
TOMORROW starts here.
cisco
Cisco live!

IPv6 Security

BRKSEC-2003

Frederic Detienne

Distinguished Engineer

Cisco live!

Session Objectives

- Leverage existing IPv4 network security knowledge
- Advanced IPv6 security topics like transition options and dual stack environments
- Main focus is on enterprise issues
- 50% of overlap with BRKSPG-2603 which is more for SP
- Requirements: basic knowledge of the IPv6 and IPsec protocols as well as IPv4 network security best practices

References...

For Your Reference

- There are more slides in the hand-outs than presented during the class
- Those slides are mainly for reference and are indicated by the book icon on the top right corner (as on this slide)
- Some slides have also a call-out to another session (see below)

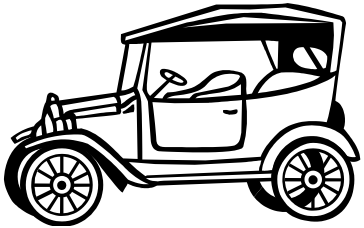
Agenda

- Debunking IPv6 Myths
- Shared Issues by IPv4 and IPv6
- Specific Issues for IPv6
  - Extension headers, IPsec everywhere, transition techniques
- Enforcing a Security Policy in IPv6
  - ACL, firewalls, IPS, content security
- Enterprise Secure Deployment
  - Secure IPv6 transport over public network
- Summary

Experiment with IPv6 over WiFi at Cisco Live

IPv6 Security Myths…

IPv6 Myths: Better, Faster, More Secure



Sometimes, newer means better and more secure

Sometimes, experience IS better and safer!

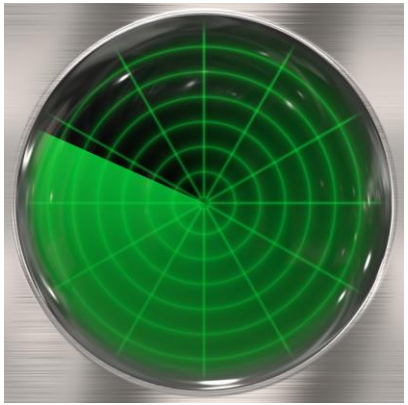
Source: Microsoft clip-art gallery

The Absence of Reconnaissance Myth

- Default subnets in IPv6 have 2^{64} addresses
  - 10 Mpps = more than 50 000 years

Source: Microsoft clip-art gallery

Reconnaissance in IPv6
Scanning Methods Will Change



Source: Microsoft clip-art gallery

- If using EUI-64 addresses, just scan 2^{48}
  - Or even 2^{24} if vendor OUI is known...
- 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
  - ::1,::80,::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

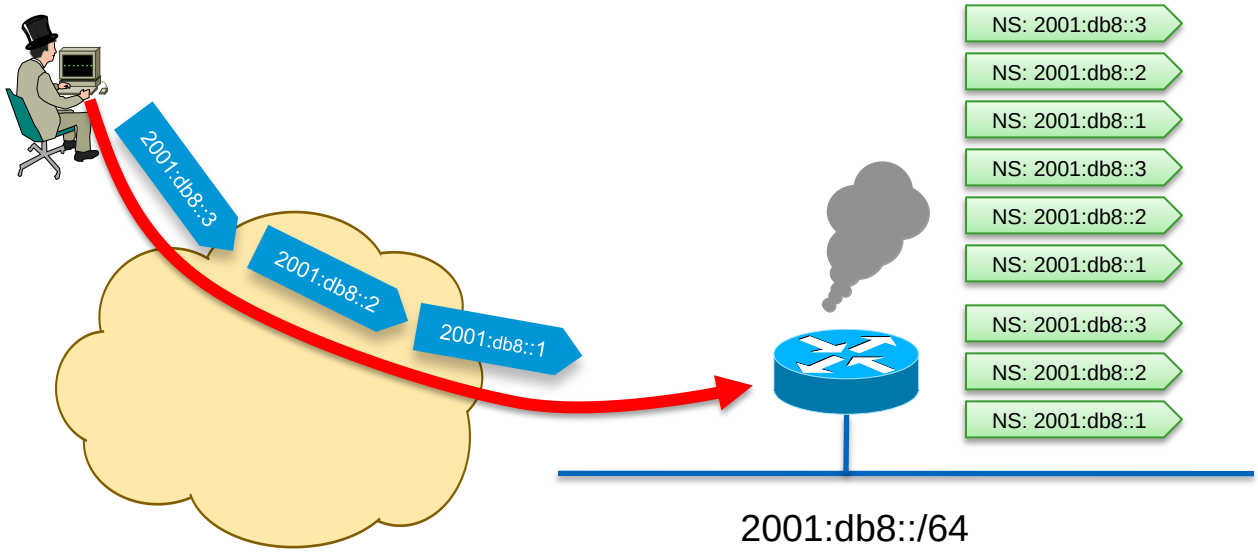
- Viruses and email, IM worms: IPv6 brings no change
- Other worms:
  - IPv4: reliance on network scanning
  - IPv6: not so easy (see reconnaissance) => will use alternative techniques

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

Scanning Made Bad for CPU

Remote Neighbour Cache Exhaustion

- Potential router CPU/memory attacks if aggressive scanning
  - Router will do Neighbour Discovery... And waste CPU and memory
- Local router DoS with NS/RS/…



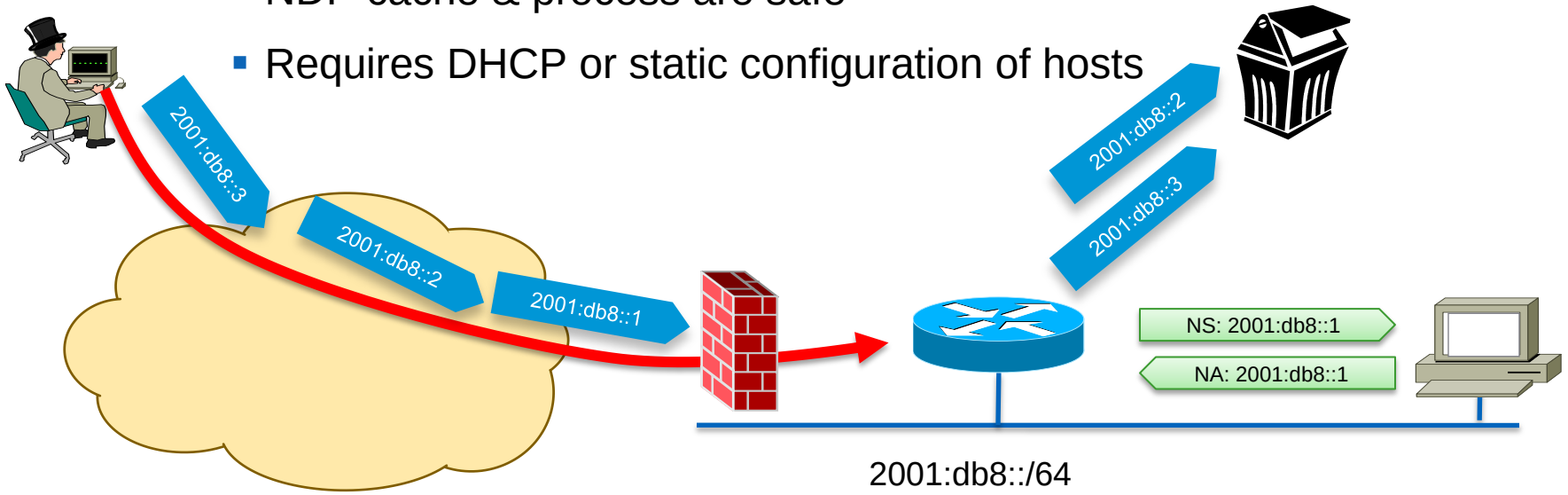
Mitigating Remote Neighbour Cache Exhaustion

- IOS built-in rate limiter with options 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 part of First Hop Security phase 3
  - Priority given to refresh existing entries vs. discovering new ones
- Using a /64 on **point-to-point links** => a lot of addresses to scan!
  - Using /127 could help (RFC 6164) but then no SLAAC
- **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 ☺

http://www.insinuator.net/2013/03/ipv6-neighbor-cache-exhaustion-attacks-risk-assessment-mitigation-strategies-part-1

Simple Fix for Remote Neighbour Cache Exhaustion

- Ingress ACL allowing only valid destination and dropping the rest
- NDP cache & process are safe
- Requires DHCP or static configuration of hosts



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

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

“Security expert, W., a professor at the University of <foo> in the UK, told <newspaper> the new protocol system – IPv6 – comes with a security code known as IPSEC that would do away with anonymity on the web.

If enacted globally, this would make it easier to catch cyber criminals, Prof W. said.”

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 organisations 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

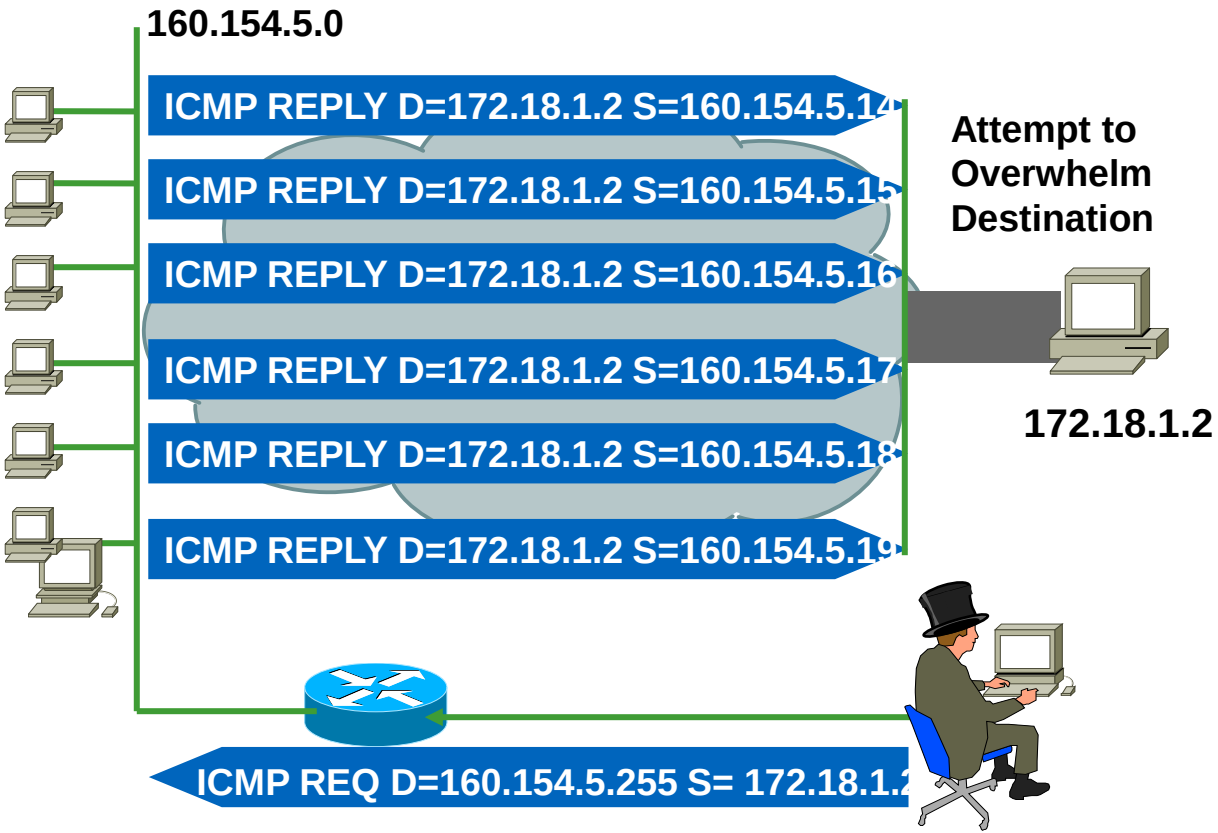
    IOS 12.4(20)T can parse the AH
  - Network telemetry is blinded: NetFlow of little use
  - Network services hindered: what about QoS?

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

Quick Reminder

IPv4 Broadcast Amplification: Smurf



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

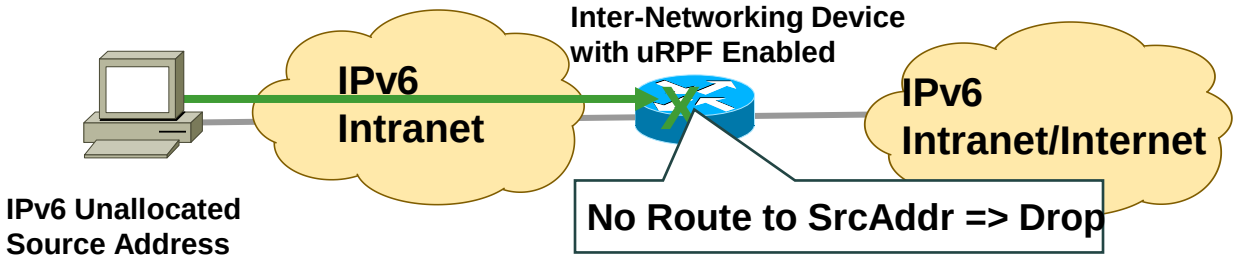
•Note: anti-spoofing also blocks amplification attacks because a remote attacker cannot masquerade as his victim




Shared Issues

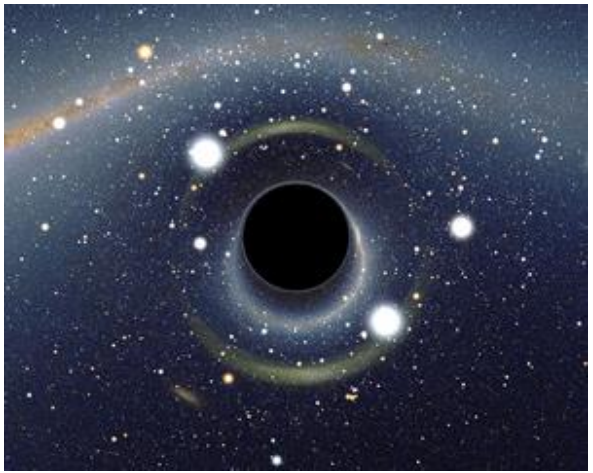
IPv6 Bogon and Anti-Spoofing Filtering

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



Remote Triggered Black Hole

- RFC 5635 RTBH is easy in IPv6 as in IPv4
- uRPF is also your friend for black hole-ing a source
- RFC 6666 has a specific discard prefix
  - 100::/64



Source: Wikipedia Commons

- http://www.cisco.com/web/about/security/intelligence/ipv6_rtbh.html

Neighbour Discovery Issue#1
SLAAC Rogue Router Advertisement

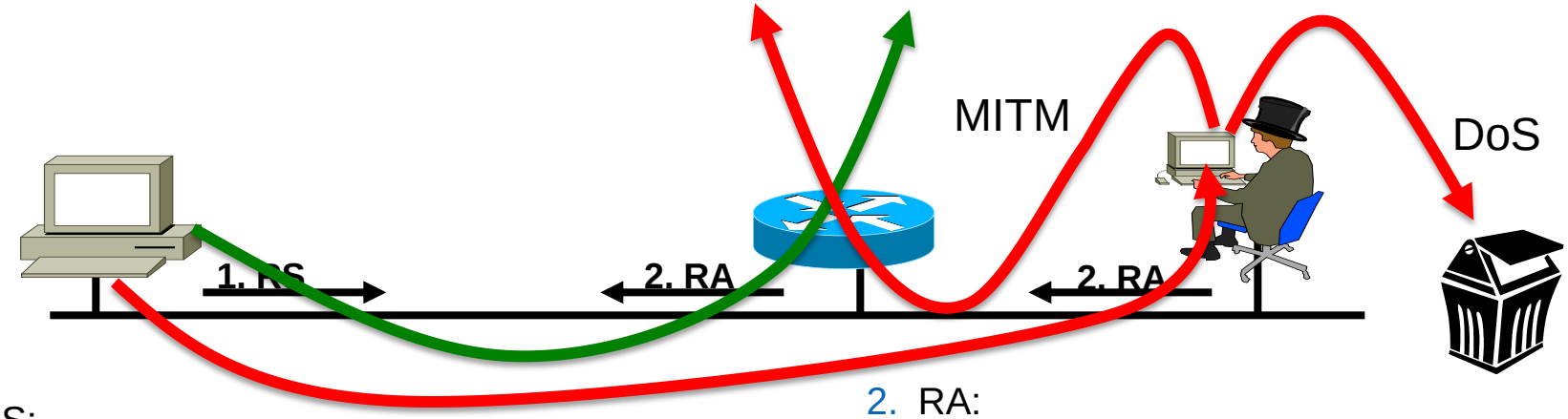
Router Advertisements (RA) contains:

-Prefix to be used by hosts

-Data-link layer address of the router

-Miscellaneous options: MTU, DHCPv6 use, …

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



1. RS:
   - –Data = Query: please send RA

2. RA:
   - –Data= options, prefix, lifetime, A+M+O flags

Neighbour Discovery Issue#2

Neighbour Solicitation

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

Security Mechanisms Built into Discovery Protocol = None

Last Come is Used

=> Very similar to ARP

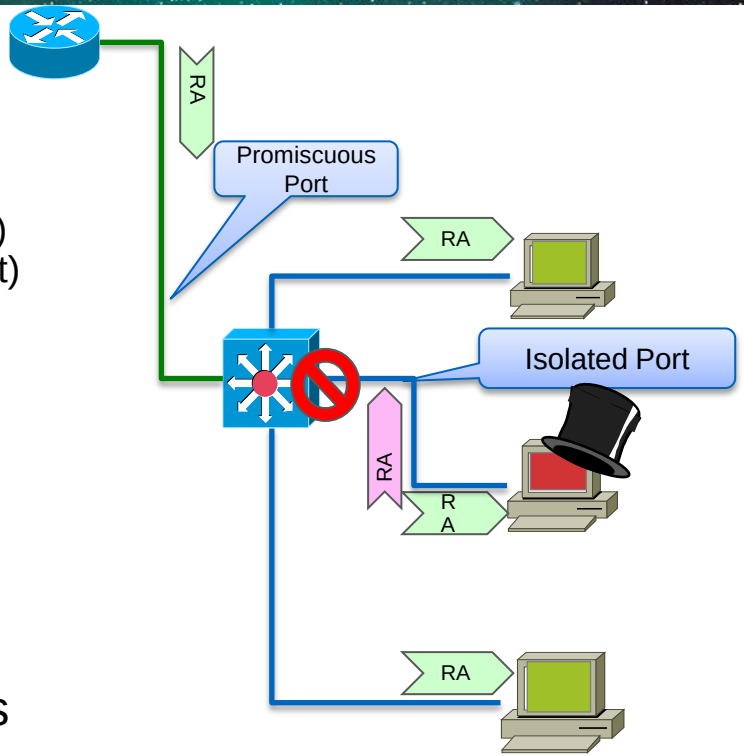
Attack Tool:
Parasite6
Answer to all NS, Claiming to Be All Systems in the LAN...

ARP Spoofing is now NDP Spoofing:
Mitigation

- **GOOD NEWS**: dynamic ARP inspection for IPv6 is available
  - First phase (Port ACL & RA Guard) available since Summer 2010
  - Second phase (NDP & DHCP snooping) available since Summer 2011
  - http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-first_hop_security.html
- **(kind of) GOOD NEWS**: Secure Neighbour 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 801.X works with IPv6 (except downloadable ACL)

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
  - Side effect: breaks Duplicate Address Detection (DAD) if prefix is advertised as on-link



First Hop Security: RAguard Since 2010 (RFC 6101)

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

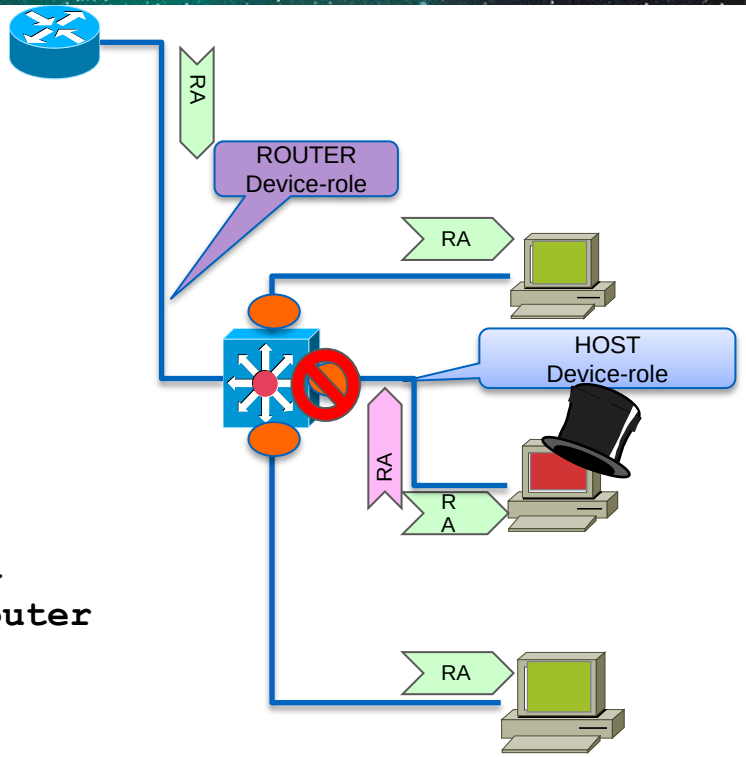
```
interface FastEthernet0/2
  ipv6 traffic-filter ACCESS_PORT in
  access-group mode prefer port
```

- **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
```

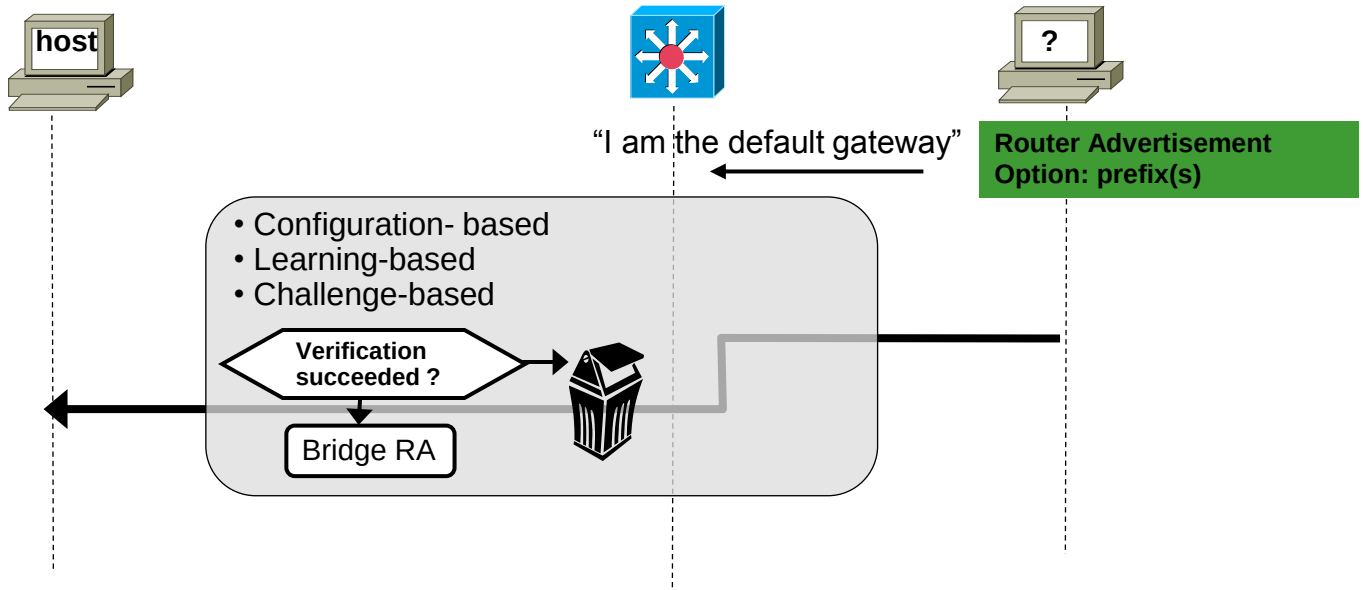
- **RA-guard** (12.2(50)SY, 15.0(2)SE)

```
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
```



RA-Guard

Goal: mitigate against rogue RA



- 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 Snooping Logging

```
Sw1(config)# ipv6 neighbor binding logging
```

```
*Oct  4 21:38:22.199: %SISF-4-PAK_DROP: Message dropped
A=FE80::60DE:29FF:FE15:2 G=- V=100 I=Et0/0 P=NDP::NA Reason=Advertise while
TENTATIVE
*Oct  4 21:38:22.199: %SISF-6-ENTRY_CREATED: Entry created
A=FE80::60DE:29FF:FE15:2 V=100 I=Et0/0 P=0005 M=
*Oct  4 21:38:23.275: %SISF-6-ENTRY_CHANGED: Entry changed
A=FE80::60DE:29FF:FE15:2 V=100 I=Et0/0 P=0005 M=
*Oct  4 21:38:33.841: %SISF-6-ENTRY_CHANGED: Entry changed
A=FE80::60DE:29FF:FE15:2 V=100 I=Et0/0 P=0005 M=62DE.2915.0002
```

REALLY key for audit-trail and attribution: the only way to know the mapping of <MAC, IPv6> addresses when using Temporary addresses

IPv6 and the LAN Access

IPv6 FHS	C6K	C4K	C3K	C2K	WLC
RA Guard	12.2(50)SY and 15.0(1)SY	12.2(54)SG	15.0(2)SE	15.0(2)SE	7.2
DHCP Guard	2013	XE 3.4.xSG 15.1(2)SG	15.0(2)SE	15.0(2)SE	7.2
Binding Integrity Guard	2013	XE 3.4.xSG 15.1(2)SG	15.0(2)SE	15.0(2)SE	7.2
Source Guard	2013	MID 2013	15.0(2)SE	15.0(2)SE	7.2
Destination Guard	2013	XE 3.4.xSG 15.1(2)SG	15.0(2)SE	15.0(2)SE	7.2

ICMPv4 vs. ICMPv6

- Significant changes
- More relied upon

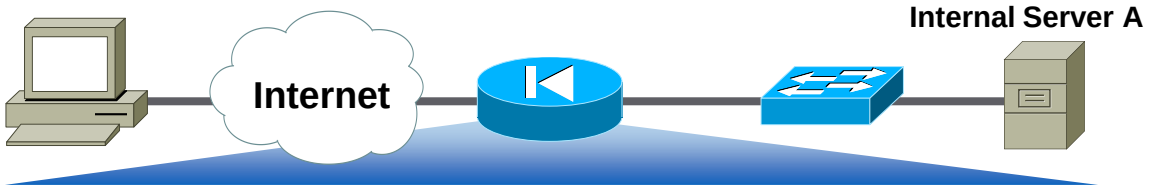
ICMP Message Type	ICMPv4	ICMPv6
Connectivity Checks	X	X
Informational/Error Messaging	X	X
Fragmentation Needed Notification	X	X
Address Assignment		X
Address Resolution		X
Router Discovery		X
Multicast Group Management		X
Mobile IPv6 Support		X

- => ICMP policy on firewalls needs to change

Generic ICMPv4

For Your Reference

Border Firewall Policy

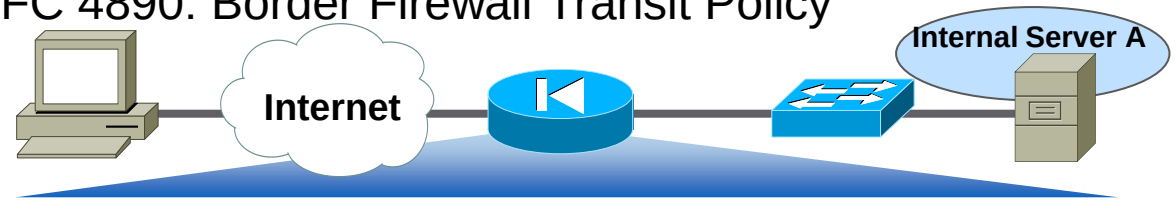


Action	Src	Dst	ICMPv4 Type	ICMPv4 Code	Name
Permit	Any	A	0	0	Echo Reply
Permit	Any	A	8	0	Echo Request
Permit	Any	A	3	0	Dst. Unreachable—Net Unreachable
Permit	Any	A	3	4	Dst. Unreachable—Frag. Needed
Permit	Any	A	11	0	Time Exceeded—TTL Exceeded

Equivalent ICMPv6

For Your Reference

RFC 4890: Border Firewall Transit Policy



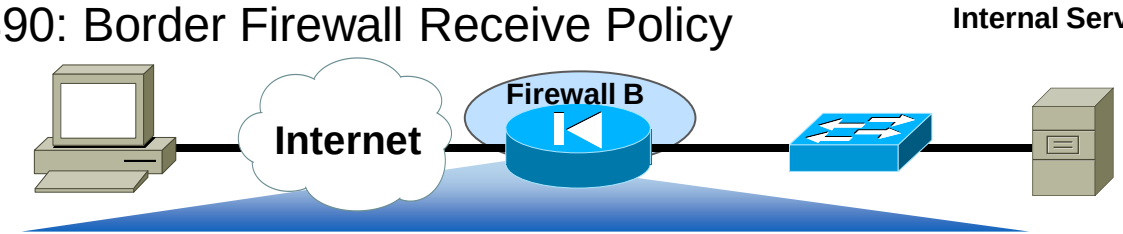
Action	Src	Dst	ICMPv6 Type	ICMPv6 Code	Name
Permit	Any	A	128	0	Echo Reply
Permit	Any	A	129	0	Echo Request
Permit	Any	A	1	0	No Route to Dst.
Permit	Any	A	2	0	Packet Too Big
Permit	Any	A	3	0	Time Exceeded—HL Exceeded
Permit	Any	A	4	0	Parameter Problem

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	135/136	0	Neighbour Solicitation and Advertisement
Deny	Any	Any			

For locally generated by the device

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 if and only if hop-limit = 255
  - Notably used by Neighbour Discovery

- Can be leveraged by malevolent people
  - Evade inspection: hackers send some IPv6 packets analysed by the IPS but further dropped by the network before reaching destination… Could evade some IPS
  - Can be used to guess topology on internal network
  - **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 rely on transport mode IPsec (for authentication and **confidentiality**)
  - But see RFC 6506 *(but not widely implemented yet)*
- IPv6 routing attack best practices
  - Use traditional authentication mechanisms on BGP and IS-IS
  - Use IPsec to secure protocols such as OSPFv3

OSPF or EIGRP Authentication

For Your Reference

```
interface Ethernet0/0
 ipv6 ospf 1 area 0
 ipv6 ospf authentication ipsec spi 500 md5
  1234567890ABCDEF1234567890ABCDEF
```

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

key chain MYCHAIN
 key 1
key-string 1234567890ABCDEF1234567890ABCDEF
accept-lifetime local 12:00:00 Dec 31 2011 12:00:00 Jan 1 2012
send-lifetime local 00:00:00 Jan 1 2012 23:59:59 Dec 31 2013
```

No crypto maps, no ISAKMP: transport mode with static session keys

IPv6 Attacks with Strong IPv4 Similarities

- Sniffing
  - IPv6 is no more or less likely to fall victim to a sniffing attack than IPv
- 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 utilising 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-2011-2393	Feb 2012	FreeBSD OpenBSD NetBSD and others	Local users DoS with RA flooding
CVE-2012-4444	Dec 2012	Linux	Bypassing fragmentation protection
CVE-2012-4623	Oct 2012	IOS	Remote DoS against DHCPv6 server
CVE-2008-1576	Jun 2008	Apple Mac OS X	Buffer overflow in Mail over IPv6
CVE-2012-0179	May 2012	Microsoft	Local privilege escalation

Source: http://cve.mitre.org/cve/

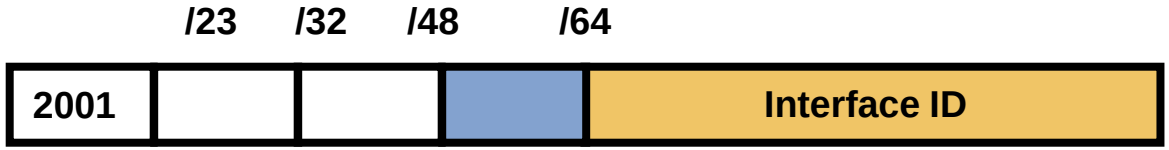
IPv6 Security shares 95% with IPv4 security




Specific IPv6 Issues

IPv6 Privacy Extensions (RFC 4941)

AKA Temporary Addresses



- 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

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)
  - Or

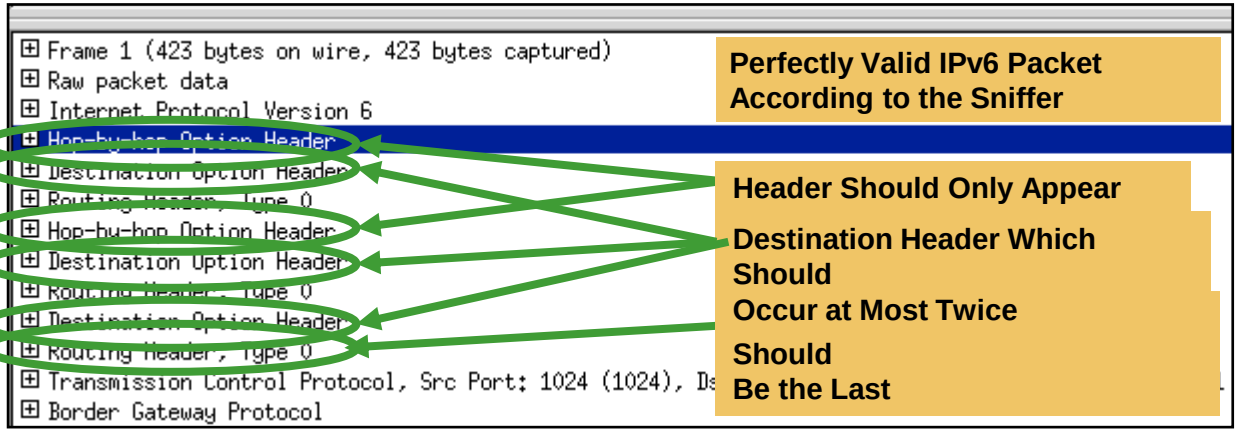
```
netsh interface ipv6 set global randomizeidentifiers=disabled
netsh interface ipv6 set global randomizeidentifiers=disabled store=persistent
netsh interface ipv6 set privacy state=disabled store=persistent
```

- 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
  - Use DHCP to a specific pool + ingress ACL allowing only this pool

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

IPv6 Header Manipulation

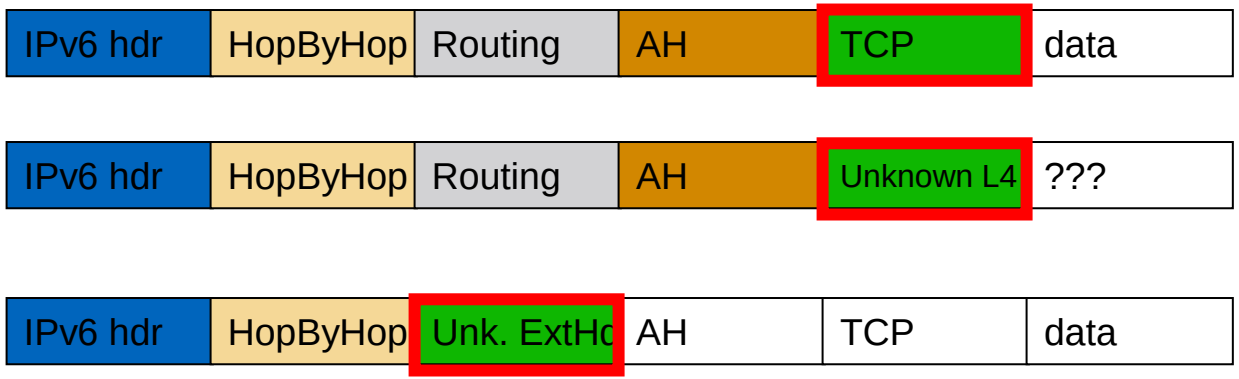
- Unlimited size of header chain (spec-wise) can make filtering difficult
- Potential DoS with poor IPv6 stack implementations
  - More boundary conditions to exploit
  - Can I overrun buffers with a lot of extension headers?
  - Mitigation: a firewall such as ASA which can filter on headers



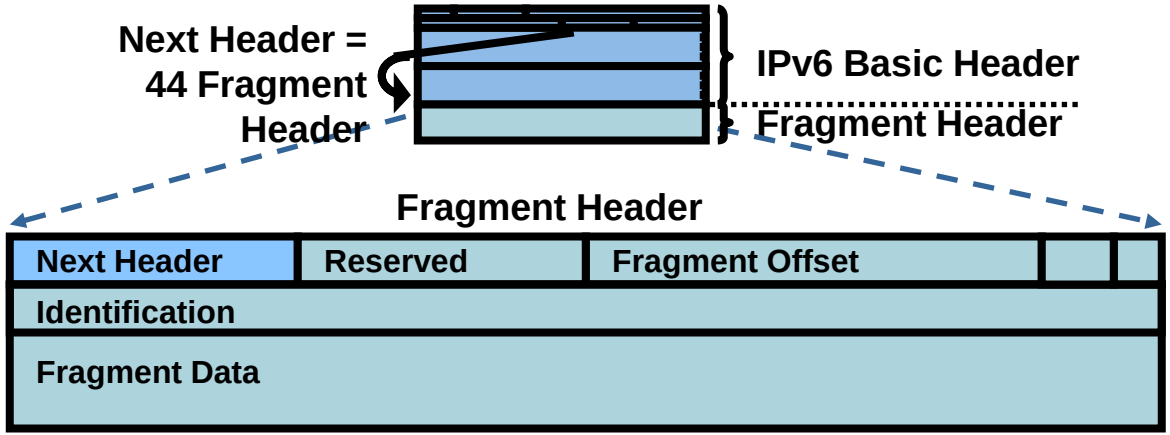
http://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8054d37d.html

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 => MATCH
  - Or unknown extension header/layer 4 header found... => NO MATCH



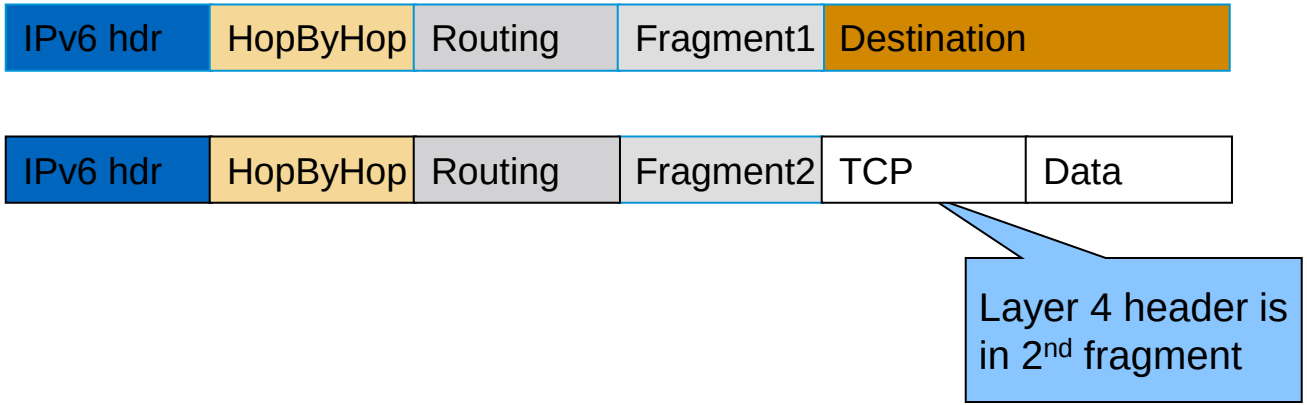
Fragment Header: IPv6



- In IPv6 fragmentation is done only by the end system
  - Tunnel end-points are end systems => Fragmentation / re-assembly can happen inside the network
- Reassembly done by end system like in IPv4
- RFC 5722: overlapping fragments => MUST drop the packet. Most OS implement it in 2012
- Attackers can still fragment in intermediate system on purpose
- ==> a great obfuscation tool

Parsing the Extension Header Chain
Fragmentation Matters!

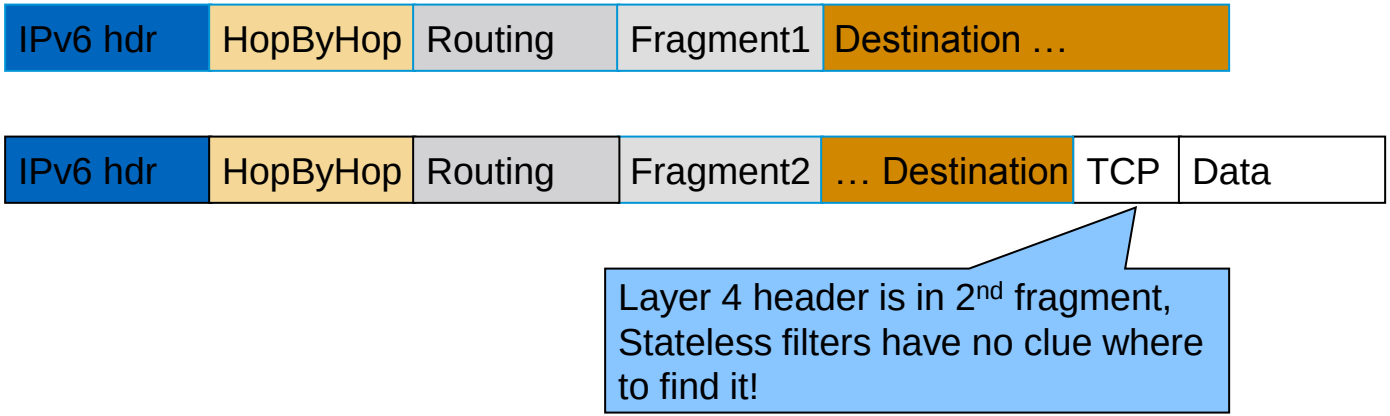
- Extension headers chain can be so large than it must be fragmented!
- RFC 3128 is not applicable to IPv6
- Layer 4 information could be in 2nd fragment



Parsing the Extension Header Chain

Fragments and Stateless Filters

- 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)
- `undertermined-transport` keyword does not match
  - If non-initial fragment
  - Or if TCP/UDP/SCTP and ports are in the fragment
  - Or if ICMP and type and code are in the fragment
  - Everything else matches (including OSPFv3, RSVP, GRE, ESP, EIGRP, PIM …)
  - Only for deny ACE

Is there NAT for IPv6?
"I need it for security"

- Network Prefix Translation, RFC 6296,
  - 1:1 stateless prefix translation allowing all inbound/outbound packets.
  - Main use case: multi-homing
- Else, IETF has not specified any N:1 stateful translation (aka overload NAT or NAPT) for IPv6
- Do not confuse stateful firewall and NAPT even if they are often co-located
- Nowadays, NAPT (for IPv4) does not help security
  - Host OS are way more resilient than in 2000
  - Hosts are mobile and cannot always be behind your 'controlled NAPT'
  - Malware are not injected from 'outside' but are fetched from the 'inside' by visiting weird sites or installing any trojanised application

"“By looking at the IP addresses in the Torpig headers we are able to determine that 144,236 (78.9%) of the infected machines were behind a NAT, VPN, proxy, or firewall. We identified these hosts by using the non-publicly routable IP addresses listed in RFC 1918: 10/8, 192.168/16, and 172.16-172.31/16”

Stone-Gross et al., “Your Botnet is My Botnet: Analysis of a Botnet Takeover”, 2009

http://www.cs.ucsb.edu/~rgilbert/pubs/torpig_ccs09.pdf

PCI DSS 2.0 Compliance and IPv6

- Payment Card Industry Data Security Standard *(latest revision October 2010)*:
  - Requirement 1.3.8 *Do not disclose private IP addresses and routing information to unauthorised parties.*
    Note: Methods to obscure IP addressing may include, but are ***not limited*** *to: Network Address Translation (NAT)*
- ➔ how to comply with PCI DSS?
  - Application proxies or SOCKS
  - Strict data plane filtering with ACL
  - Strict routing plane filtering with BGP route-maps

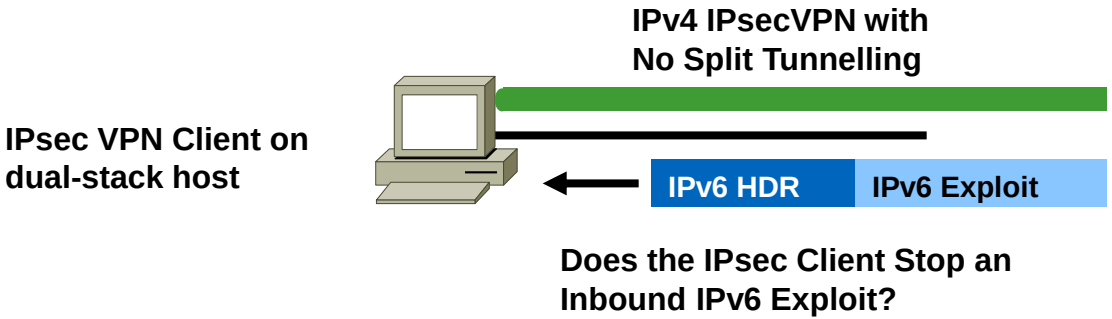
- PCI DSS 2.0 Third Edition (Summer 2013) should be IPv6 aware
- Cisco IPv6 design for PCI with IPv6
  - http://www.cisco.com/en/US/docs/solutions/Enterprise/Compliance/Compliance_DG/PCI_20_DG.pdf

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,SM                    tu 1500
             ether 00:26:bb:
             inet6 fe80::22                        peid 0x6
             inet 10.19.19.1                    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:bbff:fe
16 bytes from fe80::226:bbff:                          140 ms
. . .
16 bytes from fe80::cabc:                              02.112 ms
^C
--- ff02::1%en1 ping6 statistics
4 packets transmitted, 4 packets recei      d, +142 duplicates, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.140/316.721/2791.178/412.276 ms
```

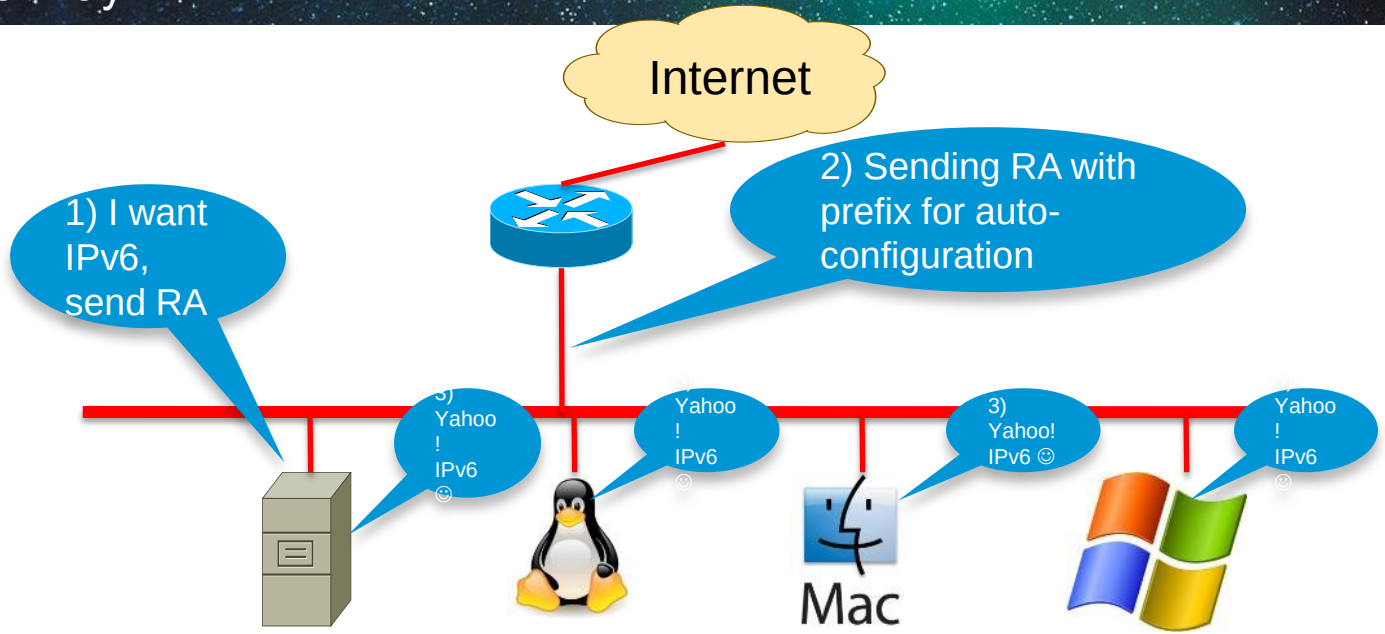
Humm…
Are there any IPv6 peers?

```
$ ndp -an
Neighb
200
. . .
$ ndp
      64
```

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

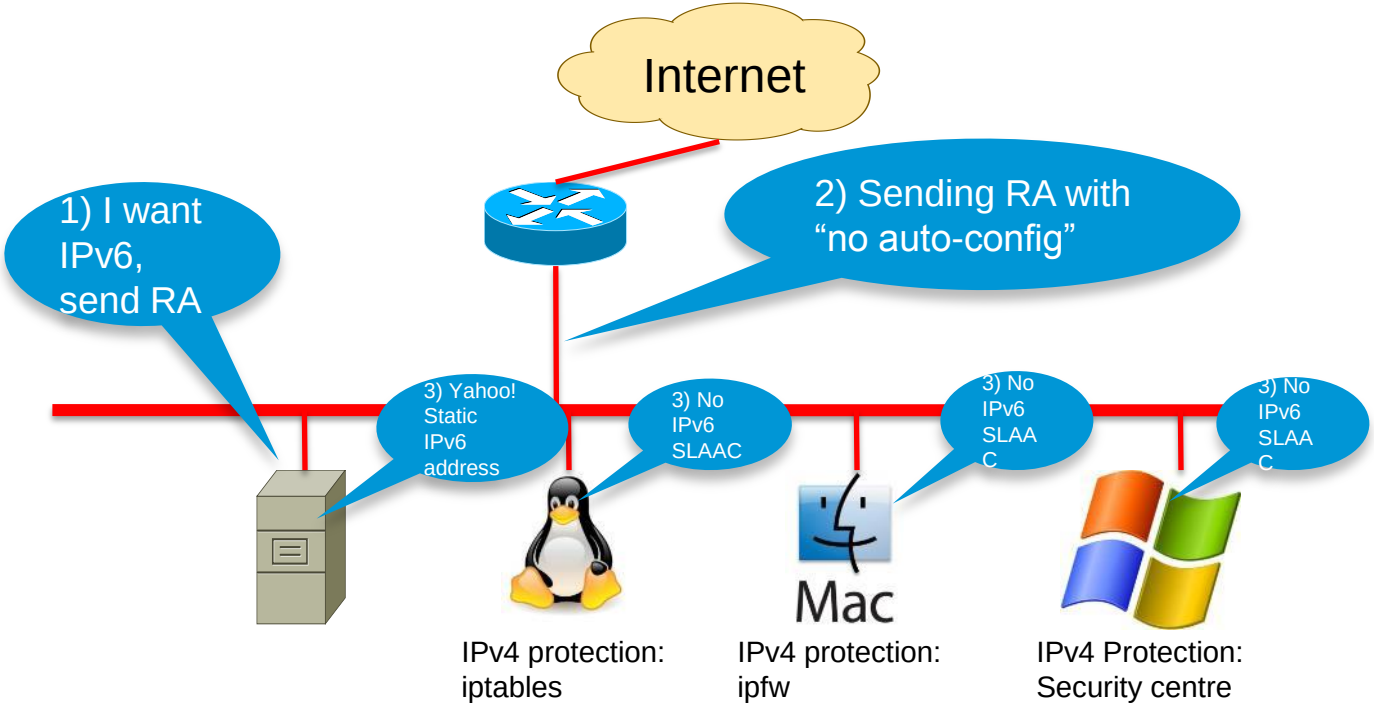
Enabling IPv6 in the IPv4 Data Centre

The Fool's Way



Mac OS X 10.7 now uses packet filter which is dual-stack

Enabling IPv6 in the IPv4 Data Centre
The Right Way



Vulnerability Scanning in a Dual-Stack World

- Finding all hosts:
  - Address enumeration does not work for IPv6
  - Need to rely on DNS or NDP caches or NetFlow
- Vulnerability scanning
  - IPv4 global address, IPv6 global address(es) (if any), IPv6 link-local address
  - Some services are single stack only (currently mostly IPv4 but who knows...)
  - Personal firewall rules could be different between IPv4/IPv6
- **IPv6 vulnerability scanning MUST be done for IPv4 & IPv6 even in an IPv4-only network**
  - IPv6 link-local addresses are active by default

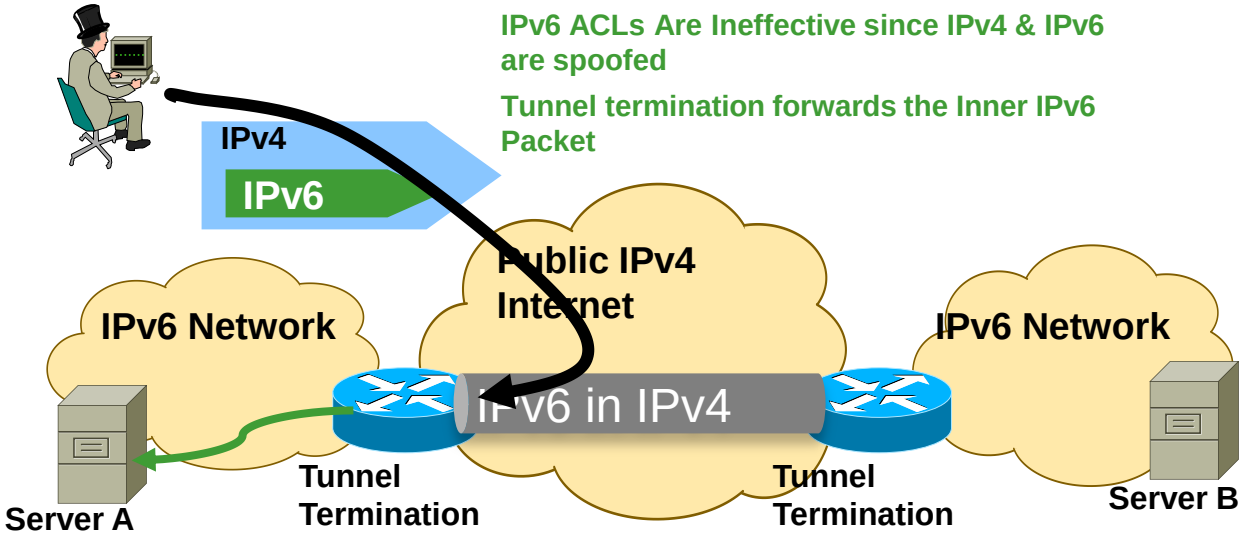
IPv6 Tunnelling Summary

- 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

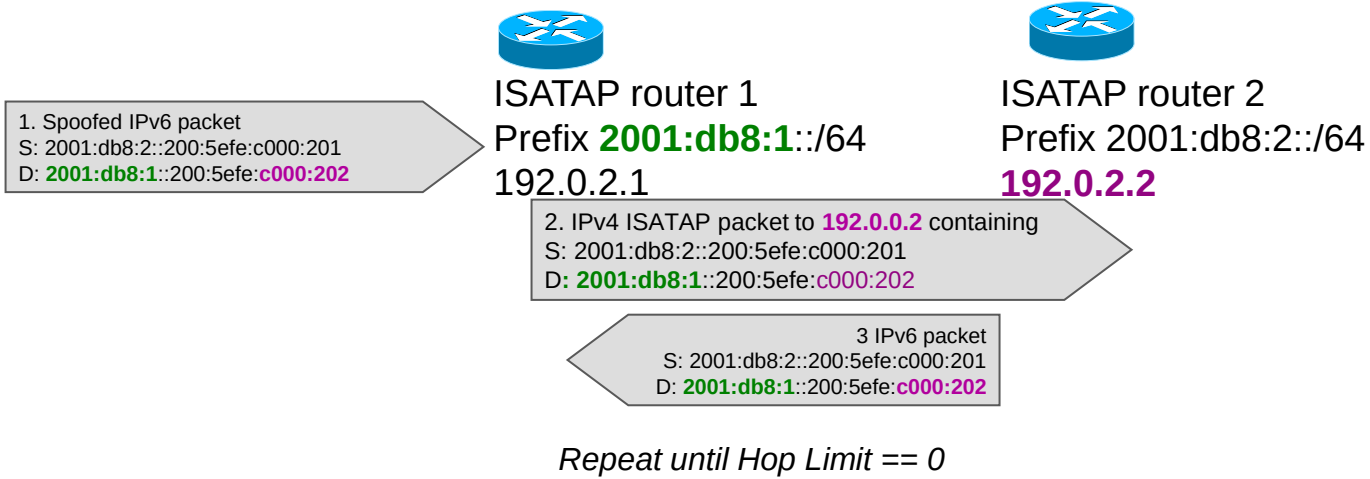
- Only allow authorised endpoints to establish tunnels
- Static tunnels are deemed as “more secure,” but less scalable
- Automatic tunnelling mechanisms are susceptible to packet forgery and DoS attacks
- These tools have the same risk as IPv4, just new avenues of exploitation
- Automatic IPv6 over IPv4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

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 IPv6 traffic** if spoofing on IPv4 and IPv6 addresses



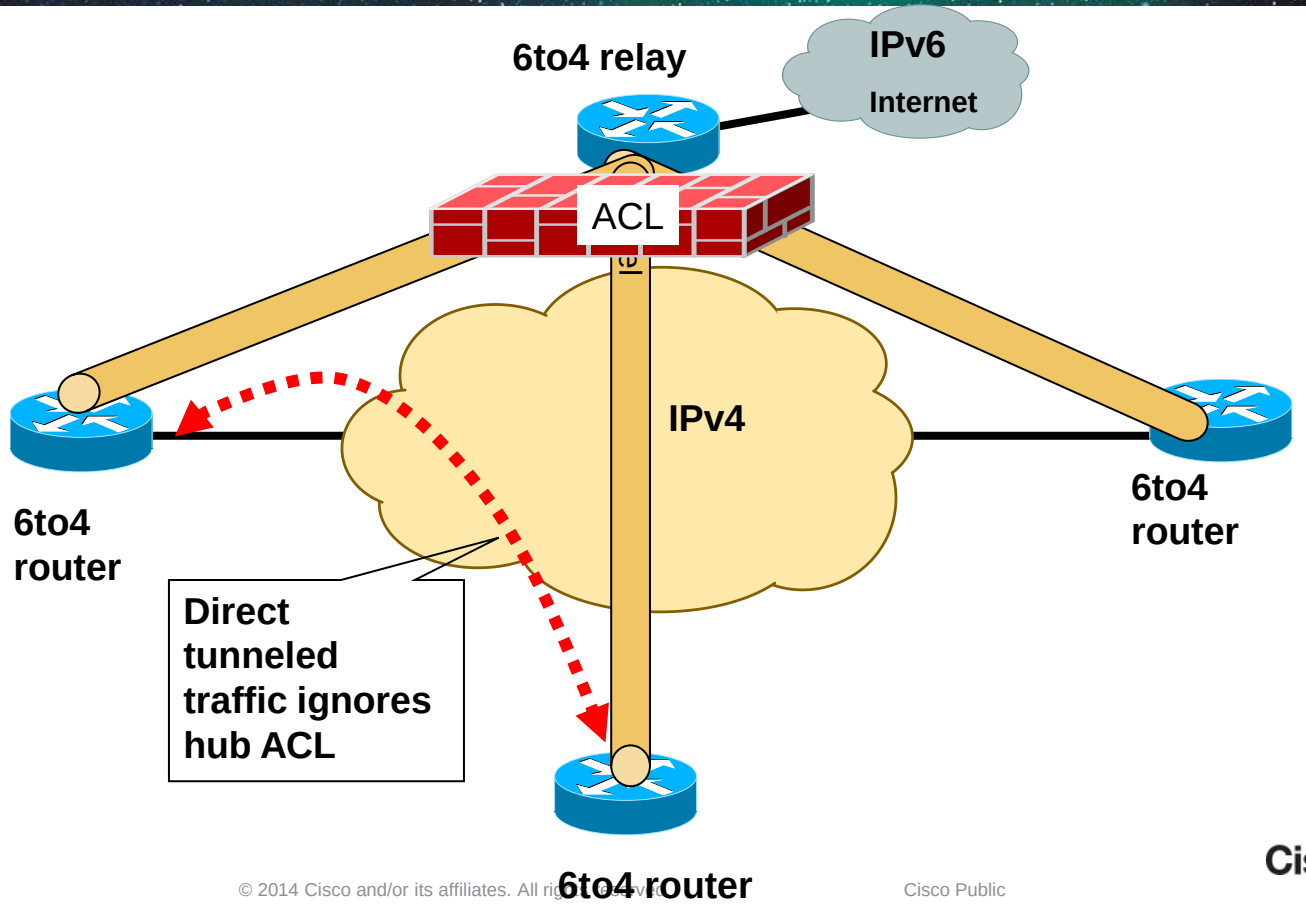
Looping Attack Between 2 ISATAP Routers
(RFC 6324)



- 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

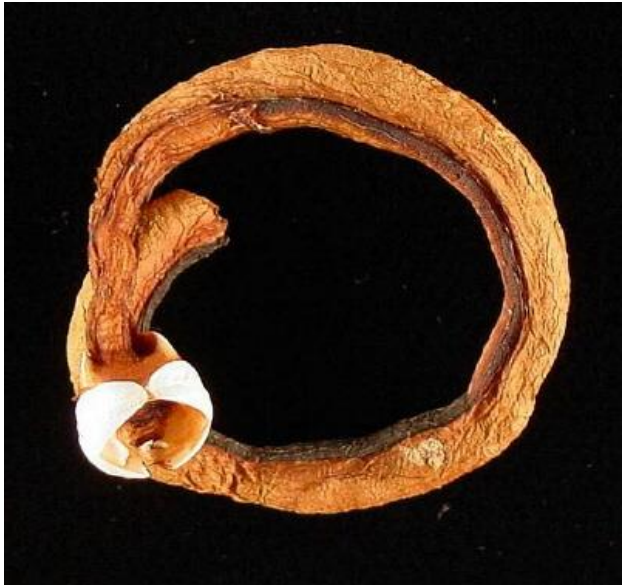
Mitigation:
- IPv6 anti-spoofing everywhere
- ACL on ISATAP routers accepting IPv4 from valid clients only
- Within an enterprise, block IPv4 ISATAP traffic between ISATAP routers
- Within an enterprise block IPv6 packets between ISATAP routers

ISATAP/6to4 Tunnels Bypass ACL



TEREDO?

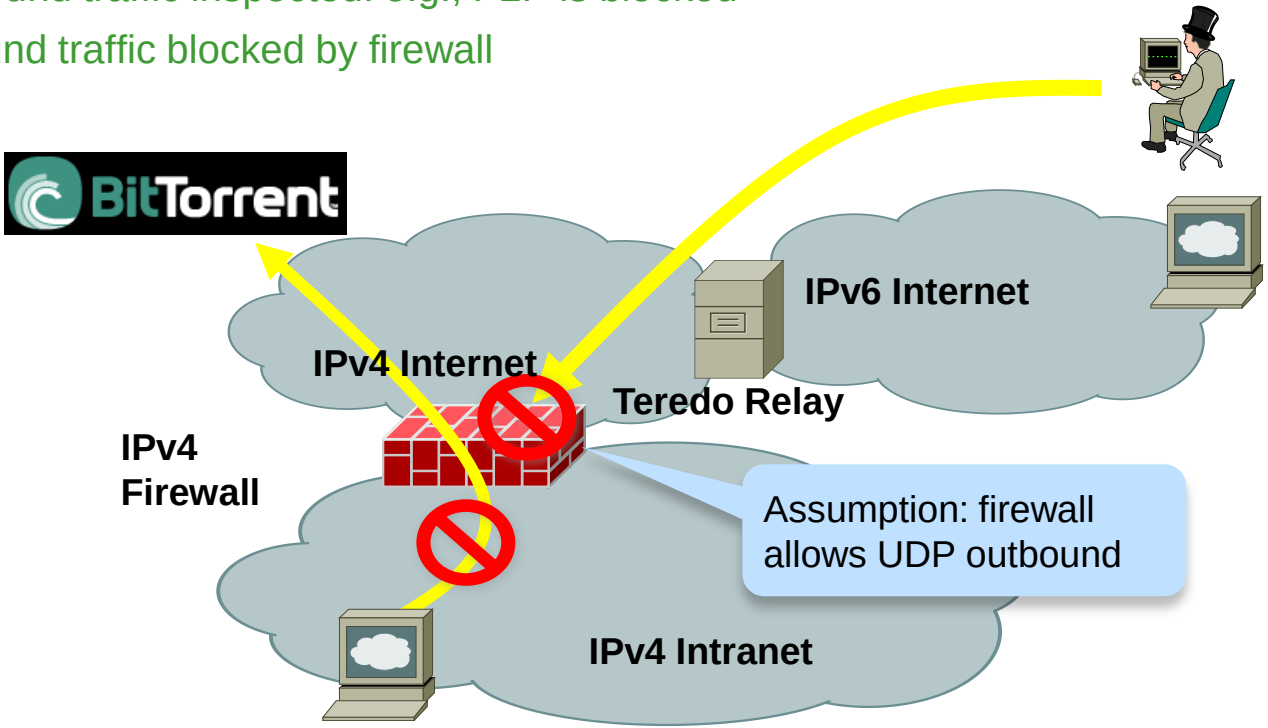
- Teredo navalis
  - A shipworm drilling holes in boat hulls
- Teredo Microsoftis
  - IPv6 in IPv4 punching holes in NAT devices
  - RFC 4380



Source: United States Geological Survey

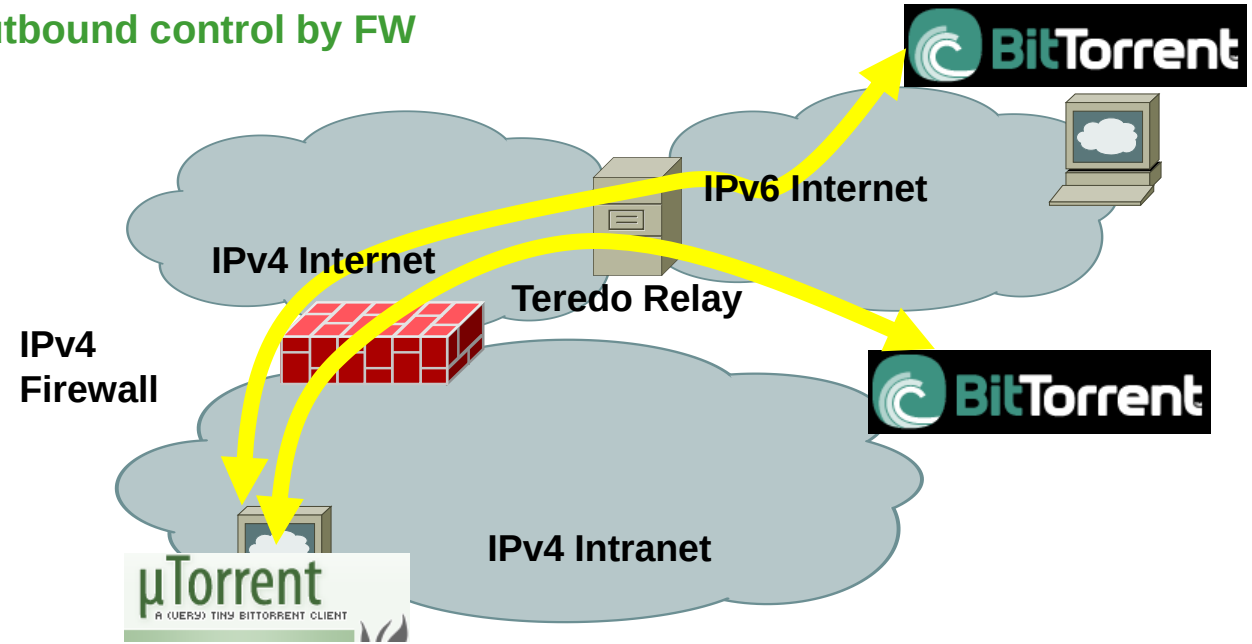
Teredo Tunnels (1/3)
Without Teredo: Controls Are in Place

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



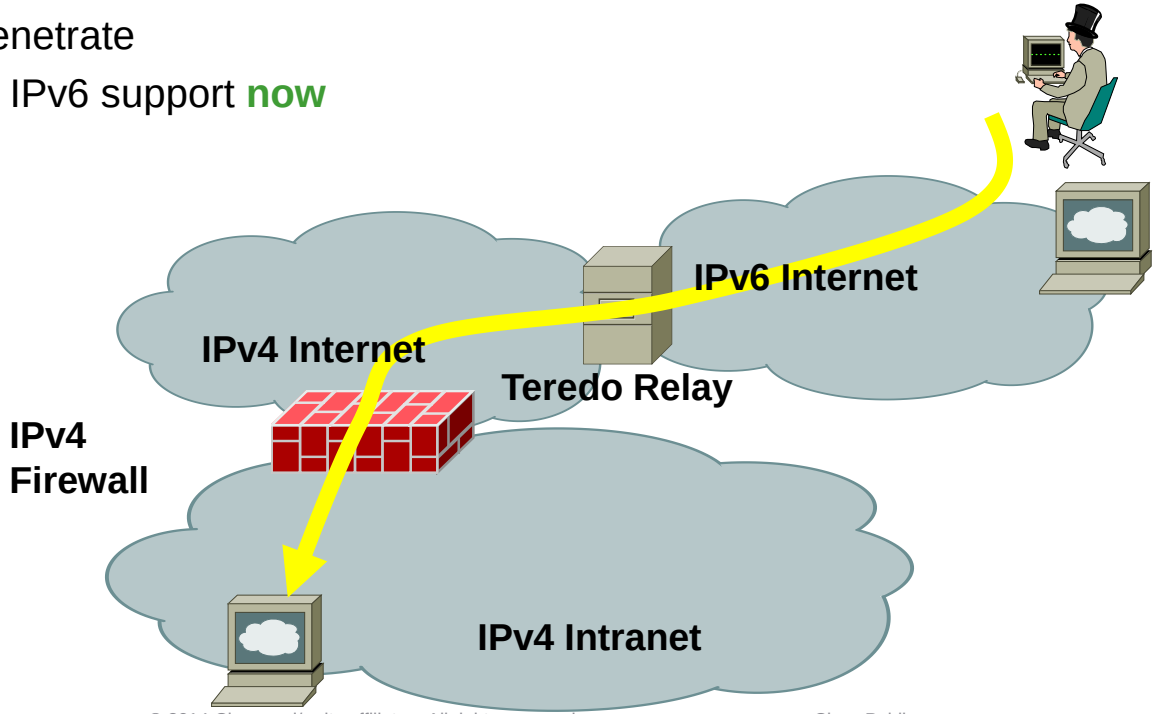
Teredo Tunnels (2/3)
No More Outbound Control

- Internal users wants to get P2P over IPv6
- Configure the Teredo tunnel (already enabled by default!)
- FW just sees IPv4 UDP traffic
- **No more outbound control by FW**

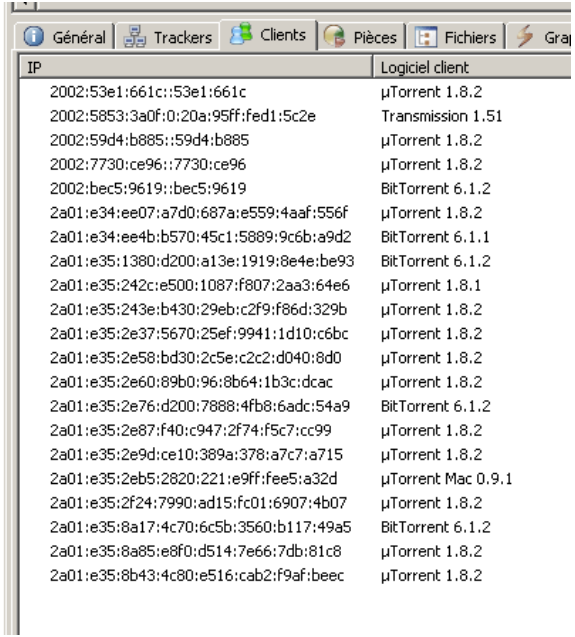


Teredo Tunnels (3/3)
No More Outbound Control

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



Is it Real?
See Windows uTorrent, or ...



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?

For Your Reference

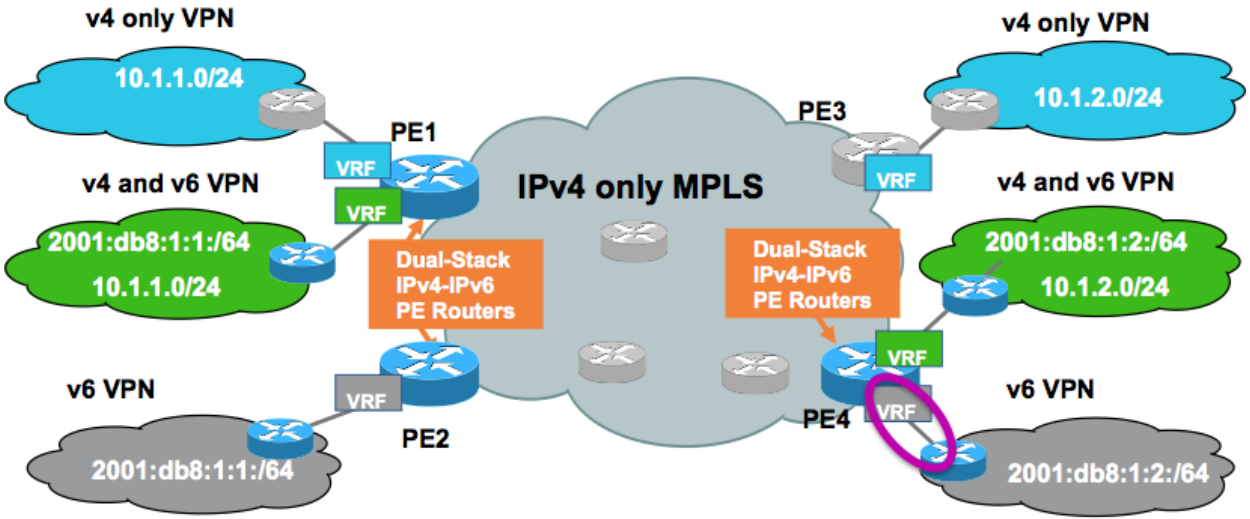
- Rogue tunnels by naïve users:
  - Sure, block IP protocol 41 and UDP/3544
  - In Windows:

```
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

SP Transition Mechanism: 6VPE

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



6VPE Security

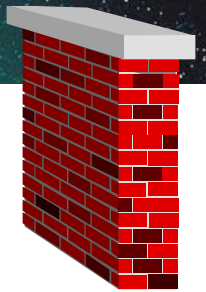
- 6PE (dual stack without VPN) is a simple case
- Security is identical to IPv4 MPLS-VPN, see RFC 4381
- Security depends on correct operation and implementation
  - QoS prevent flooding attack from one VPN to another one
  - PE routers must be secured: AAA, iACL, CoPP …
- MPLS backbones can be more 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
    - draft-ietf-opsec-lla-only
  - => completely unreachable from remote (better than IPv4)

Enforcing a Security Policy

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:
  - VLAN ACL only in 15.0(1)SY
  - 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, ICMPv6 code and type
  - TCP flags SYN, ACK, FIN, PUSH, URG, RST
  - 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 destination options
  - `auth` matches AH
  - `hbh` matches hop-by-hop (since 15.2(3)T)
- `fragments` keyword matches
  - Non-initial fragments (same as IPv4)
- `undetermined-transport` keyword does not match
  - TCP/UDP/SCTP and ports are in the fragment
  - ICMP and type and code are in the fragment
  - Everything else matches (including OSPFv3, …)
  - Only for deny ACE

Check your platform & release as your mileage can vary…

IPv6 ACL Implicit Rules

RFC 4890

- Implicit entries exist at the end of each IPv6 ACL to allow neighbour 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

For Your Reference

```
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

IPv6 ACL to Protect VTY

For Your Reference

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


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

MUST BE DONE before '***ipv6 enable***' on any interface!

Does not exist for protecting HTTP server => use ACL

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
```

Control Plane Policing for IPv6

Protecting the Router CPU

For Your Reference

- Cat 6K & 7600 with Sup720
  - 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
```

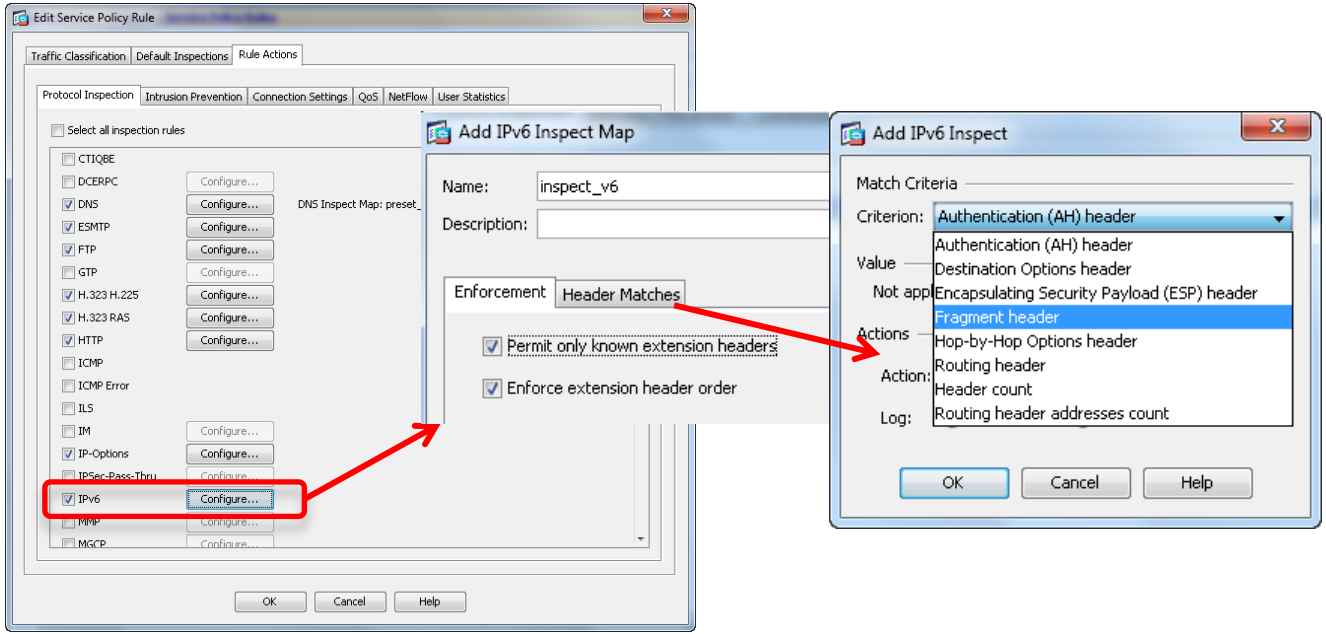
- Cat 6K with Sup-2T (IOS 12.2(50)SY)
  - IPv6 shares `class-copp-ttl-fail` and `class-copp-options` with IPv4

```
platform rate-limit ...
show platform hardware statistics
show platform qos IPv6 ...
```

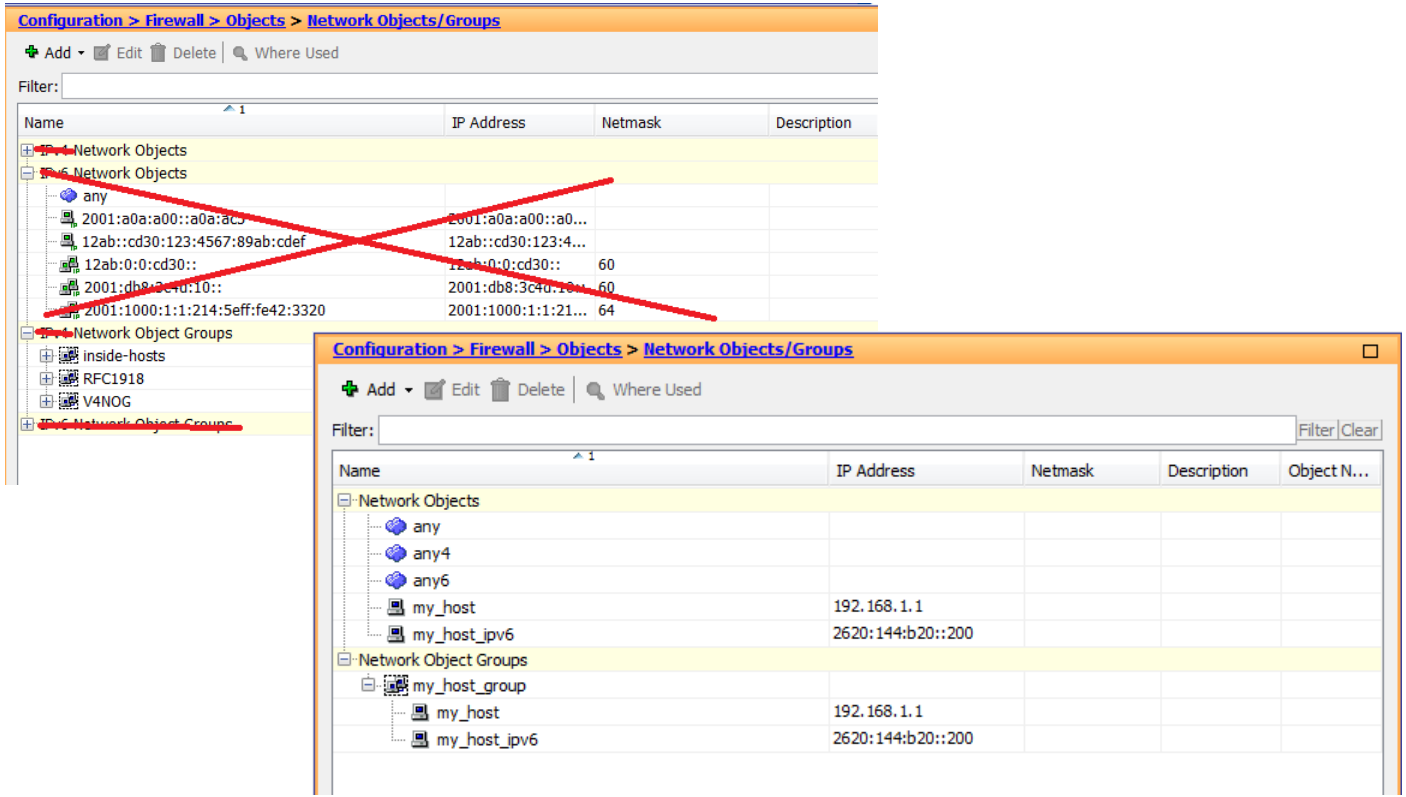
ASA Firewall IPv6 Support

- Since version 7.0 (April 2005)
- IPv6 header security checks (length & order)
- Management access via IPv6: Telnet, SSH, HTTPS, ASDM
- Routed & transparent mode, fail-over
- v6 App inspection includes: DNS,FTP, HTTP, ICMP, SIP, SMTP, and IPSec pass-through
- IPv6 support for site-to-site VPN tunnels was added in 8.3 (IKEv1 in ASA 8.3.1, and IKEv2 in ASA 8.4.1)
- Selective permit/deny of extension headers (ASA 8.4.2)
- OSPFv3, DHCPv6 relay, stateful NAT64/46/66, mixed mode objects (ASA 9.0)

ASA 8.4.2 : IPv6 Extension Header Filtering



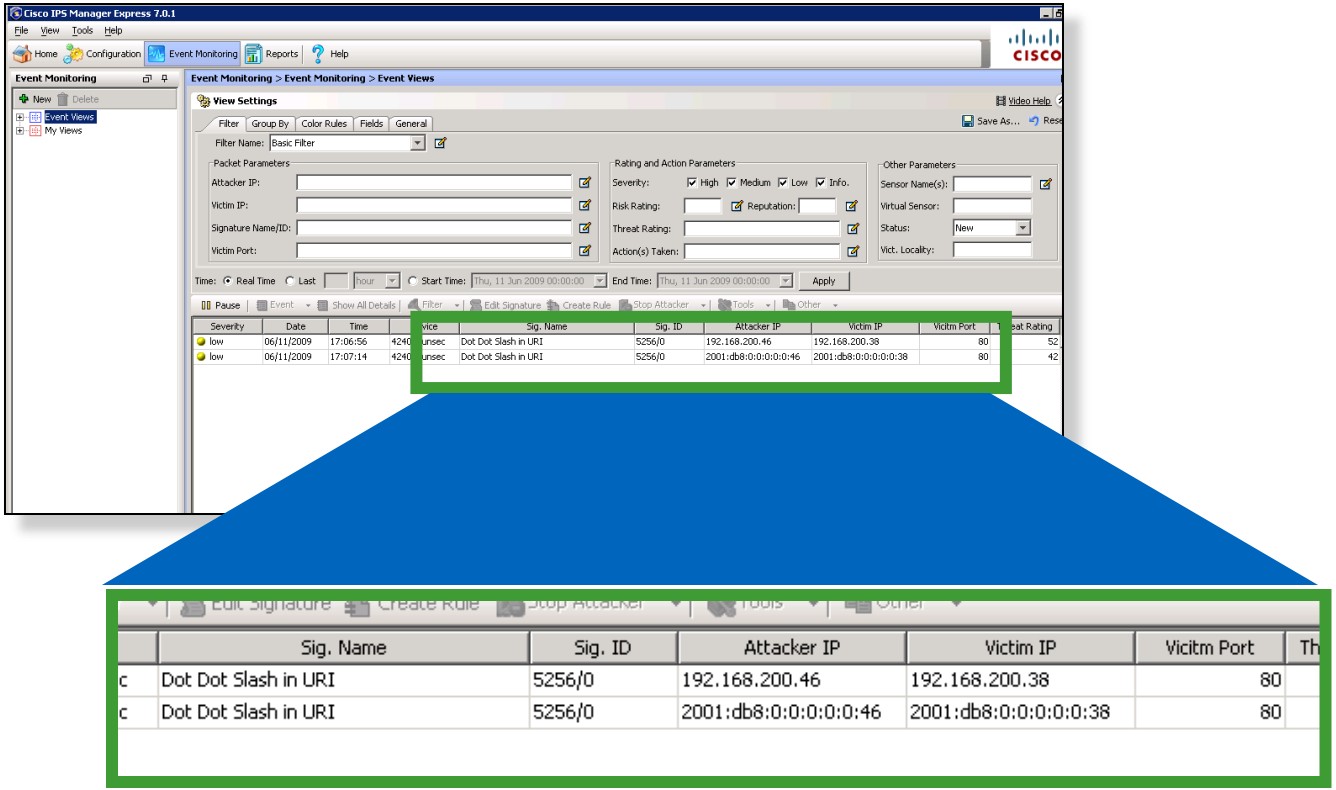
ASA 9.0 Mixed Mode Objects



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

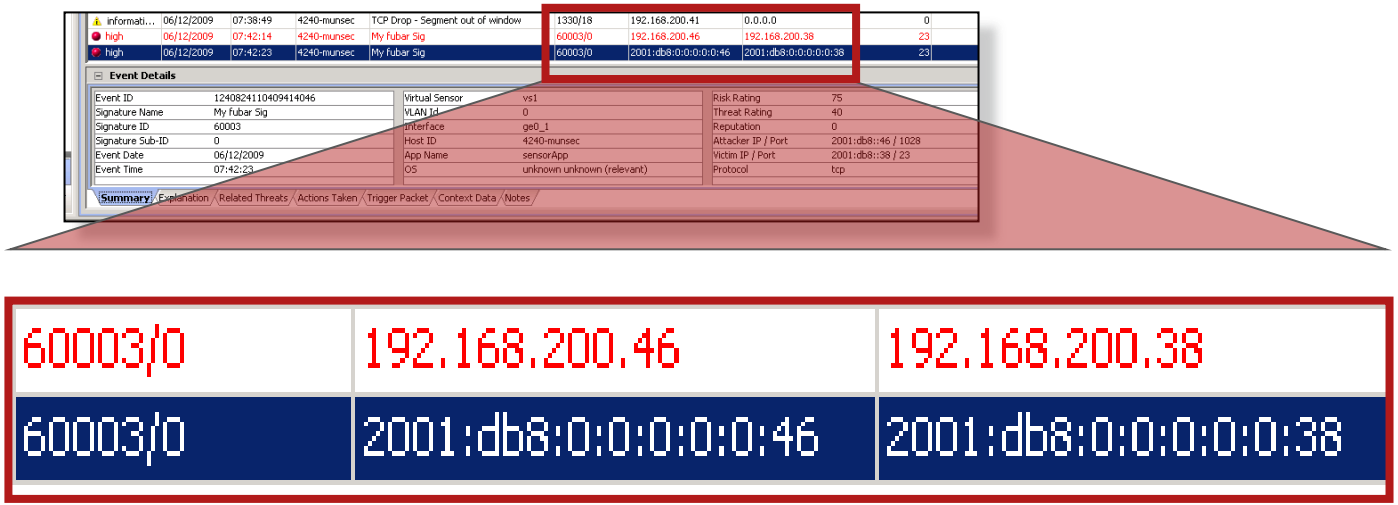
Dual-Stack IPS Engines
Service HTTP



Edit Signature Create Rule Stop Attacker Tools Other
Sig. Name Sig. ID Attacker IP Victim IP Vicitm Port
Dot Dot Slash in URI 5256/0 192.168.200.46 192.168.200.38 80
Dot Dot Slash in URI 5256/0 2001:db8:0:0:0:0:0:46 2001:db8:0:0:0:0:0:38 80

Dual-Stack Engine
String TCP with Custom Signature

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

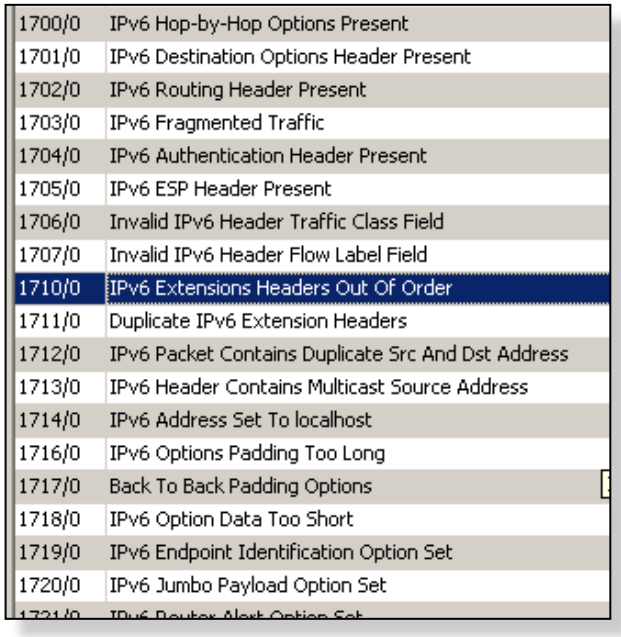


60003/0	192.168.200.46	192.168.200.38
60003/0	2001:db8:0:0:0:0:0:46	2001:db8:0:0:0:0:0:38

Custom engine can also be used to block invalid header combination ;-)

IPv6-Only Engines

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



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 over IPv4 (ASA 8.0) over IPv6 (ASA 9.0)
  - Stateful-Failover (ASA 8.2.2)
  - Extension header filtering and inspection (ASA 8.4.2)
  - Dual-stack ACL & object grouping (ASA 9.0)

- 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 since 2010, IPv6 support since 7.6.1 (May 2012)
- Web Security Appliance (WSA) with explicit proxy then transparent mode, work in progress (end of 2013 or early 2014)
- Cisco Cloud Web Security (ScanSafe) expected to be available in 2013 or early 2014

Security IPv6 Connectivity

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	▪ AnyConnect 3.1 & ASA 9.0

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

- IPv6 packets over DMVPN IPv4/IPv6 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 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
```

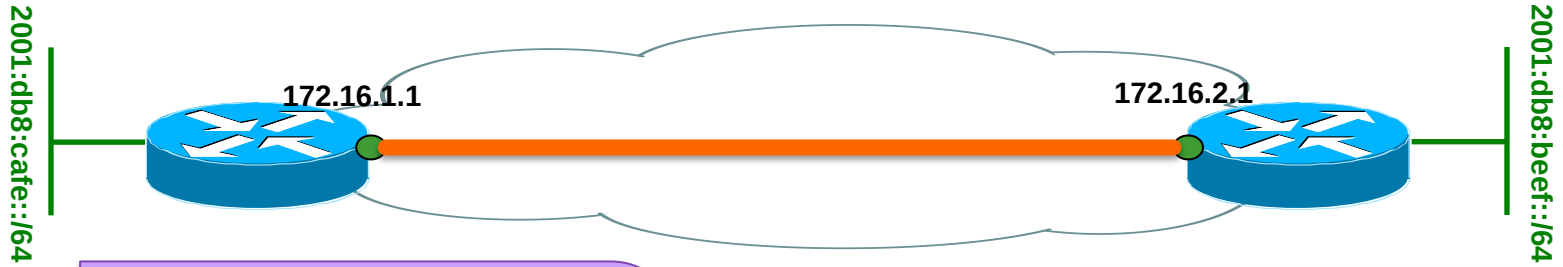
Secure Site to Site IPv6 Traffic over IPv6 Public Network

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
```

FlexVPN Site-to-site configuration over IPv4




```
interface Tunnel0
 ipv6 address FE80::1 link-local
 ipv6 ospf 1 area 0
 tunnel source FastEthernet0/0
 tunnel destination 172.16.2.1
 tunnel protection ipsec profile default

interface E0/0
 ipv6 address 2001:db8:cafe::1/64
 ipv6 ospf 1 area 0
```

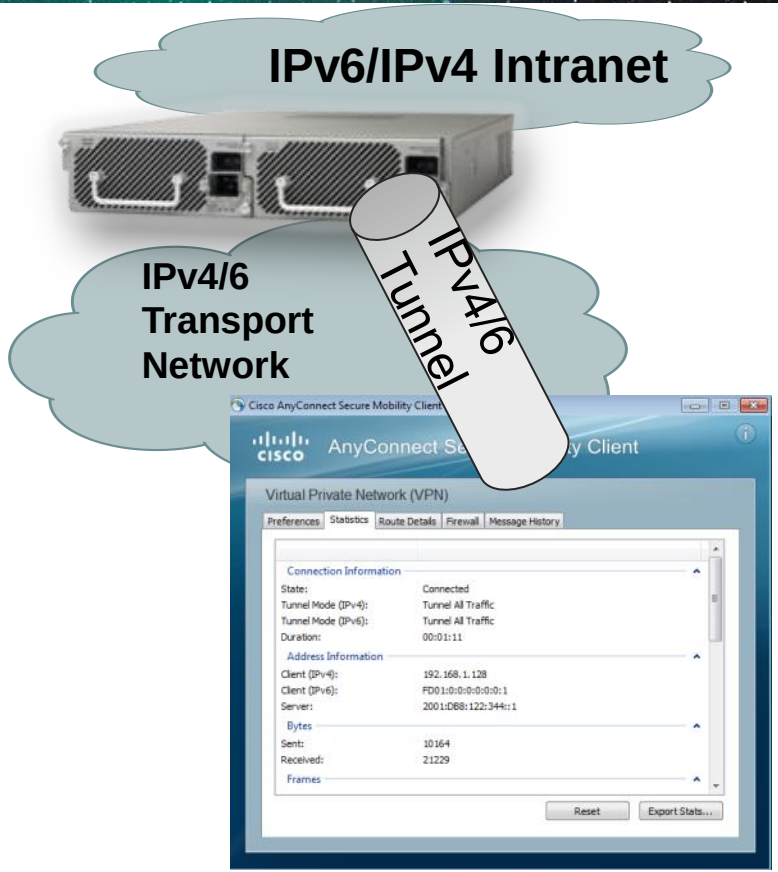
```
interface Tunnel0
 ipv6 address FE80::2 link-local
 ipv6 ospf 1 area 0
 tunnel source FastEthernet0/0
 tunnel destination 172.16.1.1
 tunnel protection ipsec profile default

interface E0/0
 ipv6 address 2001:db8:beef::1/64
 ipv6 ospf 1 area 0
```

- IPv4/IPv6 FlexVPN over IPv4 or IPv6
- IPv6 spoke to spoke (mid 2013)

Secure RA IPv* over IPv* Public Network: AnyConnect SSL VPN Client 3.1 & ASA 9.0

BRKSEC-2697

- **AnyConnect supports native IPv4/6 connectivity**
- Connecting via IPv4/6 Internet to ASA
- SSL Tunnelling IPv6 in IPv6 , IPv4 in IPv4, IPv6 in IPv4, IPv4 in IPv6
- No support for DHCPv6 yet
- Mobile does not support IPv6 transport






Summary

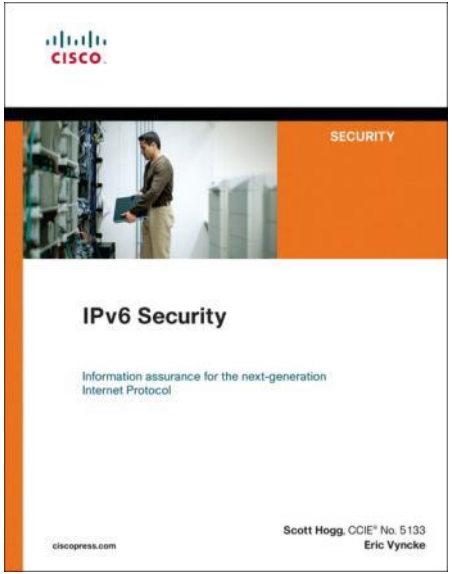
Key Take Away

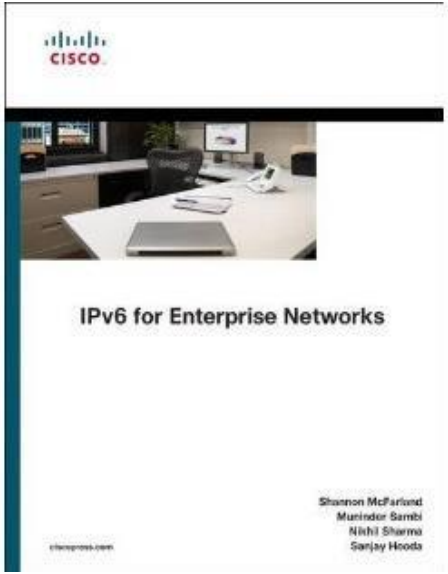
- So, **nothing really new in IPv6**
  - Reconnaissance: address enumeration replaced by DNS enumeration
  - Spoofing & bogons: uRPF is our IP-agnostic friend
  - NDP spoofing: RA guard and more feature coming
  - ICMPv6 firewalls need to change policy to allow NDP
  - Extension headers: firewall & ACL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

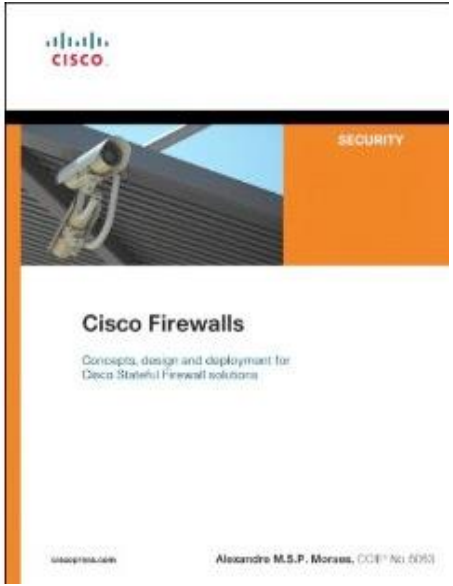
Is IPv6 in My Network?

- 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***

Recommended Reading







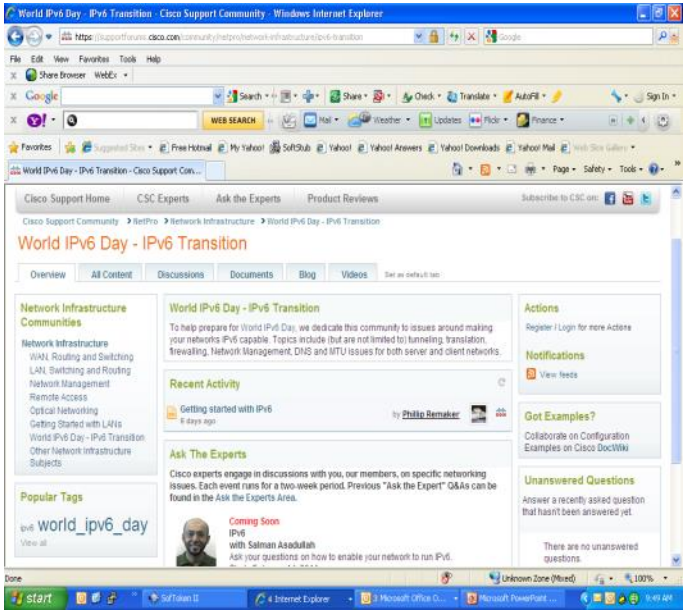
Search Session Builder: “ipv6”

IPv6-Related Sessions

Session	Title
TECSPM-2001	IPv6 LTE/EPC Design and Deployment
BRKRST-2301	Enterprise IPv6 Deployment
BRKRST-2311	IPv6 Planning, Deployment and Operation Considerations
BRKSPG-2603	How to Securely Operate an IPv6 Network
BRKSEC-2003	IPv6 Security Threats and Mitigations
BRKSEC-3003	Advanced IPv6 Security: Securing Link Operations at First Hop
BRKRST-2044	Enterprise Multi-Homed Internet Edge Architectures
PNLCRS-2303	Experiences with Deploying IPv6
LTRRST-1301, LTRSEC-3033	IPv6 Hands-on Lab, IPv6 Network Threat Defence, Countermeasures and Controls
BRKSPG-2602	IPv4 Exhaustion: NAT and Transition to IPv6 for Service Providers
COCRST-2355	Inside Cisco IT: Making the Leap to IPv6
BRKCRT-9344	IPv6 for Cert Nuts
BRKEWN-2010	Design and Deployment of Enterprise WLANs
BRKRST-2304	Hitchhiker’s Guide to Troubleshooting IPv6
BRKSPG-2606	MAP Technology - IPv6 Strategy for Solving IPv4 Address Exhaustion
BRKSPG-2607	IPv6 Deployment Best Practices for the Access Network
BRKSPG-3300	Service Provider IPv6 Deployment

Join Cisco IPv6 Support Community!

- **Free** for anyone with Cisco.com registration
- Get **timely** answers to your technical questions
- Find **relevant** technical documentation
- Engage with over 200,000 **top technical experts**
- **Seamless** transition from discussion to TAC Service Request *(Cisco customers and partners only)*
- Visit the Cisco Support Community booth in the World of Solutions for more information



The Cisco Support Community is your one-stop community destination from Cisco for sharing current, real-world technical support knowledge with peers and experts.

supportforums.cisco.com
supportforums.cisco.mobi




Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2014 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site www.ciscoliveaustralia.com/mobile
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 21 March 12:00pm - 2:00pm

Learn online with Cisco Live!

Visit us online after the conference for full access to session videos and presentations.
www.CiscoLiveAPAC.com


CISCO
TM