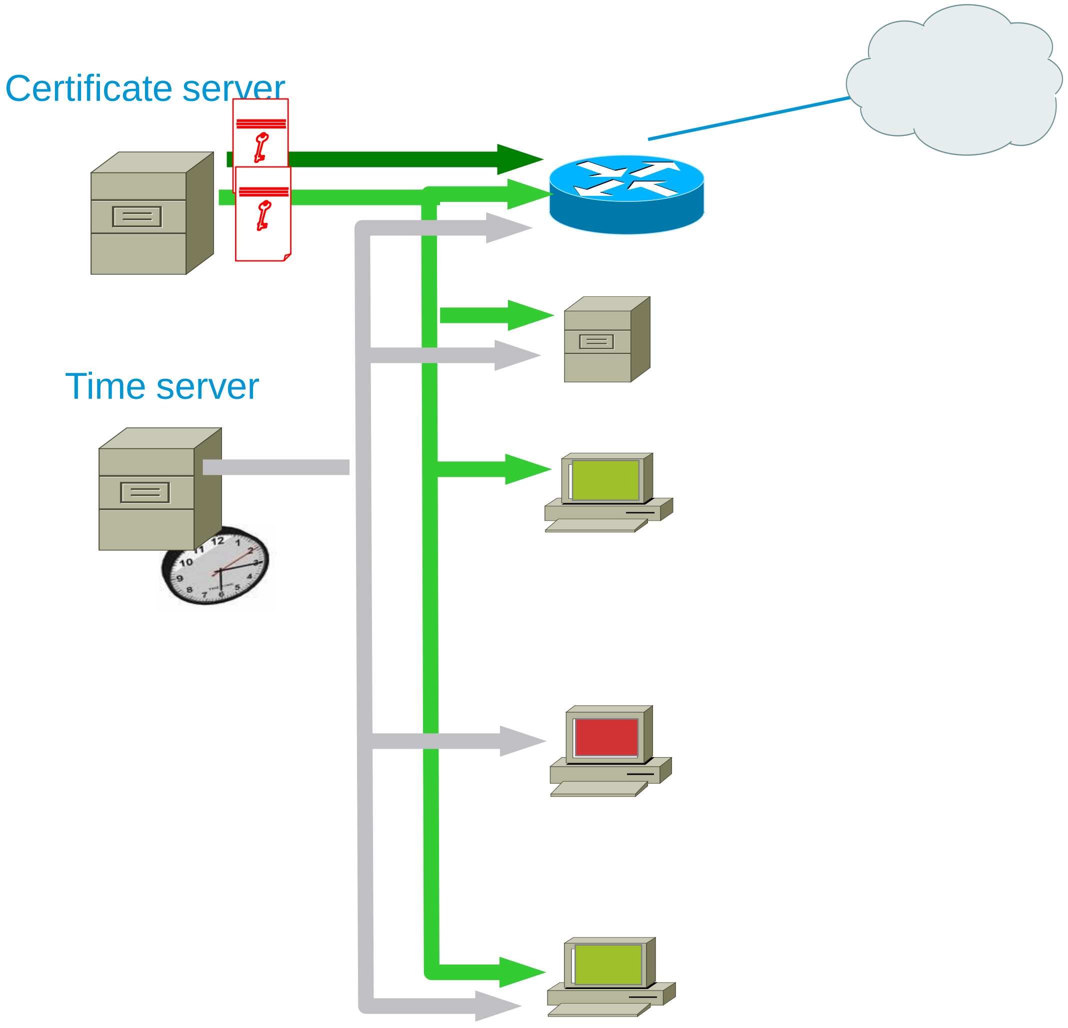
- Adding a X.509 certificate to RA
- Subject Name contains the list of authorized IPv6 prefixes



Securing Link Operations: on Nodes?

- **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

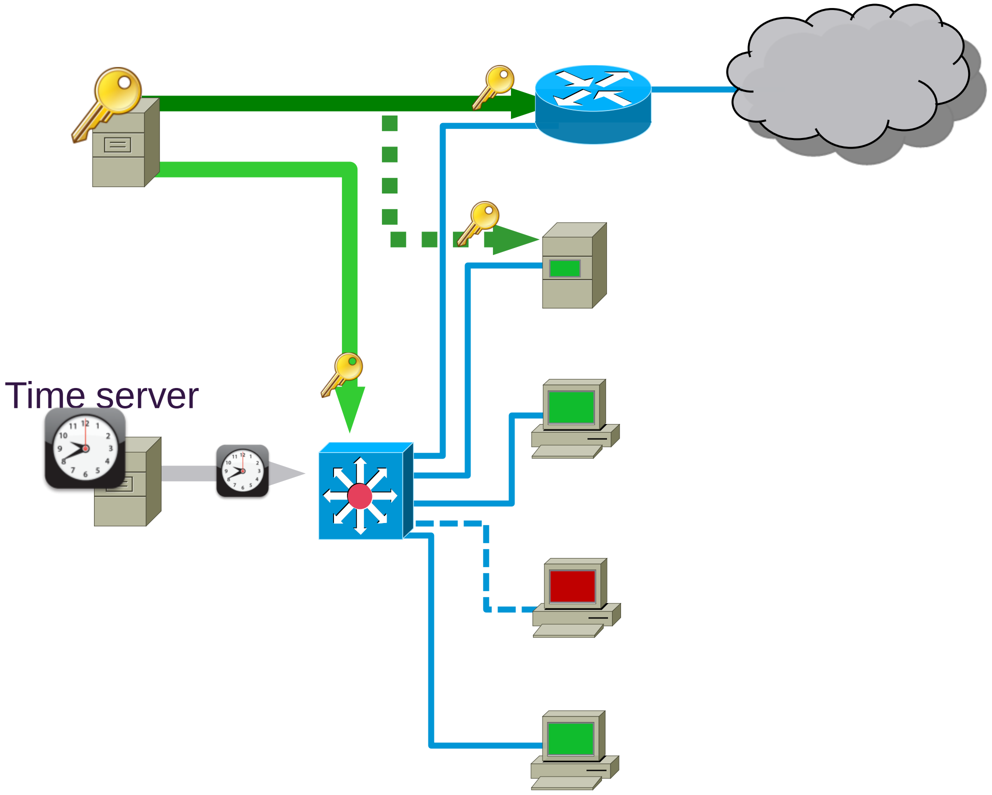
- **Disadvantages**
  - Heavy provisioning of end-nodes
  - Poor for threats coming from outside the link
  - Bootstrapping issue
  - Complexity spread all over the domain.
  - Transitioning quite painful



Securing Link Operations:
First Hop Trusted Device

Cisco Current Roadmap
IETF SAVI WG

- **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

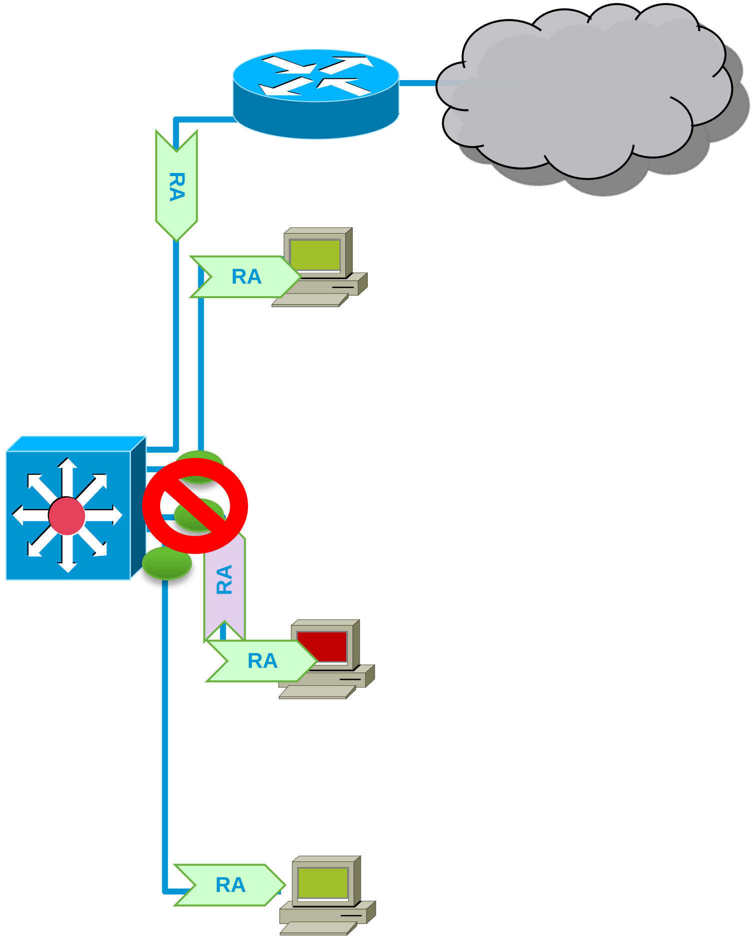
First Hop Security Phase I in 2010
Protecting against Rogue RA

- Port ACL (see later) blocks all ICMPv6 Router Advertisements from hosts

```
interface FastEthernet3/13
  switchport mode access
  ipv6 traffic-filter ACCESS_PORT in
  access-group mode prefer port
```

- RA-guard feature in host mode (12.2(33)SXI4 & 12.2(54)SG): also dropping all RA received on this port

```
interface FastEthernet3/13
  switchport mode access
  ipv6 nd raguard
  access-group mode prefer port
```



IPv6 Snooping Phase II &III

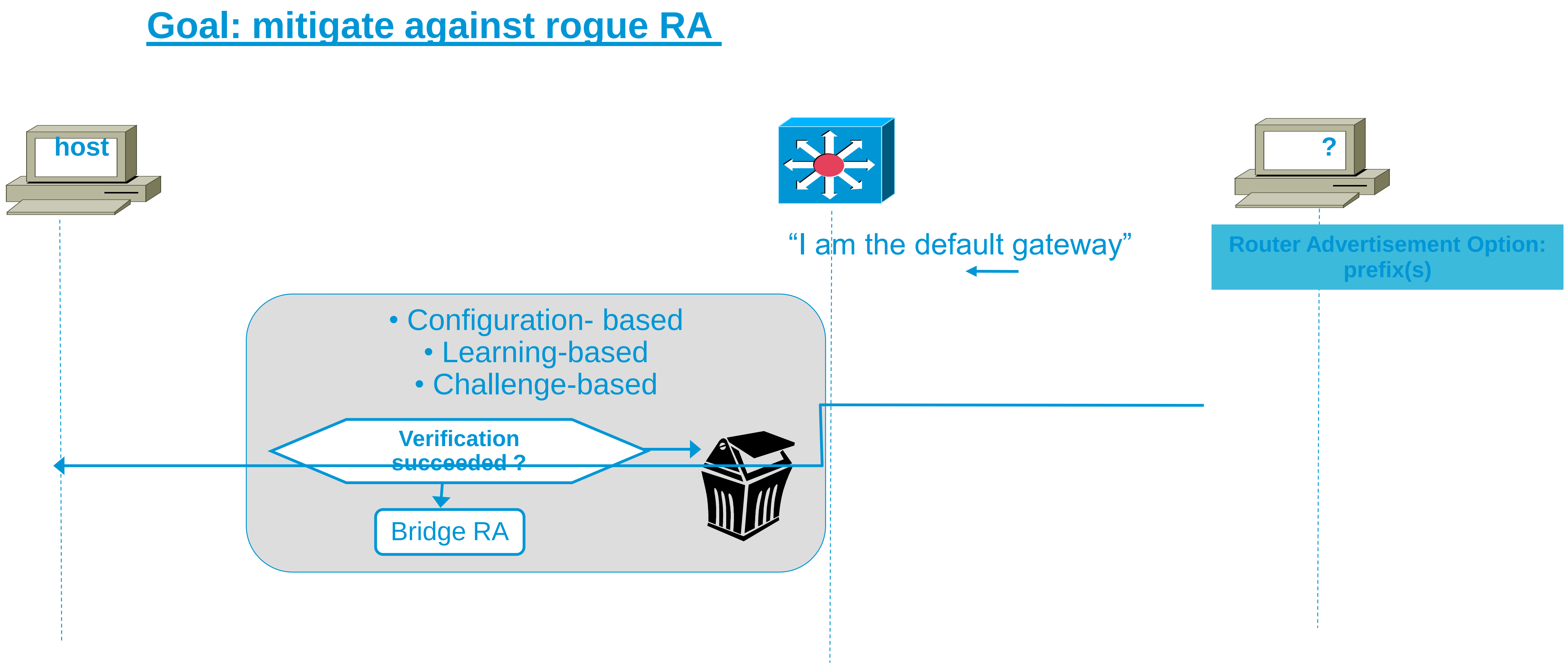
Phase II

- DHCP Guard
- Source Guard
- Multi Switch operation
- RA Throttler
- NDP Multicast Suppress

Phase III

- Destination Guard
- Prefix Guard
- DAD Proxy
- Binding Table Recovery
- SVI support

RA-Guard



- Switch selectively accepts or rejects RAs based on various criteria's
- Can be ACL based, learning based or challenge (SeND) based.
- Hosts see only allowed RAs, and RAs with allowed content

IPv6 First Hop Security Roadmap (November 2011) = not a commitment.

Cisco IOS Software Platforms	Cisco 7600 series	Cisco Catalyst 6500 Series Sup 2T	Cisco Catalyst 6500 Series Sup 720	Cisco Catalyst 4500 Series	Cisco 3750/3560 series	Cisco 3750/3560 E/X-S series	Cisco 2960S series LAN Lite	Cisco 2960S series	Existing WLC
	15S	12.2SY	12.2SX	12.2SG	12.2SE	12.2SE	12.2SE	12.2SE	Linux
NDP Inspection	RLS13 H2CY12	12.2(50)SY	roadmap	Indus Q1CY13		Nile Q3CY12		Nile Q3CY12	7.2 Q1CY12
IPv6 Source Guard	RLS13 H2CY12			Indus Q1CY13		Nile Q3CY12		Nile Q3CY12	
IPv6 prefix Guard	RLS13 H2CY12			Indus Q1CY13					
RA Guard	RLS13 H2CY12	12.2(50)SY	roadmap	Indus Q1CY13		Nile Q3CY12	Nile Q3CY12	Nile Q3CY12	7.2 Q1CY12
DHCPv6 Guard	RLS13 H2CY12			Indus Q1CY13		Nile Q3CY12		Nile Q3CY12	7.2 Q1CY12
RA Throttler									7.2 Q1CY12
ND Multicast Suppress									7.2 Q1CY12
IPv6 Port ACL	RLS13 H2CY12	12.2(50)SY	12.2(33)SXI4	12.2(54)SG	12.2(46)SE	12.2(46)SE		Nile Q3CY12	7.2 Q1CY12
ACL based RA Guard		12.2(50)SY	12.2(33)SXI4	12.2(54)SG					7.2 Q1CY12
IPv6 Device Tracking	RLS13 H2CY12	12.2(50)SY	roadmap	Indus Q1CY13		Nile Q3CY12		Nile Q3CY12	7.2 Q1CY12
IPv6 Address Protection	RLS13 H2CY12	12.2(50)SY	roadmap	Indus Q1CY13		Nile Q3CY12		Nile Q3CY12	7.2 Q1CY12
Per port Address limit	RLS13 H2CY12	12.2(50)SY	roadmap	Indus Q1CY13		Nile Q3CY12		Nile Q3CY12	7.2 Q1CY12

http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-roadmap.html

ICMPv4 vs. ICMPv6

- Significant changes
- More relied upon

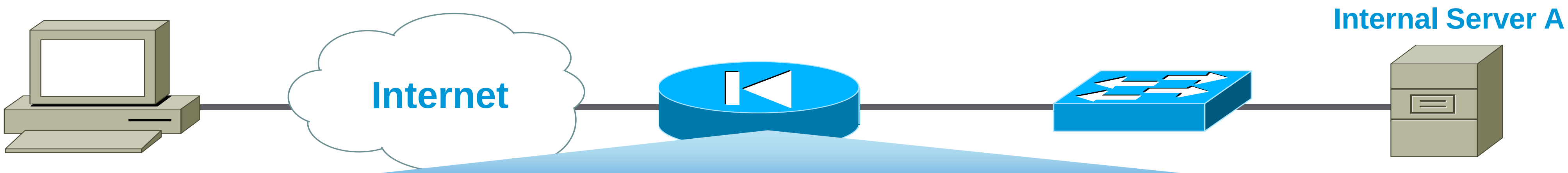
ICMP Message Type	ICMPv4	ICMPv6
Connectivity Checks	X	X
Informational/Error Messaging	X	X
Fragmentation Needed Notification	X	X
Address Assignment		X
Address Resolution		X
Router Discovery		X
Multicast Group Management		X
Mobile IPv6 Support		X

- ICMP policy on firewalls needs to change to support IPv6

Generic ICMPv4

For Your Reference

Border Firewall Policy

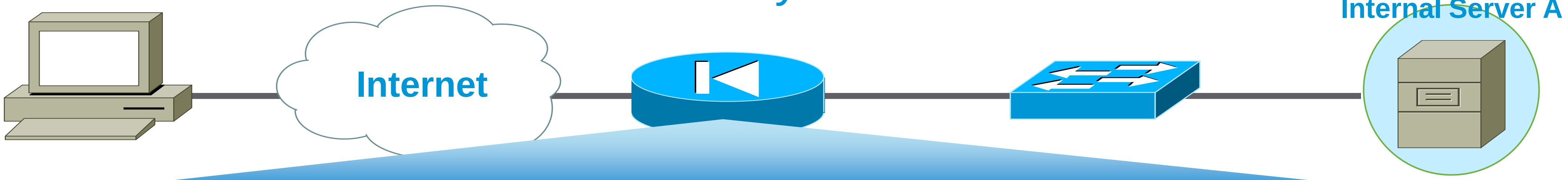


Action	Src	Dst	ICMPv4 Type	ICMPv4 Code	Name
Permit	Any	A	0	0	Echo Reply
Permit	Any	A	8	0	Echo Request
Permit	Any	A	3	0	Dst. Unreachable— Net Unreachable
Permit	Any	A	3	4	Dst. Unreachable— Frag. Needed
Permit	Any	A	11	0	Time Exceeded— TTL Exceeded

Equivalent ICMPv6

For Your Reference

RFC 4890: Border Firewall Transit Policy



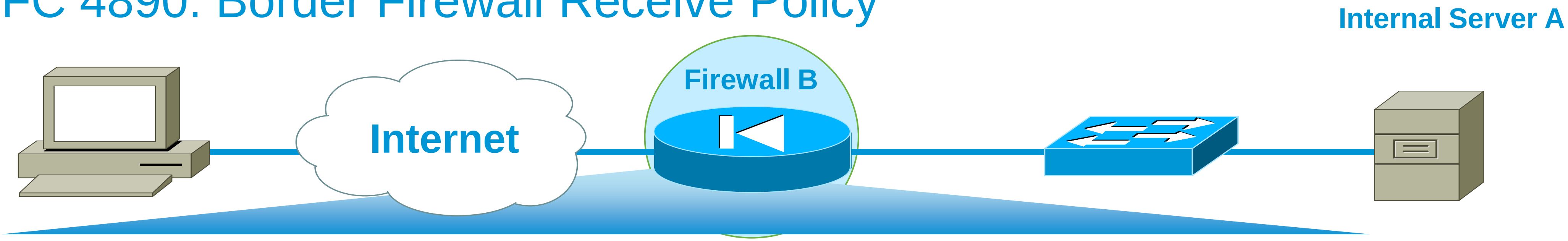
Action	Src	Dst	ICMPv6 Type	ICMPv6 Code	Name
Permit	Any	A	128	0	Echo Reply
Permit	Any	A	129	0	Echo Request
Permit	Any	A	1	0	No Route to Dst.
Permit	Any	A	2	0	Packet Too Big
Permit	Any	A	3	0	Time Exceeded—TTL Exceeded
Permit	Any	A	4	0	Parameter Problem

Needed for Teredo traffic

Potential Additional ICMPv6

For Your Reference

RFC 4890: Border Firewall Receive Policy



Action	Src	Dst	ICMPv6 Type	ICMPv6 Code	Name
Permit	Any	B	2	0	Packet too Big
Permit	Any	B	4	0	Parameter Problem
Permit	Any	B	130–132	0	Multicast Listener
Permit	Any	B	133/134	0	Neighbor Solicitation and Advertisement
Deny	Any	Any			

For locally generated traffic

Information Leak with Hop-Limit

- IPv6 hop-limit has identical semantics as IPv4 time-to-live
- Can be leveraged by design
  - To ensure packet is local iff hop-limit = 255
  - Notably used by Neighbor Discovery
- Can be leveraged by malevolent people
  - Guess the remote OS: Mac OS/X always set it to 64
  - Evade inspection: hackers send some IPv6 packets analyzed by the IPS but further dropped by the network before reaching destination… Could evade some IPS
  - Threat: low and identical to IPv4

Preventing IPv6 Routing Attacks
Protocol Authentication

- BGP, ISIS, EIGRP no change:
  - An MD5 authentication of the routing update
- OSPFv3 has changed and pulled MD5 authentication from the protocol and instead is supposed to rely on transport mode IPSec
- RIPng, PIM also rely on IPSec
- IPv6 routing attack best practices
  - Use traditional authentication mechanisms on BGP and IS-IS
  - Use IPSec to secure protocols such as OSPFv3 and RIPng

OSPF or EIGRP Authentication

For Your Reference

```
interface Ethernet0/0
 ipv6 ospf 1 area 0
 ipv6 ospf authentication ipsec spi 500 md5 1234567890ABCDEF
```

```
interface Ethernet0/0
 ipv6 authentication mode eigrp 100 md5
 ipv6 authentication key-chain eigrp 100 MYCHAIN

key chain MYCHAIN
 key 1
key-string 1234567890ABCDEF
accept-lifetime local 12:00:00 Dec 31 2006 12:00:00 Jan 1 2008
send-lifetime local 00:00:00 Jan 1 2007 23:59:59 Dec 31 2007
```

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

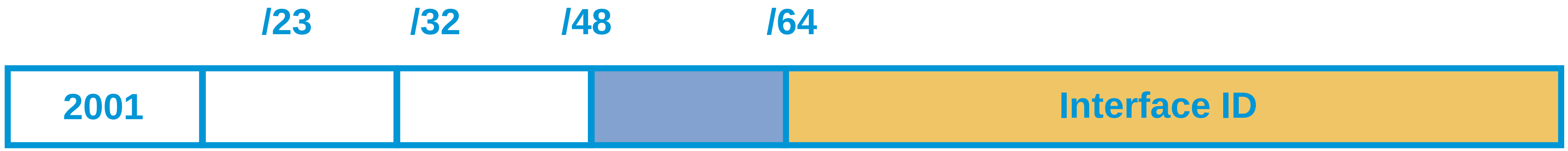
IPv6 Stack Vulnerabilities

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

CVE	Date	OS	Issue
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
- Enabled by default in Windows, Android, iOS

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

Disabling Privacy Extension

For Your Reference

- Microsoft Windows
  - Deploy a Group Policy Object (GPO)

```
netsh interface ipv6 set global randomizeidentifiers=disabled
netsh interface ipv6 set global randomizeidentifiers=disabled store=persistent
netsh interface ipv6 set privacy state=disabled store=persistent
```

- Alternatively disabling stateless auto-configuration and force DHCPv6
  - Send Router Advertisements with
    - all prefixes with A-bit set to 0 (disable SLAAC)
    - M-bit set to 1 to force stateful DHCPv6

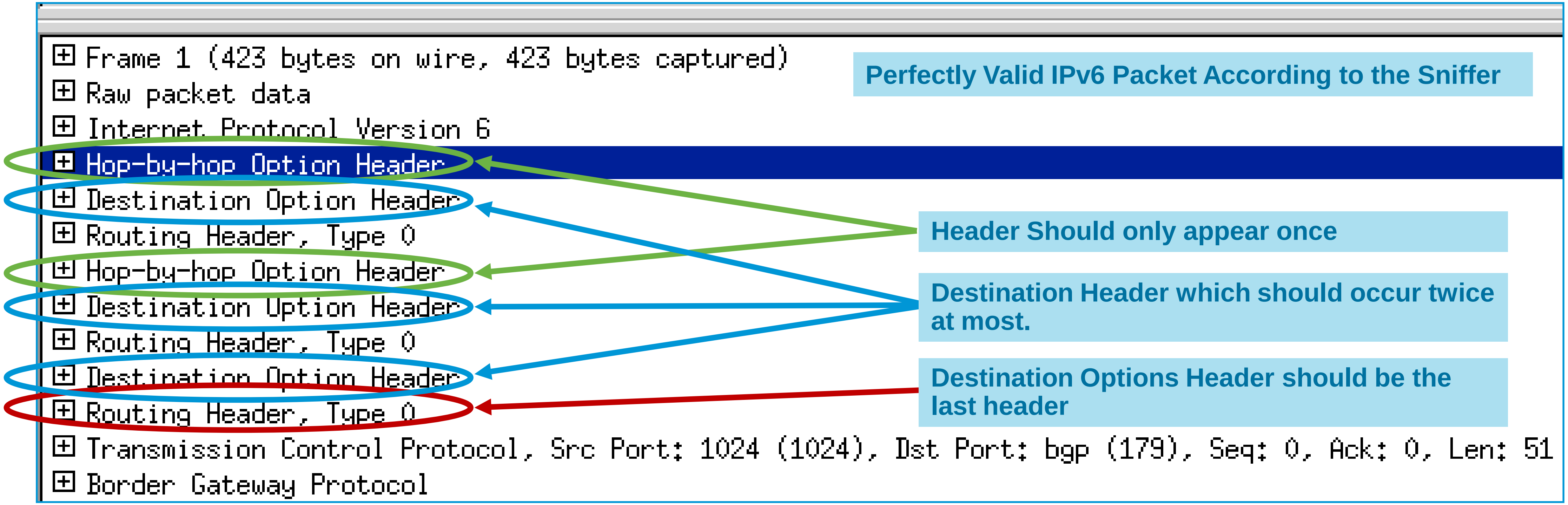
```
interface fastEthernet 0/0
  ipv6 nd prefix default no-autoconfig
  ipv6 dhcp server . . . (or relay)
  ipv6 nd managed-config-flag
```

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

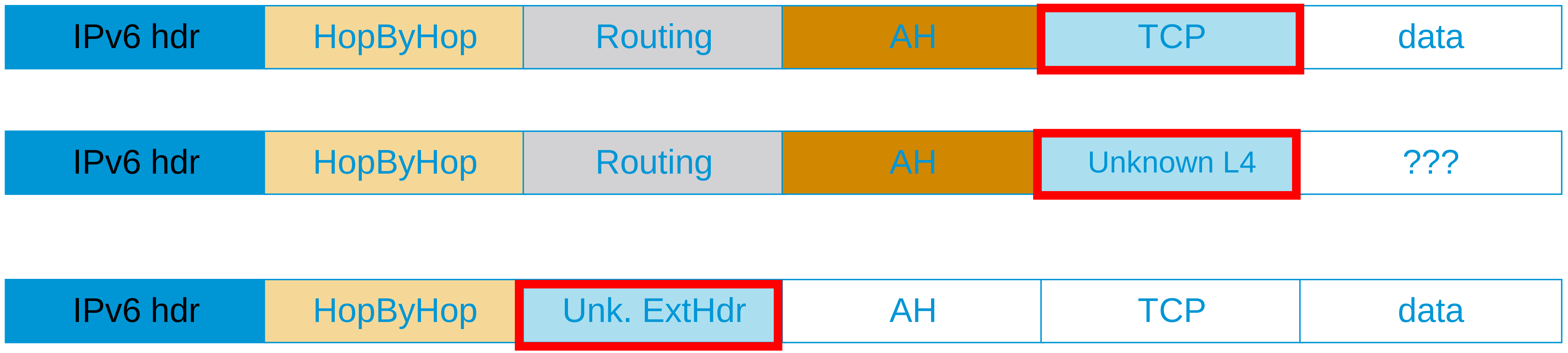
  Can I overrun buffers with a lot of extension headers?



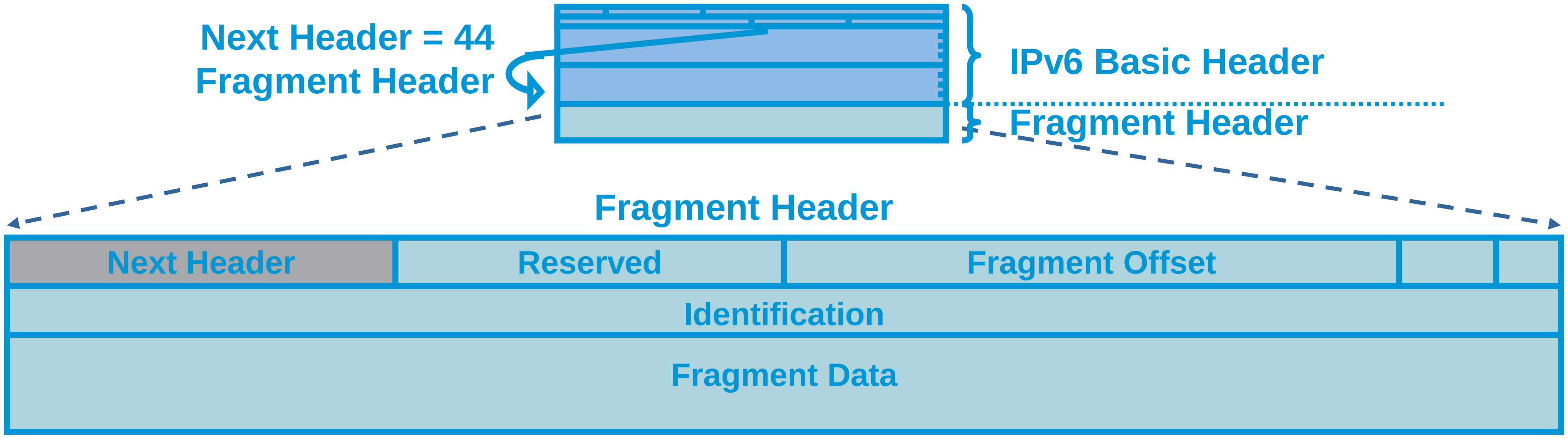
See also: http://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8054d37d.html

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**



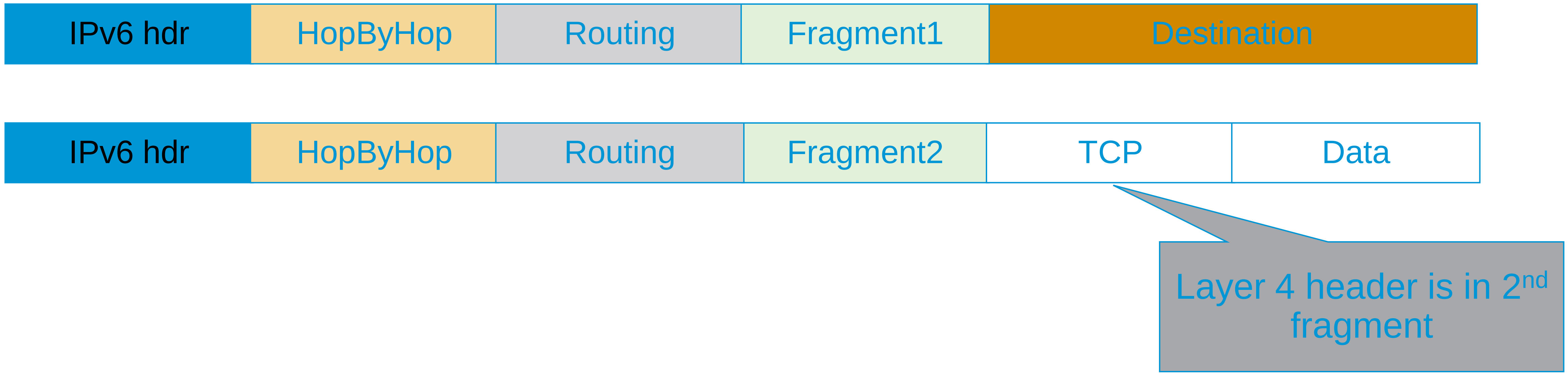
Fragment Header: IPv6



- 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

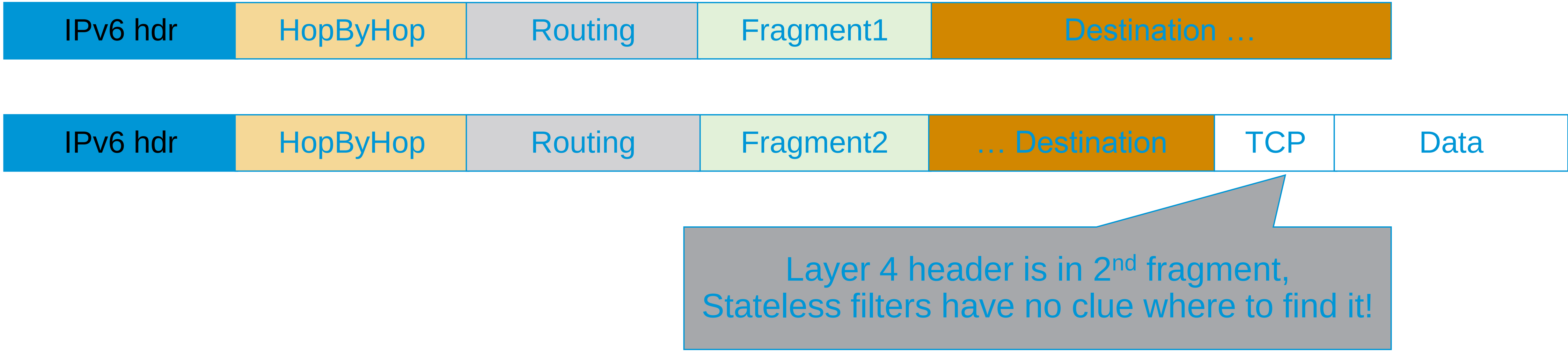
Parsing the Extension Header Chain Fragmentation Matters!

- 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

IPv4 to IPv6 Transition Challenges

- 16+ methods, possibly in combination
- Dual stack
  - Consider security for both protocols
  - Cross v4/v6 abuse
  - Resiliency (shared resources)
- Tunnels
  - Bypass firewalls (protocol 41 or UDP)
  - Can cause asymmetric traffic (hence breaking stateful firewalls)

Dual Stack Host Considerations

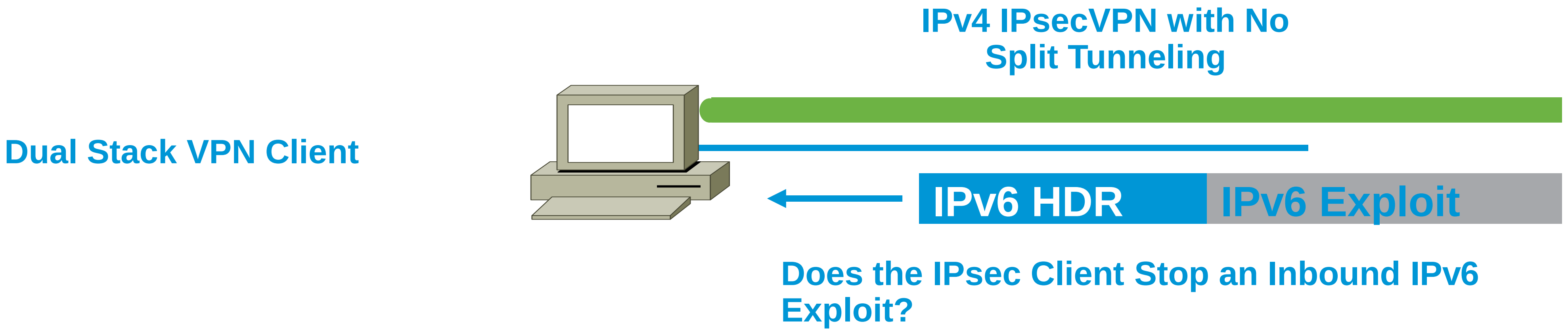
- Host security on a dual-stack device

  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, 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

Bored at BRU Airport on a Sunday at 22:00

```
$ ifconfig en1
en1: flags=8863<UP,BROADCAST,SMART,RUNNING
          ether 00:26:bb:xx:xx:xx
          inet6 fe80::226:bbff:fexx:x
          inet 10.19.19.118 netmask 0x
          media: autoselect
          status: active
```

Humm…
Is there an IPv6
Network?

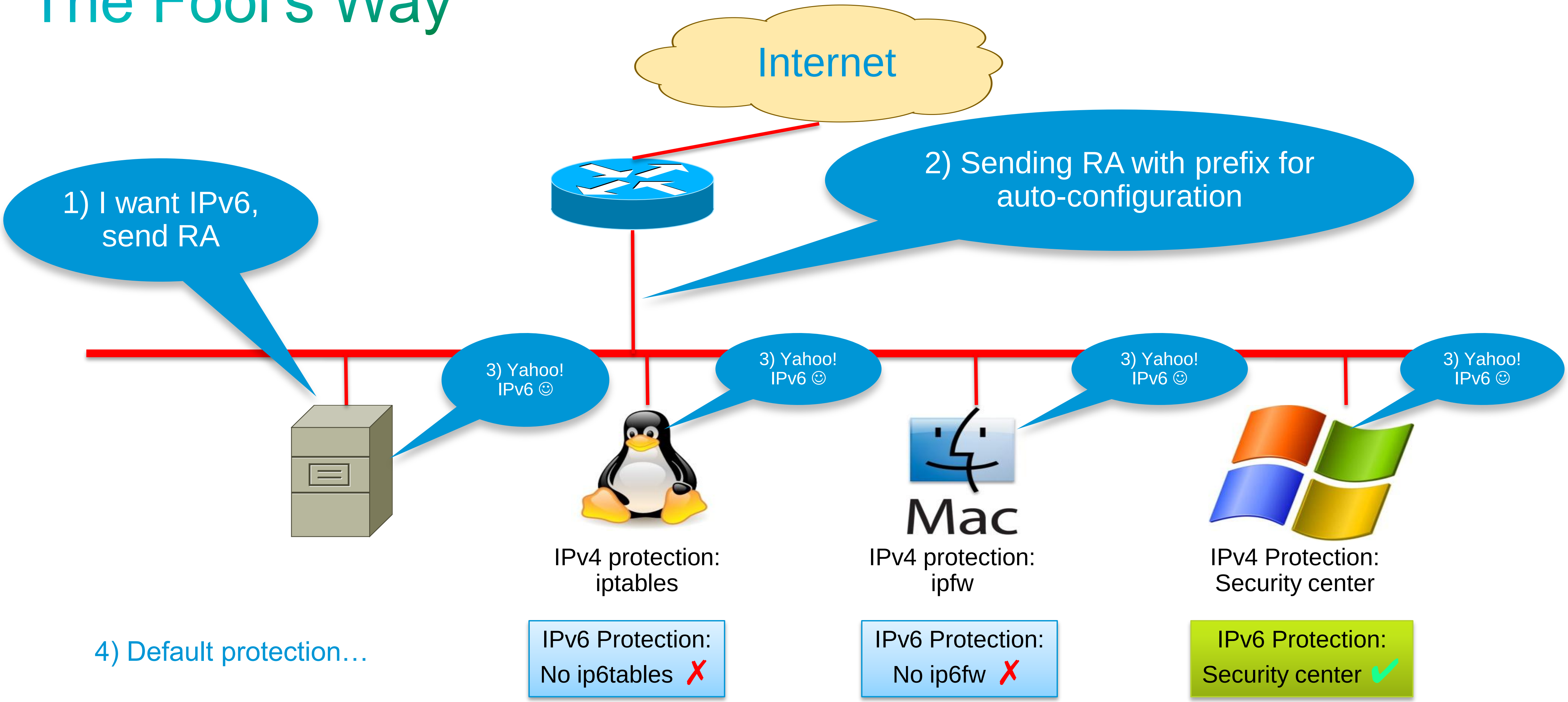
```
$ ping6 -I en1 ff02::1%en1
PING6(56=40+8+8 bytes) fe80::226:bbff:fexx:xxxx%en1 --> ff02::1
16 bytes from fe80::226:bbff:fexx:xxxx%
. . .
16 bytes from fe80::cabc:c8ff:fe
^C
--- ff02::1%en1 ping6 statistics --
4 packets transmitted, 4 packets received,                loss
round-trip min/avg/max/std-dev = 0.140/316.721/2791  78/412.276 ms
```

Humm…
Are there any IPv6
peers?

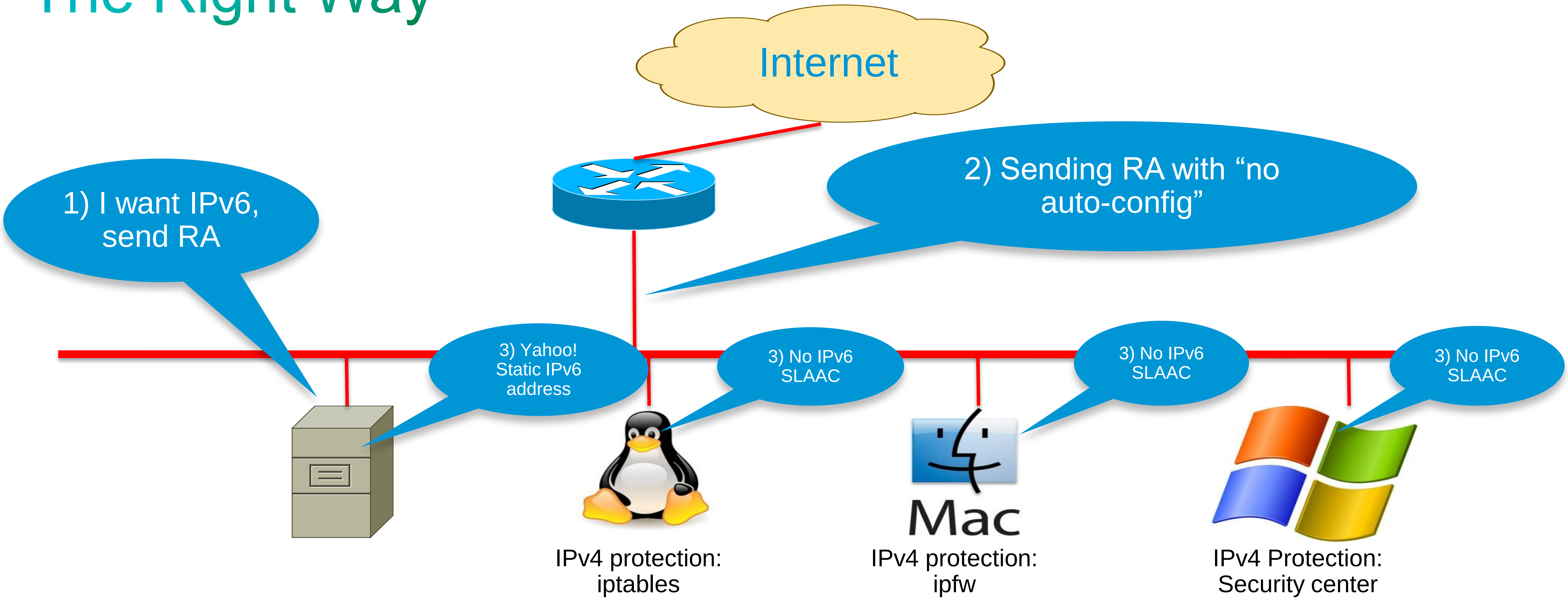
```
$ ndp -an
Neighbor
2001:
. . .
$ ndp -
      64
```

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

Enabling IPv6 in the IPv4 Data Center
The Fool's Way



Enabling IPv6 in the IPv4 Data Center
The Right Way



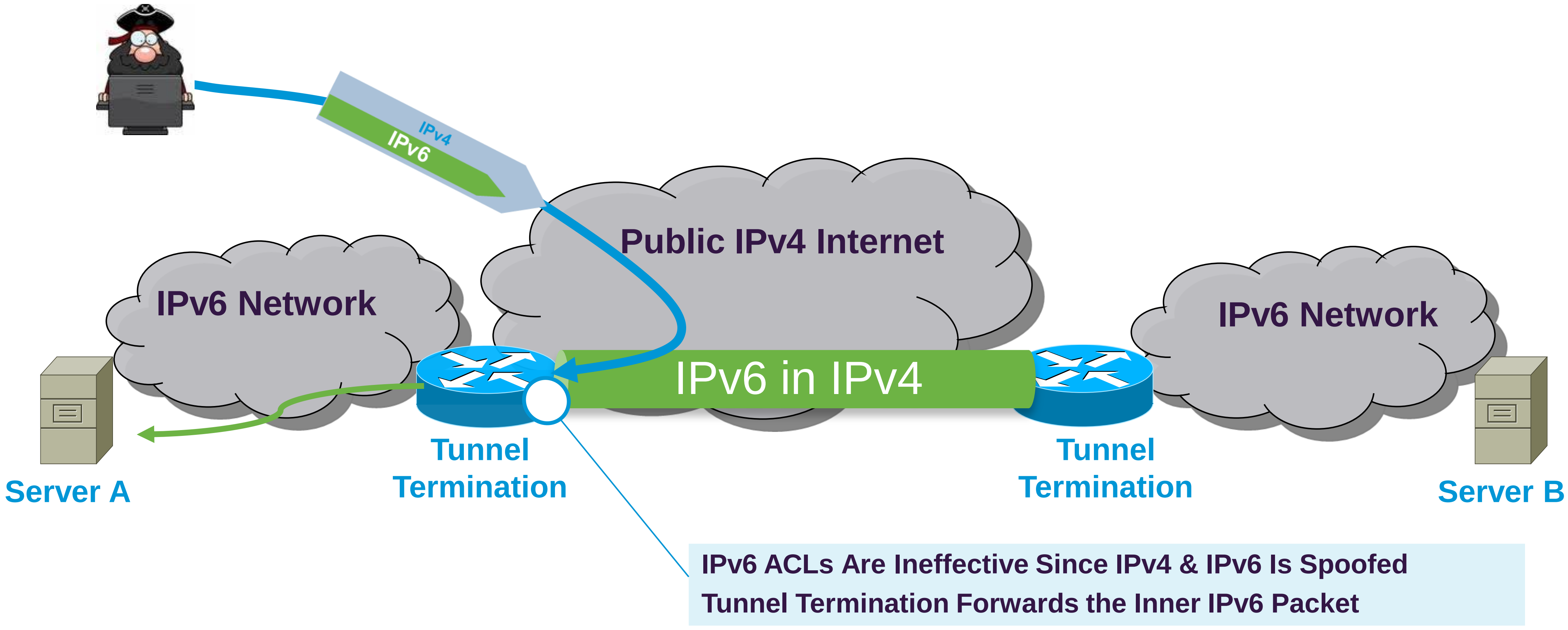
IPv6 Tunneling Summary

- RFC 1933/2893 configured and automatic tunnels
- RFC 2401 IPSec tunnel
- RFC 2473 IPv6 generic packet tunnel
- RFC 2529 6over4 tunnel
- RFC 3056 6to4 tunnel
- RFC 5214 ISATAP tunnel
- MobileIPv6 (uses RFC2473)
- RFC 4380 Teredo tunnels
- RFC 5569 6RD

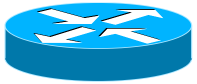
- Only allow authorized endpoints to establish tunnels
- Static tunnels are deemed as “more secure,” but less scalable
- Automatic tunneling mechanisms are susceptible to packet forgery and DoS attacks
- These tools have the same risk as IPv4, just new avenues of exploitation
- Automatic IPv6 over IPv4 tunnels could be secured by IPv4 IPSec

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

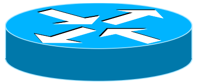
- Most IPv4/IPv6 transition mechanisms have no authentication built in therefore an IPv4 attacker can inject traffic if spoofing both IPv4 and IPv6 addresses



Looping Attack Between 2 ISATAP routers



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



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

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

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

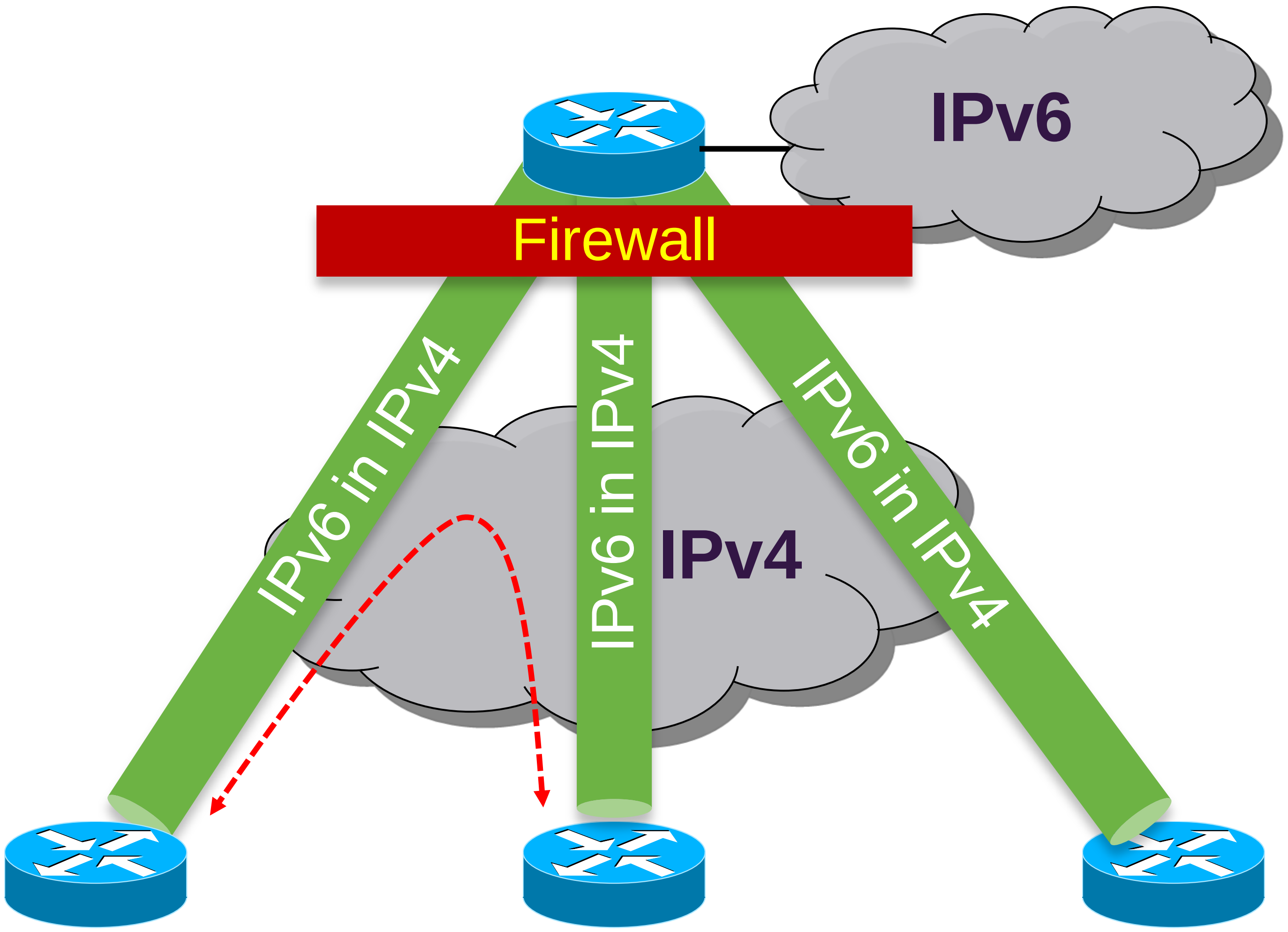
Repeat until Hop Limit == 0

- 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

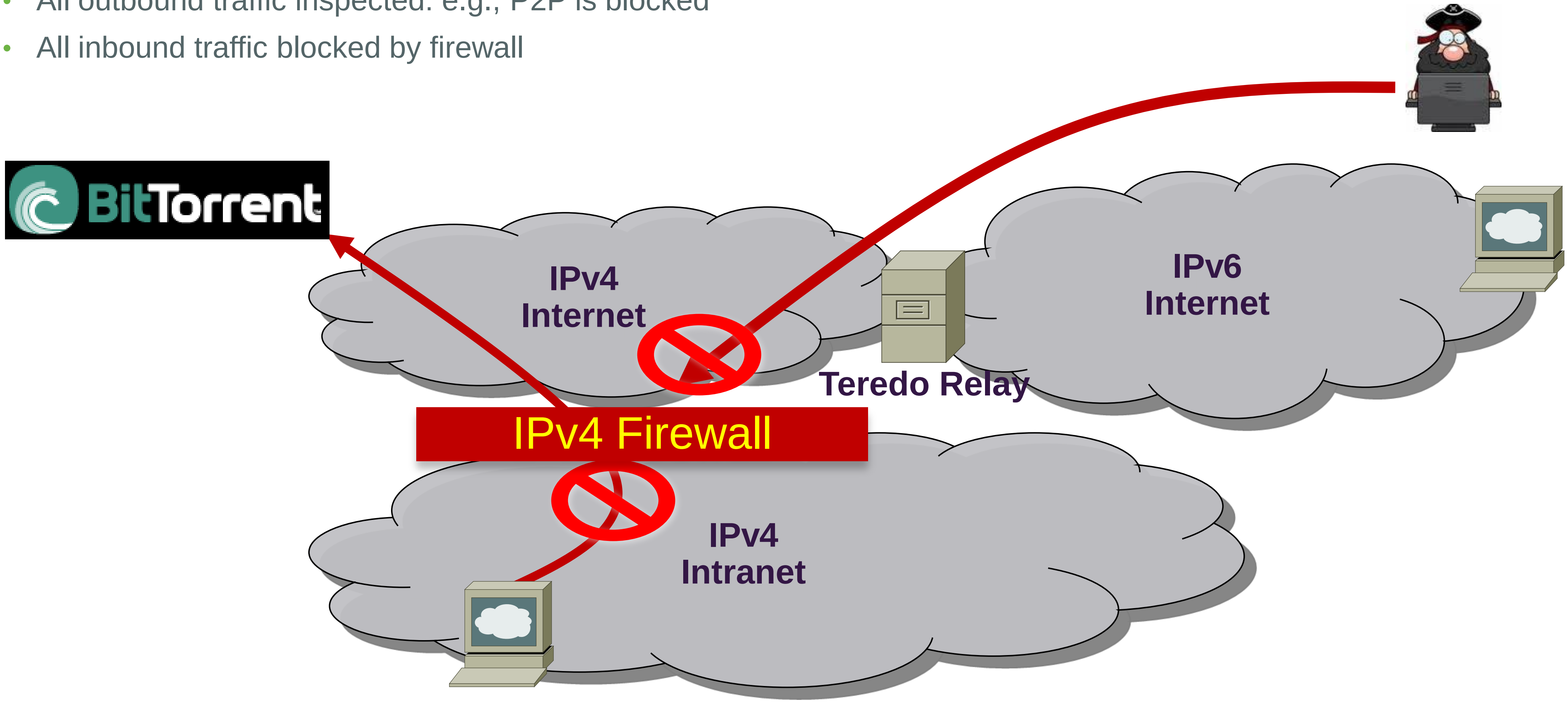
ISATAP/6to4 Tunnels Bypass ACL



Direct Tunnelled traffic ignores Hub Firewall Policy

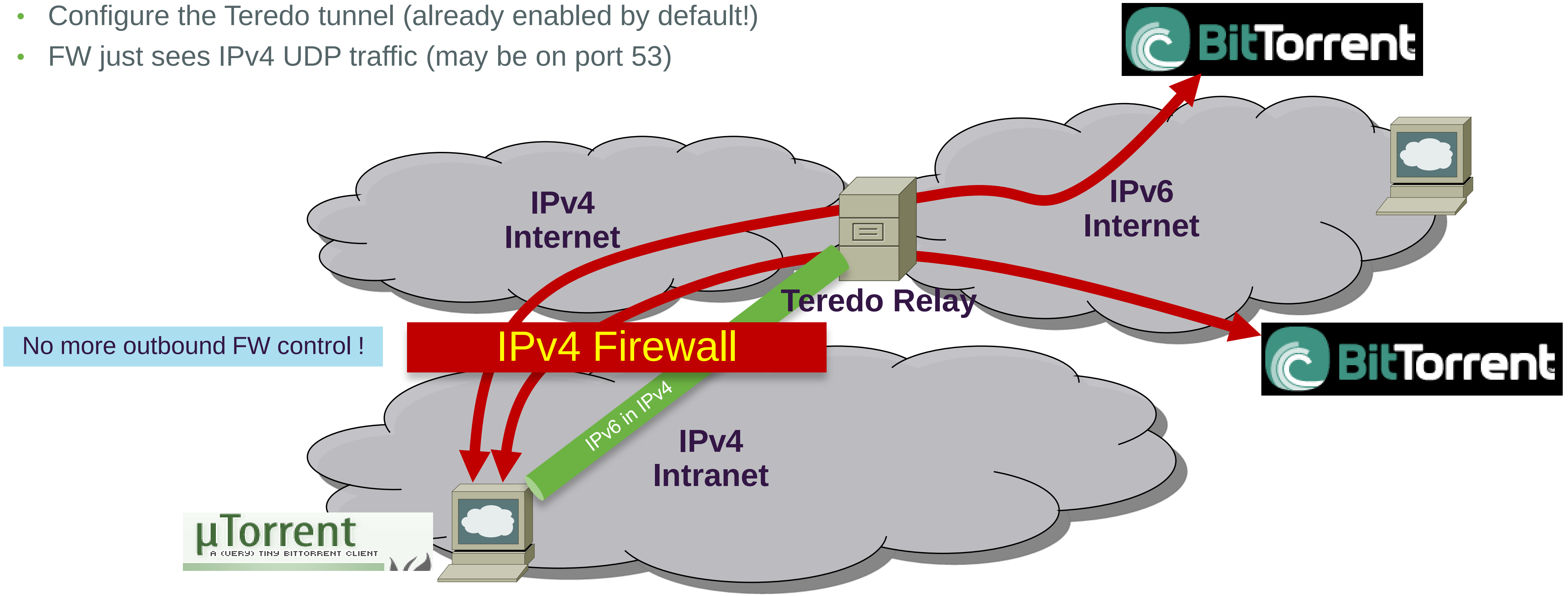
Teredo Tunnels (1/3)
Without Teredo: Controls Are in Place

- All outbound traffic inspected: e.g., P2P is blocked
- All inbound traffic blocked by firewall



Teredo Tunnels (2/3)
No More Outbound Control

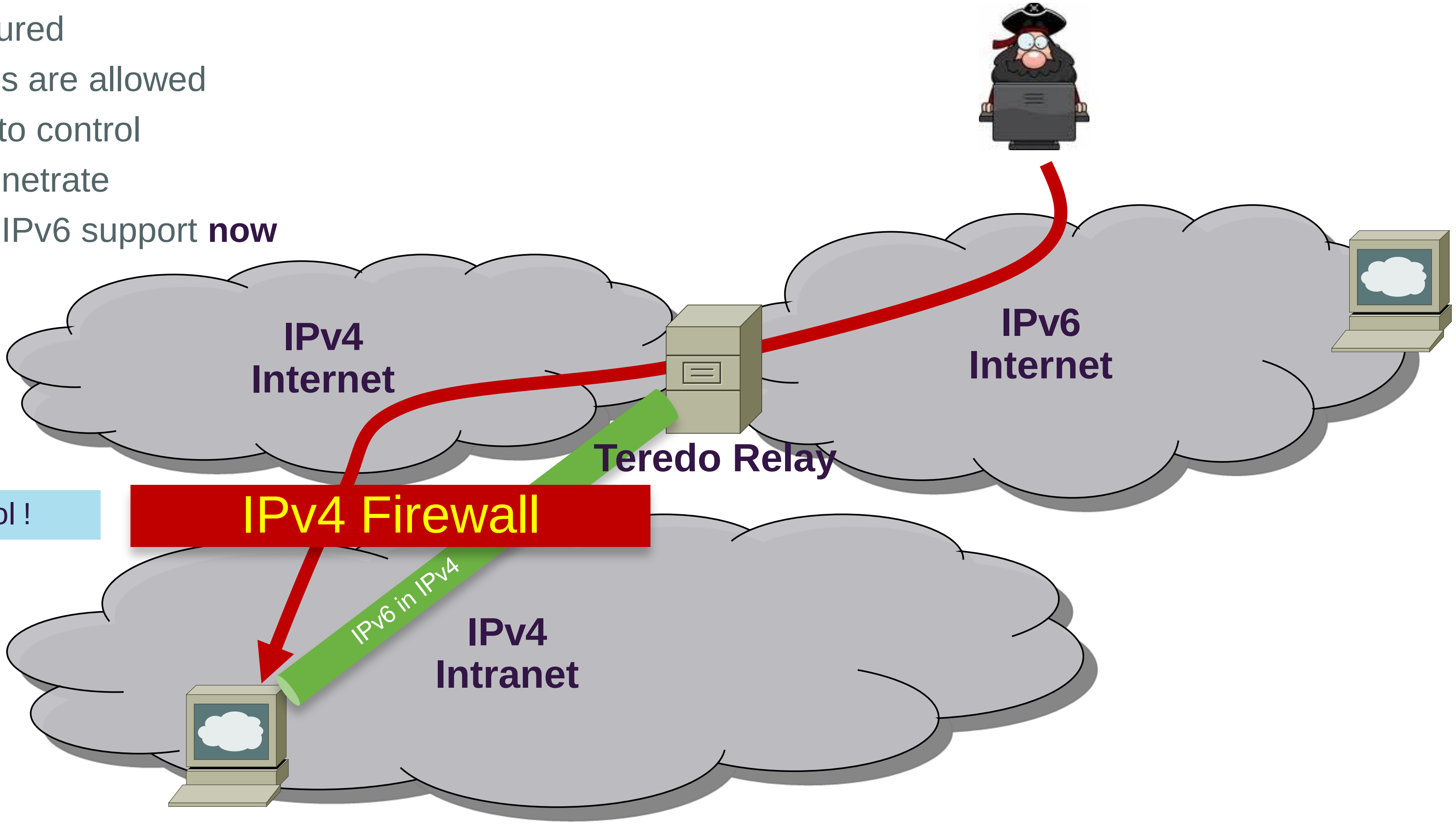
- Teredo threats—IPv6 over UDP (port 3544)
- Internal users wants to get P2P over IPv6
- Configure the Teredo tunnel (already enabled by default!)
- FW just sees IPv4 UDP traffic (may be on port 53)



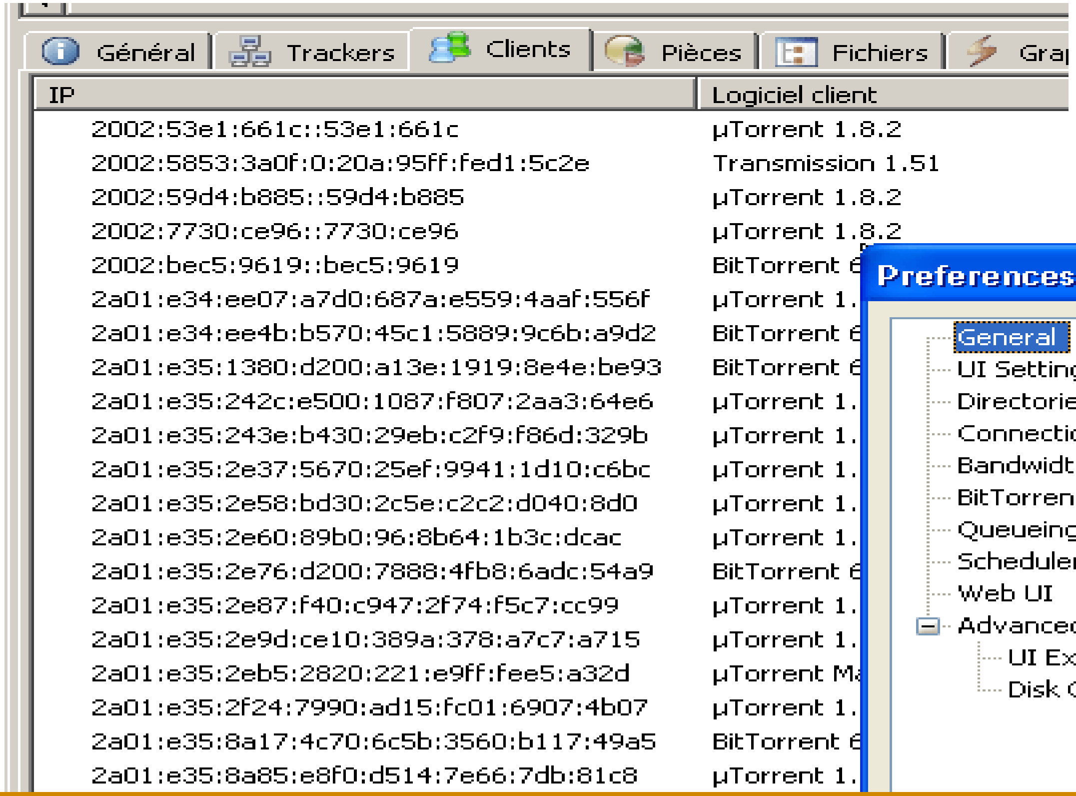
Teredo Tunnels (3/3)
No More Inbound Control

- Once Teredo Configured
- **Inbound** connections are allowed
- IPv4 firewall unable to control
- IPv6 hackers can penetrate
- Host security needs IPv6 support **now**

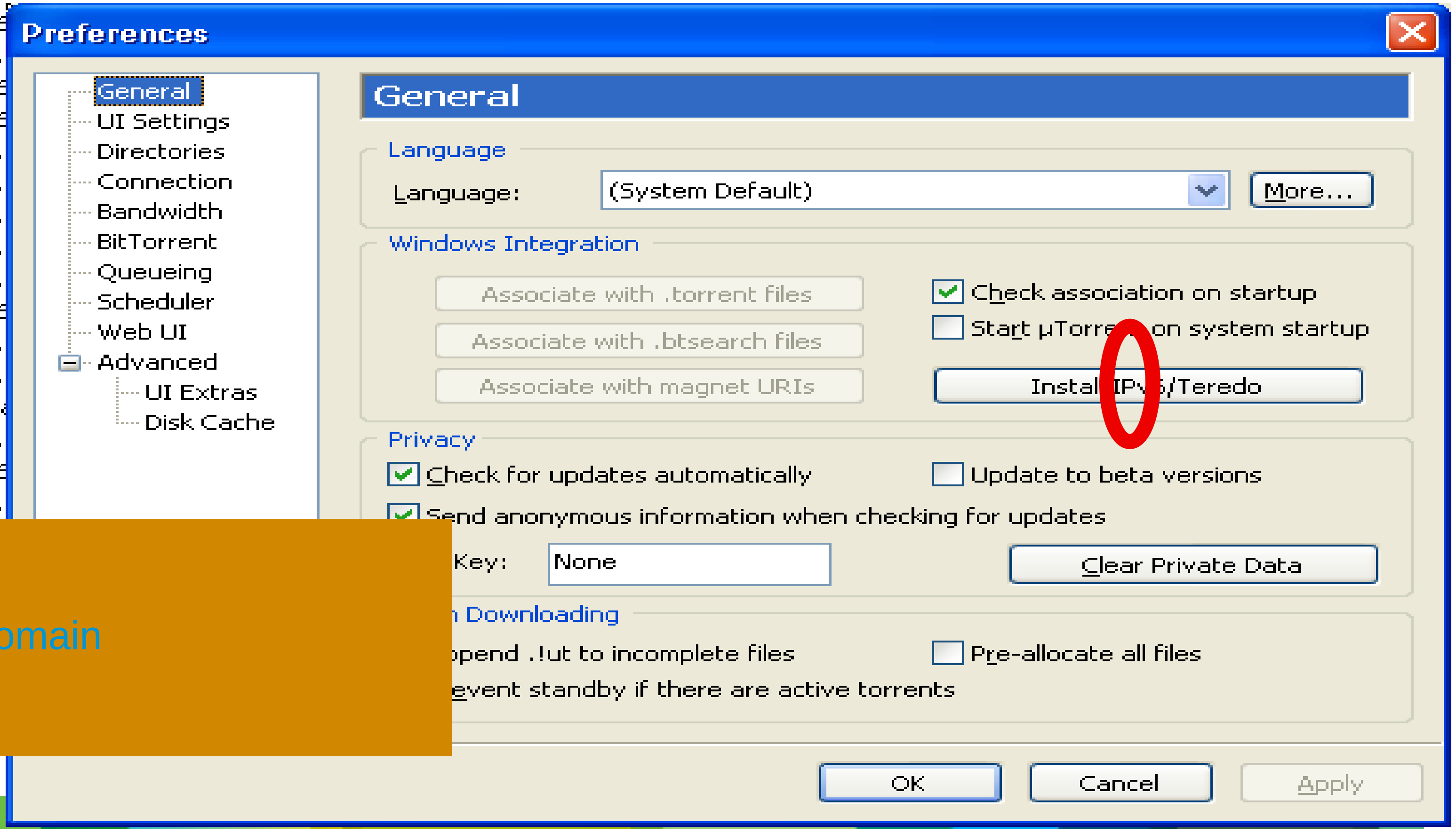
Limited inbound control !



Is it real?
May be uTorrent 1.8 (released Aug 08)



IP	Logiciel client
2002:53e1:661c::53e1:661c	µTorrent 1.8.2
2002:5853:3a0f:0:20a:95ff:fed1:5c2e	Transmission 1.51
2002:59d4:b885::59d4:b885	µTorrent 1.8.2
2002:7730:ce96::7730:ce96	µTorrent 1.8.2
2002:bec5:9619::bec5:9619	BitTorrent 6
2a01:e34:ee07:a7d0:687a:e559:4aaf:556f	µTorrent 1.
2a01:e34:ee4b:b570:45c1:5889:9c6b:a9d2	BitTorrent 6
2a01:e35:1380:d200:a13e:1919:8e4e:be93	BitTorrent 6
2a01:e35:242c:e500:1087:f807:2aa3:64e6	µTorrent 1.
2a01:e35:243e:b430:29eb:c2f9:f86d:329b	µTorrent 1.
2a01:e35:2e37:5670:25ef:9941:1d10:c6bc	µTorrent 1.
2a01:e35:2e58:bd30:2c5e:c2c2:d040:8d0	µTorrent 1.
2a01:e35:2e60:89b0:96:8b64:1b3c:dcac	µTorrent 1.
2a01:e35:2e76:d200:7888:4fb8:6adc:54a9	BitTorrent 6
2a01:e35:2e87:f40:c947:2f74:f5c7:cc99	µTorrent 1.
2a01:e35:2e9d:ce10:389a:378:a7c7:a715	µTorrent 1.
2a01:e35:2eb5:2820:221:e9ff:fee5:a32d	µTorrent Ma
2a01:e35:2f24:7990:ad15:fc01:6907:4b07	µTorrent 1.
2a01:e35:8a17:4c70:6c5b:3560:b117:49a5	BitTorrent 6
2a01:e35:8a85:e8f0:d514:7e66:7db:81c8	µTorrent 1.



Note: on Windows Teredo is:
- Disabled when firewall is disabled
- Disabled when PC is part of Active Directory domain
- Else enabled
- User can override this protection

Can We Block Rogue Tunnels?

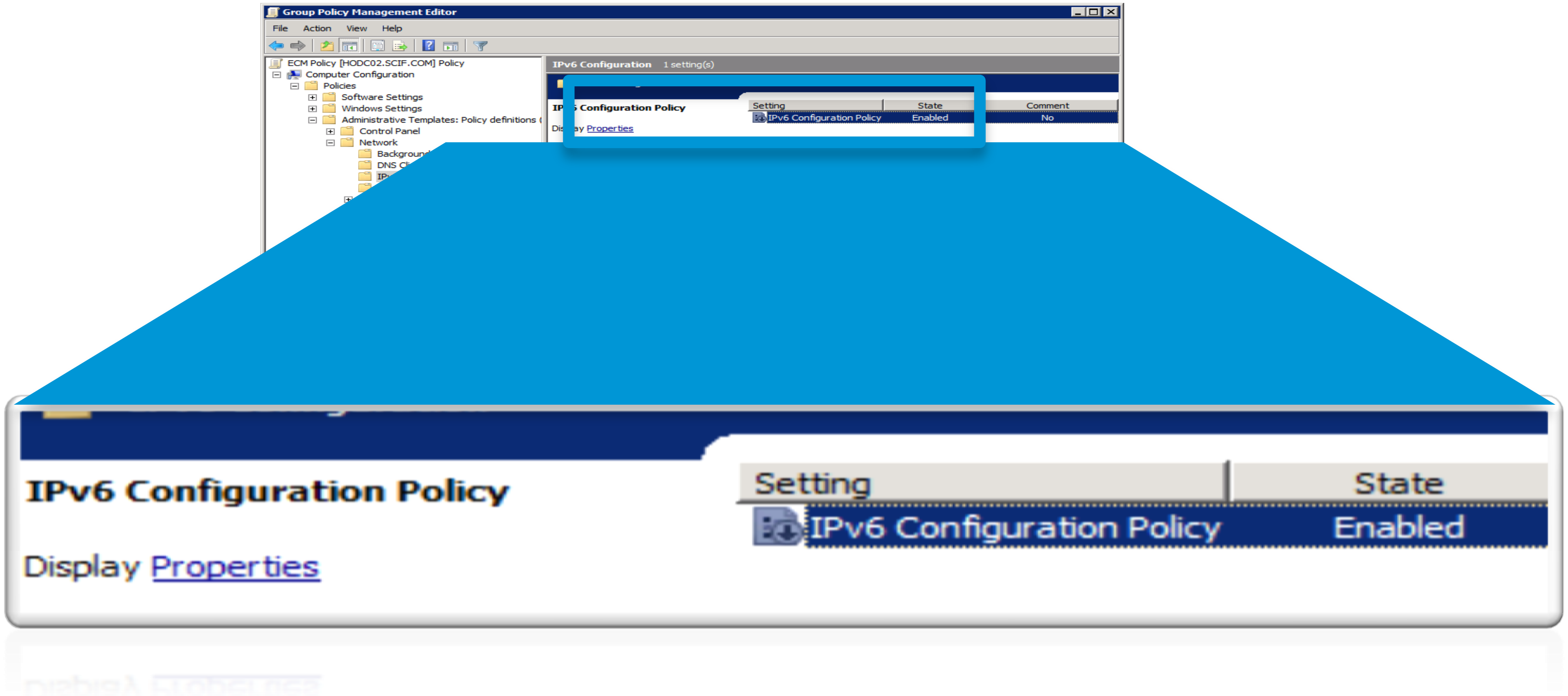
- Rogue tunnels by naïve users:
  - Sure, block IP protocol 41 and UDP/3544
  - In Windows:

```
netsh interface 6to4 set state state=disabled undoonstop=disabled
netsh interface isatap set state state=disabled
netsh interface teredo set state type=disabled
```

- Really rogue tunnels (covert channels)
  - No easy way...
  - Teredo will run over a different UDP port of course
  - Network devices can be your friend (more to come)
- **Deploying native IPv6 (including IPv6 firewalls and IPS) is probably a better alternative**
- **Or disable IPv6 on Windows through registry**
  - **HKLM\SYSTEM\CurrentControlSet\Services\tcpip6\Parameters\DisabledComponents**
    - **But Microsoft does not test any Windows application with IPv6 disabled**

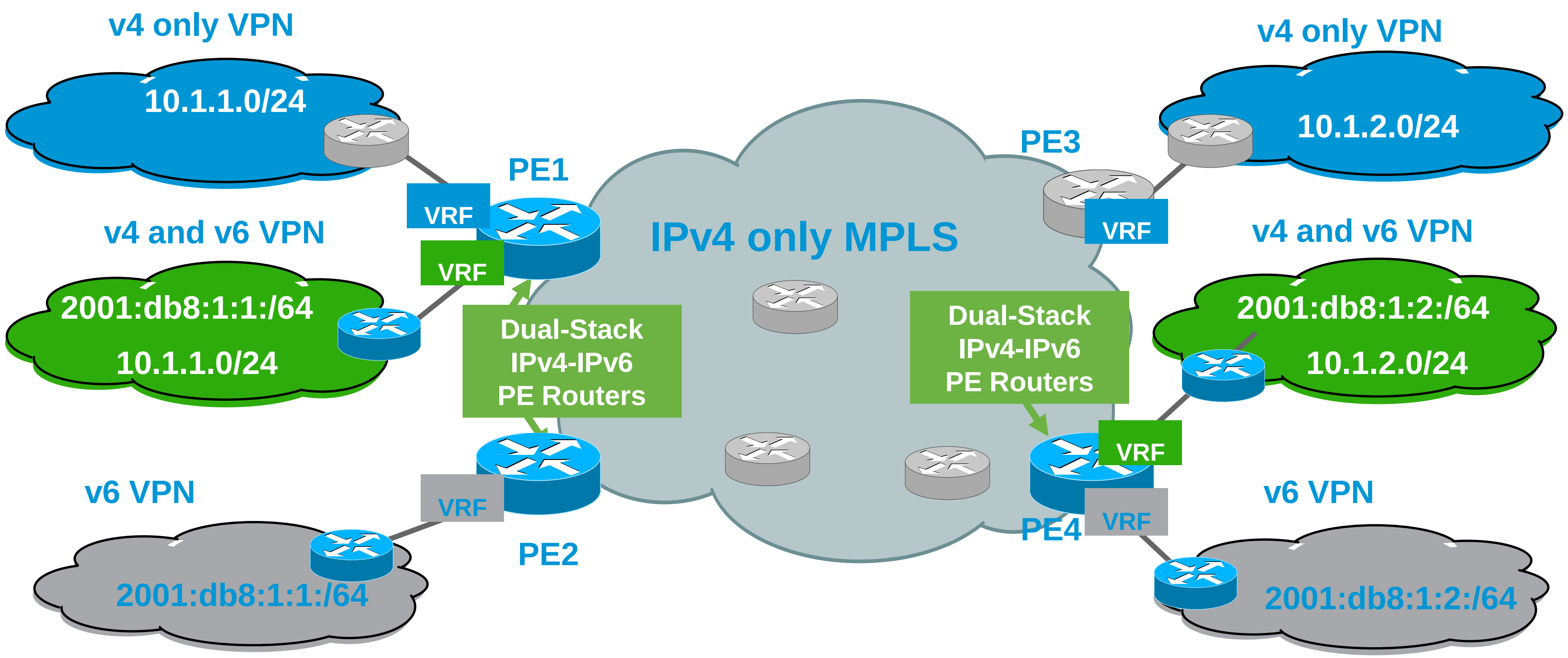
Disabling Teredo Through GPO

- Group Policy Object can be used at Active Directory to disable any transition technologies including Teredo
- Computer Configuration > Policies > Administrative Templates > Network > IPv6 Configuration
- See also http://support.microsoft.com/kb/929852 and http://www.expta.com/2009/02/how-to-configure-ipv6-using-group.html



SP Transition Mechanism: 6VPE

- 6VPE: the MPLS-VPN extension to also transport IPv6 traffic over an 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)**

Enforcing a Security Policy

PCI DSS Compliance and IPv6

- Payment Card Industry Data Security Standard requires the use of NAT for security

  Yes, weird isn't it?

  There is no NAT n:1 IPv6 <-> IPv6 in most of the firewalls

  RFC 6296 Network Prefix Translation for IPv6 (NPT6) is stateless 1:1 where inbound traffic is always mapped.

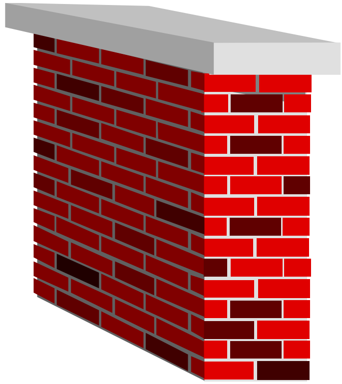
  RFC 6296 is mainly for multi-homing and does not have any security benefit (not that NAT n:1 has any…)

- ➔ PCI DSS compliance cannot be achieved for IPv6 ?

Cisco IOS IPv6 Extended Access Control Lists

- Very much like in IPv4
  - Filter traffic based on
    - Source and destination addresses
    - Next header presence
    - Layer 4 information
  - Implicit deny all at the end of ACL
  - Empty ACL means traffic allowed
  - Reflexive and time based ACL
- Known extension headers (HbH, AH, RH, MH, destination, fragment) are scanned until:
  - Layer 4 header found
  - Unknown extension header is found
- Side note for 7600 & other switches:
  - No VLAN ACL on the roadmap
  - Port ACL on Nexus-7000, Cat 3750 (12.2(46)SE not in base image), Cat 4K (12.2(54)SG), Cat 6K (12.3(33)SXI4)

IOS IPv6 Extended ACL



- Can match on
  - Upper layers: TCP, UDP, SCTP port numbers
  - TCP flags SYN, ACK, FIN, PUSH, URG, RST
  - ICMPv6 code and type
  - Traffic class (only six bits/8) = DSCP
  - Flow label (0-0xFFFFF)
- IPv6 extension header
  - `routing` matches any RH, `routing-type` matches specific RH
  - `mobility` matches any MH, `mobility-type` matches specific MH
  - `dest-option` matches any, `dest-option-type` matches specific destination options
  - `auth` matches AH
  - Can skip AH (but not ESP) since IOS 12.4(20)T
- `fragments` keyword matches
  - Non-initial fragments (same as IPv4)
  - And the first fragment if the L4 protocol cannot be determined
- `undetermined-transport` keyword matches (only for deny)
  - Any packet whose L4 protocol cannot be determined: fragmented or unknown extension header

IPv6 ACL Implicit Rules
RFC 4890

- Implicit entries exist at the end of each IPv6 ACL to allow neighbor discovery:

```
permit icmp any any nd-na
permit icmp any any nd-ns
deny ipv6 any any
```

- Nexus 7000 also allows RS & RA

IPv6 ACL Implicit Rules – Cont.
Adding a deny-log

- The beginner's mistake is to add a deny log at the end of IPv6 ACL

```
. . .
! Now log all denied packets
deny ipv6 any any log
! Heu . . . I forget about these implicit lines
permit icmp any any nd-na
permit icmp any any nd-ns
deny ipv6 any any
```

- Solution, explicitly add the implicit ACE

```
. . .
! Now log all denied packets
permit icmp any any nd-na
permit icmp any any nd-ns
deny ipv6 any any log
```

Example: Rogue RA & DHCP Port ACL

```
ipv6 access-list ACCESS_PORT
    remark for paranoid, block 1st fragment w/o L4 info
    deny ipv6 any any undetermined-transport
    remark Block all traffic DHCP server -> client
    deny udp any eq 547 any eq 546
    remark Block Router Advertisements
    deny icmp any any router-advertisement
    permit ipv6 any any

Interface gigabitethernet 1/0/1
    switchport
    ipv6 traffic-filter ACCESS_PORT in
```

Note: PACL replaces RACL for the interface (or is merged with RACL 'access-group mode prefer port')
In August 2010, Nexus-7000, Cat 3750 12.2(46)SE, Cat 4500 12.2(54)SG and Cat 6500 12.2(33)SXI4

Rogue RA & DHCP Port ACL

- Switch Based Port ACL to protect against Rogue RAs & DHCP

```
ipv6 access-list ACCESS_PORT
    remark for paranoid, block 1st fragment w/o L4 info
    deny ipv6 any any undetermined-transport
    remark Block all traffic DHCP server -> client
    deny udp any eq 547 any eq 546
    remark Block Router Advertisements
    deny icmp any any router-advertisement
    permit ipv6 any any

Interface gigabitethernet 1/0/1
    switchport
    ipv6 traffic-filter ACCESS_PORT in
```

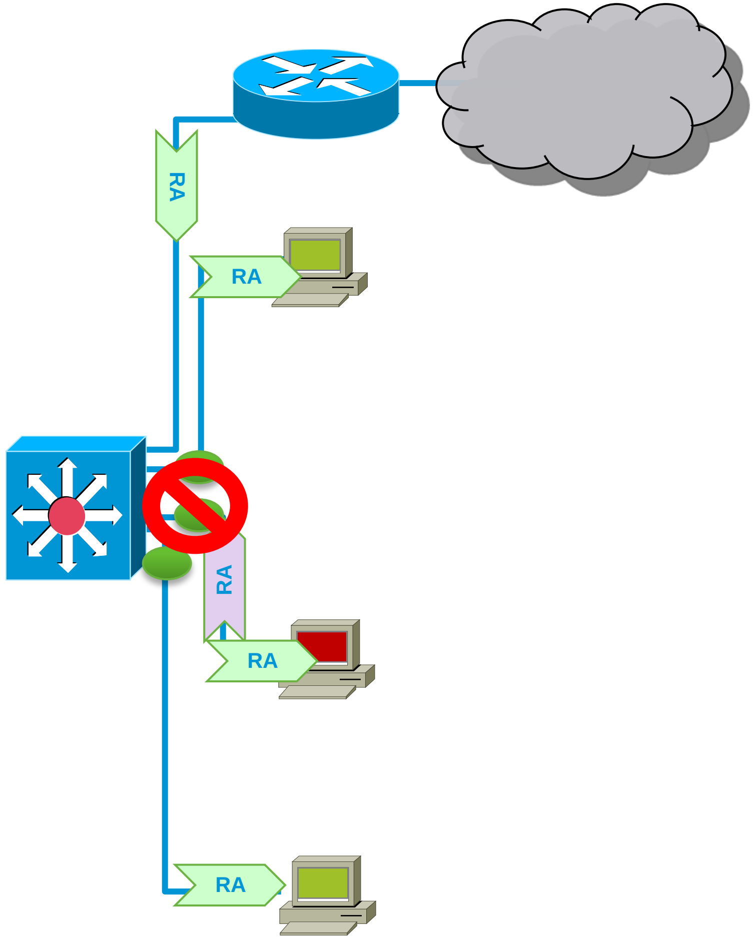
- Cat6k and 4k have a system macro for RA Guard

```
interface gigabitethernet 1/0/1
switchport
ipv6 nd raguard
```

- Port ACL replaces Router ACL starting with August 2010 releases onwards

```
interface gigabitethernet 1/0/1
switchport
access-group mode prefer port
```

Nexus-7000, Cat 3750 12.2(46)SE, Cat 4500 12.2(54)SG and Cat 6500 12.2(33)SXI4



IPv6 ACL to Protect VTY

For Your Reference

- Protect VTY access to devices like you would with IPv4

```
ipv6 access-list VTY
  permit ipv6 2001:db8:0:1::/64 any

line vty 0 4
  ipv6 access-class VTY in
```

- Assess if IPv6 access is required in the management plane.
- Some NMS still IPv4 only
- Low priority change for existing networks

Control Plane Policing for IPv6
Protecting the Router CPU

For Your Reference

- Against DoS with NDP, Hop-by-Hop, Hop Limit Expiration...
- Software routers (ISR, 7200): works with CoPPr (CEF exceptions)

```
policy-map COPPr
 class ICMP6_CLASS
   police 8000
 class OSPF_CLASS
   police 200000
 class class-default
   police 8000
!
control-plane cef-exception
 service-policy input COPPr
```

- Cat 6K & 7600

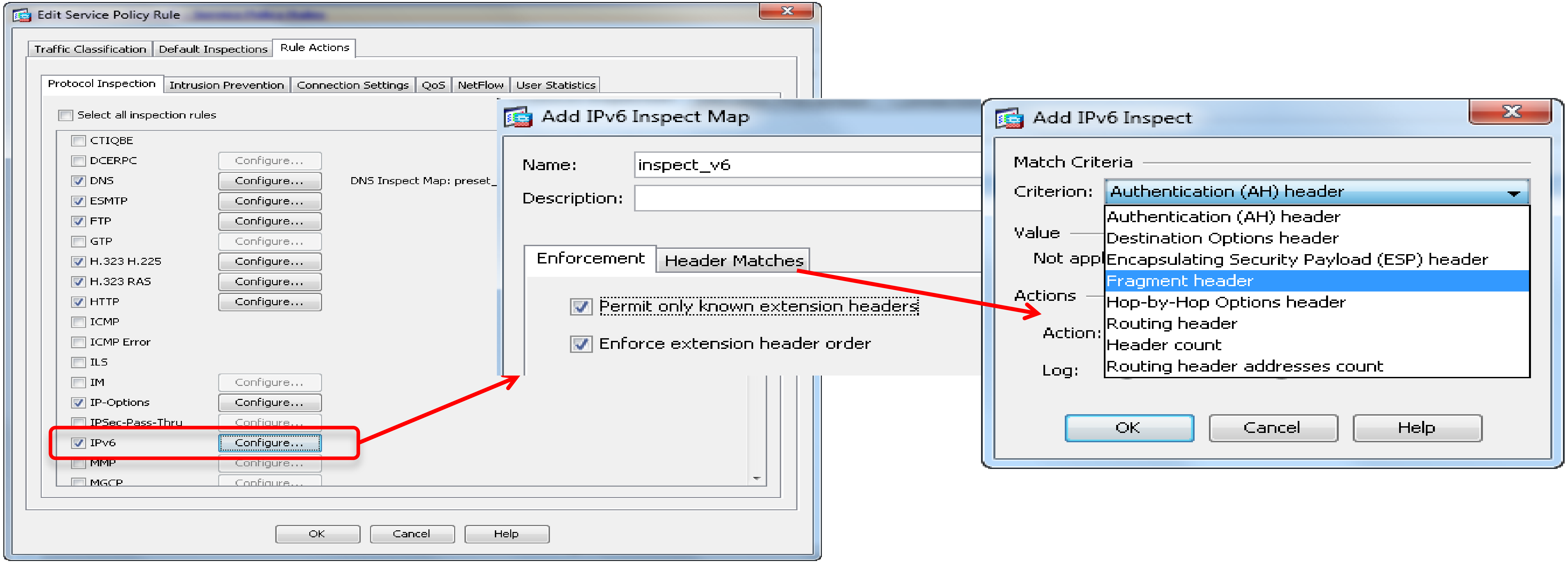
  IPv6 shares mls rate-limit with IPv4 for NDP & HL expiration

```
mls rate-limit all ttl-failure 1000
mls rate-limit unicast cef glean 1000
```

ASA Firewall IPv6 Support

- Since version 7.0 (April 2005)
- Dual-stack, IPv6-only, IPv4-only
- Extended IP ACL with stateful inspection
- Application awareness: TTP, FTP, telnet, SMTP, TCP, SSH, UDP
- uRPF and v6 Frag guard
- IPv6 header security checks (length & order)
- Management access via IPv6: Telnet, SSH, HTTPS
- ASDM support (ASA 8.2)
- Routed & transparent mode (ASA 8.2)
- Fail-over support (ASA 8.2.2)
- Selective permit/deny of extension headers (ASA 8.4.2)
- *OSPFv3, DHCPv6 relay, stateful NAT64/46/66 (expected mid 2012)*

ASA 8.4.2 : IPv6 Header Filtering



Summary of Cisco IPv6 Security Products

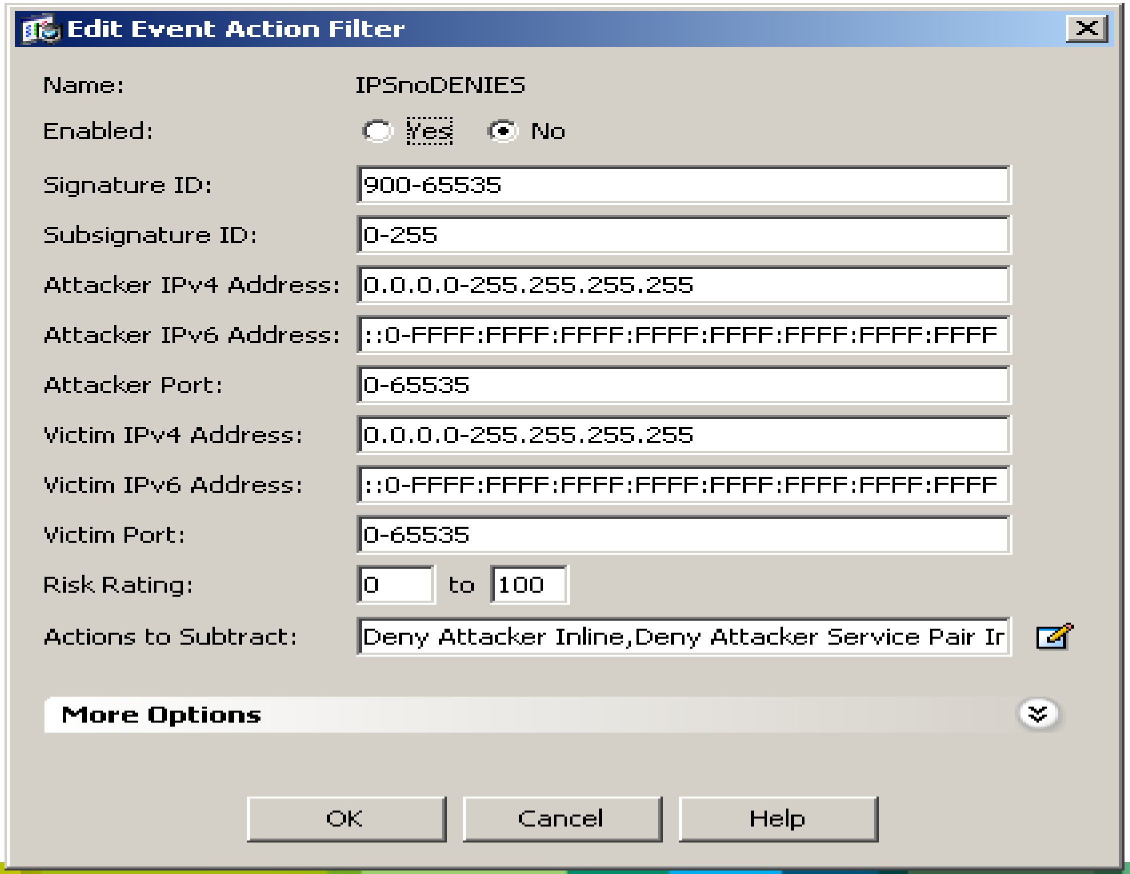
- ASA Firewall
  - Since version 7.0 (released 2005)
  - Flexibility: Dual stack, IPv6 only, IPv4 only
  - SSL VPN for IPv6 (ASA 8.0)
  - Stateful-Failover (ASA 8.2.2)
  - Cannot configure extension headers in ACL (but parsing is done)
- FWSM
  - IPv6 in software... 80 Mbps … Not an option (put an IPv6-only ASA in parallel)
- IOS Firewall
  - IOS 12.3(7)T (released 2005)
  - Zone-based firewall on IOS-XE 3.6 (2012)
- Cisco Security Agent (EOS)
  - Since version 6.0.1 for IPv6 network protection
- IPS
  - Since 6.2 (released 2008), management over IPv6: Q1 2012
- Email Security Appliance (ESA) under beta testing early 2010, shipping Q3 2011
- Web Security Appliance (WSA) Q1 2012

IPS Supports IPv6

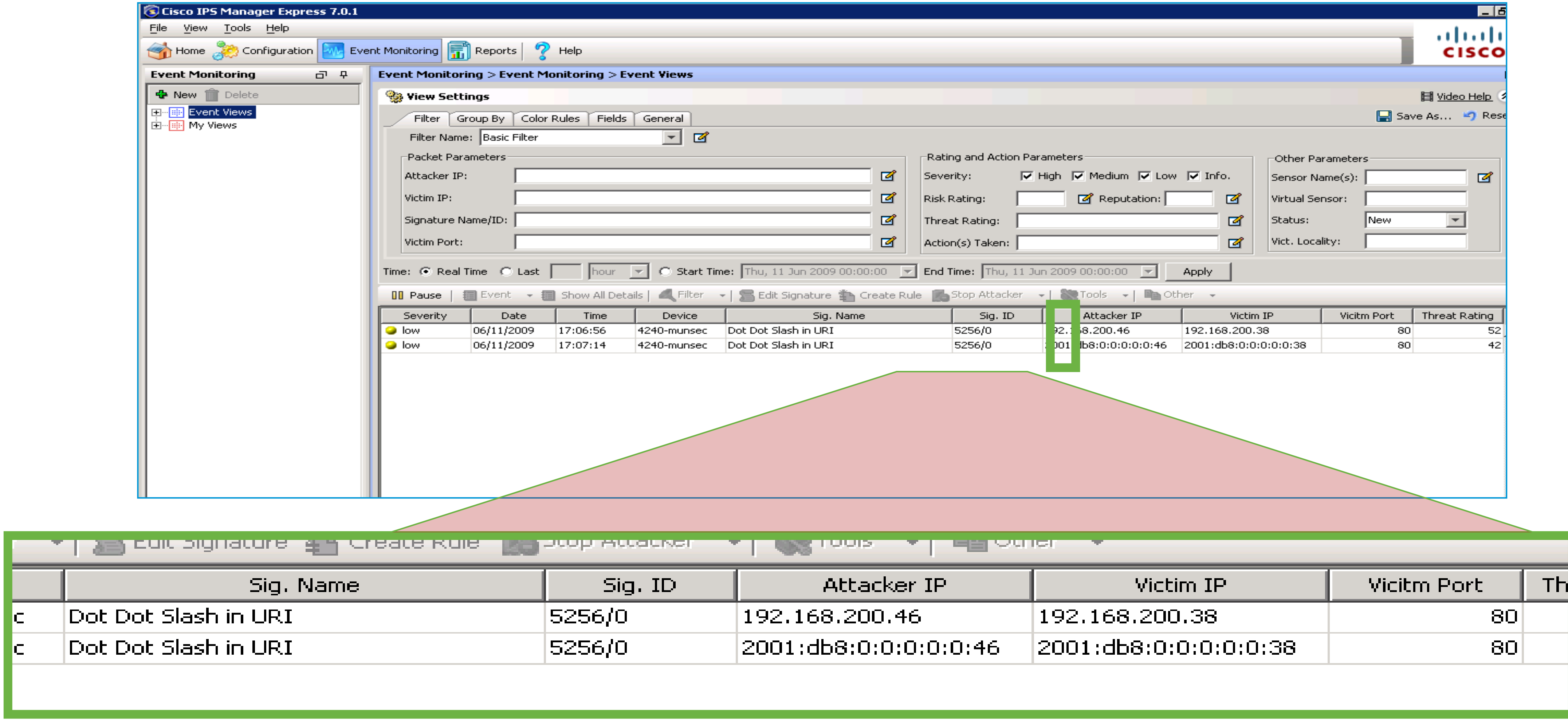
- Since IPS 6.2 (November 2008)
- Engines
  - Specific to IPv6
  - Common to IPv4 and IPv6
  - TCP reset works over IPv4
- *IPS Manager Express* can view IPv6 events
- *IPS Device Manager* can configure IPv6
- All management plane is over IPv4 only
  - Not critical for most customers

IPv6 Support in IPS Policies

- IPv6 Support in
  - Action filter
  - Event variable
  - Target value rating

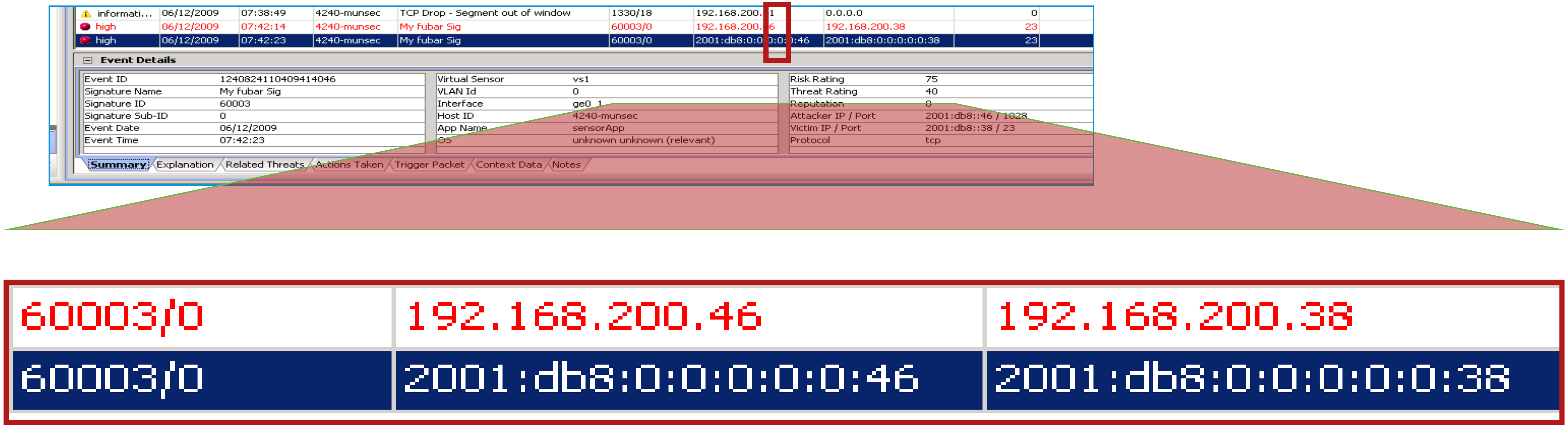


Dual-Stack IPS Engines
Service HTTP



Dual-Stack Engine
String TCP with Custom Signature

- Yet another example of an engine supporting both IPv4 and IPv6



IPv6-Only Engines

- Atomic IPv6 (mostly obsolete)
- Atomic IP Advanced
  - Routing Header type 0
  - Hop-by-Hop
  - ...
- Missing
  - Rogue RA
  - Rogue NA

1700/0	IPv6 Hop-by-Hop Options Present
1701/0	IPv6 Destination Options Header Present
1702/0	IPv6 Routing Header Present
1703/0	IPv6 Fragmented Traffic
1704/0	IPv6 Authentication Header Present
1705/0	IPv6 ESP Header Present
1706/0	Invalid IPv6 Header Traffic Class Field
1707/0	Invalid IPv6 Header Flow Label Field
1710/0	IPv6 Extensions Headers Out Of Order
1711/0	Duplicate IPv6 Extension Headers
1712/0	IPv6 Packet Contains Duplicate Src And Dst Address
1713/0	IPv6 Header Contains Multicast Source Address
1714/0	IPv6 Address Set To localhost
1716/0	IPv6 Options Padding Too Long
1717/0	Back To Back Padding Options
1718/0	IPv6 Option Data Too Short
1719/0	IPv6 Endpoint Identification Option Set
1720/0	IPv6 Jumbo Payload Option Set
1721/0	IPv6 Router Alert Option Set

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)
- ASA-SM
  - Leverage ASA code base, same features ;-) 16 Gbps of IPv6 throughput
- IOS Firewall
  - IOS 12.3(7)T (released 2005)
  - Zone-based firewall on IOS-XE 3.6 (2012)
- IPS
  - Since 6.2 (released 2008)
- Email Security Appliance (ESA) under beta testing early 2010, shipping Q1 2012
- Web Security Appliance (WSA) H2 2012 with explicit proxy
- ScanSafe in two phqses Q2 2012 then Q3 2012

Secure IPv6 Connectivity

Secure IPv6 over IPv4/6 Public Internet

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

Public Network	Site to 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	Q1 2012

Secure Site to Site IPv6 Traffic over IPv4 Public Network with DMVPN

- IPv6 packets over DMVPN IPv4 tunnels
  - In IOS release 12.4(20)T (July 2008)
  - In IOS-XE release 3.5 (end 2011)
  - IPv6 and/or IPv4 data packets over same GRE tunnel
- Complete set of NHRP commands
  - network-id, holdtime, authentication, map, etc.
- NHRP registers two addresses
  - Link-local for routing protocol (Automatic or Manual)
  - Global for packet forwarding (Mandatory)

DMVPN for IPv6
Phase 1 Configuration

For Your Reference

Hub

```
interface Tunnel0
 !... IPv4 DMVPN configuration may be required...
  ipv6 address 2001:db8:100::1/64
  ipv6 eigrp 1
  no ipv6 split-horizon eigrp 1
  no ipv6 next-hop-self eigrp 1
  ipv6 nhrp map multicast dynamic
  ipv6 nhrp network-id 100006
  ipv6 nhrp holdtime 300
  tunnel source Serial2/0
  tunnel mode gre multipoint
  tunnel protection ipsec profile vpnprof
!
interface Ethernet0/0
  ipv6 address 2001:db8:0::1/64
  ipv6 eigrp 1
!
interface Serial2/0
  ip address 172.17.0.1 255.255.255.252
!
ipv6 router eigrp 1
  no shutdown
```

Spoke

```
interface Tunnel0
!... IPv4 DMVPN configuration may be required...
  ipv6 address 2001:db8:100::11/64
  ipv6 eigrp 1
  ipv6 nhrp map multicast 172.17.0.1
  ipv6 nhrp map 2001:db8:100::1/128 172.17.0.1
  ipv6 nhrp network-id 100006
  ipv6 nhrp holdtime 300
  ipv6 nhrp nhs 2001:db8:100::1
  tunnel source Serial1/0
  tunnel mode gre multipoint
  tunnel protection ipsec profile vpnprof
!
interface Ethernet0/0
  ipv6 address 2001:db8:1::1/64
  ipv6 eigrp 1
!
interface Serial1/0
  ip address 172.16.1.1 255.255.255.252
!
ipv6 router eigrp 1
  no shutdown
```

Secure Site to Site IPv6 Traffic over IPv6 Public Network

For Your Reference

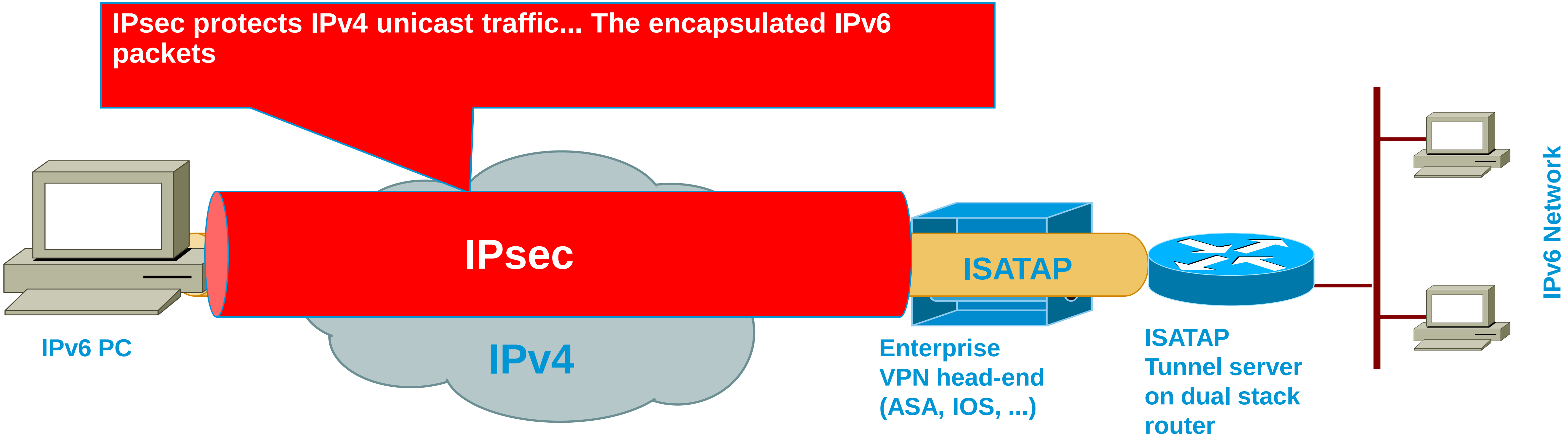
- Since 12.4(6)T, IPsec also works for IPv6
- Using the Virtual Interface

```
interface Tunnel0
 no ip address
 ipv6 address 2001:DB8::2811/64
 ipv6 enable
 tunnel source Serial0/0/1
 tunnel destination 2001:DB8:7::2
 tunnel mode ipsec ipv6
 tunnel protection ipsec profile ipv6
```


IPv6 for Remote Devices Solutions

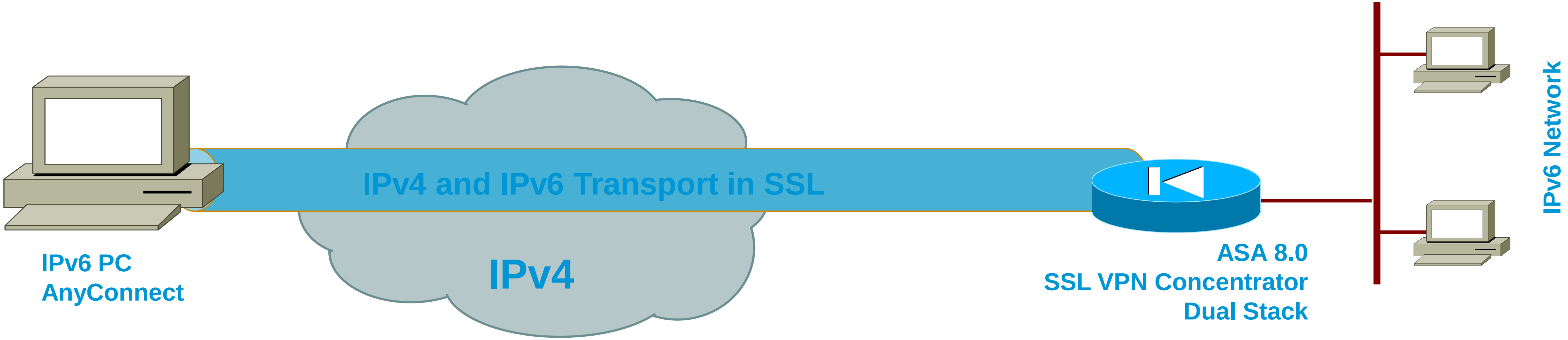
- Enabling IPv6 traffic inside the Cisco VPN Client tunnel
  - NAT and Firewall traversal support
  - Allow remote host to establish a v6-in-v4 tunnel either automatically or manually
    - ISATAP—Intra Site Automatic Tunnel Addressing Protocol
    - Fixed IPv6 address enables server's side of any application to be configured on an IPv6 host that could roam over the world
- Use of ASA 8.0 and SSL VPN Client AnyConnect 3.0 (Windows, Android, iPhone)
  - Can transfer IPv4+IPv6 traffic over public IPv4
    - DNS is still IPv4-only, no split tunneling only
  - Mid-2012 with ASA 8.6 and AC 3.1, IPv4+IPv6 traffic over public IPv6 and over IPsec or SSL *(roadmap, date can change)*

Secure RA IPv6 Traffic over IPv4 Public Network: ISATAP in IPSec



IPsec with NAT-T can traverse NAT
ISATAP encapsulates IPv6 into IPv4

Secure RA IPv6 Traffic over IPv4 Public Network: AnyConnect SSL VPN Client



ASA 8.0 and AnyConnect 2.0 for IPv6 transport

- Since 8.0 ASA SSL VPN and AnyConnect can transport IPv6

```
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface

ipv6 local pool POOL_V6 2001:db8:5fff:81::1:1/64 8

tunnel-group DefaultWEBVPNGroup general-attributes
...
ipv6-address-pool POOL_V6
```

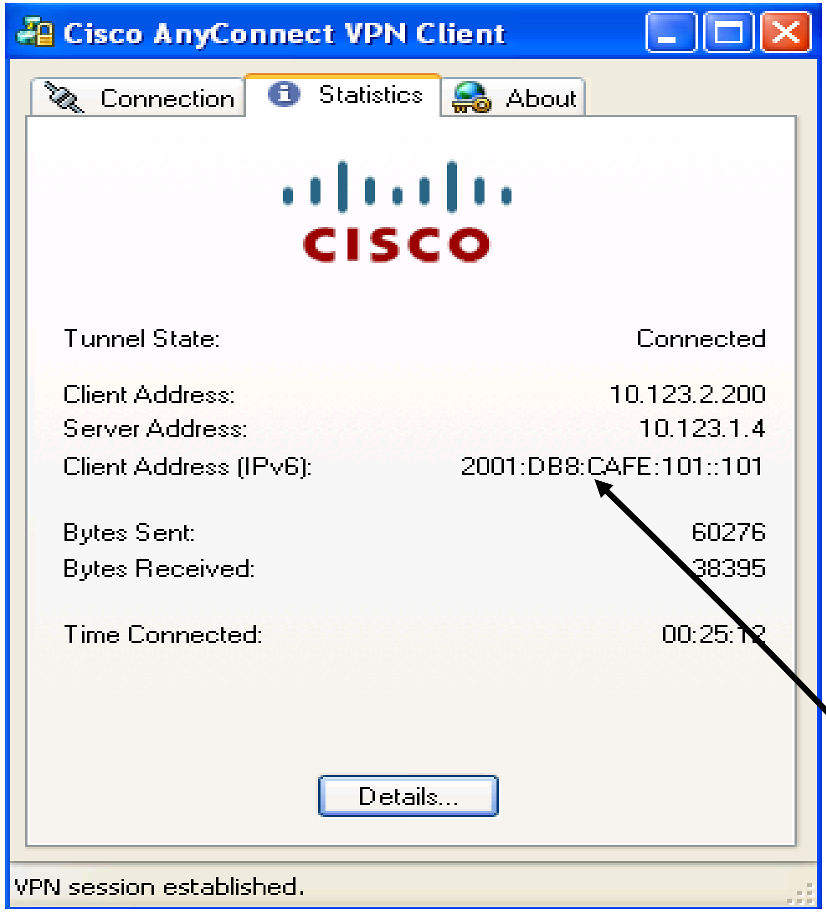
```
Ethernet adapter Cisco AnyConnect VPN Client Connection:

        Connection-specific DNS Suffix  . : cisco.com
        IP Address. . . . . . . . . . . . : 192.168.0.200
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        IP Address. . . . . . . . . . . . : 2001:db8:5fff:81::1:1
        IP Address. . . . . . . . . . . . : fe80::205:9aff:fe3c:7a00%13
        Default Gateway . . . . . . . . . : 192.168.0.1
                                            2001:db8:5fff:81::
```

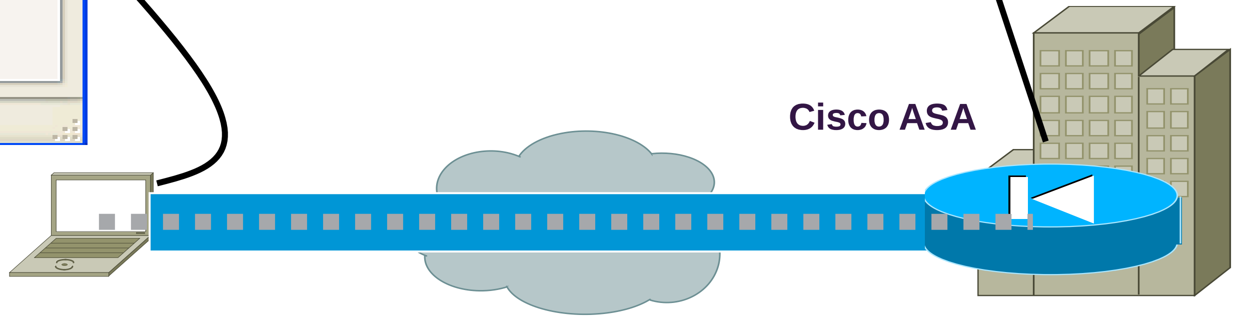
ASA with IPv6

```
name 2001:db8:cafe:1003:: BR1-LAN description VLAN on EtherSwitch
name 2001:db8:cafe:1004:9db8:3df1:814c:d3bc Br1-v6-Server
!
interface GigabitEthernet0/0
 description TO WAN
 nameif outside
 security-level 0
 ip address 10.124.1.4 255.255.255.0 standby 10.124.1.5
 ipv6 address 2001:db8:cafe:1000::4/64 standby 2001:db8:cafe:1000::5
!
interface GigabitEthernet0/1
 description TO BRANCH LAN
 nameif inside
 security-level 100
 ip address 10.124.3.1 255.255.255.0 standby 10.124.3.2
 ipv6 address 2001:db8:cafe:1002::1/64 standby 2001:db8:cafe:1002::2
!
ipv6 route inside BR1-LAN/64 2001:db8:cafe:1002::3
ipv6 route outside ::/0 fe80::5:73ff:fea0:2
!
ipv6 access-list v6-ALLOW permit icmp6 any any
ipv6 access-list v6-ALLOW permit tcp 2001:db8:cafe::/48 host Br1-v6-Server object-group RDP
!
failover
failover lan unit primary
failover lan interface FO GigabitEthernet0/2
failover link FO-LINK GigabitEthernet0/3
failover interface ip FO 2001:db8:cafe:bad::1/64 standby 2001:db8:cafe:bad::2
failover interface ip FO-LINK 2001:db8:cafe:bad1::1/64 standby 2001:db8:cafe:bad1::2
!
access-group v6-ALLOW in interface outside
```

AnyConnect 2.x—SSL VPN




```
asa-edge-1#show vpn-sessiondb svc
Session Type: SVC
Username     : ciscoese                    Index       : 14
Assigned IP  : 10.123.2.200                Public IP   : 10.124.2.18
Assigned IPv6: 2001:db8:cafe:101::101
Protocol     : Clientless SSL-Tunnel DTLS-Tunnel
License      : SSL VPN
Encryption   : RC4 AES128                  Hashing     : SHA1
Bytes Tx     : 79763                       Bytes Rx    : 176080
Group Policy : AnyGrpPolicy                Tunnel Group: ANYCONNECT
Login Time   : 14:09:25 MST Mon Dec 17 2007
Duration     : 0h:47m:48s
NAC Result   : Unknown
VLAN Mapping : N/A                         VLAN        : none
```



Dual-Stack Host AnyConnect Client

Summary

Key Take Away

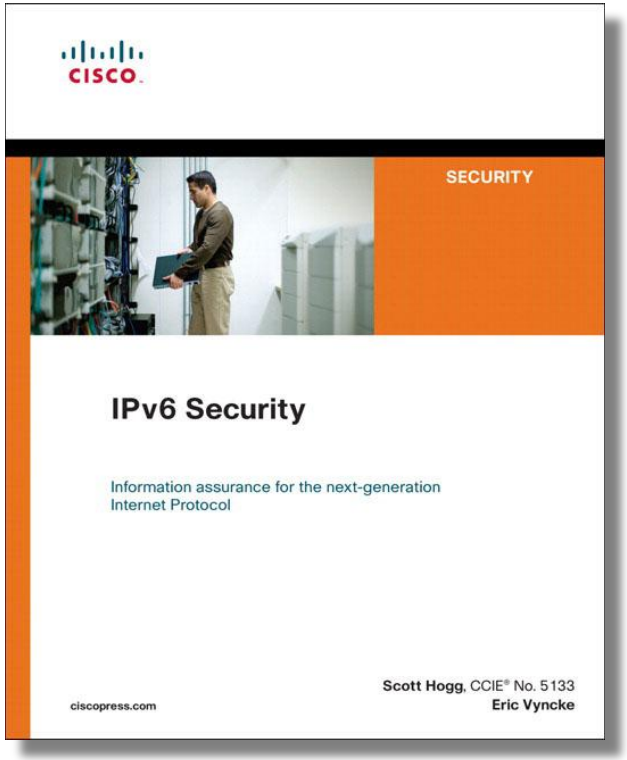
- So, nothing really new in IPv6
  - Reconnaissance: address enumeration replaced by DNS enumeration
  - Spoofing & bogons: uRPF is our IP-agnostic friend
  - NDP spoofing: RA guard and more feature coming
  - ICMPv6 firewalls need to change policy to allow NDP
  - Extension headers: firewall & ACL can 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

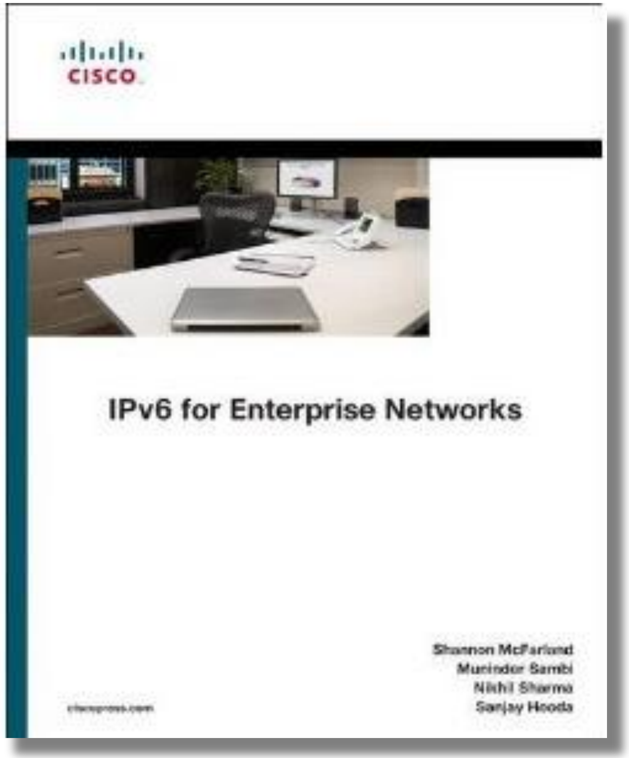
Is IPv6 in My Network?

- Easy to check!
- Look inside NetFlow records
  - Protocol 41: IPv6 over IPv4 or 6to4 tunnels
  - IPv4 address: 192.88.99.1 (6to4 anycast server)
  - UDP 3544, the public part of Teredo, yet another tunnel
- Look into DNS server log for resolution of ISATAP
- Beware of the IPv6 latent threat: ***your IPv4-only network may be vulnerable to IPv6 attacks NOW***

Q&A

Recommended Reading





Source: Cisco Press

Thank you.