Tunnels leading to somewhere

VPN, IPv6, etc

Native when you can, Tunnel when you must

Tunnels

Tunnels

BC Rockies Snow Tunnel

Chicago Airport

Goldstream Tunnel to the water fall

NRC Wind Tunnel

Network Tunnels

- Tunnels are just encapsulation of one protocol in another
  - Virtual Private Networks
  - IPv6 inside IPv4 (protocol 41)
  - Carrier Ethernet (MAC in MAC)
  - PPPoE
  - Not TLS/SSL

VLANs are just Tunneling

- Ethernet/VLAN ID/IP
  - https://packetlife.net/media/captures/802_1ad.pcapng.cap

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.85.1.22	192.85.1.14	IPv4	1500	Unknown (253)
2	0.000019	192.85.1.23	192.85.1.15	IPv4	1500	Unknown (253)

```
▸ Frame 1: 1500 bytes on wire (12000 bits), 1500 bytes captured (12000 bits) on interface \\.\pipe\vie
▸ Ethernet II, Src: Performa_00:00:14 (00:10:94:00:00:14), Dst: Performa_00:00:0c (00:10:94:00:00:0c)
▸ IEEE 802.1ad, ID: 30
▸ 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 100
▸ Internet Protocol Version 4, Src: 192.85.1.22, Dst: 192.85.1.14
▸ Data (1454 bytes)
```

IPSec Tunnel

- Ethernet/IP/ESP
  - https://packetlife.net/media/captures/IPv6-ESP.pcapng.cap

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	2001:470:e5bf:1001:8519:2…	2001:470:e5bf:dea…	ESP	62	ESP (SPI=0x49507636)

```
▸ Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface \Device\NPF_{E29A5FA1-5F27-435E-AF55
▸ Ethernet II, Src: Cisco_c9:0b:81 (54:75:d0:c9:0b:81), Dst: LiteonTe_f9:49:f6 (68:a3:c4:f9:49:f6)
▸ Internet Protocol Version 6, Src: 2001:470:e5bf:1001:8519:2d1f:c57d:fc4f, Dst: 2001:470:e5bf:dead:7db0:921:a2e9:1c21
▾ Encapsulating Security Payload
    ESP SPI: 0x49507636 (1230009910)
    ESP Sequence: 541414224
```

VPN with AH & ESP

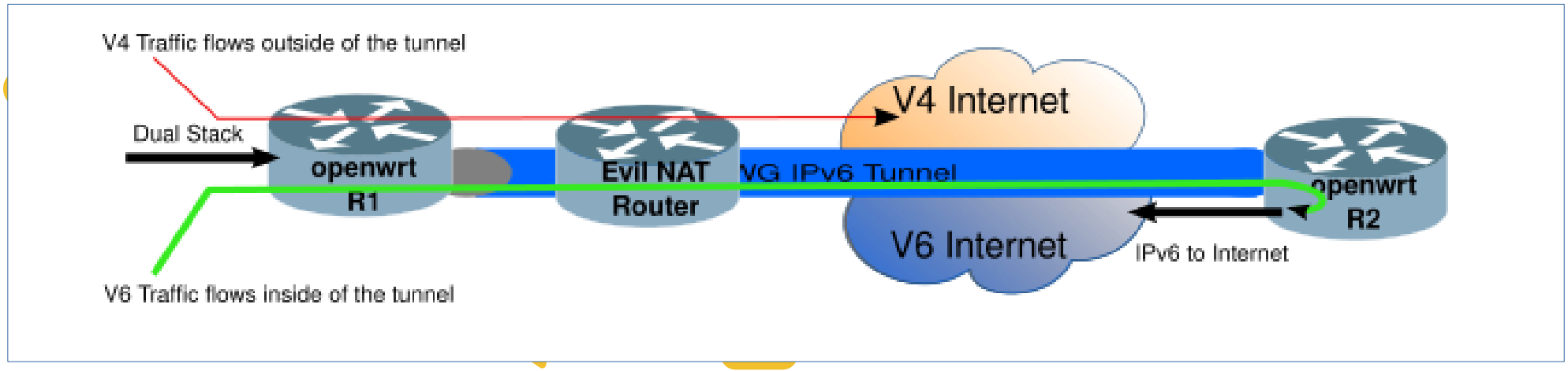
- Authenticated Header (AH) Data Integrity
  - https://packetlife.net/media/captures/IPsec_ESP-AH_tunnel_mode.cap

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.0.1	10.0.0.2	ESP	194	ESP (SPI=0x48dac2e4)
2	0.008010	10.0.0.2	10.0.0.1	ESP	194	ESP (SPI=0xfb5128a6)
3	0.023991	10.0.0.1	10.0.0.2	ESP	194	ESP (SPI=0x48dac2e4)
4	0.031999	10.0.0.2	10.0.0.1	ESP	194	ESP (SPI=0xfb5128a6)

```
▸ Frame 1: 194 bytes on wire (1552 bits), 194 bytes captured (1552 bits)
▸ Ethernet II, Src: c2:00:57:75:00:00 (c2:00:57:75:00:00), Dst: c2:01:57:75:00:00 (c2:01:57:75:00:00)
▸ Internet Protocol Version 4, Src: 10.0.0.1, Dst: 10.0.0.2
▾ Authentication Header
    Next header: Encap Security Payload (50)
    Length: 4 (24 bytes)
    Reserved: 0000
    AH SPI: 0x8179b705
    AH Sequence: 1
    AH ICV: 27cfc0a5e43d69b3728ec5b0
▸ Encapsulating Security Payload
```

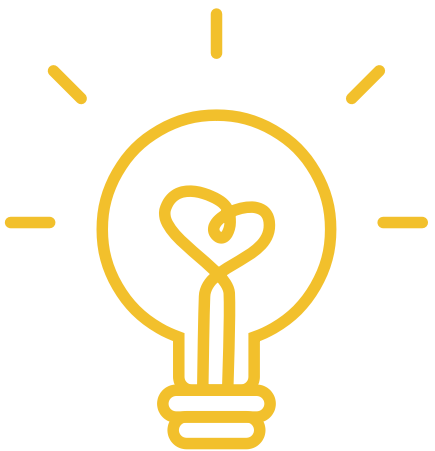
VPN Leakage

- Leakage is when traffic does not flow through the VPN tunnel
  - Most often happens when VPN provider doesn't support IPv6. Solution: Get a better provider



Tunnels within tunnels

- If Encapsulating is good, then adding more encapsulations must be better right?
  - MTU (Max Transfer Unit) limitations
  - Overhead



Encapsulation on Encapsulation

- IPv6/IPv4/GRE/PPP/IPv4/UDP
  - https://packetlife.net/media/captures/gre_and_4over6.cap

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.44.3	8.8.8.8	DNS	197	Standard query 0xa62c AAAA
2	0.213894	8.8.8.8	172.16.44.3	DNS	268	Standard query response 0xa

```
▸ Frame 1: 197 bytes on wire (1576 bits), 197 bytes captured (1576 bits)
▸ Ethernet II, Src: JuniperN_f2:61:3d (00:12:1e:f2:61:3d), Dst: c5:00:00:00:82:c4 (c5:00:00:00:82:c4)
▸ 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 100
▸ Internet Protocol Version 6, Src: 2402:f000:1:8e01::5555, Dst: 2607:fcd0:100:2300::b108:2a6b
▸ Internet Protocol Version 4, Src: 16.0.0.200, Dst: 192.52.166.154
▸ Generic Routing Encapsulation (PPP)
▸ Point-to-Point Protocol
▸ Internet Protocol Version 4, Src: 172.16.44.3, Dst: 8.8.8.8
▸ User Datagram Protocol, Src Port: 40768, Dst Port: 53
▸ Domain Name System (query)
```

Common non-VPN Tunnels

- Tunnels are more than just VPNs or VLANs
  - Accessing the Internet, PPPoE
  - Accessing the whole Internet Protocol 41

PPPoE Tunnel

- PPPoE is often used by DSL ISPs
  - https://packetlife.net/media/captures/PPPoE_Dual-Stack_IPv4_IPv6-with_DHCPv6.cap

No.	Time	Source	Destination	Protocol	Length	Info
34	6.183000	fe80::ce05:eff:fe88:0	ff02::2	ICMPv6	70	Router Solicitation
35	6.247000	fe80::c801:eff:fe88:8	fe80::ce05:eff:fe…	ICMPv6	86	Router Advertisement
36	11.182000	fe80::ce05:eff:fe88:0	ff02::1:2	DHCPv6	120	Solicit XID: 0xfc24ab CID: 00
37	11.234000	fe80::c801:eff:fe88:8	fe80::ce05:eff:fe…	DHCPv6	166	Advertise XID: 0xfc24ab CID:
38	11.260000	fe80::ce05:eff:fe88:0	ff02::1:2	DHCPv6	134	Request XID: 0xfcf776 CID: 00
39	11.330000	fe80::c801:eff:fe88:8	fe80::ce05:eff:fe…	DHCPv6	166	Reply XID: 0xfcf776 CID: 0003
40	12.736000	ca:01:0e:88:00:06	cc:05:0e:88:00:00	PPP LCP	60	Echo Request
41	12.750000	cc:05:0e:88:00:00	ca:01:0e:88:00:06	PPP LCP	60	Echo Reply

```
▸ Frame 36: 120 bytes on wire (960 bits), 120 bytes captured (960 bits)
▸ Ethernet II, Src: cc:05:0e:88:00:00 (cc:05:0e:88:00:00), Dst: ca:01:0e:88:00:06 (ca:01:0e:88:00:06)
▸ PPP-over-Ethernet Session
▸ Point-to-Point Protocol
▸ Internet Protocol Version 6, Src: fe80::ce05:eff:fe88:0, Dst: ff02::1:2
▸ User Datagram Protocol, Src Port: 546, Dst Port: 547
▸ DHCPv6
```

Protocol 41 IPv6 in IPv4

- Used by Hurricane Electric
  - https://packetlife.net/media/captures/IPv6_in_IP.cap

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	2001:db8:0:1::1	2001:db8:0:1::2	ICMPv6	134	Echo (ping) request id=
2	0.008035	2001:db8:0:1::2	2001:db8:0:1::1	ICMPv6	134	Echo (ping) reply id=0x
3	0.016001	2001:db8:0:1::1	2001:db8:0:1::2	ICMPv6	134	Echo (ping) request id=
4	0.024016	2001:db8:0:1::2	2001:db8:0:1::1	ICMPv6	134	Echo (ping) reply id=0x

```
▸ Frame 1: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits)
▸ Ethernet II, Src: c2:00:42:02:00:00 (c2:00:42:02:00:00), Dst: c2:01:42:02:00:00 (c2:01:42:02:00:00)
▸ Internet Protocol Version 4, Src: 10.0.0.1, Dst: 10.0.0.2
▸ Internet Protocol Version 6, Src: 2001:db8:0:1::1, Dst: 2001:db8:0:1::2
▸ Internet Control Message Protocol v6
```

THANK YOU

Tunnels
Credit by : cvmiller@gmail.com, 2021.