

Top IPv6 Security Issues Today

And what you can do to mitigate them



Jeremy Duncan
IPv6 Architect/Network Engineer

Bottom Line Up Front (BLUF)

- Security issues surrounding IPv6 is getting better
- There still remains a lot of work to do
- With the right tools and smart engineering you can mitigate them

Top IPv6 Security Issues

- Issue #1: Accidental IPv6 deployment in an unmanaged IPv4 enterprise
- Issue #2: Malicious IPv6 Deployment
- Issue #3: Security Tools are not capable to protect basic threats
- Issue #4: Mis-configured IPv6 Deployments
- Issue #5: Growing IPv6 Exploitation Tools
- Issue #6: Lack of IPv6 Trained Security Engineers

Issue 1 - Accidental IPv6 Deployment

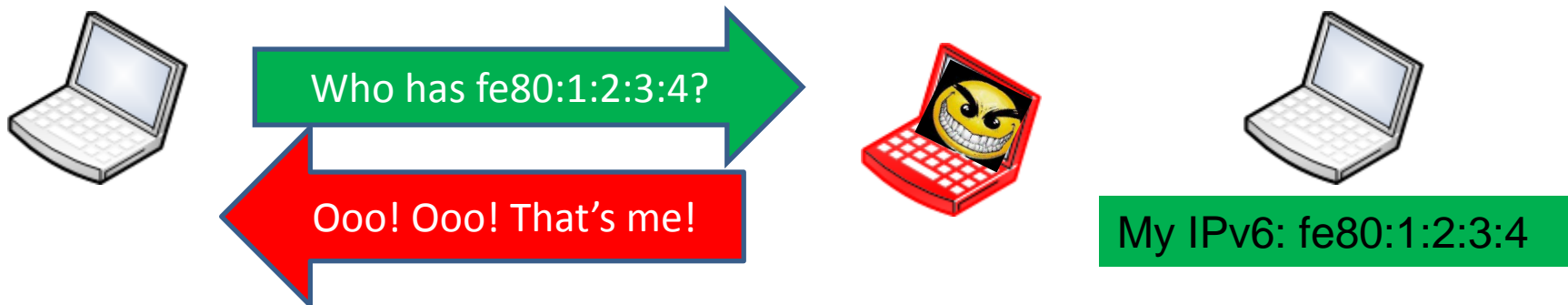
- All operating systems now include IPv6 on by default – including IPv6 tunnel mechanisms
 - Windows Server 2008 + includes native IPv6, 6to4 and ISATAP
 - Windows Vista+ includes native IPv6, 6to4 and ISATAP (and Teredo when not domain joined)
 - Except when you type: “netsh int teredo set state enterpriseclient”
 - Apple Mac includes native IPv6 (no tunneling by default)
 - Linux (RHEL, SuSE, Ubtuntu) includes native IPv6 (no tunneling by default)

Issue 1 - Accidental IPv6 Deployment

- When these tunnel adapters are enabled they try to “call home”
 - Teredo will attempt IPv6 bubble packets for Teredo relays when an address is received
 - These relays could exist anywhere in the world (use of Anycast, can go up and down)
 - 6to4 will try to access IPv6 internet if protocol 41 is allowed
 - These 6to4 tunnel brokers exist all around the world as well

Issue 1 - Accidental IPv6 Deployment

- These IPv6-enabled nodes are listening for **ANYONE** to talk to without authentication:
 - Routers, other nodes, etc



Issue 2 – Malicious IPv6 Deployment

- Tech-savvy users are learning about ways to avoid detection on un-managed IPv4 networks
 - Bypass firewalls by using IPv6 UDP-based tunnels over non-standard ports for:
 - Bit torrent
 - Data Exfiltration through public cloud services (Google Drive)
 - Accessing IPv6-IPv4 Proxy service from SixXS to reach IPv6-only content: <https://www.sixxs.net/tools/gateway/>
- Cause havoc on enterprise LANs with internal DoS with expanding tool sets
 - THC-IPv6, Scapy, etc

IPv6 Attacks on the Local Segment

- Man-in-the-Middle Attacks during neighbor advertisement/solicitation
 - Parasite6 – THC-IPv6
 - Spoofs every NS sent out by any host



The Hacker's Choice



Who has fe80:1:2:3:4?

Ooo! Ooo! That's me!



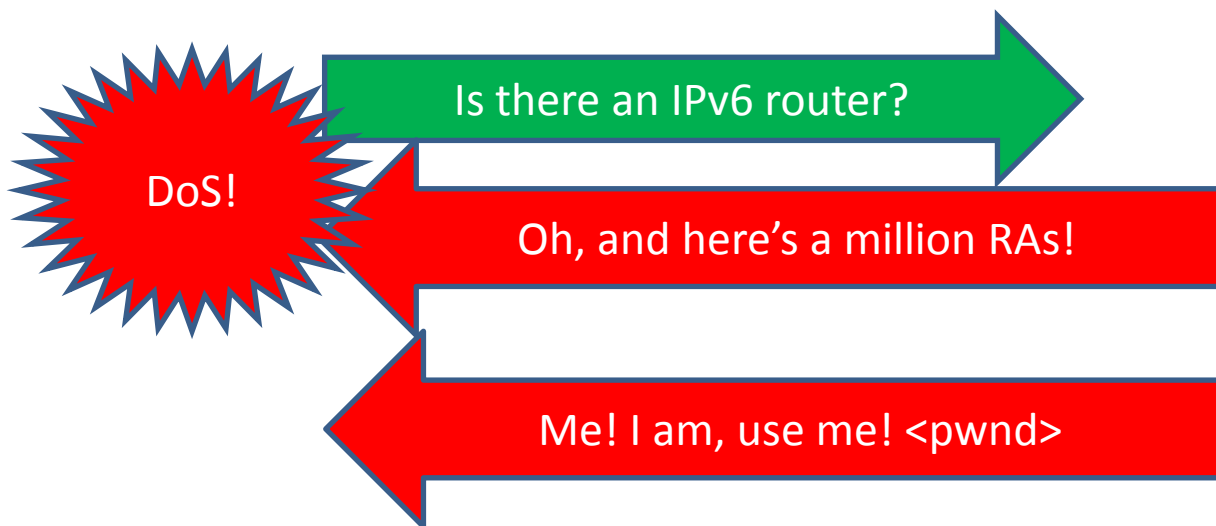
My IPv6: fe80:1:2:3:4

IPv6 Attacks on the Local Segment, cont

- Denial of Service (DoS) or Session Hijacking using a Rogue Router
 - Fake_router6 and/or flood_router6 – THC-IPv6
 - Acts like a router with highest priority
 - Floods route tables and interface address config



The Hacker's Choice



IPv6 Attacks on the Local Segment, cont

- Denial of Service (DoS) with IP conflicts
 - Dos-new-ip6– THC-IPv6
 - Always responds to a Duplicate Address Detection (DAD) with a positive
 - Hosts will never be able to address their link-local or Global address



The Hacker's Choice



Hey, anyone have this address?

Yes, I own that one, try again!


OK, what about this one?

Yep, got that one too! <pwnd>

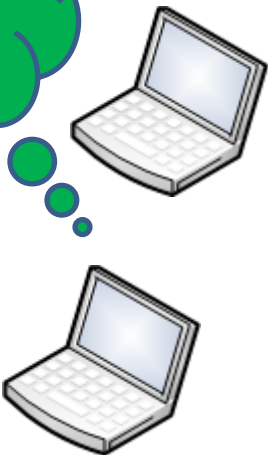


IPv6 Attacks on the Local Segment, cont

- Denial of Service (DoS) with Neighbor floods
 - Flood_advertise6 – THC-IPv6
 - Floods all hosts on a network with bogus neighbor advertisements
 - Performance on host IPv6 neighbor tables will degrade and cause a DoS



I feel bloated



The Hacker's Choice



NA for fe80::2



NA for fe80::3

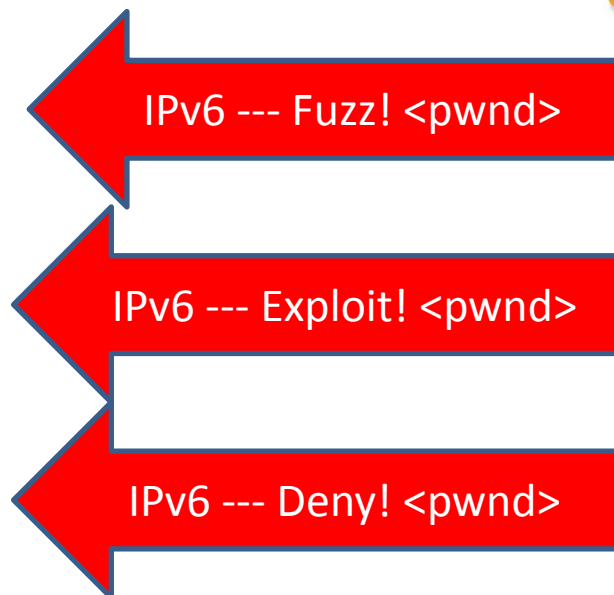


NA for fe80::4 <pwnd>



IPv6 Attacks on the Local Segment, cont

- IPv6 Exploitation and Fuzzing attacks
 - fuzz6, exploit6, denial6 – THC-IPv6
 - Runs a series of fuzzing and link-local exploitation attacks on hosts



The Hacker's Choice



Issue 3 – Security Tools Lacking

- Every commercial and enterprise-grade firewall and IPS/IDS **lack** broad threat awareness
 - Native IPv6 with obfuscating Extension Headers
 - Full IPv6 tunnel detection (most only provide basic Teredo and 6to4)
 - Application firewall rules for anything but HTTP/HTTPS and SSH (everything else is wide open)
 - Providing basic SEIM awareness in alerting (most use a modified IPv4 address (e.g. 255.255.2.1 instead of ff02::1))

Issue 3 – Security Tools Lacking

- Most provide basic TCP SYN flood and SMURF attack capability
- No local network awareness on Rogue Router Advertisements, Neighbor Discovery Floods, etc (anything done by THC-IPv6)
- Popular Host-Based IDS tools either break valid IPv6 traffic or provide useless false-positives (need heavy tuning)

Issue 4 – Mis-Configured IPv6

- Not securing IPv6 routing protocols using IPsec
 - OSPFv3 uses IPsec SPIs instead of MD5/SHA
- Switch interfaces not using RA Guard or NDP Guard ACLs/VACLs
- Not auditing IPv6 firewall rules to ensure they match 100% of the IPv4 rules (if you can)
- Not doing X-Forward-For for NAT64/CGN to DMZ servers
 - XFF provides real IPv6 address to translated IPv4 address

Issue 4 – Mis-Configured IPv6

- Perimeter router ACLs:
 - Neighbor Discovery on routed interfaces (DISA STIG issue) ← permit this
 - Path MTU Discovery blocked ← permit this
 - Allowing Protocol 41 and UDP tunnel ports:
 - 3544, 3545, 5072, 3874, 3740, 3653 ← block this
- Not having IPv6 ACLs at all!
- Windows Servers not set with 0x1 DisableComponents
 - Disallow all tunnels
 - Keeping 2002::/16 6to4 prefixes (will break Windows AD)

Issue 4 – Mis-Configured IPv6

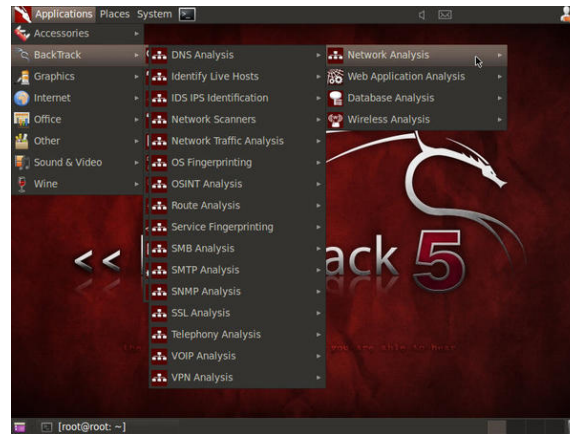
- Improperly configuring Windows Direct Access Firewalls
 - Required for DA to function but not allowing ICMPv6 type/codes
- Too reliant on Static IPv6 addressing for servers
 - Use DHCPv6 with static reservations
 - Do not use Stateless Address Autoconfiguration

Issue 5 – Expansion of Exploitation Tools

- More tools are coming out each year built to break IPv6 security:



Kali Linux



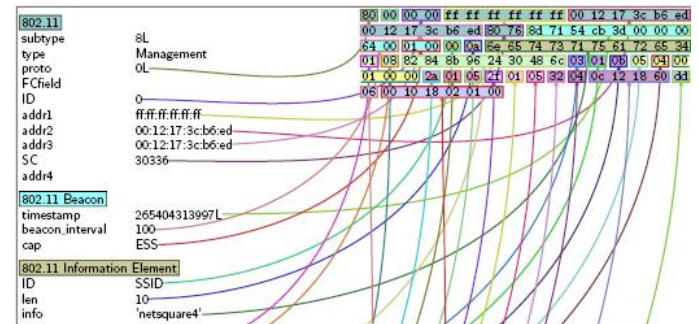
BackTrack



IPv6 Toolkit



THC-IPv6



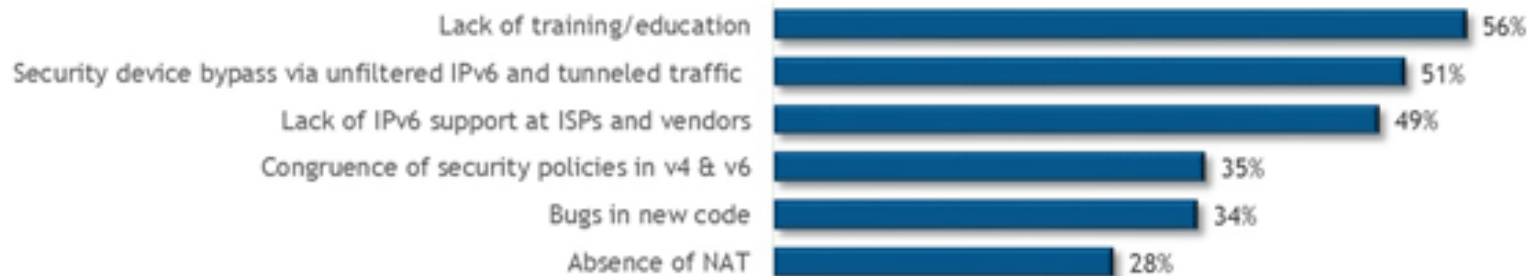
Scapy

Issue 6 – Lack of IPv6 Trained Engineers

- Serious implication: Solving IPv6 problems with IPv4 solutions
 - Too different to layer the same broken philosophy
- 28% of survey still thinks NAT is a security “feature”

What are the Top 6 IPv6 Security Risks?

(340 responses)



Source: <http://www.networkworld.com/news/tech/2013/110413-ipv6-security-275583.html>

Mitigating Accidental Deployments

- If you aren't using it, turn it off with these exceptions:
 - Windows Server and Workstation (set to enable but disable tunneling)
 - Windows Direct Access servers require Teredo and 6to4 to be enabled
- Audit your Security Tools for views into internal IPv6:
 - Ensure SPAN/Taps are configured to see all multicast traffic (this is where NDP lives)
- Lock-Down IPv6 on the end-node (use a host-based IDS/IPS, but spend time testing rules)

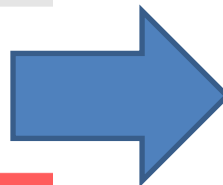
Mitigating Malicious Deployments

- Lock-Down IPv6 on the end-node (use a host-based IDS/IPS, but spend time testing rules)
- Monitor SEIM tools for odd behavior over DNS
 - Many UDP-based tunnel tools can use ports allowed on the end nodes like DNS (UDP port 53)

```

Frame 1 (146 bytes on wire, 146 bytes captured)
Ethernet II, Src: b8:16:19:7b:52:20 (b8:16:19:7b:52:20), Dst: c4:85:08:01:a8:10 (c4:85:08:01:a8:10)
Internet Protocol, Src: 174.142.134.198 (174.142.134.198), Dst: 192.168.1.67 (192.168.1.67)
User Datagram Protocol, Src Port: domain (53), Dst Port: 48928 (48928)
Domain Name System (query)
  Transaction ID: 0x6000
  Flags: 0x0000 (Standard query)
  Questions: 64
  Answer RRs: 14912
  Authority RRs: 8193
  Additional RRs: 1472
  Queries
  [Malformed Packet: DNS]
  [Expert Info (Error/Malformed): Malformed Packet (Exception occurred)]
  [Message: Malformed Packet (Exception occurred)]
  [Severity level: Error]
  [Group: Malformed]

```



```

Frame 1 (146 bytes on wire, 146 bytes captured)
Ethernet II, Src: b8:16:19:7b:52:20 (b8:16:19:7b:52:20), Dst: c4:85:08:01:a8:10 (c4:85:08:01:a8:10)
Internet Protocol, Src: 174.142.134.198 (174.142.134.198), Dst: 192.168.1.67 (192.168.1.67)
User Datagram Protocol, Src Port: domain (53), Dst Port: 48928 (48928)
  Source port: domain (53)
  Destination port: 48928 (48928)
  Length: 112
  Checksum: 0xae71 [validation disabled]
  Teredo IPv6 over UDP tunneling
  Internet Protocol Version 6
  0110 .... = Version: 6
  .... 0000 0000 .... = Traffic class: 0x00000000
  .... 0000 0000 0000 0000 = Flowlabel: 0x00000000
  Payload length: 64
  Next header: ICMPv6 (0x3a)
  Hop limit: 64
  Source: 2001:5c0:1001::1000 (2001:5c0:1001::1000)
  Destination: 2001:5c0:1001:fe00::339 (2001:5c0:1001:fe00::339)
  Internet Control Message Protocol v6
  Type: 129 (Echo reply)
  Code: 0
  Checksum: 0x9bf2 [correct]
  ID: 0x105c
  Sequence: 0x0001

```

Mitigating Security Tools

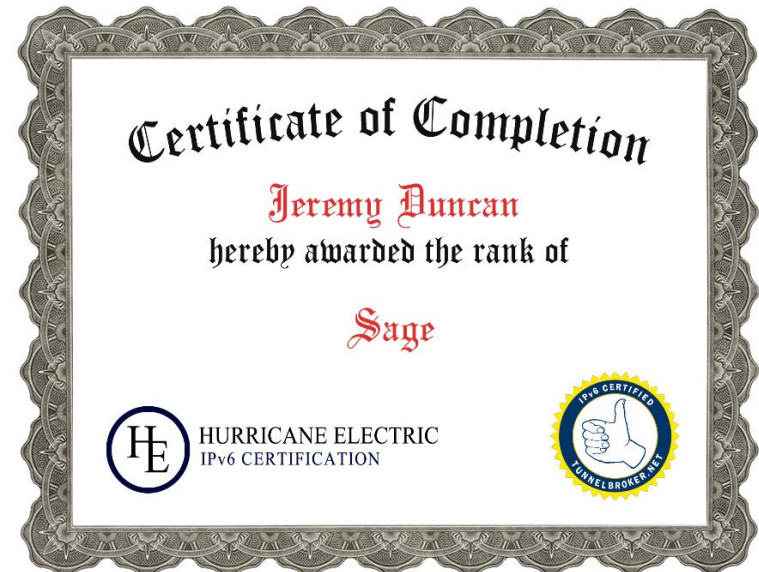
- This is a difficult thing to mitigate
- Start by auditing what you have and ask them the tough *and* specific questions about what they can or can't do
- Get with me after if you want details on your vendors

Mitigating Mid-Configured Deployments

- Follow IPv6 best practices
 - OSPFv3 authentication in Cisco: [OSPFv3 Cisco](#)
 - OSPFv3 authentication (address families) in Cisco: [OSPFv3 AF in Cisco](#)
 - IPv6 BGP Peering: <http://www.ipbcop.org/drafts/bcop-ipv6-peering-and-transit/>
 - EIGRP IPv6 Authentication: [EIGRP Authentication](#)
 - [Cisco Implementing First-Hop Security](#)
 - Microsoft IPv6 DisableComponents key settings: <http://support.microsoft.com/kb/929852>

Mitigating IPv6 Training

- Training for security personnel should never be a “nice-to-have”
 - They are the first to spot attacks (or not spot)
- There are many good IPv6 training programs out there
- Get started with these:



Summary

- There are six very important security issues
- Lack of IPv6 training is the most important
- Follow good security practice and industry recommendations
- Audit your security vendors now
- Be very intentional about your IPv6 deployment

Questions?



Backup Slides



What an IPv6 Extension Header Looks Like

```
Internet Protocol Version 6, Src: 2001:5c0:1107:4c00:21b:fcff:fe9a:c6ae (2001:5c0:1107:4c00
```

```

  ▾ 0110 .... = Version: 6
    [0110 .... = This field makes the filter "ip.version == 6" possible: 6]
  ▸ .... 0000 0000 .... .. = Traffic class: 0x00000000
    .... .. 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
  Payload length: 52
  Next header: IPv6 fragment (0x2c)
  Hop limit: 64
  Source: 2001:5c0:1107:4c00:21b:fcff:fe9a:c6ae (2001:5c0:1107:4c00:21b:fcff:
  [Source SA MAC: AsustekC_9a:c6:ae (00:1b:fc:9a:c6:ae)]
  Destination: 2001:4860:8006::85 (2001:4860:8006::85)

```

```

  ▾ Fragmentation Header
    Next header: IPv6 fragment (0x2c)
    0000 0000 0000 0... = Offset: 0 (0x0000)
    .... .. 0 = More Fragment: No
    Identification: 0x00000000

```

```

  ▾ Fragmentation Header
    Next header: IPv6 fragment (0x2c)
    0000 0000 0000 0... = Offset: 0 (0x0000)
    .... .. 0 = More Fragment: No
    Identification: 0x00000000

```

```

  ▾ Fragmentation Header
    Next header: IPv6 fragment (0x2c)
    0000 0000 0000 0... = Offset: 0 (0x0000)
    .... .. 0 = More Fragment: No
    Identification: 0x00000000

```

```

  ▾ Fragmentation Header
    Next header: TCP (0x06)
    0000 0000 0000 0... = Offset: 0 (0x0000)
    .... .. 0 = More Fragment: No

```

```
Internet Protocol Version 6, Src: 2001:5c0:1107:4c00:21b:fcff:fe9a:c6ae (2001:5c0:1107:4c00:21b:fcff:fe9a:c6ae)
```

```

  ▾ 0110 .... = Version: 6
    [0110 .... = This field makes the filter "ip.version == 6" possible: 6]
  ▸ .... 0000 0000 .... .. = Traffic class: 0x00000000
    .... .. 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
  Payload length: 28
  Next header: IPv6 destination option (0x3c)
  Hop limit: 64
  Source: 2001:5c0:1107:4c00:21b:fcff:fe9a:c6ae (2001:5c0:1107:4c00:21b:fcff:fe9a:c6ae)
  [Source SA MAC: AsustekC_9a:c6:ae (00:1b:fc:9a:c6:ae)]
  Destination: 2001:4860:8006::85 (2001:4860:8006::85)

```

```

  ▾ Destination Option
    Next header: TCP (0x06)
    Length: 0 (8 bytes)
    Option Type: 201 (0xc9) - Home Address Option
    Option Length: 3
    Home Address: 301:100:14:50:: (301:100:14:50::)

```

```
Transmission Control Protocol, Src Port: ftp-data (20), Dst Port: http (80), Seq: 0, Len: 0
```

```
Internet Protocol Version 6, Src: 2001:5c0:1107:4c00:21b:fcff:fe9a:c6ae (2001:5c0:1107:4c00:21b:fcff:fe9a:c6ae)
```

```

  ▾ 0110 .... = Version: 6
    [0110 .... = This field makes the filter "ip.version == 6" possible: 6]
  ▸ .... 0000 0000 .... .. = Traffic class: 0x00000000
    .... .. 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
  Payload length: 20
  Next header: ESP (0x32)
  Hop limit: 64
  Source: 2001:5c0:1107:4c00:21b:fcff:fe9a:c6ae (2001:5c0:1107:4c00:21b:fcff:fe9a:c6ae)
  [Source SA MAC: AsustekC_9a:c6:ae (00:1b:fc:9a:c6:ae)]
  Destination: 2001:4860:8006::85 (2001:4860:8006::85)

```

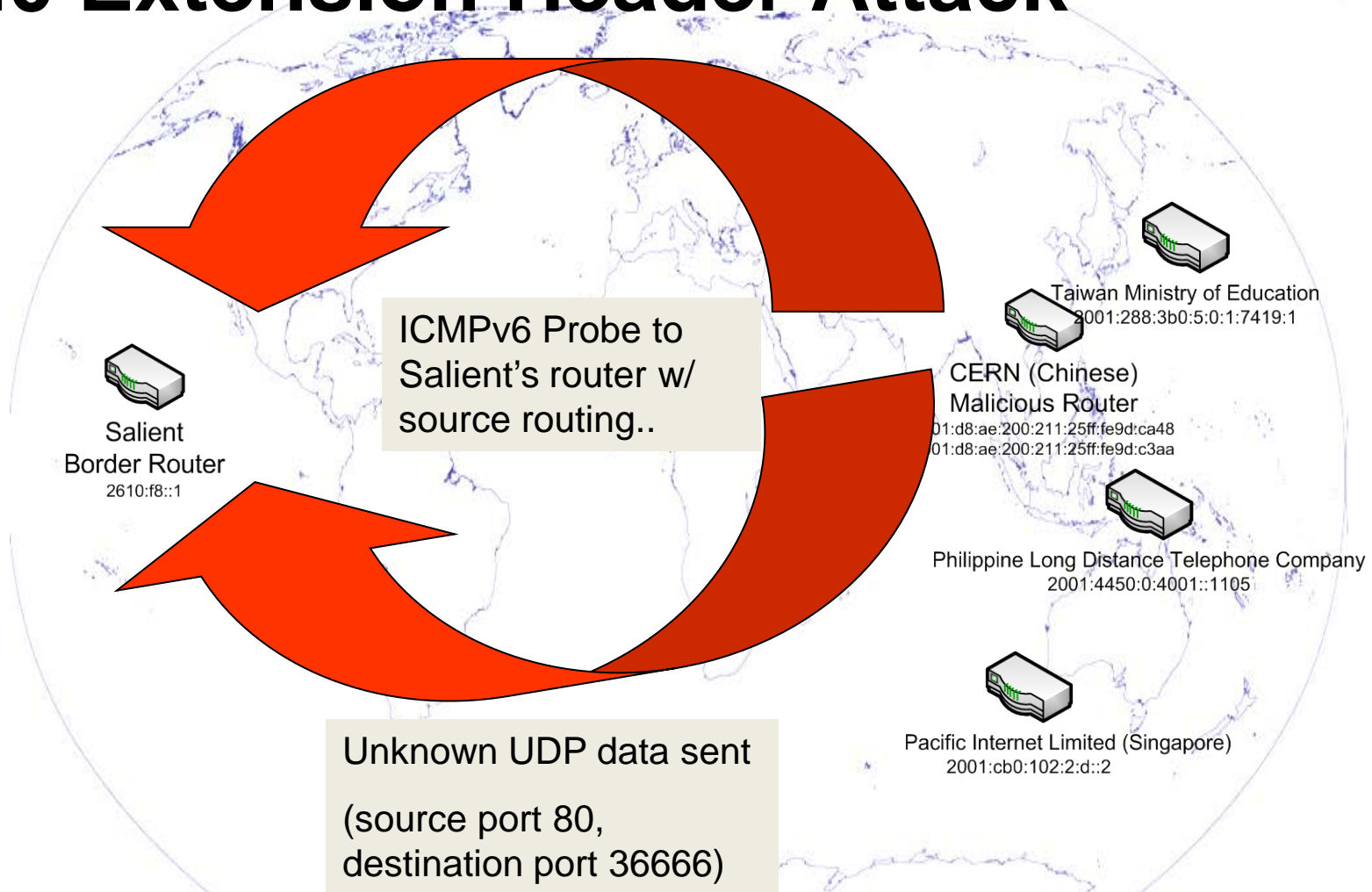
```
Encapsulating Security Payload
```

```

  ESP SPI: 0x00140050
  ESP Sequence: 0

```

RH0 Extension Header Attack



Because Salient Router was not online

ICMPv6 Probe to
Salient's router w/
source routing..



Border Router
2610:f8::1



CERN (Chinese)
Malicious Router
2001:d8:ae:200:211:25ff:fe9d:ca48
2001:d8:ae:200:211:25ff:fe9d:c3aa

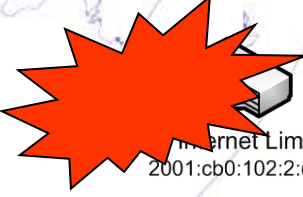


Taiwan
2001:28:0c:5:0-1:7419:1

Malicious traffic from
authorized network
(using Salient as
friendly network to
attack from)



Philippine Long Distance Telephone Company
2001:4450:0:4001::1105



Internet Limited (Singapore)
2001:cb0:102:2:d::2

If Salient router had been online...

Tunnels Need to be Protected

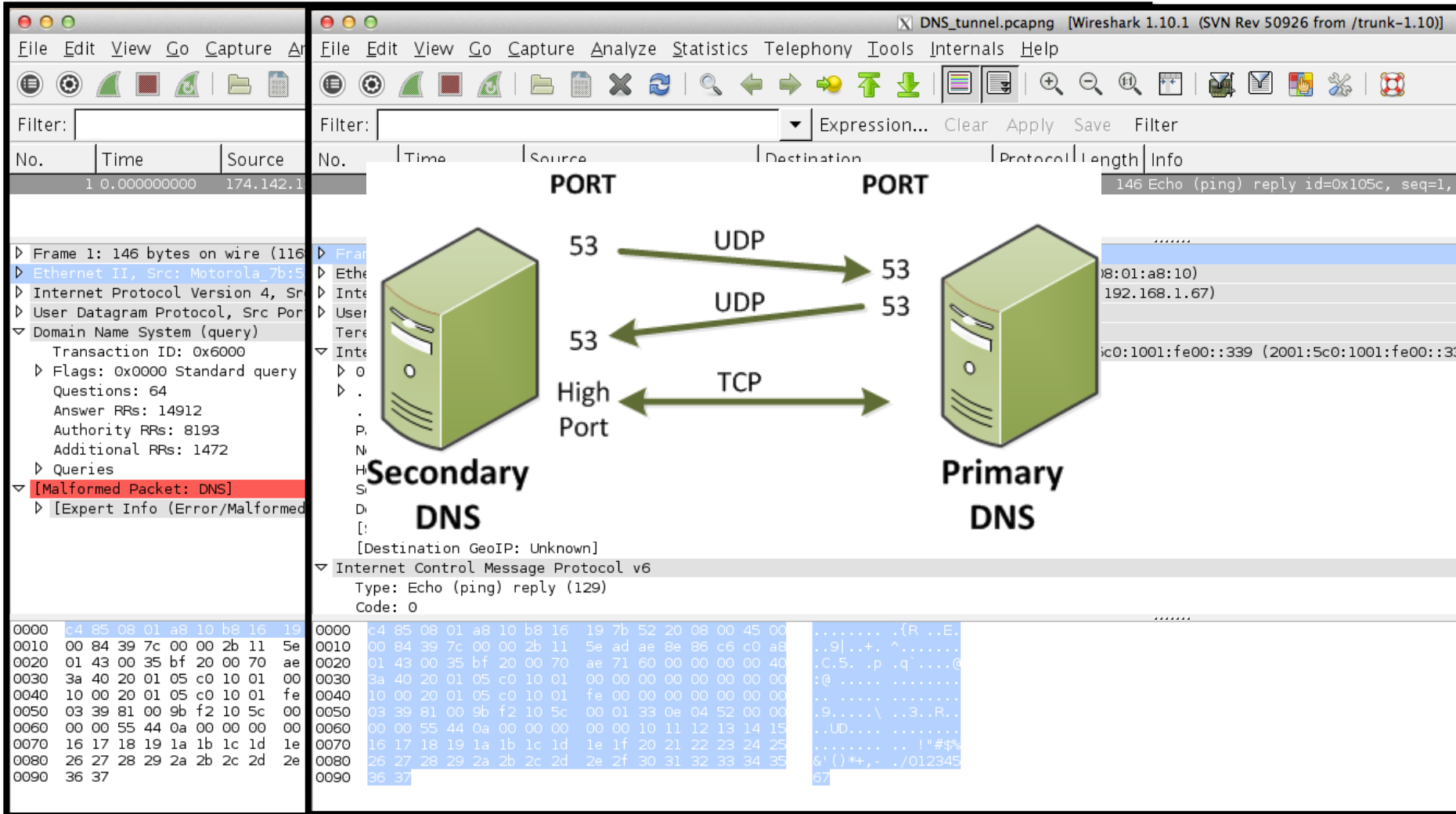
ACLs can protect against Protocol 41, 47, IPSec
and port specific UDP traffic

What if you don't know the Port?

Miredo: Teredo configured to run on any port

GoGoNet6: TSP can listen on any UDP port (ie 53,
80, 443, etc)

Typically Undetectable UDP Tunnel



The image displays two Wireshark capture windows and a network diagram. The left window shows a DNS query packet (Frame 1) from 174.142.1.1. The right window shows a corresponding DNS response packet (Frame 146) from 192.168.1.67. The network diagram illustrates the flow of traffic between a Secondary DNS server and a Primary DNS server. It shows three types of connections: two UDP connections on port 53 (one outgoing and one incoming) and one TCP connection on a high port (outgoing).

Secondary DNS **Primary DNS**

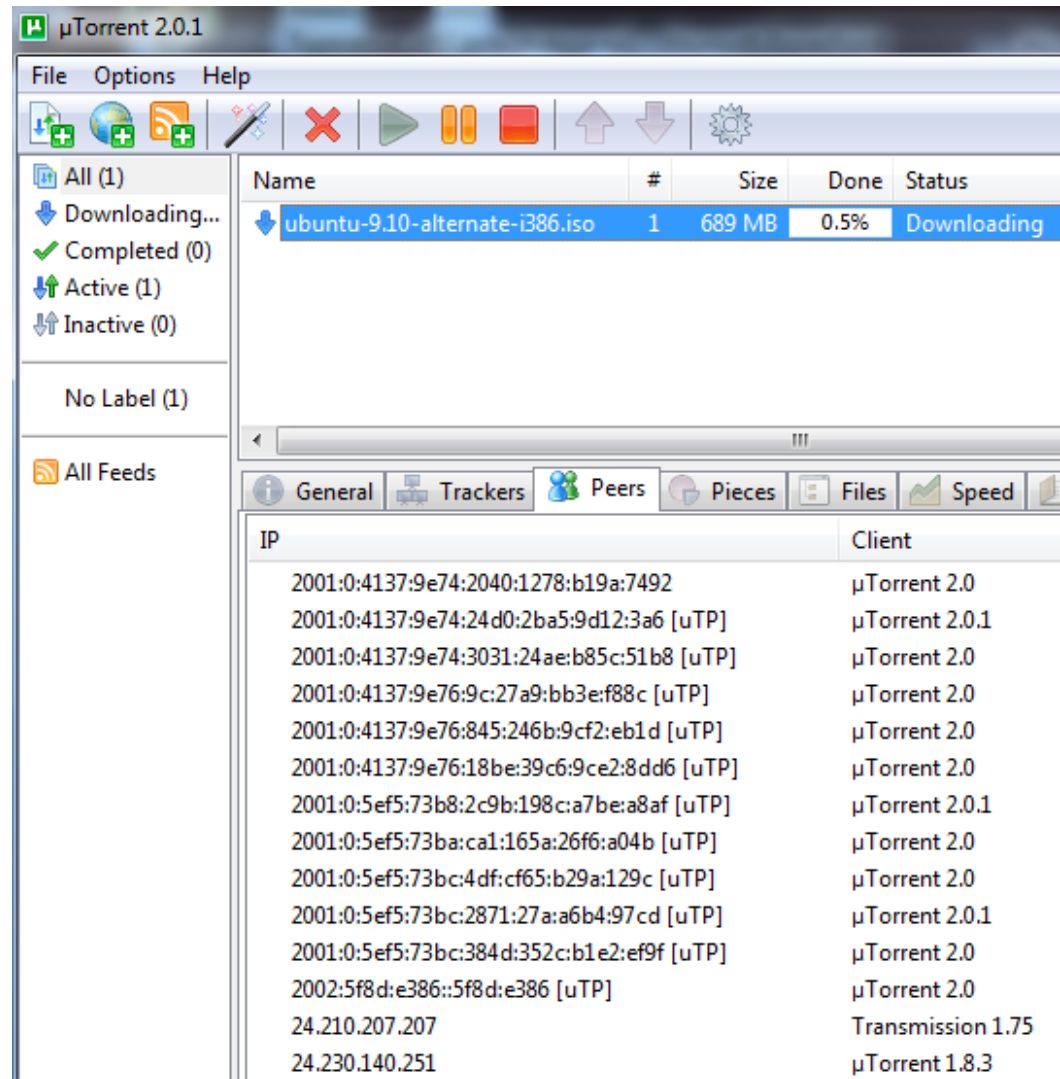
53 → UDP → 53
 53 ← UDP ← 53
 High Port → TCP →

Packet 146 details: Echo (ping) reply id=0x105c, seq=1, 8:01:a8:10, 192.168.1.67, ic0:1001:fe00::339 (2001:5c0:1001:fe00::339)

uTorrent – Teredo Peers



- uTorrent runs well over Teredo
- BitTorrent community is discovering IPv6

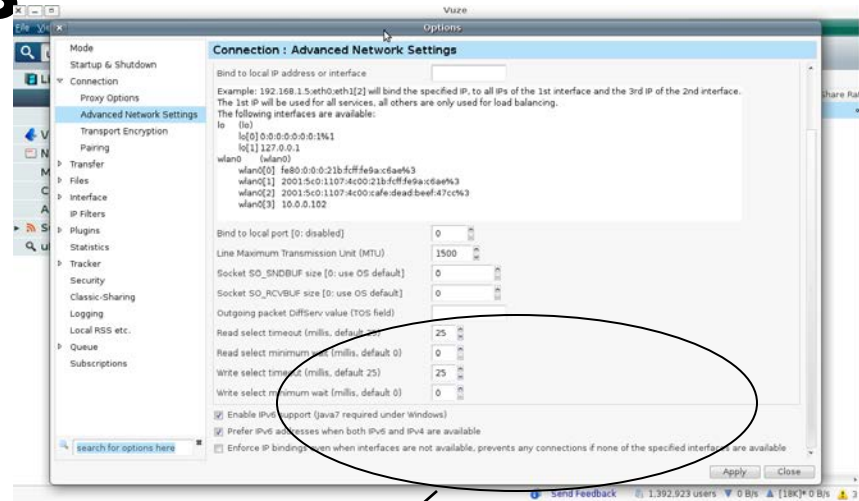


The screenshot shows the uTorrent 2.0.1 interface. The main window displays a download of 'ubuntu-9.10-alternate-i386.iso' (689 MB, 0.5% done). Below the download list, the 'Peers' tab is selected, showing a list of peers connected via Teredo IPv6 addresses.

Name	#	Size	Done	Status
ubuntu-9.10-alternate-i386.iso	1	689 MB	0.5%	Downloading

IP	Client
2001:0:4137:9e74:2040:1278:b19a:7492	µTorrent 2.0
2001:0:4137:9e74:24d0:2ba5:9d12:3a6 [uTP]	µTorrent 2.0.1
2001:0:4137:9e74:3031:24ae:b85c:51b8 [uTP]	µTorrent 2.0
2001:0:4137:9e76:9c:27a9:bb3e:f88c [uTP]	µTorrent 2.0
2001:0:4137:9e76:845:246b:9cf2:eb1d [uTP]	µTorrent 2.0
2001:0:4137:9e76:18be:39c6:9ce2:8dd6 [uTP]	µTorrent 2.0
2001:0:5ef5:73b8:2c9b:198c:a7be:a8af [uTP]	µTorrent 2.0.1
2001:0:5ef5:73ba:ca1:165a:26f6:a04b [uTP]	µTorrent 2.0
2001:0:5ef5:73bc:4df:cf65:b29a:129c [uTP]	µTorrent 2.0
2001:0:5ef5:73bc:2871:27a:a6b4:97cd [uTP]	µTorrent 2.0.1
2001:0:5ef5:73bc:384d:352c:b1e2:ef9f [uTP]	µTorrent 2.0
2002:5f8d:e386::5f8d:e386 [uTP]	µTorrent 2.0
24.210.207.207	Transmission 1.75
24.230.140.251	µTorrent 1.8.3

Vuze – IPv6 Peers



- Enable IPv6 support (Java7 required under Windows)
- Prefer IPv6 addresses when both IPv6 and IPv4 are available
- Enforce IP bindings even when interfaces are not available, p

- Vuze (formerly Azureus) is another fully IPv6-enabled bit torrent client
- See how easy it is to “prefer” IPv6!

ubuntu-10.04-desktop...	89.133.83.39	µTorrent 1.8.3	L		100.0%	146 B/s
ubuntu-10.04-desktop...	62.83.35.208	Azureus 4.4.0.4	R		99.2%	0 B/s
ubuntu-10.04-desktop...	2607:f2c0:f00e:5b00:217:f2ff:fee7:6a4c	µTorrent Mac 1.0	R		100.0%	6.8 kB/s

IPv4 “AAAA” DNS Queries Broadcast IPv6

- Microsoft Dual Stack enabled on ALL Windows 7/8/Server 2008 systems
- AAAA Queries present on **every** network we monitored.
- Considered ‘harmless’ by many mainstream security and network engineers
- Must be disabled by DoD MO2 guidelines (section 3.3.6.1)
 - *“AAAA records may not transit beyond the intra-enclave security zone”*

IPv4 “AAAA” DNS– The Loaded Gun

- Remote Hacker sees an organization sending 100,000+ AAAA queries a day
- Hacker Floods an organization’s mail servers with SPAM
 - It only takes one user with elevated privileges to open one SPAM message to execute the encapsulated malware
 - Consider [MS 10-009](#), [“New Ping of Death,”](#) and [MS10-029](#) as examples
- Malware establishes an IPv6 in UDP tunnel through an organization’s firewall to Remote Hacker on UDP port 53
 - Such as Miredo or GoGoNet6
- Remote Hacker exfiltrates sensitive data from an organization’s enterprise network
 - Health record data/confidential patient records

ICMPv6 is Required for IPv6

Type	Description	Traceroute
1	Destination Unreachable	
2	Packet to Big	
3	Time exceeded	PING
4	Parameter problem	
128	Echo Request	MLD
129	Echo Reply	Prefix Advertisement
130	Multicast Listener Query – sent to ff02::1 (all nodes)	
131	Multicast Listener Report	
132	Multicast Listener Done – sent to ff02::2 (all routers)	
133	Router Solicitation (RS) – sent to ff01::2 (all routers)	
134	Router Advertisement (RA) – sent to ff01::1 (all nodes)	
135	Neighbor Solicitation (NS) – sent to ff02:0:0:0:0:1:ff00::/104	
136	Neighbor Advertisement (NA)	ARP Replacement
137	Redirect message	Router Redirection

Rogue RAs: the threat inside

- IPv6-enabled workstations (untouched Vista, 7/8, Server 2008/2012, Linux, Mac, etc) always listen for Router Advertisements
- User A downloads some pesky malware
 - Sets up tunnel like the non-standard UDP port example (or port 53)
 - Installs basic router advertisement daemon & IPv6 forwarding
- It sends RAs out to those IPv6-enabled machines with User A as it's default gateway for IPv6
- Now there is active IPv6 malware on an enterprise that can't be detected