IPv6 Security

ISP/IXP Workshops

Acknowledgements

- With grateful thanks to:

  Éric Vyncke <evyncke@cisco.com>

  For much of the material contained in this presentation

Before we begin…

- Enabling IPv6 on any device means that:
  - The device is accessible by IPv6
  - Interface filters and firewall rules already present in IPv4 **must** be replicated for IPv6
  - Router vty filters already present in IPv4 **must** be replicated for IPv6
- Failure to protect the device after enabling IPv6 means that it is wide open to abuse through IPv6 transport
  - Even though the IPv4 security is in place

Agenda

- Should I care about IPv6?
- Issues shared by IPv4 and IPv6
- Specific Issues for IPv6
- Enforcing a Security Policy in IPv6
- Secure IPv6 transport over public network
- IPv6 Security Best Practices

Should I care?

- Is IPv6 in my IPv4 network?

  Easy to check!

- Look inside IPv4 NetFlow records

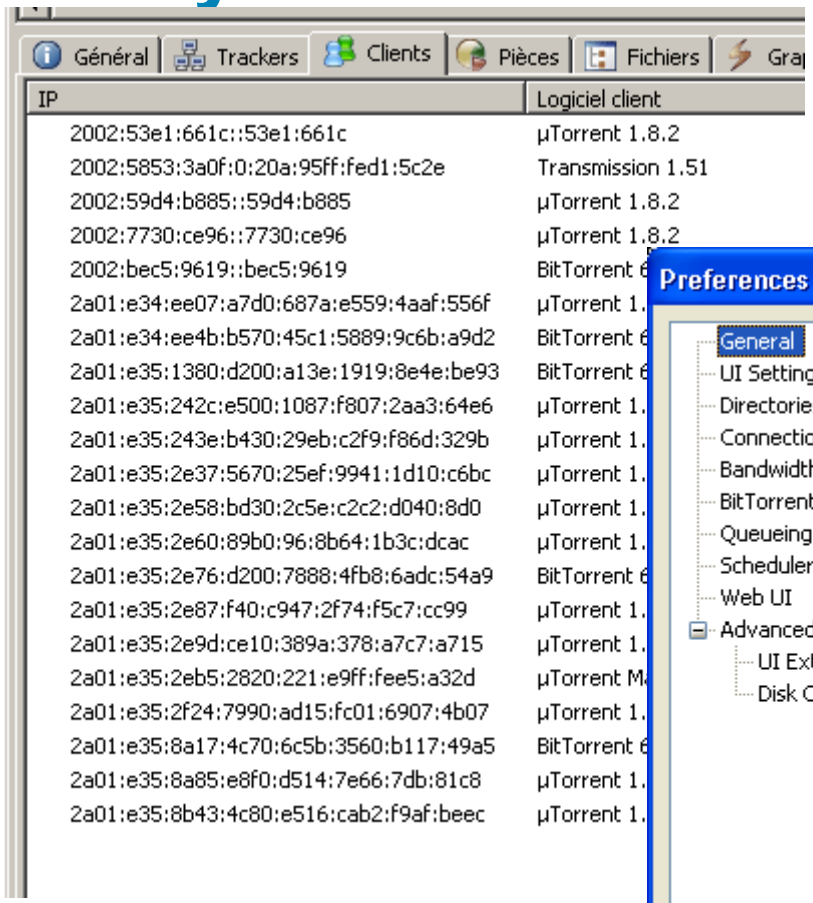
  Protocol 41: IPv6 over IPv4 or 6to4 tunnels

  IPv4 address: 192.88.99.1 (6to4 anycast server)

  UDP 3544, the public part of Teredo, yet another tunnel

- Look into DNS requests log for ‘ISATAP’

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



Issues shared by IPv4 and IPv6

Issues facing IPv4 that we can find in IPv6…

Issues shared by IPv4 and IPv6

- Scanning methods
- Viruses and Worms
- Filtering
- Amplification attacks
- Layer-2 attacks
- Broadcasts
- Routing Authentication
- Hacking

Reconnaissance in IPv6 Scanning Methods Are Likely to Change

- Default subnets in IPv6 have 2^{64} addresses
  - 10 Mpps = more than 50 000 years to scan
- Public servers will still need to be DNS reachable
  - More information collected by Google...
  - Cfr SensePost BiDiBLAH
- Administrators may adopt easy-to-remember addresses (::10,::20,::F00D, ::C5C0 or simply IPv4 last octet for dual stack)
- By compromising hosts in a network, an attacker can learn new addresses to scan
- Transition techniques (see later) derive IPv6 address from IPv4 address ⇒ can scan again

Viruses and Worms in IPv6

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

  IPv4: reliance on network scanning

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

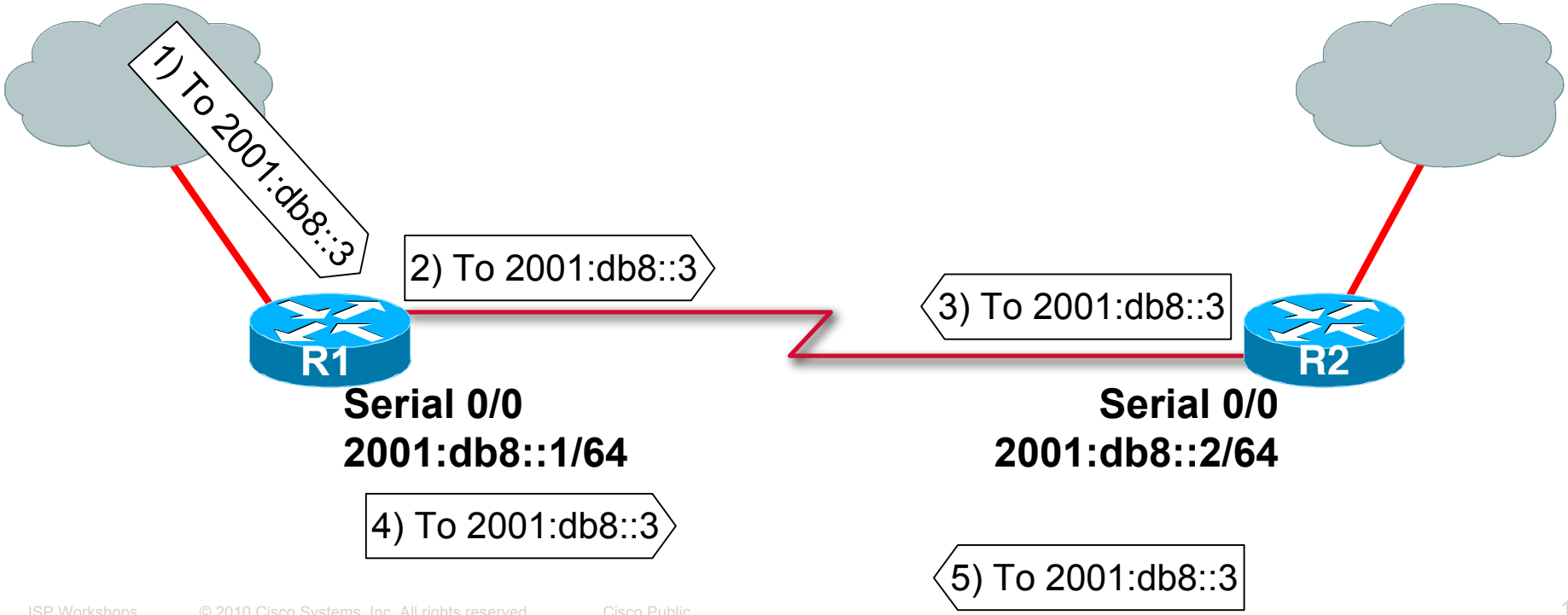
- Worm developers will adapt to IPv6
- IPv4 best practices around worm detection and mitigation remain valid

Scanning Made Bad for CPU

- Potential router CPU attacks if aggressive scanning
  - Router will do Neighbor Discovery... And waste CPU and memory
  - Built-in rate limiter but no option to tune it
  - Destination Guard is coming ☺
- Using a /64 on point-to-point links ⇒ a lot of addresses to scan!
- Using infrastructure ACL to prevent this scanning
  - Easy with IPv6 because new addressing scheme can be done ☺

DoS Example
Ping-Pong over Physical Point-to-Point

- IOS implements RFC 4443 so this is not a threat
- Else use /127 on P2P link (see also RFC 3627)
- Same as in IPv4, on real P2P, if not for me send it on the other side... Could produce looping traffic



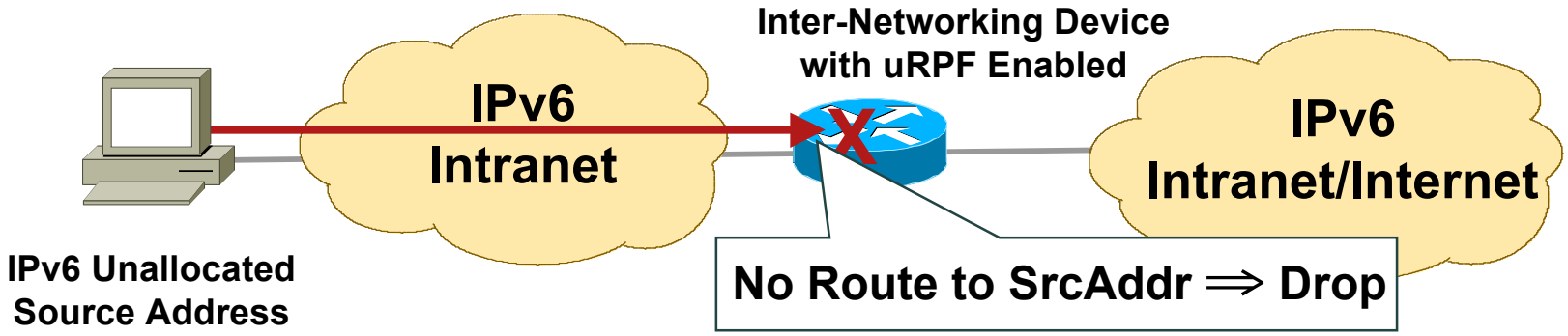
IPv6 Bogon Filtering and Anti-Spoofing

- IPv6 nowadays has its bogons:

  http://www.cymru.com/Bogons/ipv6.txt

- Similar situation as IPv4

  ⇒ Same technique = uRPF



IPv6 uRPF and Cisco Devices The Theory-Practice Gap

- Supported everywhere except:
  - 7600 & Cat 6K: no IPv6 uRPF at all
    - Will require a new Supervisor...
  - GSR only strict mode with E5 (else not supported)

```
ipv6 verify unicast source reachable-via {any|rx}
```

ICMPv4 vs. ICMPv6

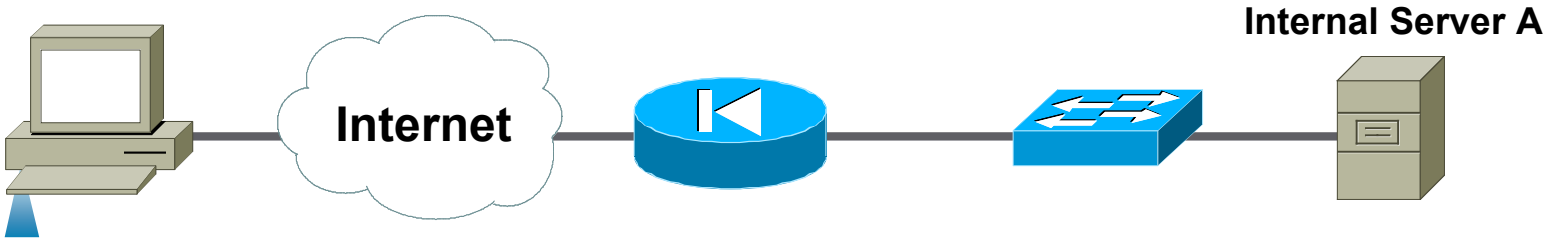
- Significant changes from IPv4
- More relied upon

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

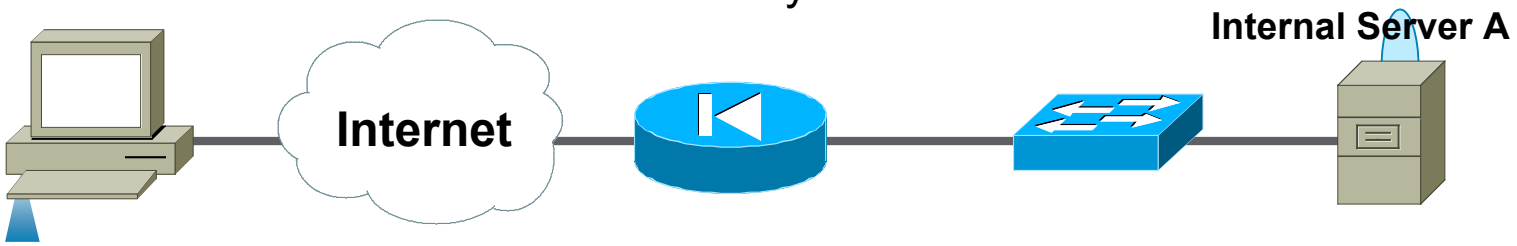
Border Firewall Policy



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

RFC 4890: Border Firewall Transit Policy

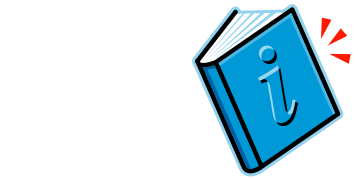


For Your Reference

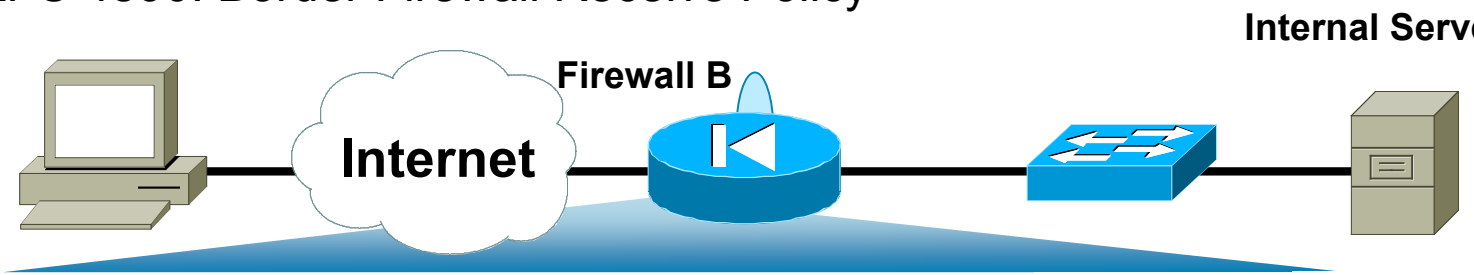
Action	Src	Dst	ICMPv6 Type	ICMPv6 Code	Name
Permit	Any	A	128	0	Echo Reply
Permit	Any	A	129	0	Echo Request
Permit	Any	A	1	0	No Route to Dst.
Permit	Any	A	2	0	Packet Too Big
Permit	Any	A	3	0	Time Exceeded—TTL Exceeded
Permit	Any	A	4	0	Parameter Problem

Potential Additional ICMPv6

RFC 4890: Border Firewall Receive Policy



For Your Reference



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			

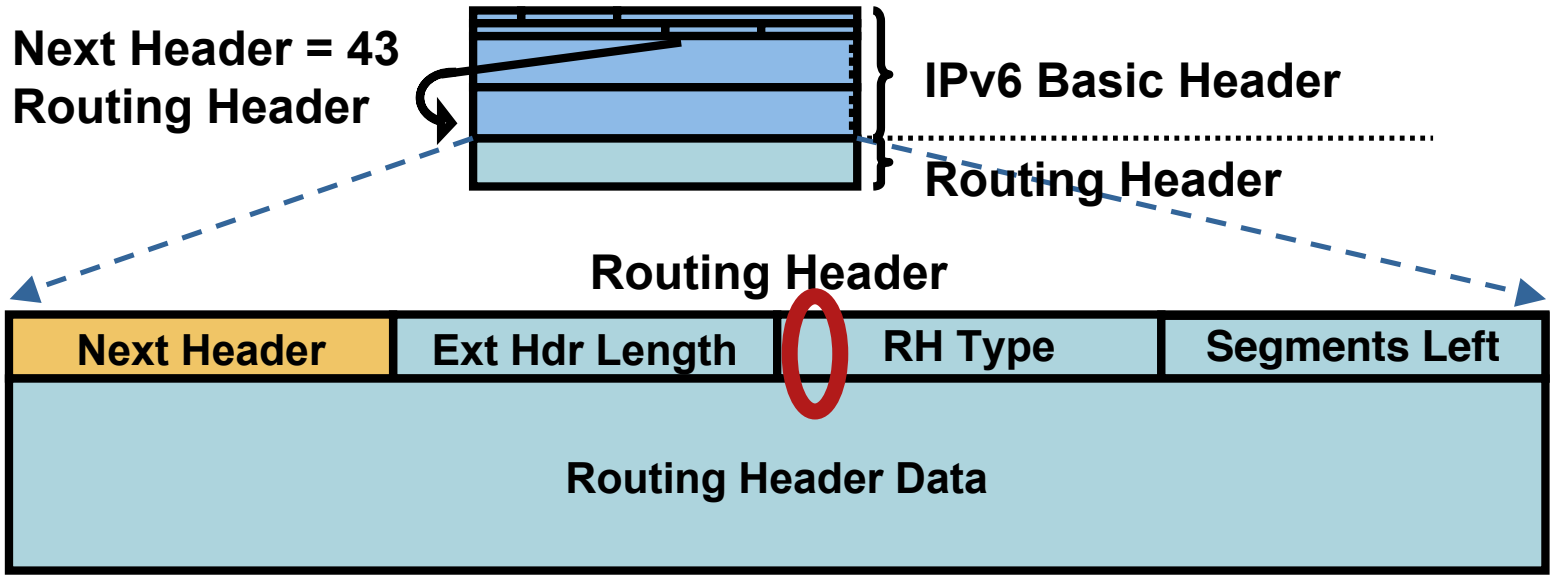
For locally generated traffic

IPv6 Routing Header

- An extension header
- Processed by the listed intermediate routers
- Two types

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

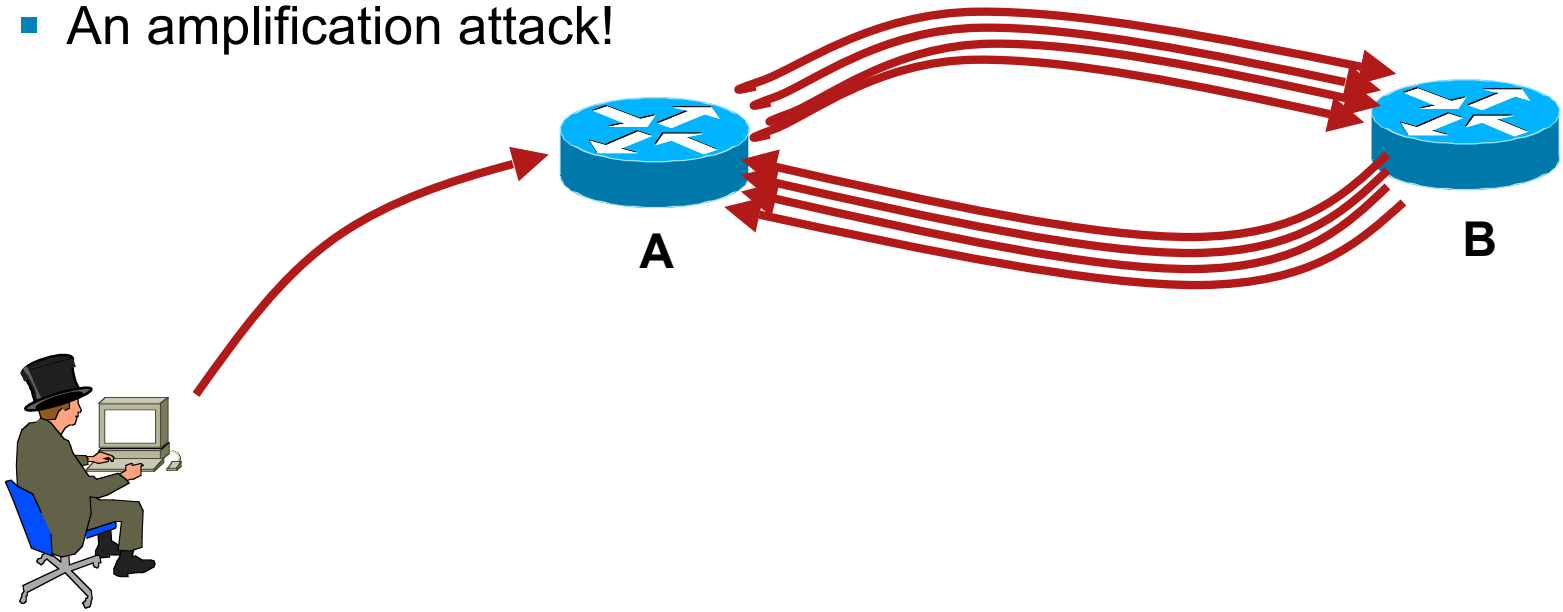
  Type 2: used for mobile IPv6 (single intermediate router)



Type 0 Routing Header
One issue: Amplification Attack

- Beside the well known firewall evasion...
- What if attacker sends a packet with RH containing

  A -> B -> A -> B -> A -> B -> A -> B -> A ....
- Packet will loop multiple time on the link R1-R2
- An amplification attack!



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 (in IOS only)
  - IOS-XR 3.7 a bug prevents the processing of RH
  - Windows, Linux, Mac OS: default setting
- At the edge
  - With an ACL blocking routing header specially type 0 (IOS can do)
- RFC 5095 (Dec 2007) RH0 is deprecated
  - Default IOS changed in 12.4(15)T: no need to type ‘no ipv6 source-route’

Threats on the Layer-2 Link

- IPv4 has several threats against layer-2
  - ARP spoofing
  - Rogue DHCP
  - …
- What about IPv6?
  - On WLAN hotspot
  - On ETTx network
  - On hosting service Data Center
  - On some ADSL/cable aggregation

ARP Spoofing is now NDP Spoofing: Threats

- ARP is replaced by Neighbor Discovery Protocol
  - Nothing authenticated
  - Static entries overwritten by dynamic ones
- Stateless Address Autoconfiguration
  - rogue RA (malicious or not)
  - All nodes badly configured
    - DoS
    - Traffic interception (Man In the Middle Attack)
- Attack tools exist (from THC – The Hacker Choice)
  - Parasit6
  - Fakerouter6
  - ...

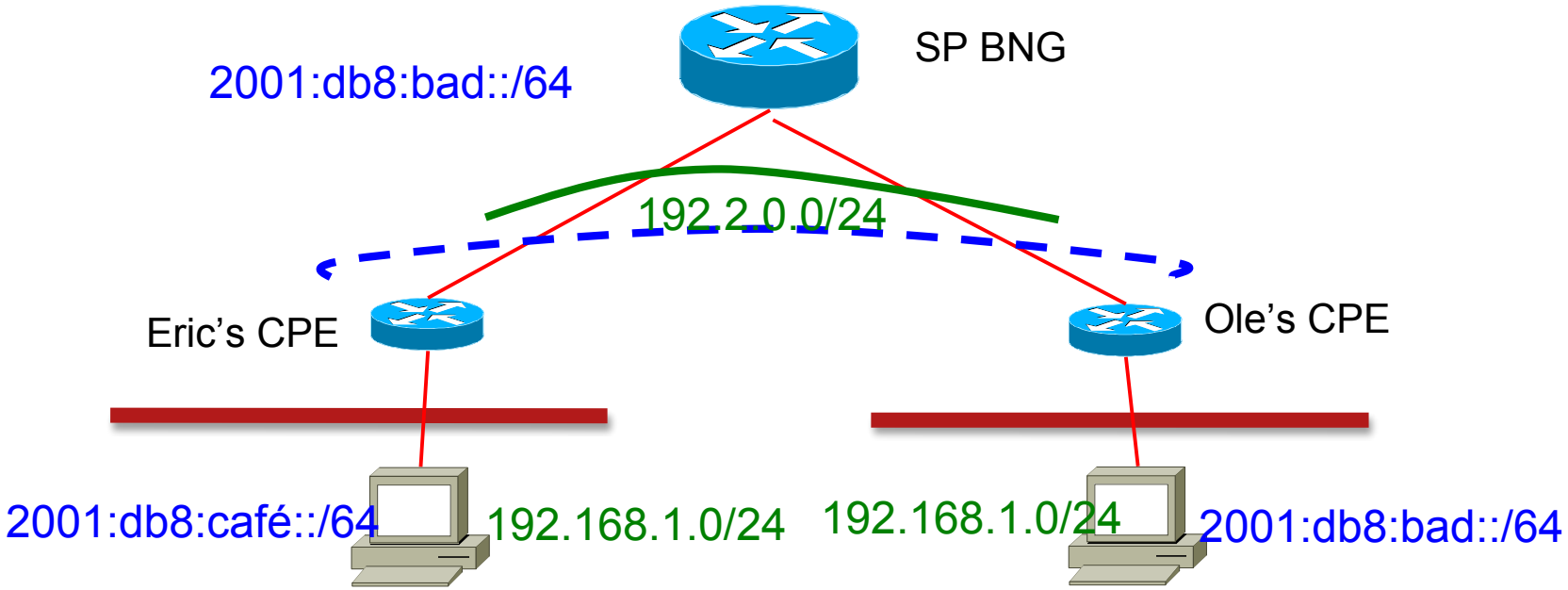
The Hacker's Choice

ARP Spoofing is now NDP Spoofing: Mitigation

- **BAD NEWS**: nothing like dynamic ARP inspection for IPv6
  - Will require new hardware on some platforms
  - Not before mid-2010...
- **GOOD NEWS**: Secure Neighbor Discovery
  - SEND = NDP + crypto
  - IOS 12.4(24)T
  - But not in Windows Vista, 2008, 7...
  - Crypto means slower...
- Other **GOOD NEWS**:
  - Private VLAN works with IPv6
  - Port security works with IPv6
  - 801.x works with IPv6
  - For FTTH & other broadband, DHCP-PD means not need to NDP-proxy

CPE to CPE Communication IPv4 vs. IPv6

- SP wants to see all user to user traffic
- IPv4 WAN addresses must communicate
  - Usually in the same layer 2 domain… tricks to force traffic to BNG
- IPv6 WAN addresses have no reason to communicate
  - IPv6 LAN addresses must communicate (easy: this is routed)



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::F

Anti-spoofing also blocks amplification attacks because a remote attacker cannot masquerade as his victim

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

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 and 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
  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 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

  Without IPSec, 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

By the Way: It Is Real ☹ IPv6 Hacking/Lab Tools

- Sniffers/packet capture
  - Snort
  - TCPdump
  - Sun Solaris snoop
  - COLD
  - Wireshark
  - Analyzer
  - Windump
  - WinPcap

- Scanners
  - IPv6 security scanner
  - Halfscan6
  - Nmap
  - Strobe
  - Netcat
- DoS Tools
  - 6tunneldos
  - 4to6ddos
  - Imps6-tools
- Packet forgers
  - Scapy6
  - SendIP
  - Packit
  - Spak6
- Complete tool - www.thc.org/thc-ipv6/

Specific IPv6 issues

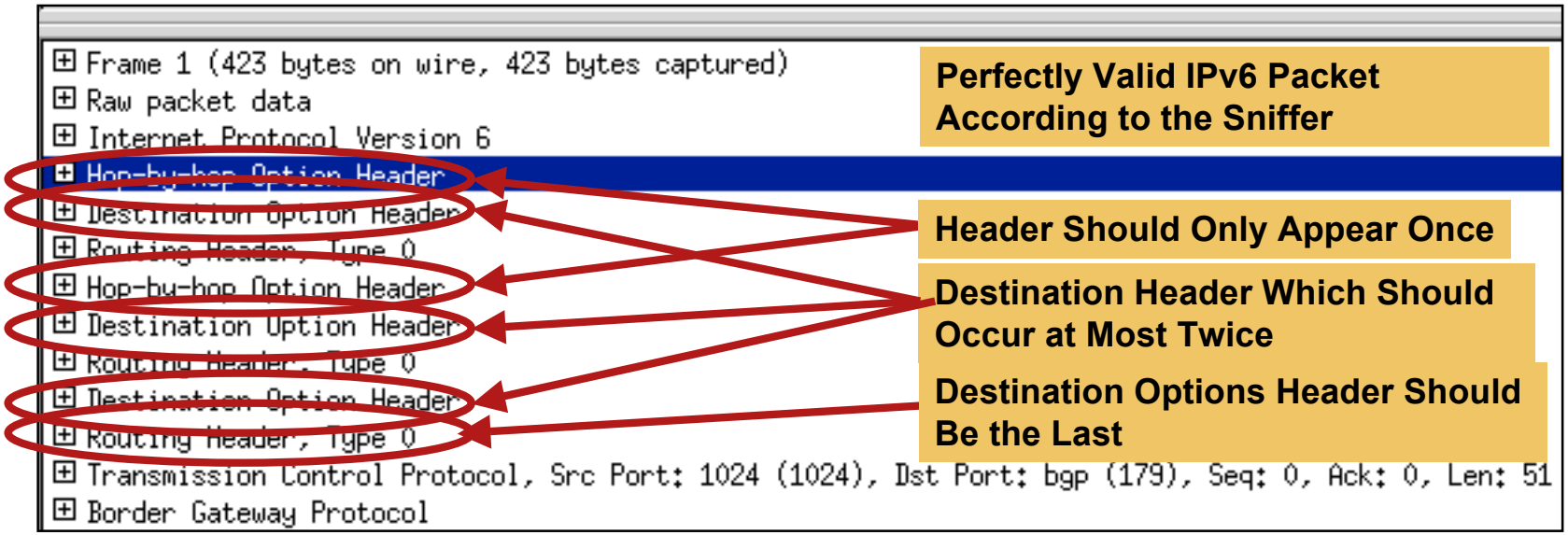
Problems unique to IPv6…

Specific IPv6 Issues

- IPv6 header manipulation
- Link Local vs Gobal Addressing
- Transition Challenges
- 6to4, 6VPE
- v4/v6 translation issues
- IPv6 stack issues

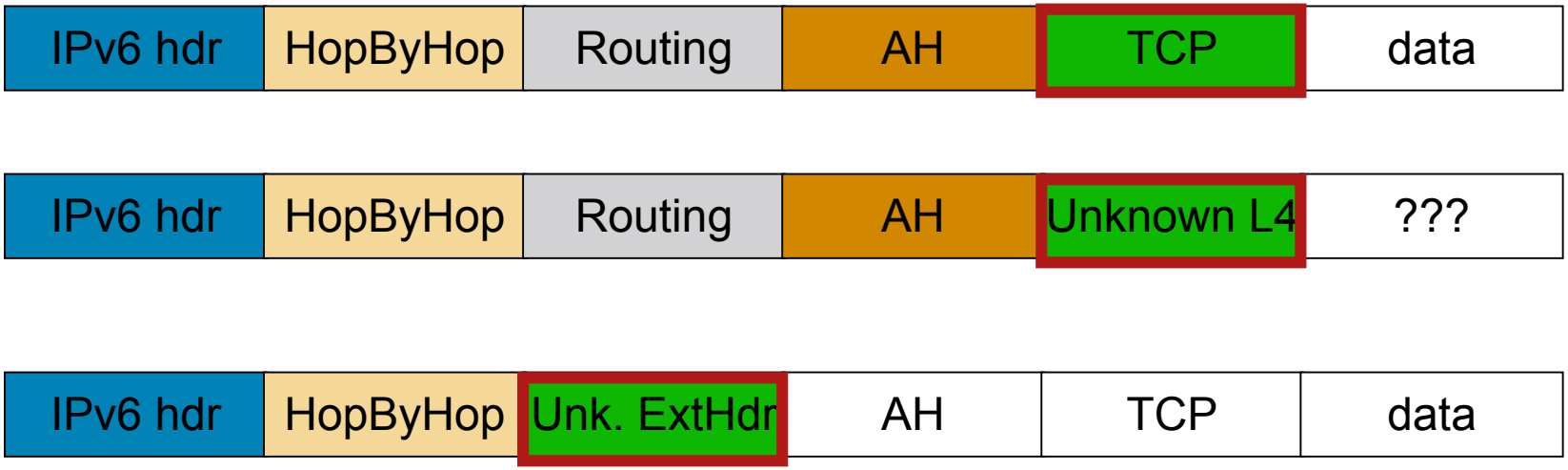
IPv6 Header Manipulation

- 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?

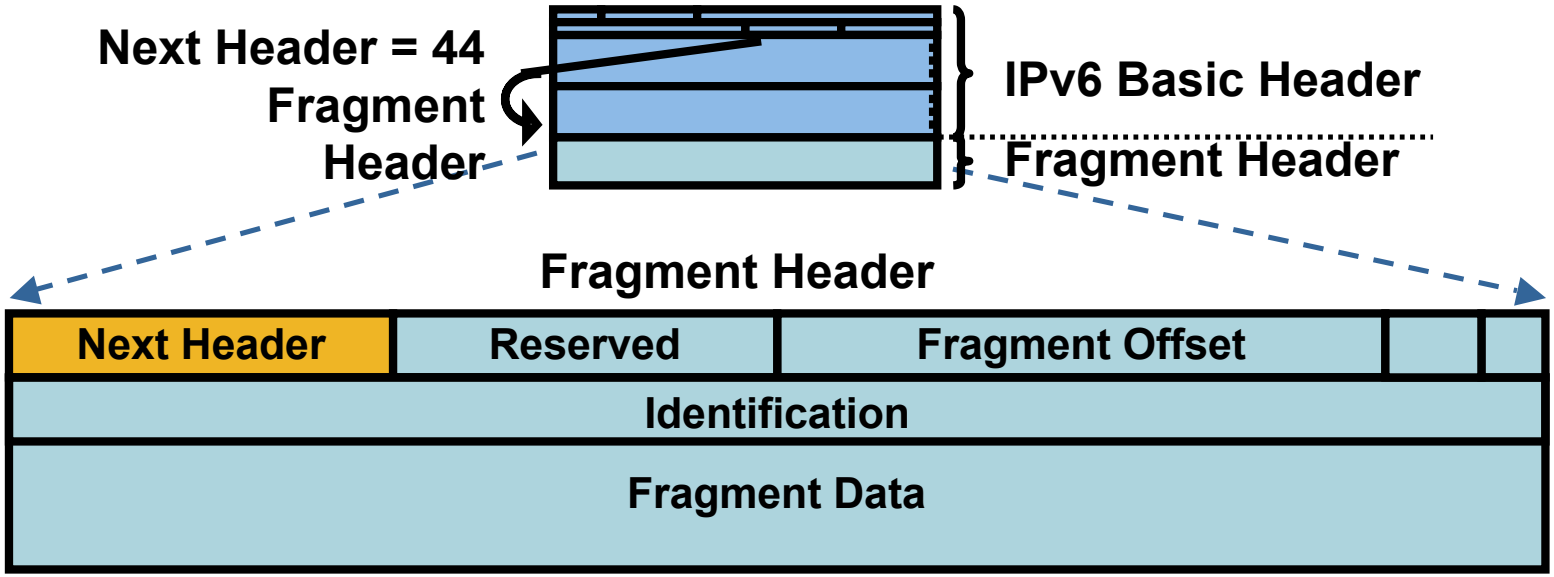


Parsing the Extension Header Chain

- 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**



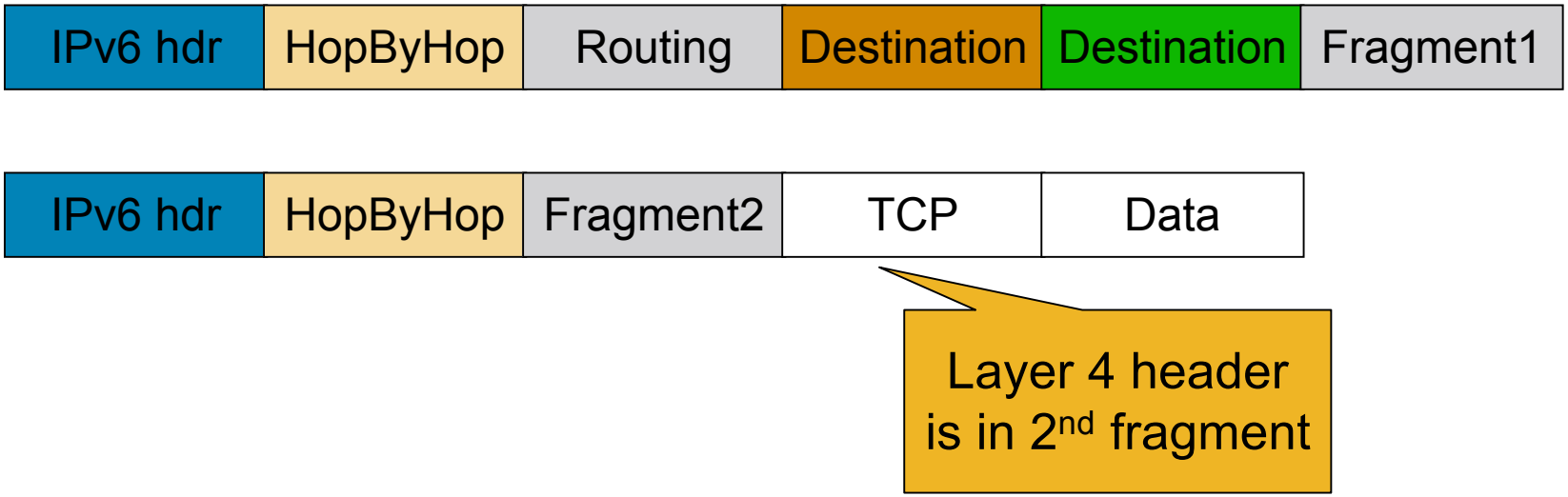
Fragment Header: IPv6



- By IPv6 RFC, fragmentation is done **only** by the end system
  - In some cases, routers act as a end system
- Reassembly done by end system like in IPv4
- Attackers can still fragment in end/intermediate system on purpose
  - a great obfuscation tool to hide attacks to IPS & firewall

Parsing the Extension Header Chain Fragmentation Matters!

- Extension headers chain can be so large than it is fragmented!
- Finding the layer 4 information is not trivial in IPv6
  - Skip all known extension headers
  - Until either known layer 4 header found => **SUCCESS**
  - Or unknown extension header/layer 4 header found... => **FAILURE**
  - Or end of extension headers => **FAILURE**



IPv6 Fragmentation and 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
- `undetermined-transport` keyword matches
  - the first fragment if the L4 protocol cannot be determined
  - Only for deny ACE

Link-Local vs. Global Addresses

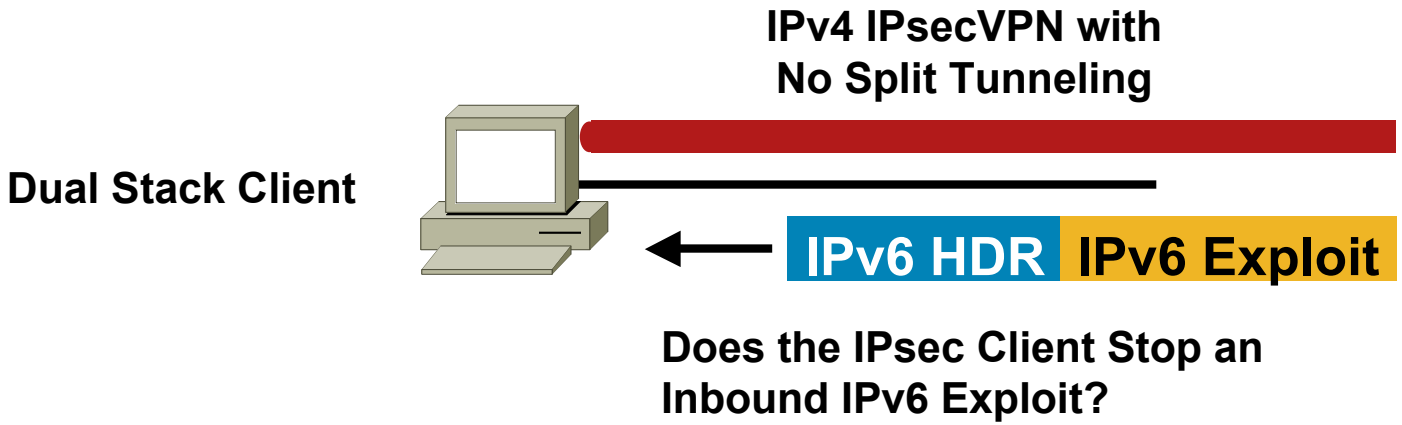
- Link-Local addresses (fe80::/16) are isolated
  - Cannot reach outside of the link
  - **Cannot be reached from outside of the link ☺**
- Could be used on the infrastructure interfaces
  - Routing protocols (inc BGP) work with LLA
  - Benefit: no remote attack against your infrastructure
    - Implicit infrastructure ACL
  - Note: need to provision loopback for ICMP generation
  - LLA can be configured statically (not the EUI-64 default) to avoid changing neighbor statements when changing MAC

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)
  - Bypass other inspection systems (SCE etc.)
  - Render Netflow blind
  - Traffic engineering becomes though
  - Asymmetrical flows (6to4)

Dual Stack Host Considerations

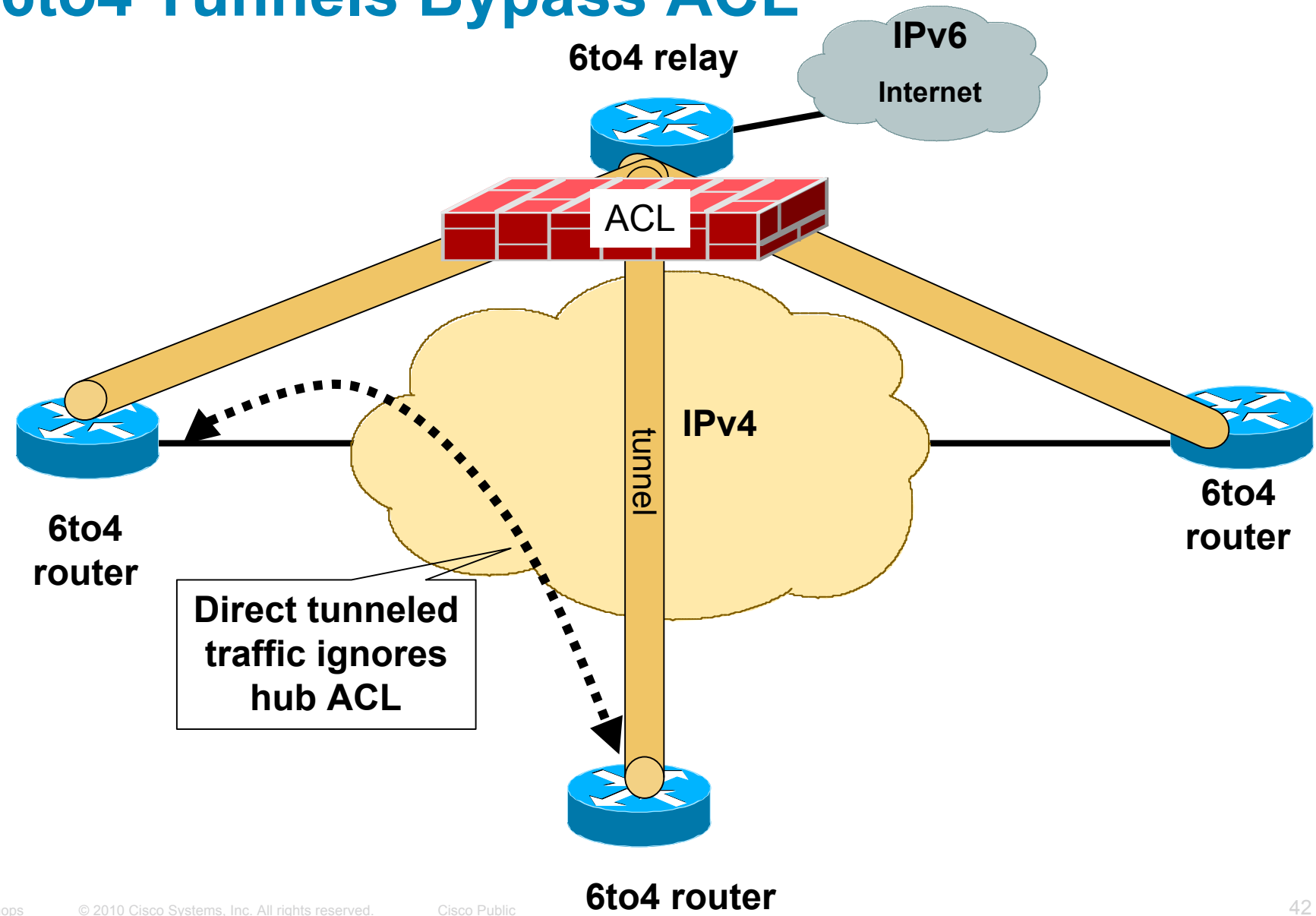
- Host security on a dual-stack device
  - Applications can be subject to attack on both IPv6 and IPv4
  - **Fate sharing**: as secure as the least secure stack...
- Host security controls should block and inspect traffic from both IP versions
  - Host intrusion prevention, personal firewalls, VPN clients, etc.



Dual Stack with Enabled IPv6 by Default Aka IPv6 Latent Threat

- 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

6to4 Tunnels Bypass ACL



6to4 Relay Security Issues

- Traffic injection & IPv6 spoofing
  - Prevent spoofing by applying uRPF check
  - Drops 6to4 packets whose addresses are built on IPv4 bogons
    - Loopback
    - RFC 1918
- Redirection and DoS
  - Block most of the ICMPv6 traffic:
    - No Neighbor Discovery
    - No link-local traffic
    - No redirect

6to4 Relay Security Issues

- Traffic is asymmetric
  - 6to4 client/router → 6to4 relay → IPv6 server:
    - client IPv4 routing selects the relay
  - IPv6 server → 6to4 relay → 6to4 client/router:
    - server IPv6 routing selects the relay
  - Cannot insert a stateful device (firewall, ...) on any path
- Potential amplification attack (looping IPv6 packet) between ISATAP server & 6to4 relay
  - Where to route: 2002:isatap::/48 ?
  - Where to route: isatap_prefix::200:5efe:6to4?

Enterprises will Ask: Can You 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 GPO or CSA 6.0**

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)**

IPv4 & IPv6 Co-Existence Translation Issues

- Whether NAT-PT or NAT444 or Address Family Translation
  - Shared IPv4 address among different subscribers
  - Per-IP address reputation, one bad behavior =>multiple subscribers impacted
  - Sending ICMP Packet-too-big to common server => bandwidth reduction for all subscribers
  - Huge amount of log for LI (but there are other ways to keep track)
- This is currently under investigation at the IETF and would deserve a session on its own.

IPv6 Stack Vulnerabilities

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

CVE-2009-2208	Jun 2009	FreeBSD OpenBSD NetBSD and others	Local users can disable IPv6 without privileges
CVE-2010-0006	Jan 2010	Linux	DoS for jumbo frames
CVE-2008-1153	Mar 2008	IOS	Cisco IOS dual-stack router IPv6 DoS
CVE-2007-4689	Nov 2007	Apple Mac OS X	Packet processing double-free memory corruption
CVE-2010-0241	Feb 2010	Microsoft	Remote code execution in Vista linked to some ICMP messages

IPv6 Security Policies

So how do we go about securing the network…?

IPv6 Security Policy

- Access control lists
  - Configuration
  - Implicit Rules
- Interface and VTY filtering
- IPv6 NetFlow
- Enterprise Security

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

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

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 IPv6 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
```

ACL and Platforms 1/2

For Your Reference

	Deny RH	Deny HbH	Max EH chain parsed in 'hardware'	Deny any other extension header
IOS software routers	Yes	No	Not applicable	Yes
Cat 3750 (doc)	Yes (not specific)	No	200 bytes	No
Cat 4500	Yes (not specific)	HW capable but not in current SW	No limit	No
Cat 6500 Sup720			128 bytes (= 50 bytes of extension headers), else L4 ignored (pass through)	No
Cat 6500 – Sup 2T				
Nexus 7000 (doc)	No	No		No
ASR 1K	Yes	No	Unlimited	Yes
GSR				
CRS-1	Yes	Not yet	Unlimited	Yes
ASA	Always	No	Not applicable (no limit in software)	No

ACL and Platforms 2/2

For Your Reference

	1st fragment w/o L4 information	uRPF	VLAN ACL	Port ACL
IOS software routers	Undetermined-transport	Yes	Not applicable	Not applicable
Cat 3750 (doc)	No	No	No	12.2(46)SE
Cat 4500	To be analyzed	To be checked	No	Zanzibar 12.2(53)SG
Cat 6500 Sup720	Not handled (pass through)	No	Half-Dome & Whitney 3	Not planned
Cat 6500 – Sup 2T		Yes		
Nexus 7000 (doc)	Can drop tiny-fragments	No	Yes	Yes
ASR 1K			Not applicable	Not applicable
GSR			Not applicable	Not applicable
CRS-1	Not handled	Yes	Not applicable	Not applicable
ASA	Not handled	Yes	Not applicable	Not applicable

For Your Reference

Example: RFC 4890 ICMP ACL

```
ipv6 access-list RFC4890
    permit icmp any any echo-reply
    permit icmp any any echo-request
    permit icmp any any 1 3
    permit icmp any any 1 4
    permit icmp any any packet-too-big
    permit icmp any any time-exceeded
    permit icmp any any parameter-problem
    permit icmp any any mld-query
    permit icmp any any mld-reduction
    permit icmp any any mld-report
    permit icmp any any nd-na
    permit icmp any any nd-ns
    permit icmp any any router-solicitation
```

For Your Reference

Example: Rogue RA & DHCP Port ACL

```
ipv6 access-list ACCESS_PORT
    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 any any

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

Note: PACL replaces RACL for the interface
In May 2009, only on Nexus-7000 and Cat 3750 12.2(46)SE

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
```

In IOS-XR, the command is '`access-class VTY ingress`',
the IPv4 and IPv6 ACL must have the same name

IPv6 Filtering

- IPv6 access-lists (ACL) are used to filter traffic and restrict access to the router
  - Used on router interfaces
  - Used to restrict access to the router
  - ACLs matching source/destination addresses, ports and various other IPv6 options
- IPv6 prefix-lists are used to filter routing protocol updates
  - Used on BGP peerings
  - Matching source and destination addresses

Cisco IOS IPv6 NetFlow

- Netflow supports IPv6
  - Type 9 flow records
  - Available from 12.4 IOS releases
- Activated by:
  - Interface subcommands:
  - **`ipv6 flow ingress`**
  - **`ipv6 flow egress`**
- Status:
  - **`show ipv6 flow cache`**

IPv6 NetFlow

```
gw>show ipv6 flow cache
IP packet size distribution (520293627 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .837 .130 .031 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 475168 bytes
  29 active, 4067 inactive, 11258417 added
  293481382 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 33992 bytes
  0 active, 1024 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
SrcAddress                InpIf    DstAddress                  OutIf    Prot SrcPrt DstPrt Packets
2001:7F8:4:1::44FC:1      Local    2001:7F8:4:1::219F:1        Gi0/0    0x06 0x00B3 0x9658 11
2001:7F8:4:1::219F:1      Gi0/0    2001:7F8:4:1::44FC:1        Local    0x06 0x9658 0x00B3 11
2001:7F8:4:1::44FC:1      Local    2001:7F8:4:1::220A:2        Gi0/0    0x06 0x00B3 0x8525 110
2001:7F8:4:1::44FC:1      Local    2001:7F8:4:1::847:1         Gi0/0    0x3A 0x0000 0x8800 14
2001:7F8:4:1::32E6:1      Gi0/0    FE80::222:55FF:FEE4:1F1B    Local    0x3A 0x0000 0x8800 256
2001:7F8:4:1::220A:2      Gi0/0    2001:7F8:4:1::44FC:1        Local    0x06 0x8525 0x00B3 82
FE80::212:F2FF:FEF2:3C61  Gi0/0    FE80::222:55FF:FEE4:1F1B    Local    0x3A 0x0000 0x8800 256
2001:7F8:4:1::1F8B:1      Gi0/0    2001:7F8:4:1::44FC:1        Local    0x06 0x00B3 0x4533 4
```

Summary of Cisco IPv6 Enterprise Security Products

- ASA Firewall Since version 7.0
  - SSL VPN for IPv6 (ASA 8.0)
  - No header extension parsing,
  - Stateful-failover (ASA 8.2.2)
- FWSM
  - IPv6 in software... 80 Mbpps not suitable
  - IOS Firewall IOS 12.3(7)T (released 2005)
- Email Security Appliance
  - IPv6 currently under beta
- Cisco Security Agent
  - Since version 6.0 for IPv6 network protection
  - IPS Since 6.2 (November 2008)
  - Shared signatures + specific IPv6 signatures (including tunnel detection)

Securing IPv6 Connectivity

How do we secure our end-to-end connections…?

Securing IPv6 Connectivity

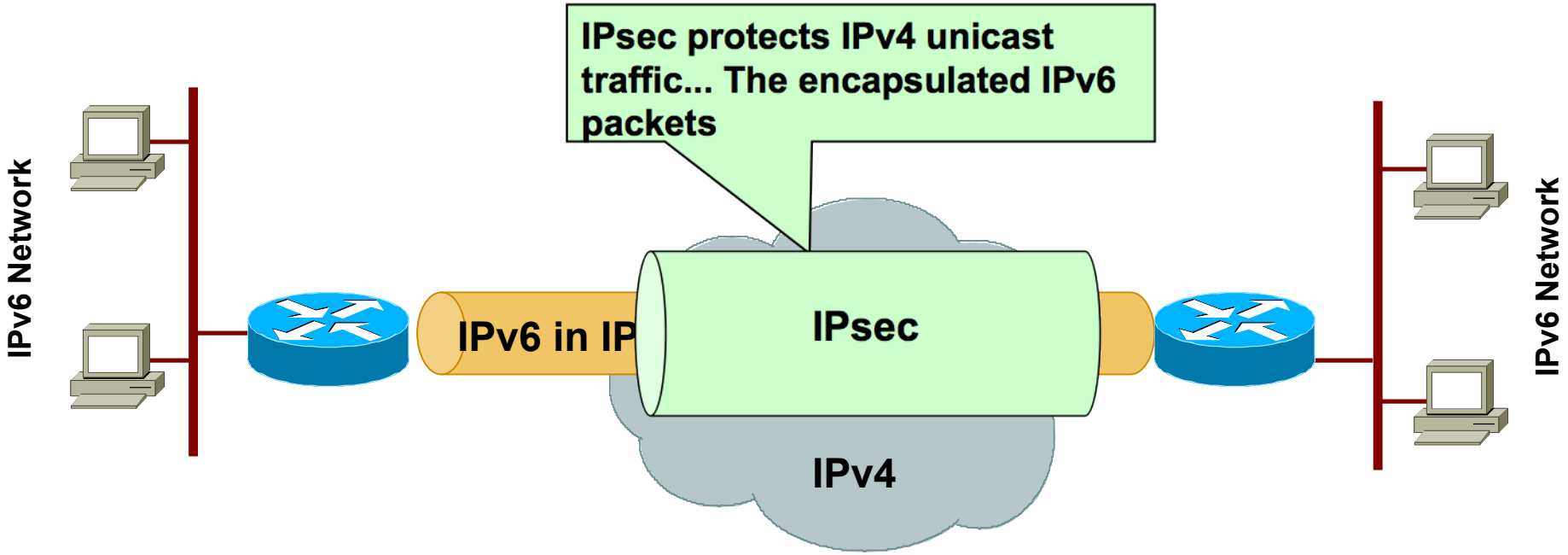
- Over Internet
- Site to Site VPNs

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	N/A

Secure Site to Site IPv6 Traffic over IPv4 Public Network with GRE IPsec



GRE tunnel can be used to transport both IPv4 and IPv6 in the same tunnel

Similar technique for remote access with ISATAP tunnels

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)
  - 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)

IPv6 Security Best Practices

Recommendations…

Candidate Best Practices

- **Train your network operators and security managers on IPv6**
- **Train your network operators and security managers on IPv6**
- Selectively filter ICMP (RFC 4890)
- Block Type 0 Routing Header at the edge
- Copy the IPv4 Best Common Practices
  - Implement RFC 2827-like filtering
  - If management plane is only IPv4,block IPv6 to the core devices (else infrastructure ACL for IPv6)
  - Determine what extension headers will be allowed through the access control device
  - Deny IPv6 fragments destined to an internetworking device when possible
  - Use traditional authentication mechanisms on BGP and IS-IS
  - Use IPsec to secure protocols such as OSPFv3 and RIPng
  - Document procedures for last-hop traceback

Candidate Best Practices (Cont.) Mainly for Enterprise Customers

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

Conclusion

- So, nothing really new in IPv6
- 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

IPv6 Security

Philip Smith <pfs@cisco.com>

CTO Consulting Engineer