The IPv6 (in)security

Łukasz Bromirski
lbromirski@cisco.com

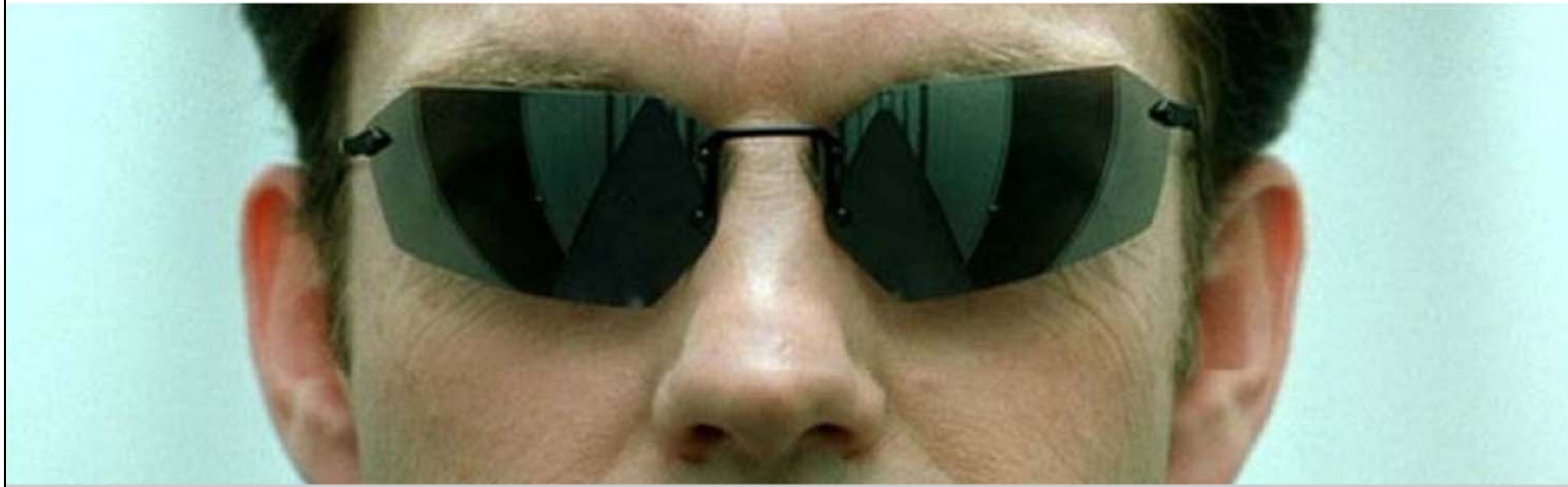
Confidence 2010.11, Prague, XI.2010

Disclaimer

- The IPv6 should be treated as **another protocol** – there's no inherent security problem in the idea itself, but as usual, **many mechanism need to be mastered** to be applied **securely**
- We will migrate to IPv6 at some point in time, so you'll either spend time now to learn and apply the knowledge in practice, or be forced to learn it very fast later on – with obvious drawbacks
- **You're running IPv6 anyway propably today**, even if you don't know it

Agenda

- The security problems in IPv4 solved in IPv6
- Attack environment for IPv6
- Protecting the network
    - Management plane
    - Control plane
    - Data plane
- Other issues and areas of concern
- Real life implementation info
- Q&A



Security problems of IPv4 solved in IPv6

None

- All layers above IPv4 are equally „insecure” as the ones over the IPv6
- IPv6 makes some things better, other things worse and some things differently than in IPv4
- IPv6 is more complex than IPv4

  complexity brings problems in **security**
- All vendors leading IPv6 efforts have already published bugs, and they’ll publish more

  Cisco, Juniper, Microsoft, Sun/Oracle and a lot of Open Source software

IPv6 attack environment

Nothing changed fundamentally

- Sniffing

  IPv6 mandates IPsec capabilities, do you use it end-to-end after finally getting connected?

- Application-level attacks

  Even if IPsec is turned on – most of the attacks happen in this layer anyway, so „did you install a Service Pack today”?

- Rogue devices & MITM attacks

  Still can and will be executed

Reconnaissance In IPv6

Subnet Size Difference

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

  14.8 Mpps (roughly a 10GE interface) = ~40 000 years

- This makes scanning blindly inefficient
- There are interesting studies for real world assignment behaviors for IPv6 addressing*

$$\frac{2^{128}}{6.5 \text{ Billion}}$$ **= 52 Trillion Trillion IPv6 addresses per person**

World’s population is approximately 6.5 billion

*** Malone, D. 2008. *Observations of IPv6 Addresses*. Passive and Active Measurement Conference (PAM 2008, LNCS 4979), 29–30 April 2008.**

Reconnaissance In IPv6

Scanning Methods Are Likely to Change

- Public servers will still need to be DNS reachable

  More information collected by Google...

- Increased deployment/reliance on dynamic DNS

  More information will be in DNS

- Using peer-to-peer clients gives IPv6 addresses of peers
- Administrators may adopt easy-to-remember addresses (::10,::20,::F00D, ::DEAD, ::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 derive IPv6 address from IPv4 address

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-limiters, or just pushing a separate FPGA to do the job is not an solution, it’s just a way to address the problem, not solve the root cause

- Using a /64 on point-to-point links => a lot of addresses to scan!

- 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!

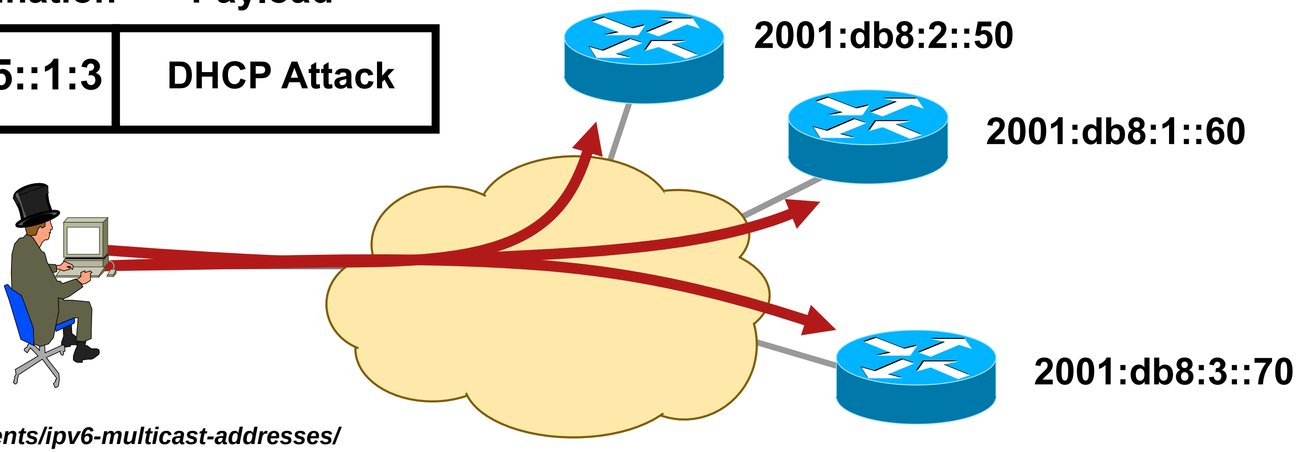
- No need for reconnaissance anymore
- 3 site-local multicast addresses

  FF05::2 all-routers, FF05::FB mDNSv6, FF05::1:3 all DHCP servers
- Several link-local multicast addresses

  FF02::1 all nodes, FF02::2 all routers, FF02::F all UPnP, ...
- Some deprecated (RFC 3879) site-local addresses but still used

  FEC0:0:0:FFFF::1 DNS server

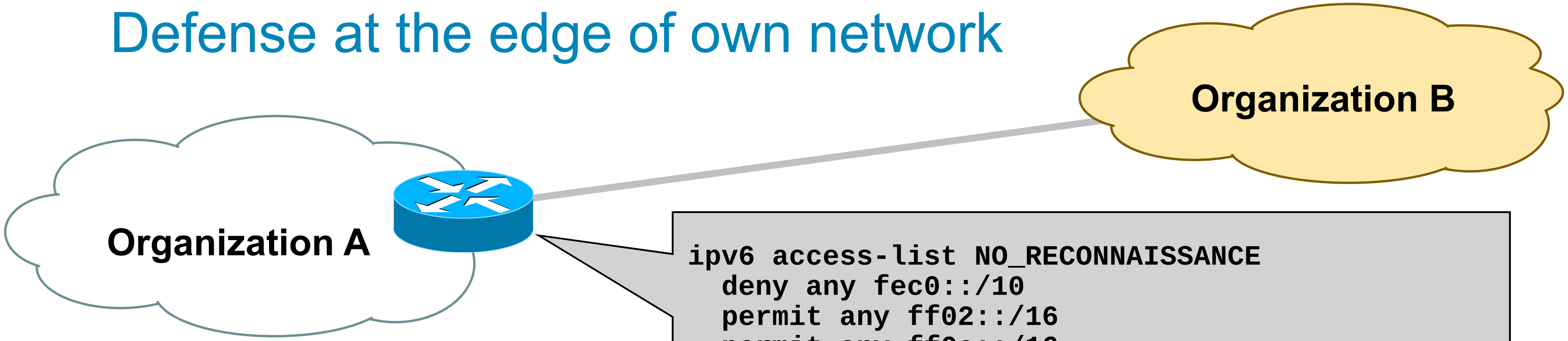
Source	Destination	Payload
Attacker	FF05::1:3	DHCP Attack



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

Reconnaissance In IPv6?

Defense at the edge of own network



```
ipv6 access-list NO_RECONNAISSANCE
  deny any fec0::/10
  permit any ff02::/16
  permit any ff0e::/16
  deny any ff00::/8
  permit any any
```

- The site-local/anycast addresses must be filtered at the border in order to make them unreachable from the outside
- ACL block ingress/egress traffic to

  Block FEC0::/10 (deprecated site-local addresses)

  Permit mcast to FF02::/16 (link-local scope)

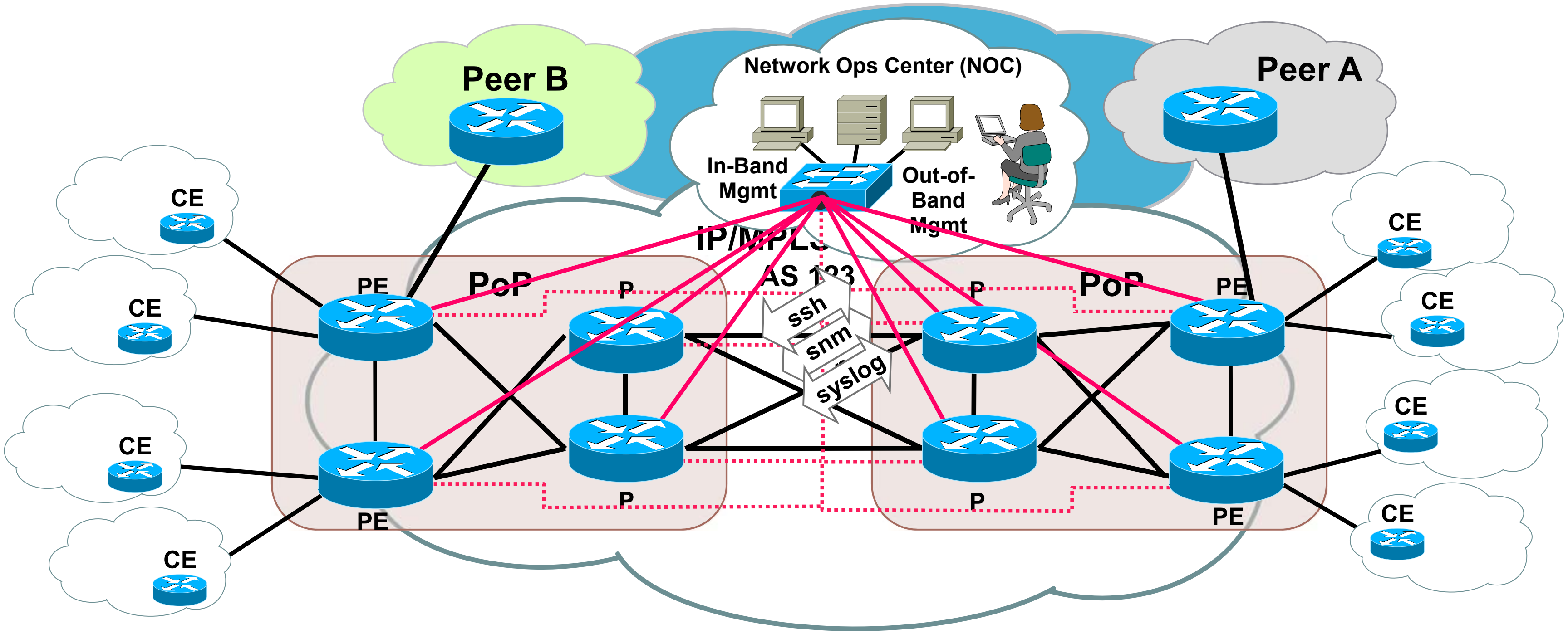
  Permit mcast to FF0E::/16 (global scope)

  Block all mcast

Protecting the management plane

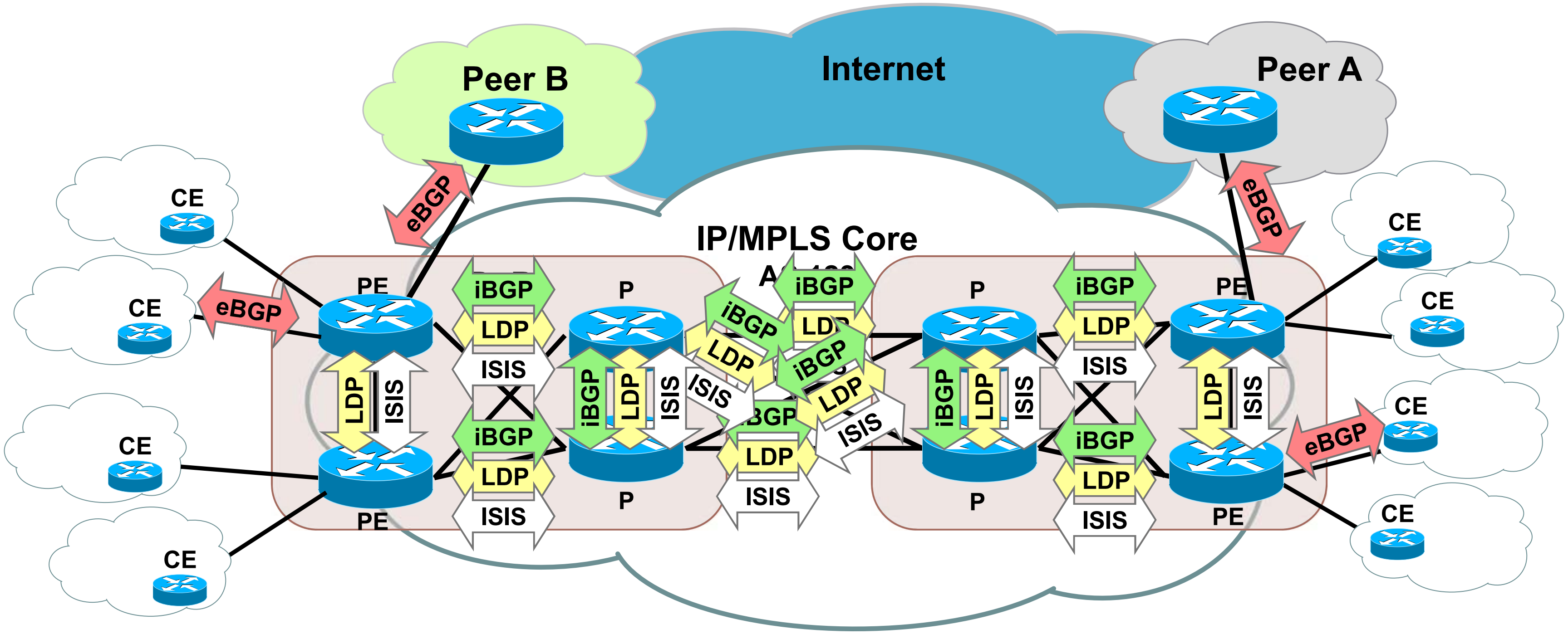
Management plane

- Management, provisioning, monitoring with protocols like SSH, FTP, SNMP, Syslog, TACACS+ i RADIUS, DNS, NetFlow, ROMMON, CDP, LLDP, others



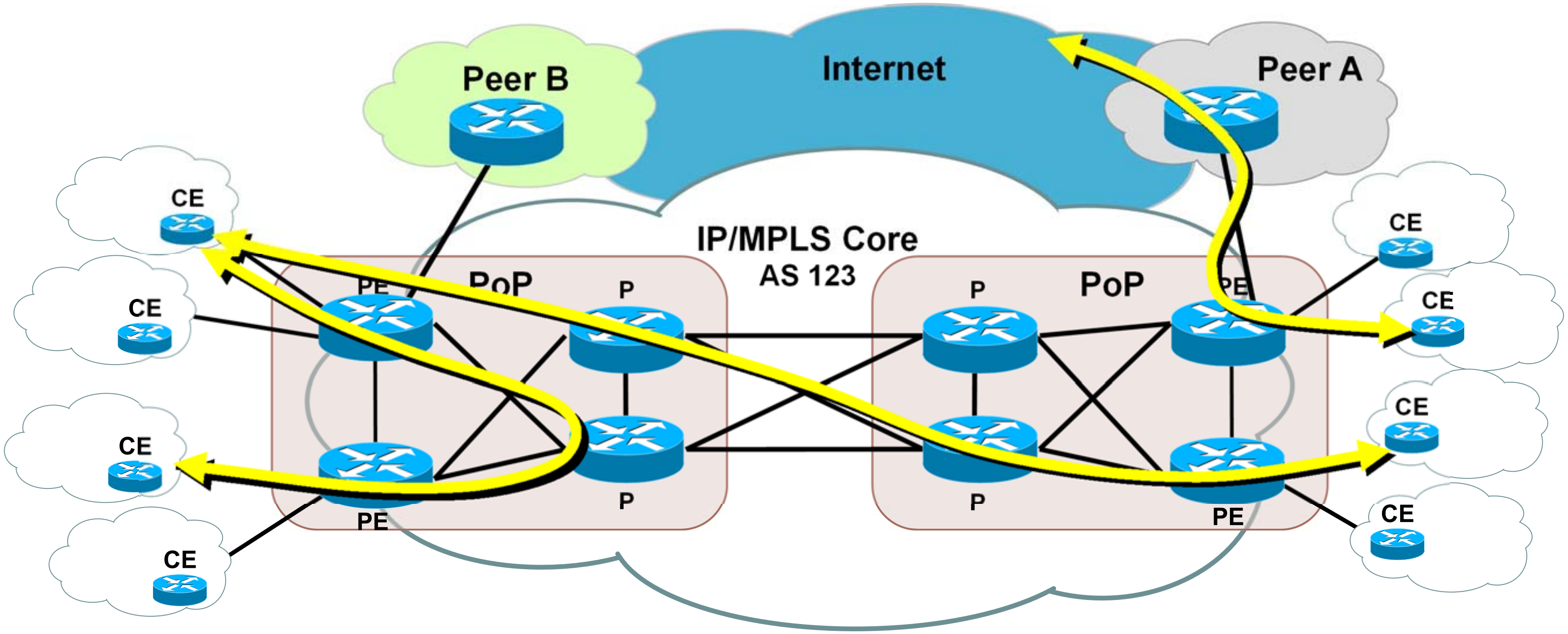
Control plane

- All the protocols that are making the network to work – forward packets, establish adjacencies with new routers, etc. – protocols like BGP, OSPF, LDP, IS-IS, ARP, Layer 2 keepalives, ATM OAM, PPP LCP, others



Data plane

- Traffic going from and to customers – it's the traffic SP shouldn't touch, but contains all of the protocols customers can use



Management over IPv6

- SSH, syslog, SNMP, NetFlow all work over IPv6
- Dual-stack management plane

  More resilient: works even if one IP version is down

  More exposed: can be attacked over IPv4 and IPv6
- Currently under development: RADIUS

  But, IPv6 RADIUS attributes can be transported over IPv4

- As usual, infrastructure ACL is your friend

Protecting the control plane

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

Link-Local vs. Global Addresses

- Link-Local addresses, fe80::/16, (LLA) 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 (including BGP) work with LLA

    Benefit: no remote attack against your infrastructure

        Implicit infrastructure ACL

    Note: need to provision loopback for ICMP generation (notably *traceroute* and PMTUD)

    LLA can be configured statically (not the EUI-64 default) to avoid changing neighbor statements when changing MAC

```
interface FastEthernet 0/0
   ipv6 address fe80::1/16 link-local
```

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
  - ...

ARP Spoofing is now NDP Spoofing:
Mitigation

- **BAD NEWS**: nothing like dynamic ARP inspection for IPv6

  Platforms dealing with the traffic in hardware will need to be upgraded – meaning either forklift upgrade (whole chassis/RP/LC) or just a firmware update on the FPGAs

- **GOOD NEWS**: Secure Neighbor Discovery (RFC 3971)

  SEND = NDP + crypto

  Present in Cisco IOS and an open source implementations

  But not in Windows Vista, 2008, 7... (incompatible with SLAAC privacy extensions enabled by default)

  Crypto means slower – while it may not hit your workstation it will hit many small computers (the case as it was with vendors not implementing WEP and then WPA because ‚it slows down the network') and needs PKI infrastructure

- Other **GOOD NEWS**:

  Private VLAN works with IPv6

  Port security works with IPv6

  801.x works with IPv6

  Port ACL on IPv6 capable switches

  For FTTH & other broadband access, DHCP-PD means not need to layer-2 communication between CPE

Secure Neighbor Discovery (SEND)

RFC 3971

- 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

- Certification paths for authorized Routers

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

Protecting the data plane

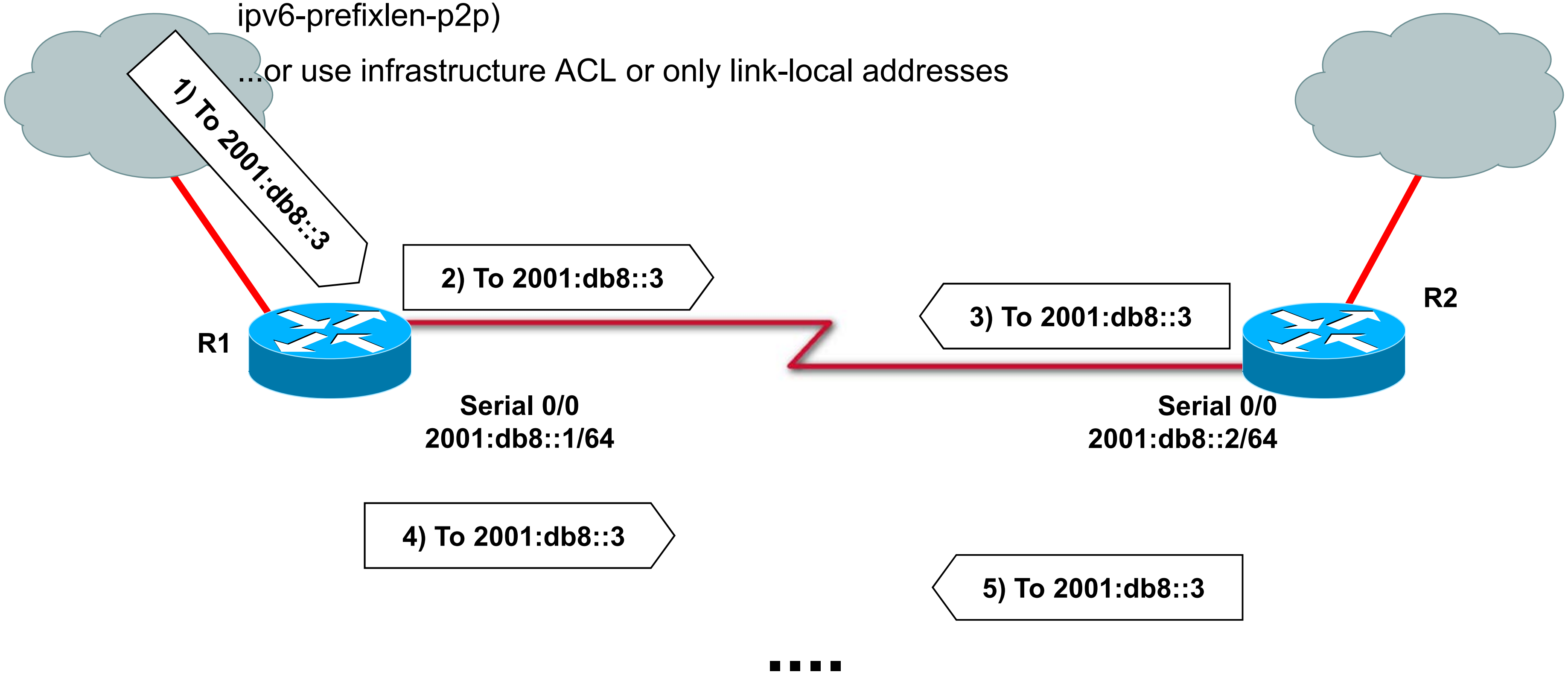
DoS Example

Ping-Pong over Physical Point-to-Point

- Same as in IPv4, on real P2P, if not for me send it on the other side... Could produce looping traffic
- Platforms implementing RFC 4443 (ICMPv6) correctly are not affected here

  Use /127 on P2P link (see also RFC 3627 and http://tools.ietf.org/html/draft-kohno-ipv6-prefixlen-p2p)

  ...or use infrastructure ACL or only link-local addresses



1) To 2001:db8::3

2) To 2001:db8::3

3) To 2001:db8::3

4) To 2001:db8::3

5) To 2001:db8::3

....

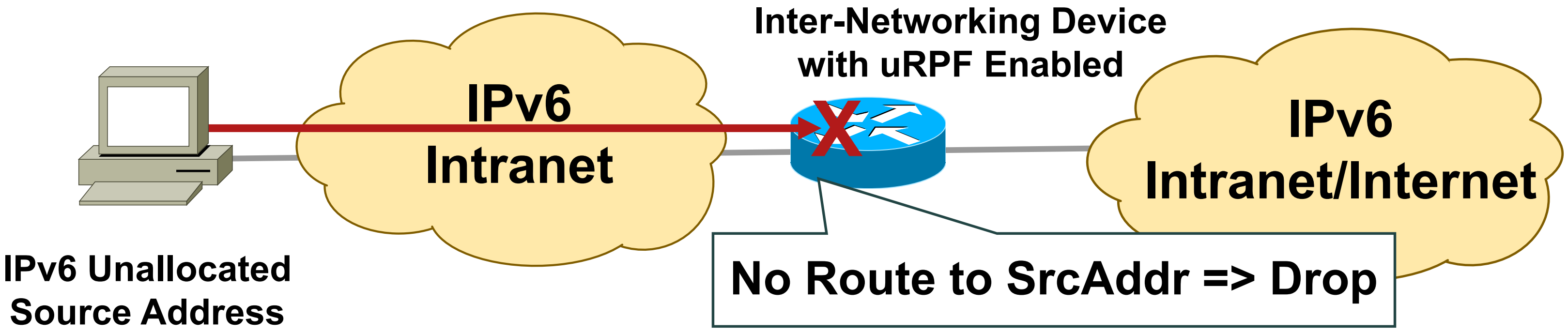
IPv6 Bogon Filtering and Anti-Spoofing

- IPv6 nowadays has its bogons:

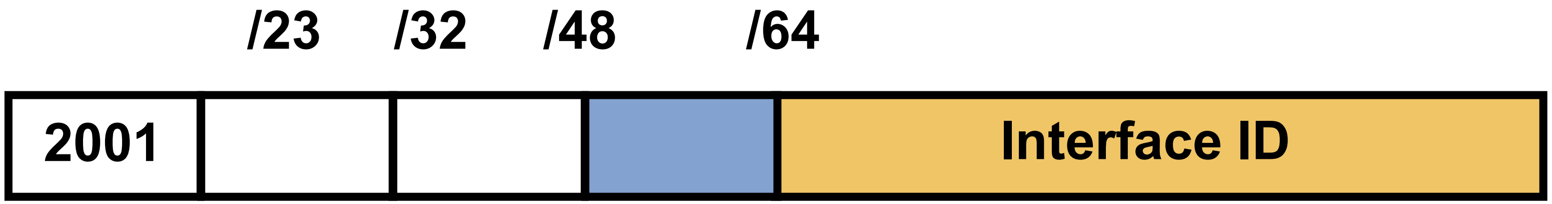
  http://www.team-cymru.org/Services/Bogons/fullbogons-ipv6.txt

- Similar situation as IPv4

  => Same technique for single-homed edge= uRPF



IPv6 Privacy Extensions (RFC 3041)



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

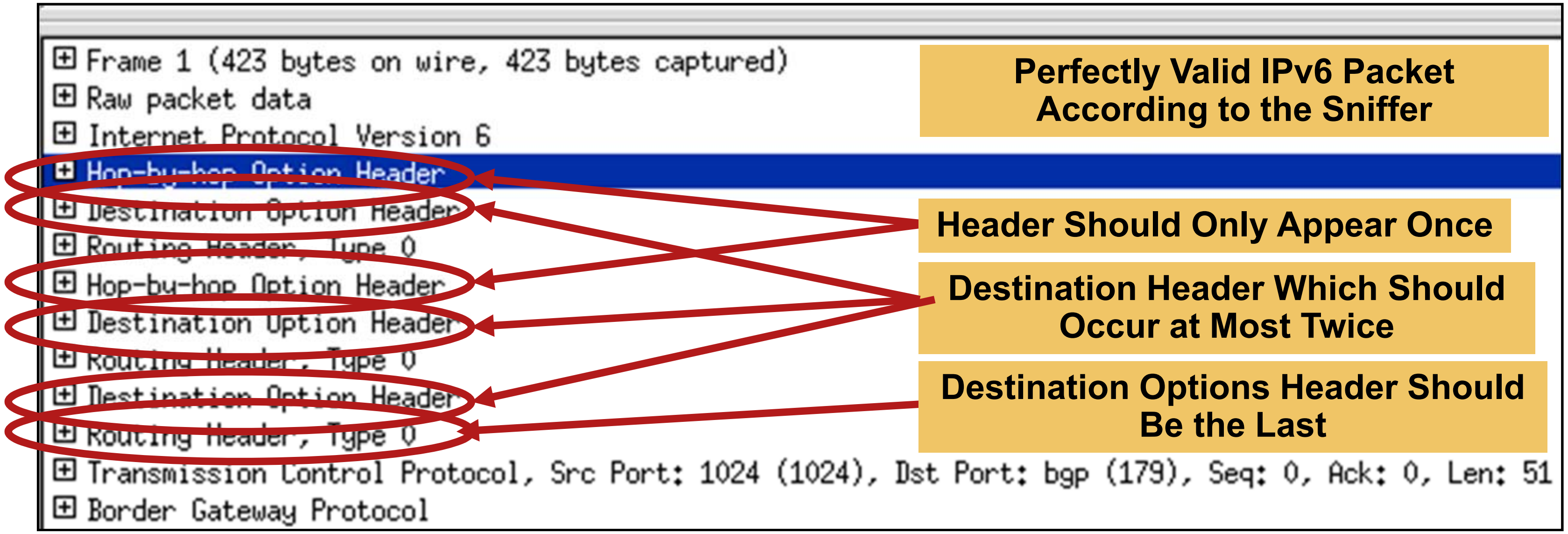
Recommendation: Use Privacy Extensions for External Communication but not for Internal Networks (Troubleshooting and Attack Trace Back)

IPv6 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?



```
⊞ Frame 1 (423 bytes on wire, 423 bytes captured)
⊞ Raw packet data
⊞ Internet Protocol Version 6
⊞ Hop-by-hop Option Header
⊞ Destination Option Header
⊞ Routing Header, Type 0
⊞ Hop-by-hop Option Header
⊞ Destination Option Header
⊞ Routing Header, Type 0
⊞ Destination Option Header
⊞ Routing Header, Type 0
⊞ Transmission Control Protocol, Src Port: 1024 (1024), Dst Port: bgp (179), Seq: 0, Ack: 0, Len: 51
⊞ Border Gateway Protocol
```

Perfectly Valid IPv6 Packet According to the Sniffer

Header Should Only Appear Once

Destination Header Which Should Occur at Most Twice

Destination Options Header Should Be the Last

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

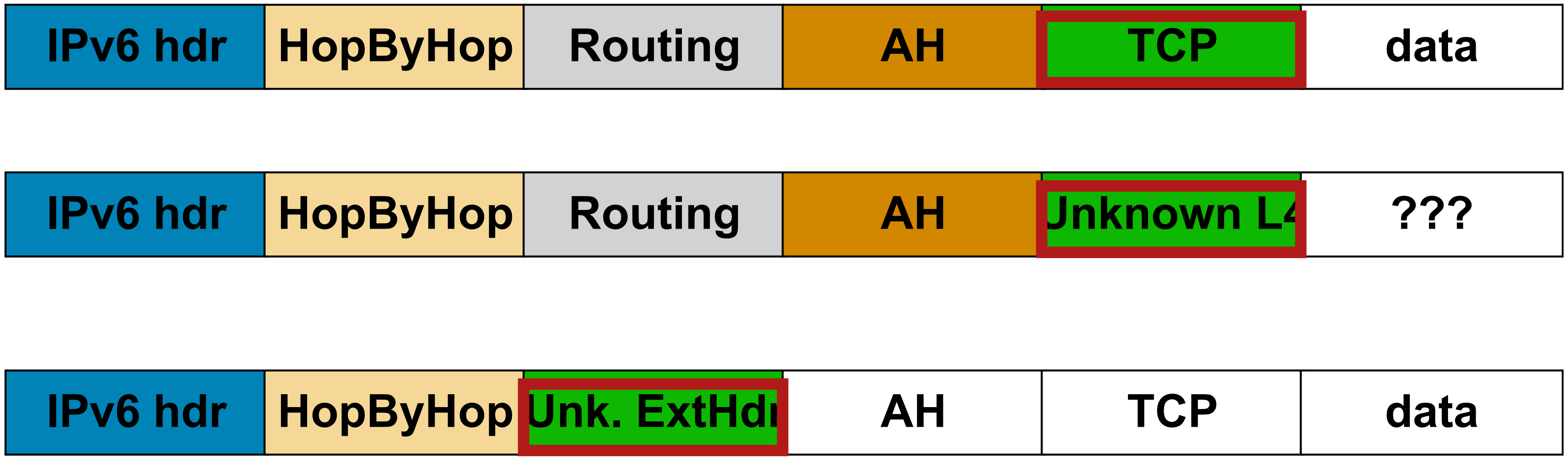
Parsing the Extension Header Chain

- 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**

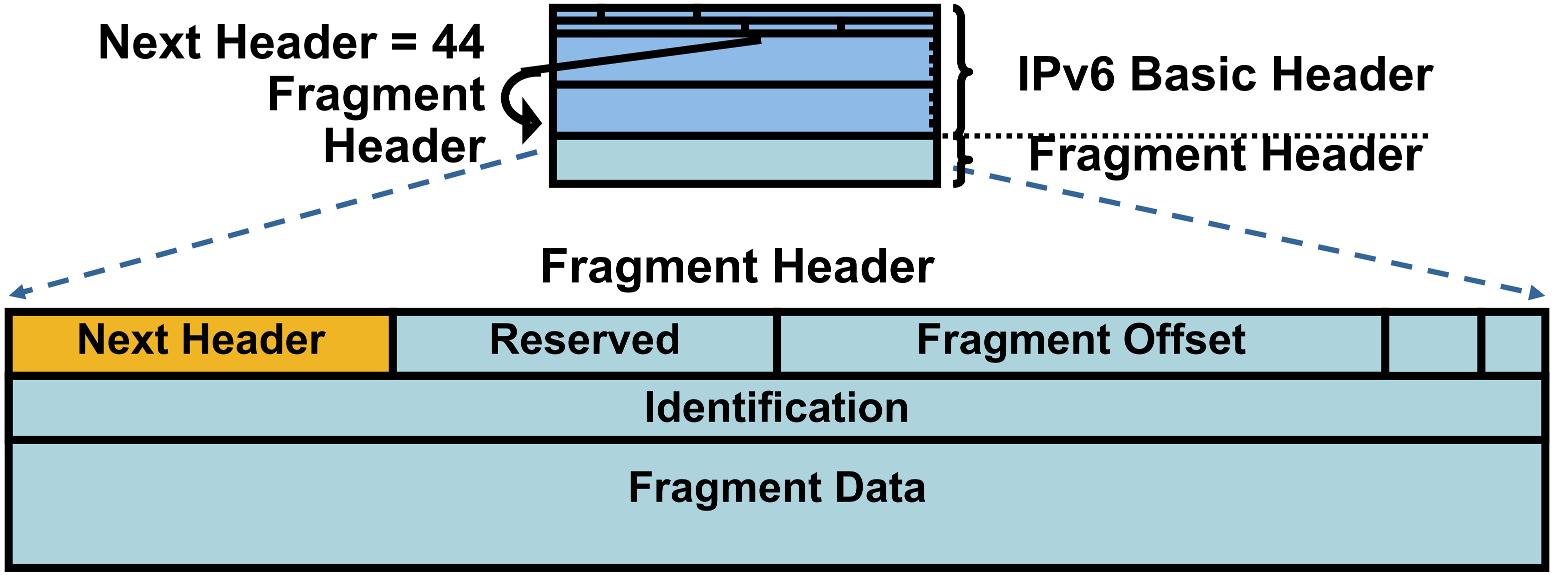


IPv6 hdr | HopByHop | Routing | AH | TCP | data

IPv6 hdr | HopByHop | Routing | AH | Unknown L4 | ???

IPv6 hdr | HopByHop | Unk. ExtHdr | AH | TCP | data

Fragment Header: IPv6



Next Header = 44 Fragment Header

IPv6 Basic Header

Fragment Header

Fragment Header

Next Header	Reserved	Fragment Offset		
Identification				
Fragment Data				

- In IPv6 fragmentation is done only by the end system

  Tunnel end-points are end systems => Fragmentation / re-assembly can happy inside the network

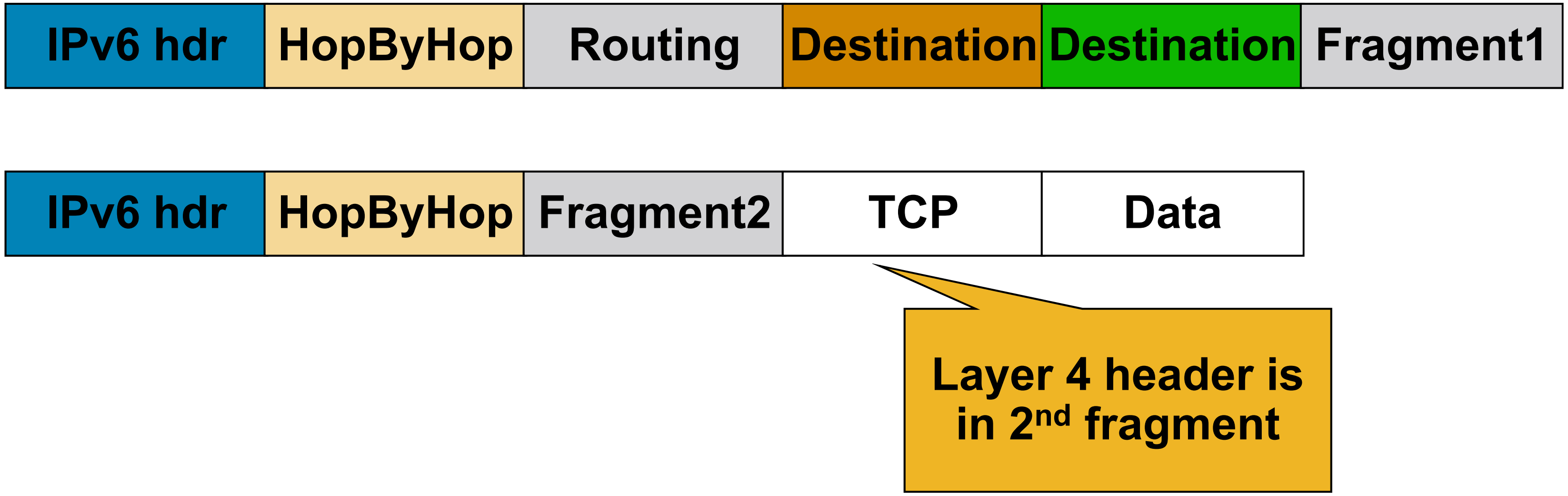
- Reassembly done by end system like in IPv4

- 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!
- 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**
  - Or end of extension header => **FAILURE**



IPv6 hdr | HopByHop | Routing | Destination | Destination | Fragment1

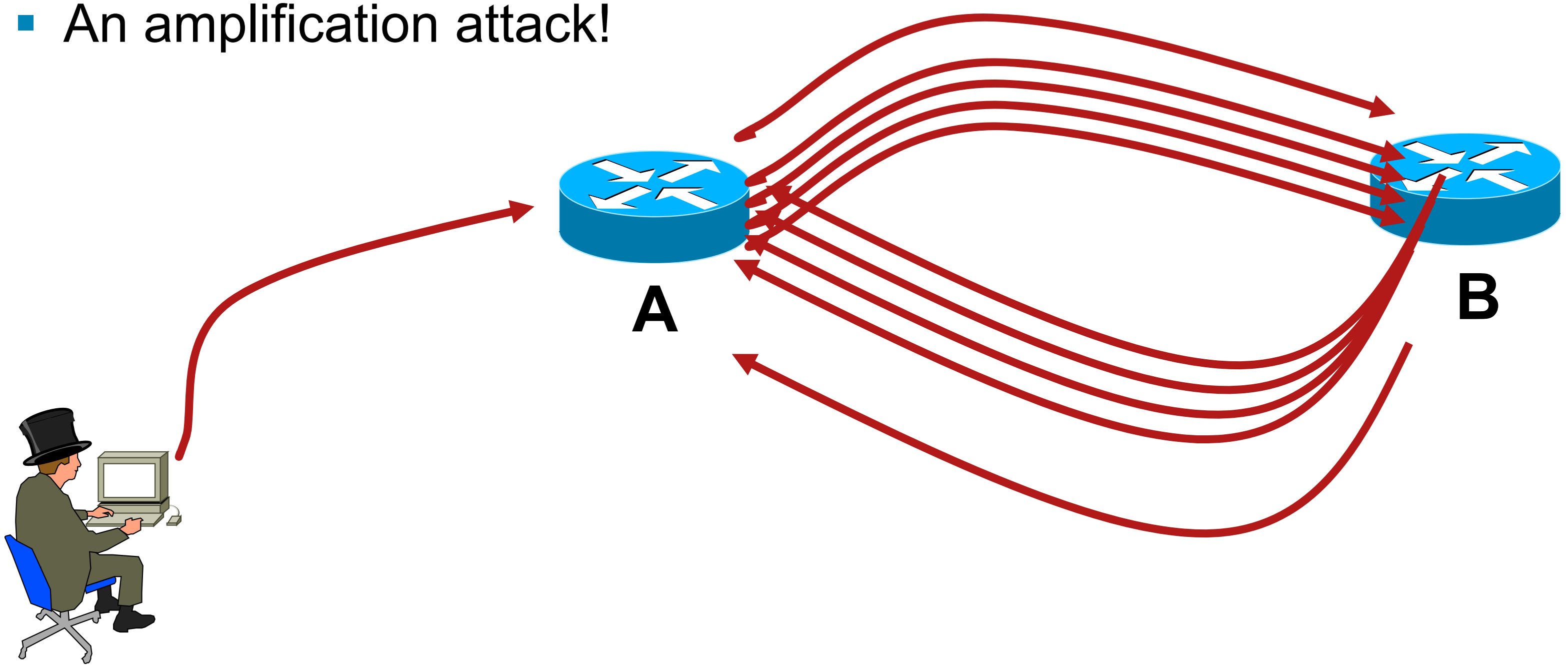
IPv6 hdr | HopByHop | Fragment2 | TCP | Data

Layer 4 header is in 2nd fragment

Type 0 Routing Header
One issue: Amplification Attack

- Beside the well-known dumb firewall by-pass...
- 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!



* As of RFC 5095 (Dec 2007) RH0 is deprecated

„IPsec End-to-End will Save the World”?

- IPv6 mandates the implementation of IPsec
- IPv6 does not require the use of IPsec
- Some organizations believe that IPsec should be used to secure all flows...
  - Interesting **scalability** issue (n^2 issue with IPsec)
  - Need to **trust endpoints and end-users** because the network cannot secure the traffic: no IPS, no ACL, no firewall
  - Network **telemetry is blinded**: NetFlow 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.

IPv6

Other issues and areas of concern

IPv6 tools ready to be used

Let the Games Begin

- 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

Tools of trade

- THC IPv6 Attack Toolkit

  parasite6, alive6, fake_router6, redir6, toobig6, detect-new-ip6, dos-new-ip6, fake_mld6, fake_mipv6, fake_advertiser6, smurf6, rsmurf6

- Scanners

  nmap, halfscan6

- Packet forgery

  Scapy6, SendIP, Packit, Spak6

- DoS Tools

  6tunneldos, 4to6ddos, Imps6-tools

The Hacker's Choice

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

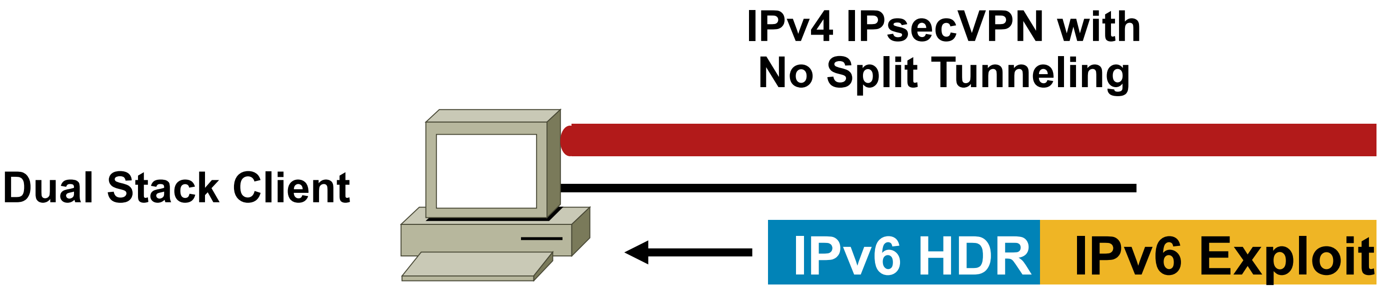
- Host security on a dual-stack device

  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.

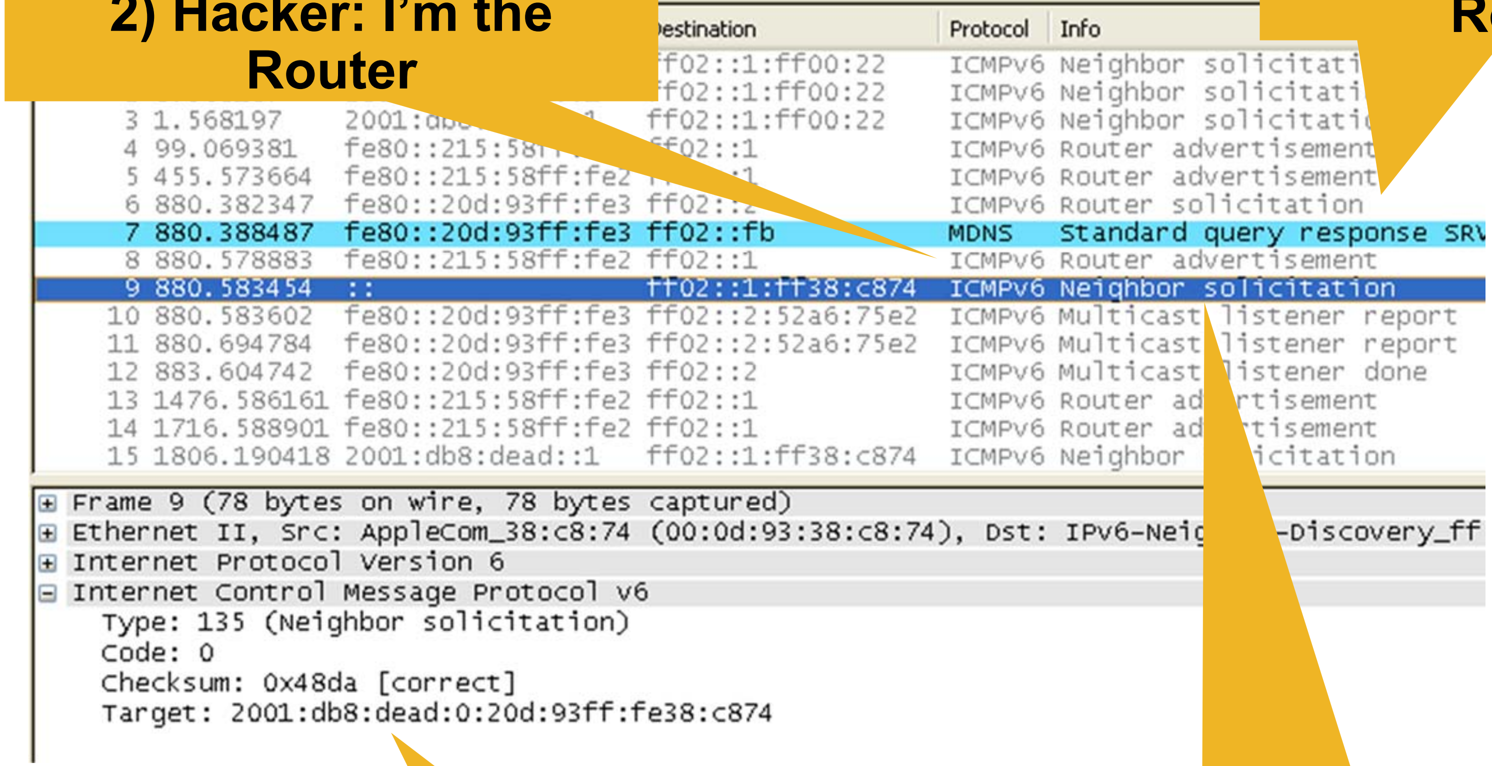


Does the IPsec Client Stop an Inbound IPv6 Exploit?

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**

Enabling IPv6 on a Remote Host
(in this Case Mac OS/X)



```
                                  estination          Protocol Info
                                  ff02::1:ff00:22     ICMPv6 Neighbor solicitati
                                  ff02::1:ff00:22     ICMPv6 Neighbor solicitati
  3 1.568197    2001:db           ff02::1:ff00:22     ICMPv6 Neighbor solicitati
  4 99.069381   fe80::215:58      ff02::1             ICMPv6 Router advertisement
  5 455.573664  fe80::215:58ff:fe2      :1            ICMPv6 Router advertisement
  6 880.382347  fe80::20d:93ff:fe3 ff02::2            ICMPv6 Router solicitation
  7 880.388487  fe80::20d:93ff:fe3 ff02::fb           MDNS   Standard query response SRV
  8 880.578883  fe80::215:58ff:fe2 ff02::1            ICMPv6 Router advertisement
  9 880.583454  ::                 ff02::1:ff38:c874  ICMPv6 Neighbor solicitation
 10 880.583602  fe80::20d:93ff:fe3 ff02::2:52a6:75e2  ICMPv6 Multicast listener report
 11 880.694784  fe80::20d:93ff:fe3 ff02::2:52a6:75e2  ICMPv6 Multicast listener report
 12 883.604742  fe80::20d:93ff:fe3 ff02::2            ICMPv6 Multicast listener done
 13 1476.586161 fe80::215:58ff:fe2 ff02::1            ICMPv6 Router ad  rtisement
 14 1716.588901 fe80::215:58ff:fe2 ff02::1            ICMPv6 Router ad  rtisement
 15 1806.190418 2001:db8:dead::1   ff02::1:ff38:c874  ICMPv6 Neighbor   icitation

⊞ Frame 9 (78 bytes on wire, 78 bytes captured)
⊞ Ethernet II, Src: AppleCom_38:c8:74 (00:0d:93:38:c8:74), Dst: IPv6-Neig    -Discovery_ff
⊞ Internet Protocol Version 6
⊟ Internet Control Message Protocol v6
    Type: 135 (Neighbor solicitation)
    Code: 0
    Checksum: 0x48da [correct]
    Target: 2001:db8:dead:0:20d:93ff:fe38:c874
```

1) Dual-Stack MacOS: any IPv6 Router?

2) Hacker: I’m the Router

3) Newly Enabled IPv6 MacOS does DAD

4) The Full IPv6 Address of the MacOS

Transition Threats—ISATAP

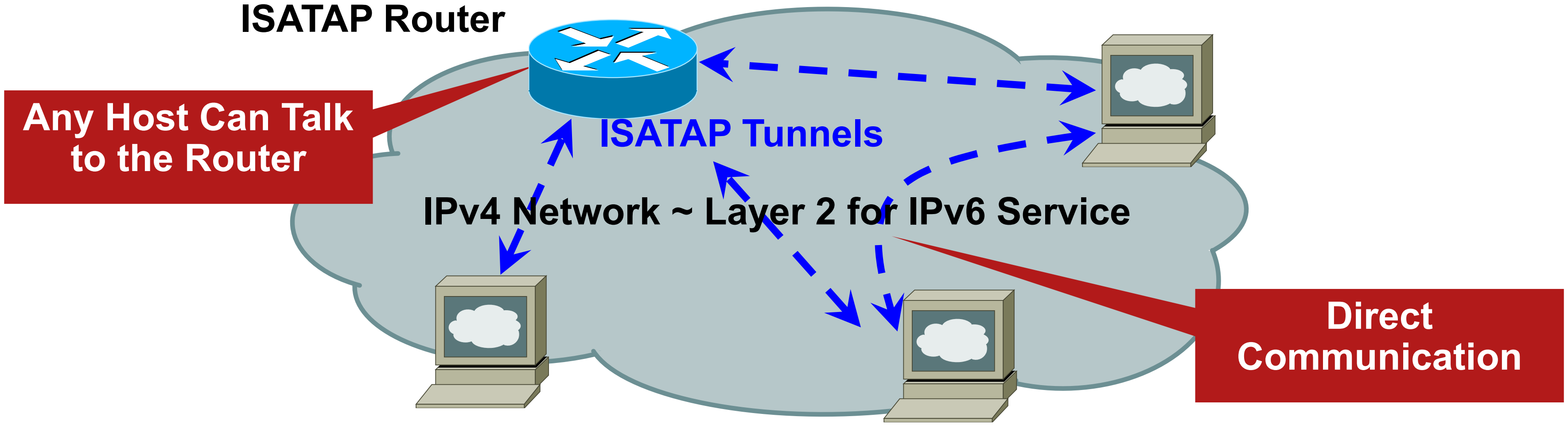
- Unauthorized tunnels—firewall bypass (protocol 41)
- IPv4 infrastructure looks like a Layer 2 network to ALL ISATAP hosts in the enterprise

  This has implications on network segmentation and network discovery

- No authentication in ISATAP—rogue routers are possible

  Windows default to isatap.example.com

- Ipv6 addresses can be guessed based on IPv4 prefix


ISATAP Router
Any Host Can Talk to the Router
ISATAP Tunnels
IPv4 Network ~ Layer 2 for IPv6 Service
Direct Communication

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
- 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

TEREDO?

- Teredo navalis

  A shipworm drilling holes
  in boat hulls

- Teredo Microsoftis

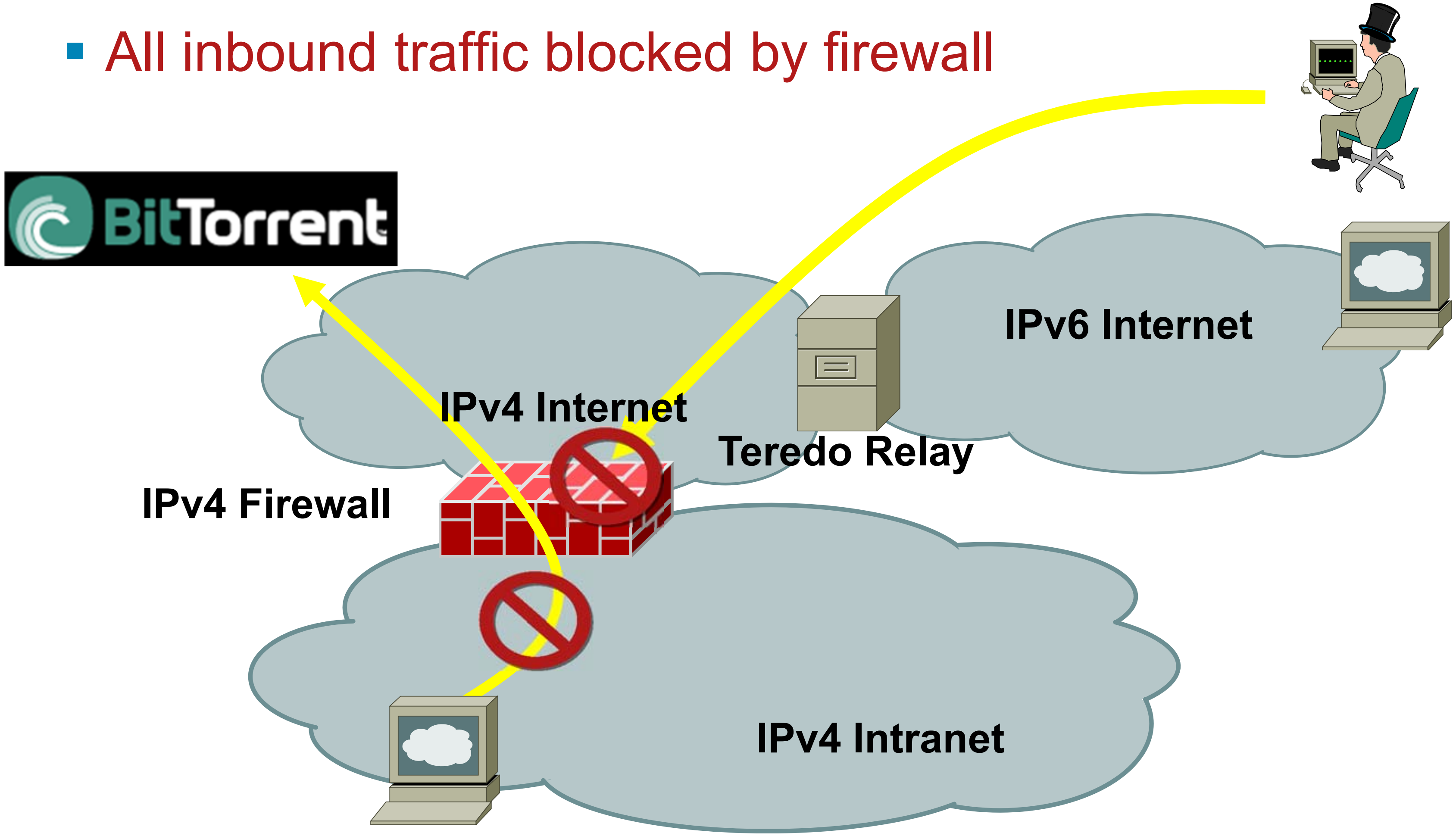
  IPv6 in IPv4 punching holes
  in NAT devices

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

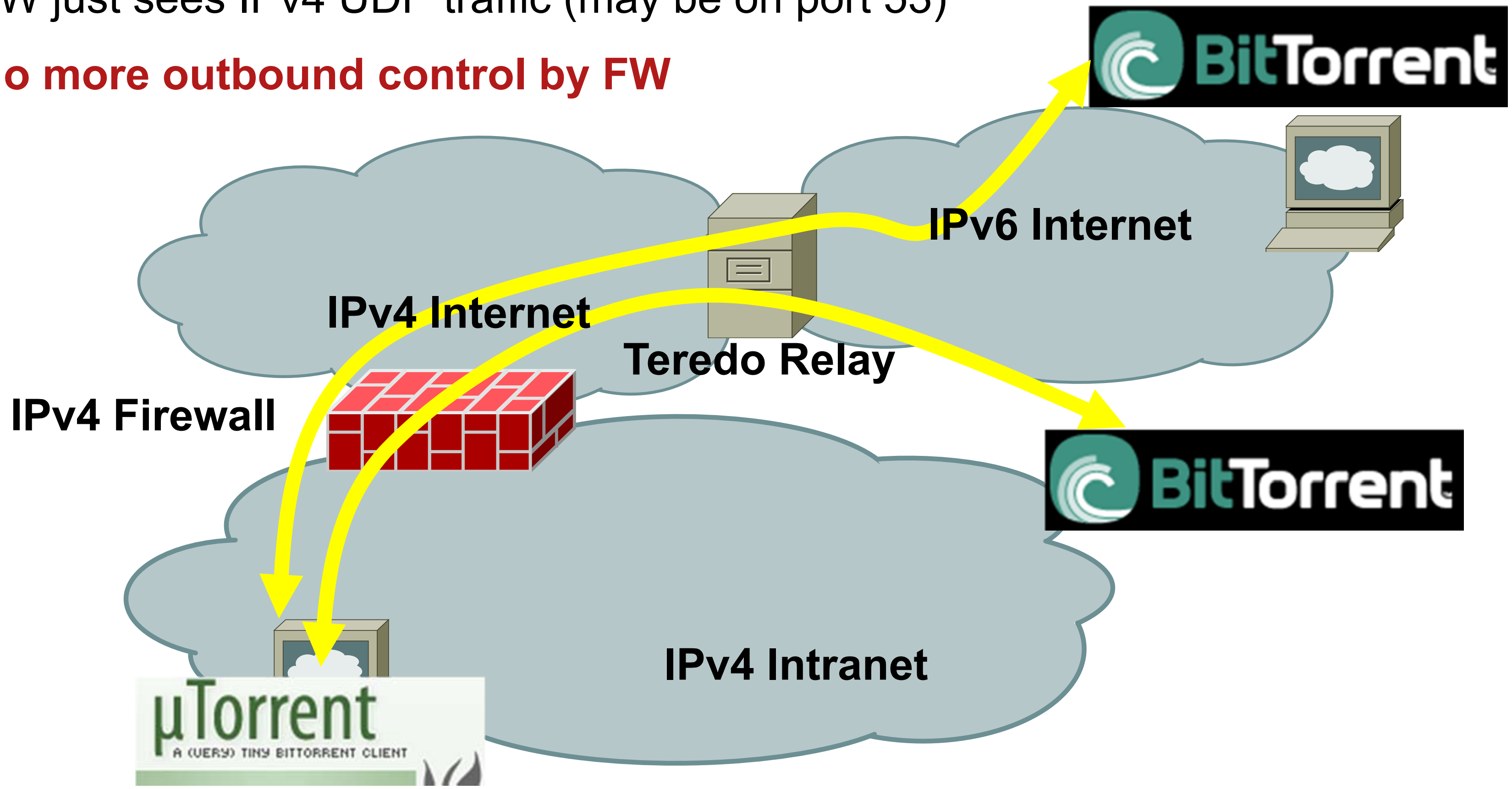


Teredo Tunnels (2/3)

No More Outbound Control

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)
- **No more outbound control by FW**

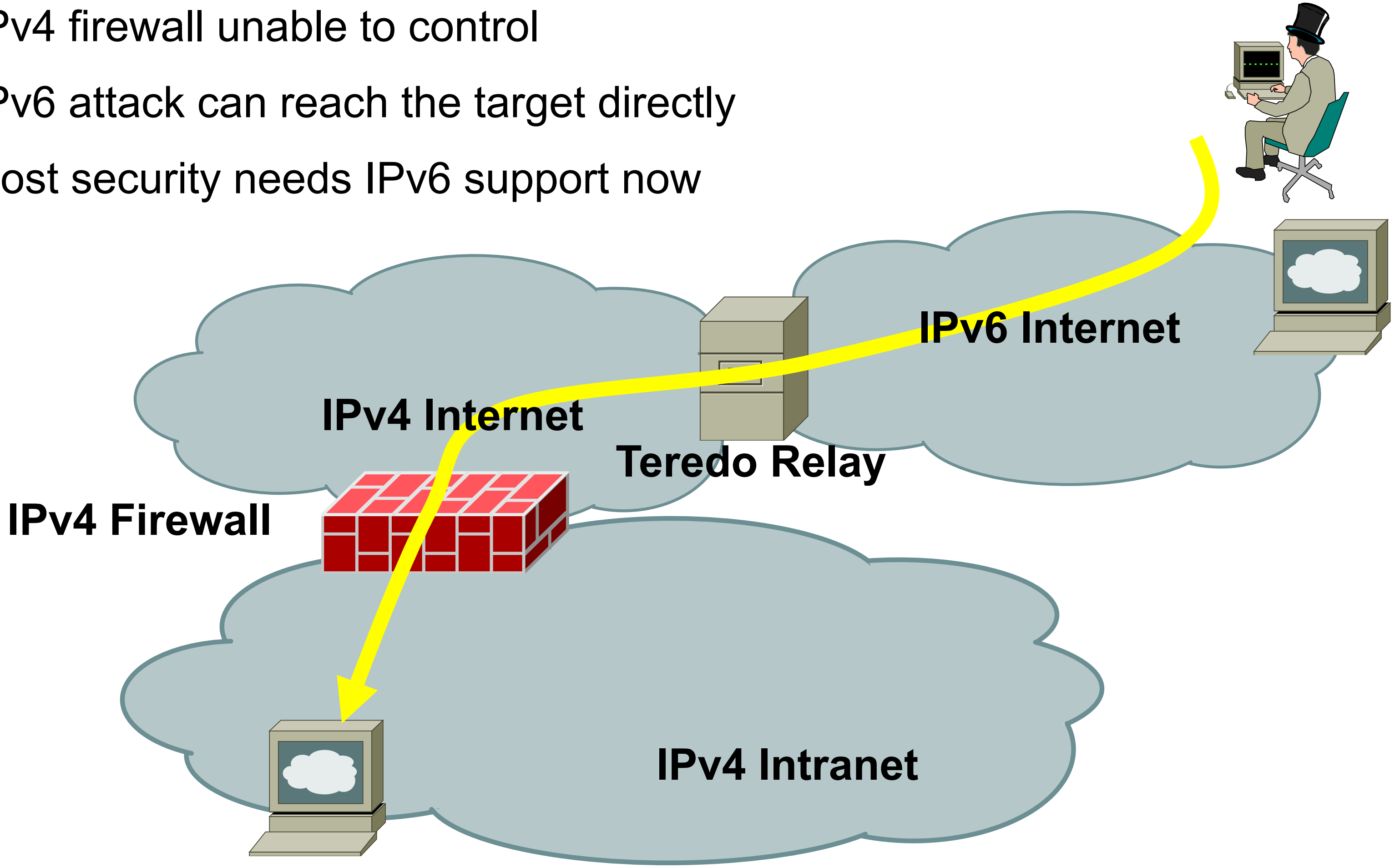


Teredo Tunnels (3/3)

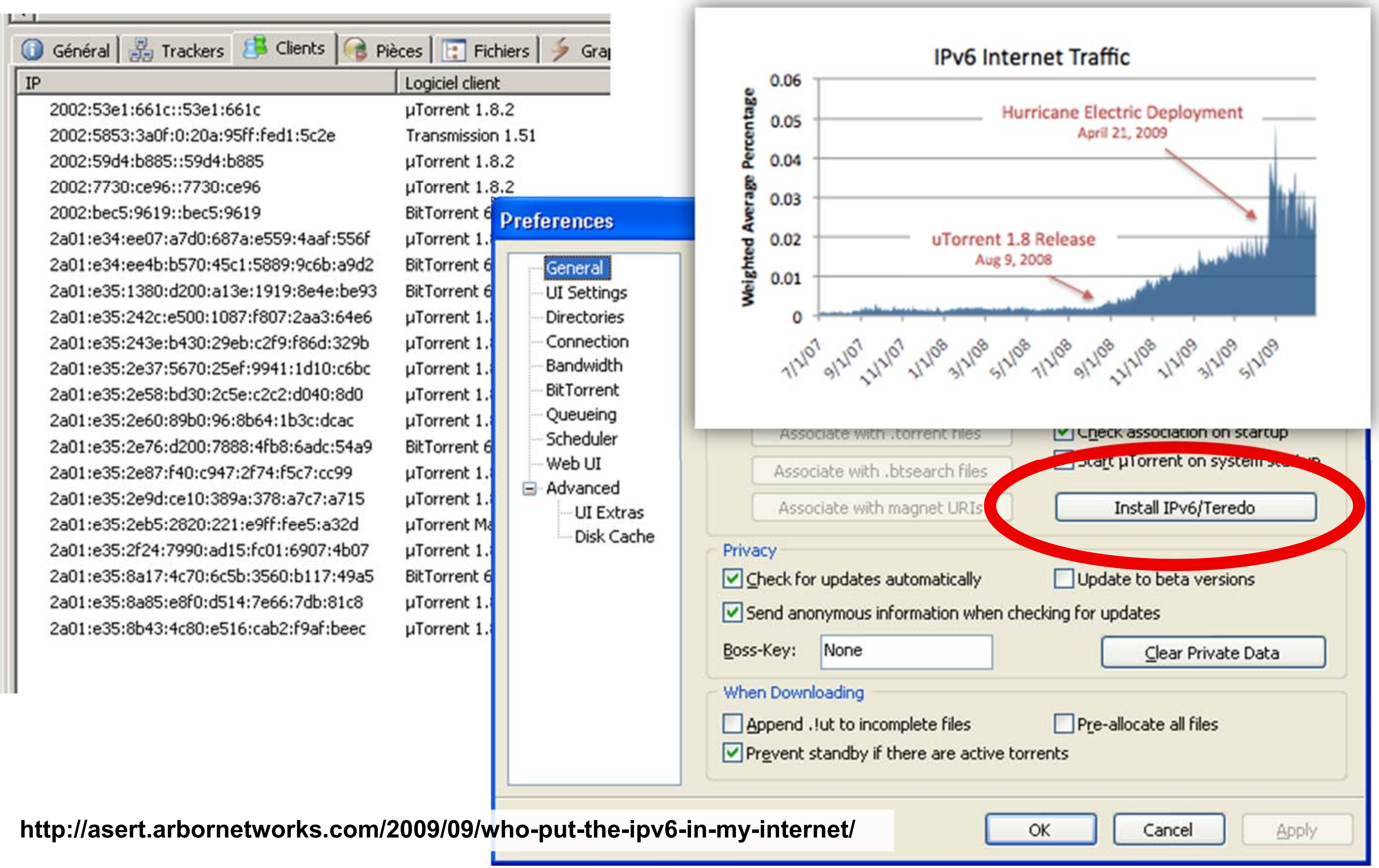
No More Outbound Control

Once Teredo Configured

- **Inbound** connections are allowed
- IPv4 firewall unable to control
- IPv6 attack can reach the target directly
- Host security needs IPv6 support now



µTorrrent 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.
2a01:e35:8b43:4c80:e516:cab2:f9af:beec	µTorrent 1.

☑ Check association on startup

□ Start µTorrent on system startup

Privacy

☑ Check for updates automatically

□ Update to beta versions

☑ Send anonymous information when checking for updates

Boss-Key: None

When Downloading

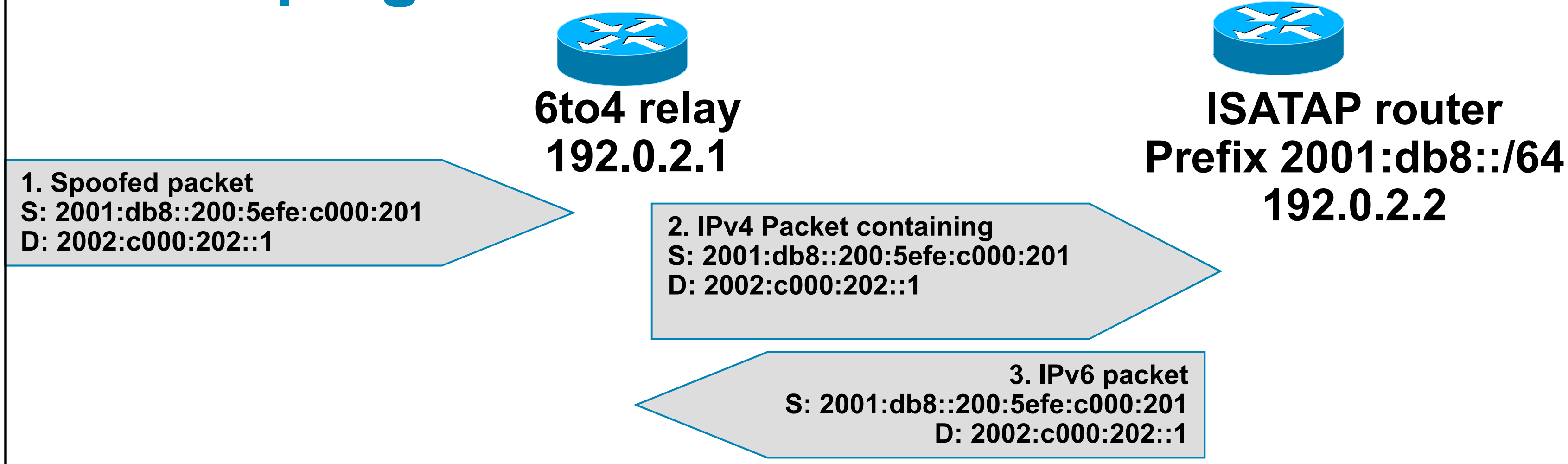
□ Append .!ut to incomplete files

□ Pre-allocate all files

☑ Prevent standby if there are active torrents

http://asert.arbornetworks.com/2009/09/who-put-the-ipv6-in-my-internet/

Looping Attack Between 6to4 and ISATAP



6to4 relay
192.0.2.1

ISATAP router
Prefix 2001:db8::/64
192.0.2.2

1. Spoofed packet
S: 2001:db8::200:5efe:c000:201
D: 2002:c000:202::1

2. IPv4 Packet containing
S: 2001:db8::200:5efe:c000:201
D: 2002:c000:202::1

3. IPv6 packet
S: 2001:db8::200:5efe:c000:201
D: 2002:c000:202::1

Repeat until Hop Limit == 0

- Root cause

  Same IPv4 encapsulation (protocol 41)

  Different ways to embed IPv4 address in the IPv6 address

- ISATAP router:

  accepts 6to4 IPv4 packets

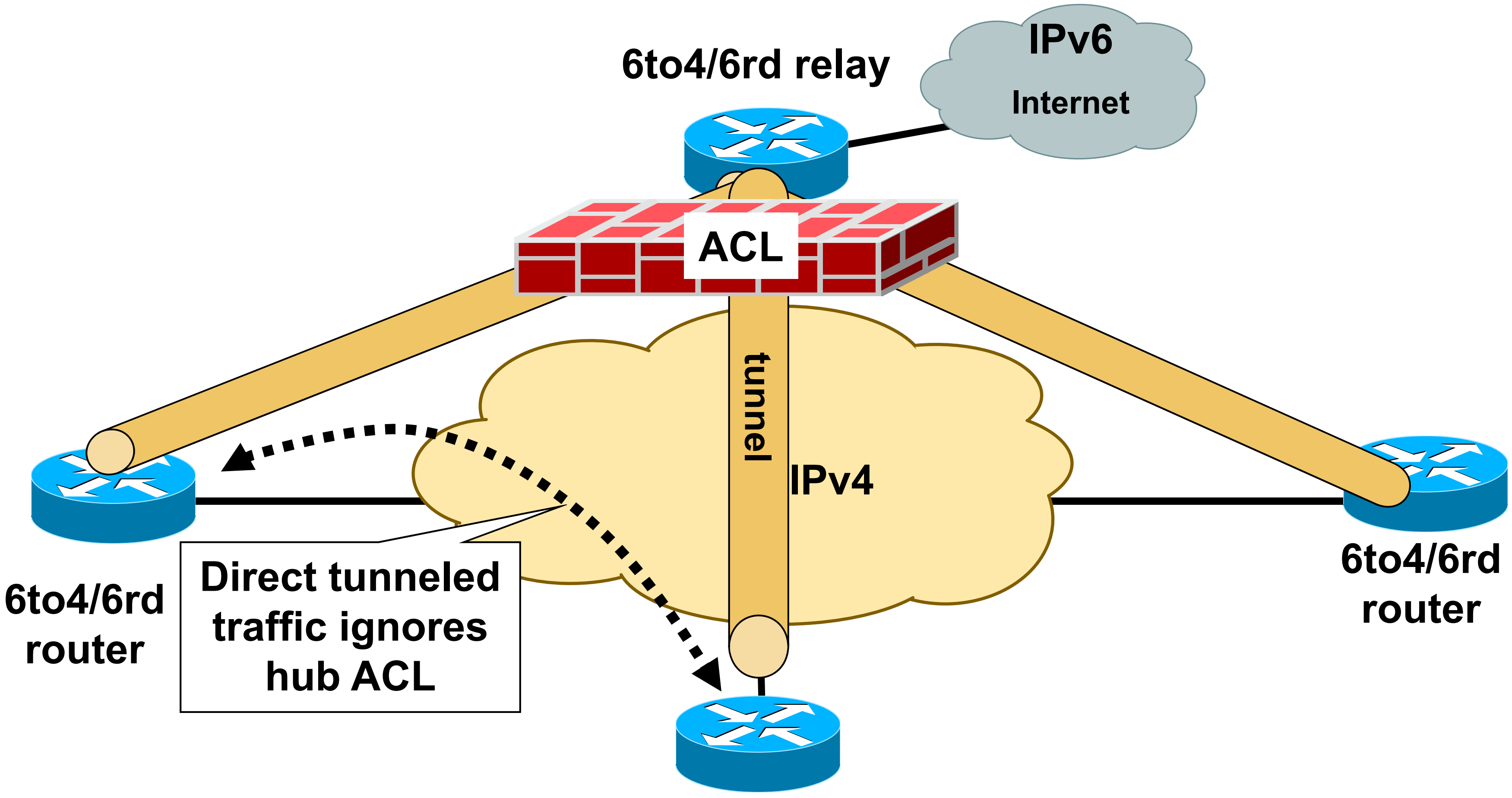
  Can forward the inside IPv6 packet back to 6to4 relay

- Symmetric looping attack exists

Mitigation:
•Easy on ISATAP routers: deny packets whose IPv6 is its 6to4
•Less easy on 6to4 relay: block all ISATAP-like local address?
•Good news: not so many open ISATAP routers on the Internet

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

6to4/6rd Tunnels Bypass Centralized ACL



Direct tunneled traffic ignores hub ACL

6rd CPE router can be configured to always go through hub
Direct CPE-CPE communication must then be forbidden by IPv4 network

Notes from a real world

Summary

IPv6 (in)security

- Any network is as secure as You can make it
- Do not blindly copy IPv4 templates to IPv6 ones – use caution and knowledge

  ...most of the work is already done, but needs rethinking when applied to a new protocol

- Do not fight with IPv6 – try to embrace it’s capabilities

  NAT no longer needed, one less step to correlate events/configure the user account

  Stateless or stateful autoconfiguration, mobility

IPv6 (in)security

- If you don’t have IPv6-enabled ISP, go to HE or SixxS and get an IPv6 tunnel to start practicing

  http://ipv6.he.net/

  http://www.sixxs.net

HE HURRICANE ELECTRIC INTERNET SERVICES

SixXS

Any questions?

Thanks!

IPv6 (in)security

Łukasz Bromirski
lbromirski@cisco.com