IPv6 Cyber Security Briefing

May 27, 2010

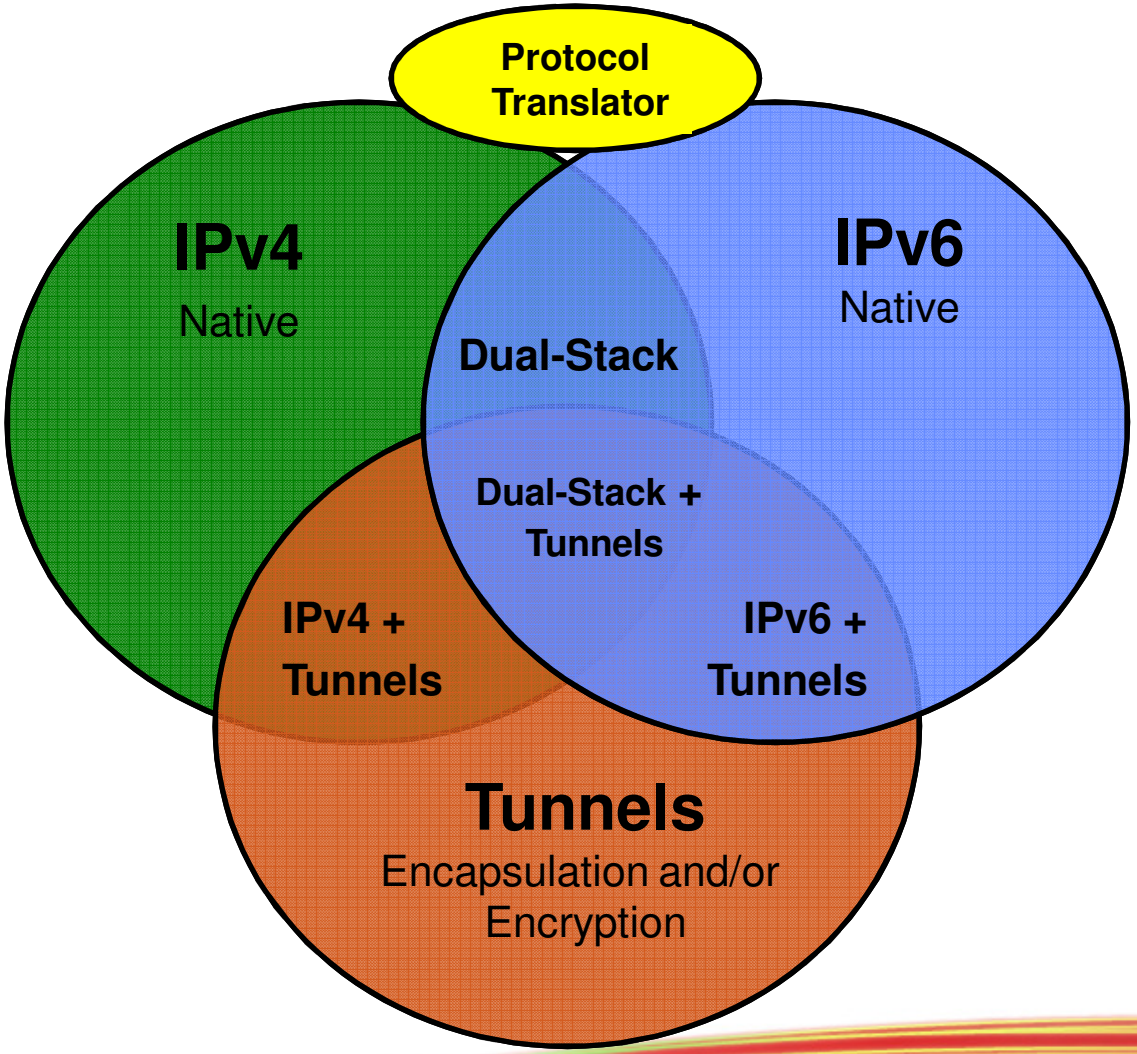
Ron Hulen

VP and CTO Cyber Security Solutions

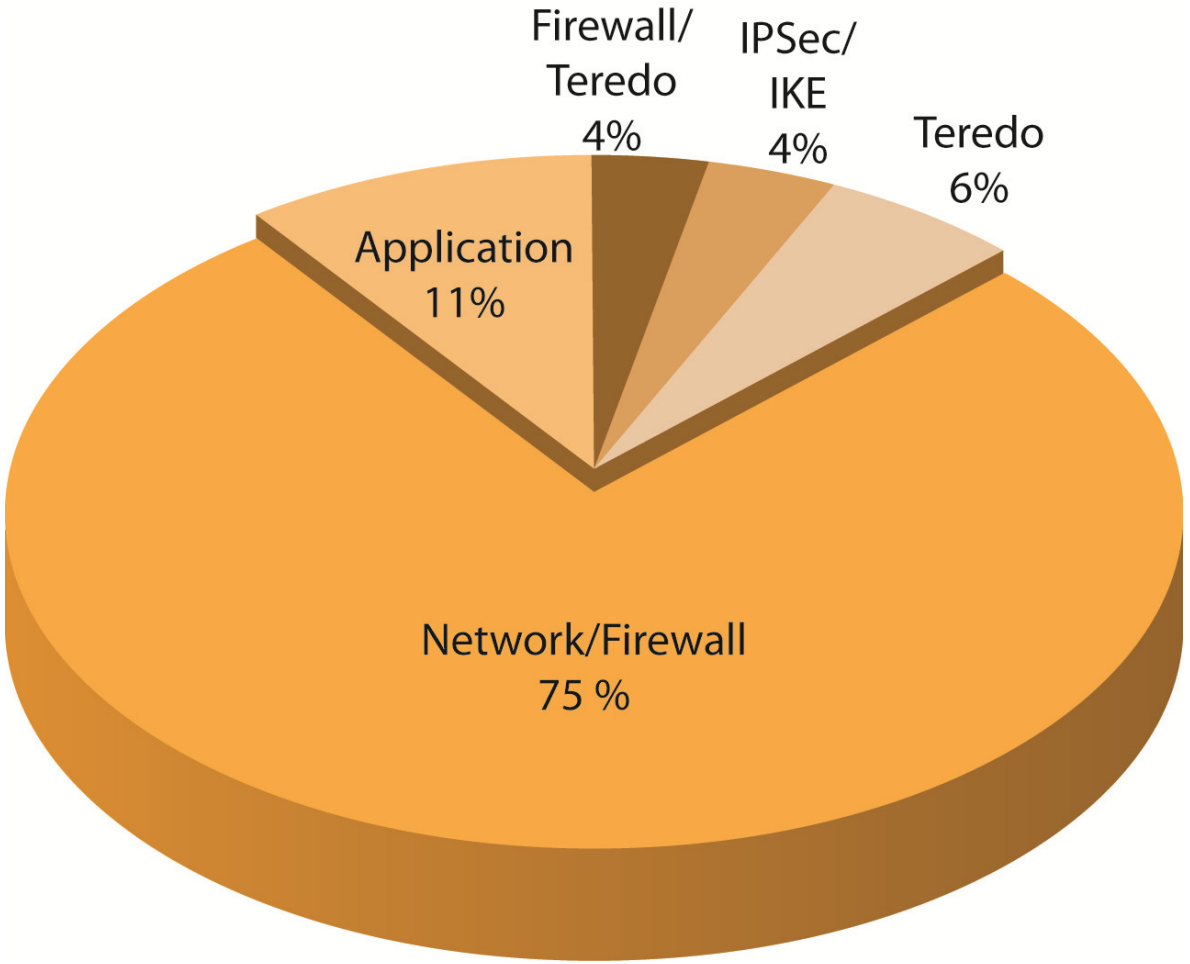
Command Information, Inc.

COMMAND INFORMATION

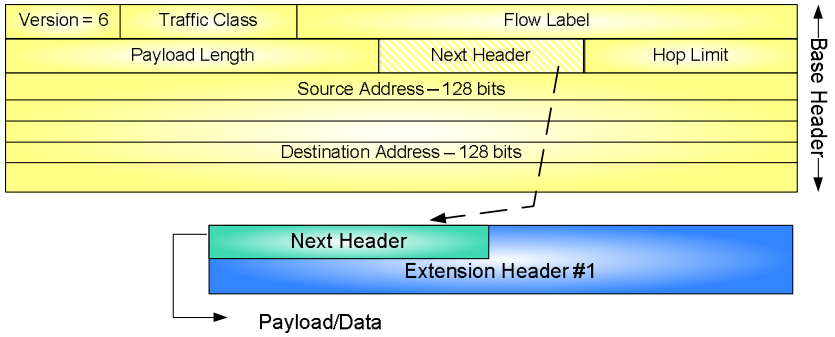
Attack Surfaces



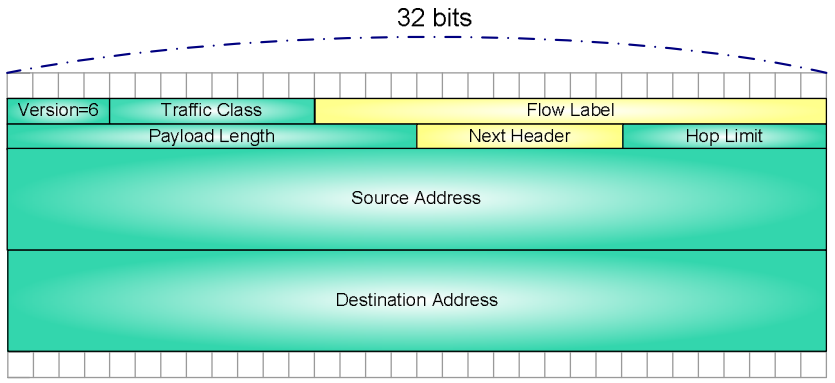
Known IPv6 Vulnerabilities



The IPv6 Header is completely different

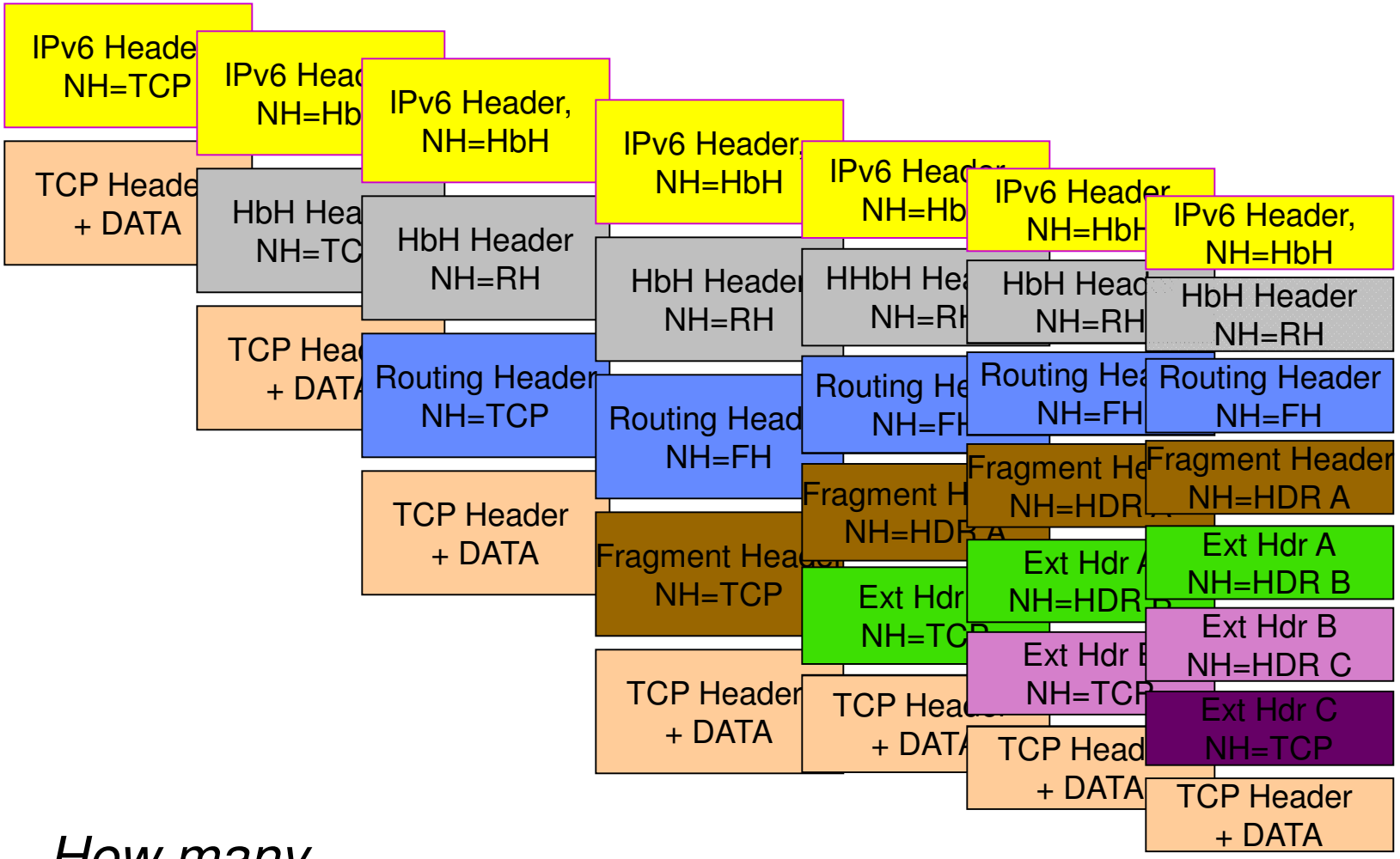


- The Next Header field indicates what type of header follows the IPv6 base header
- All extension header information is within the payload, and not the IPv6 base header



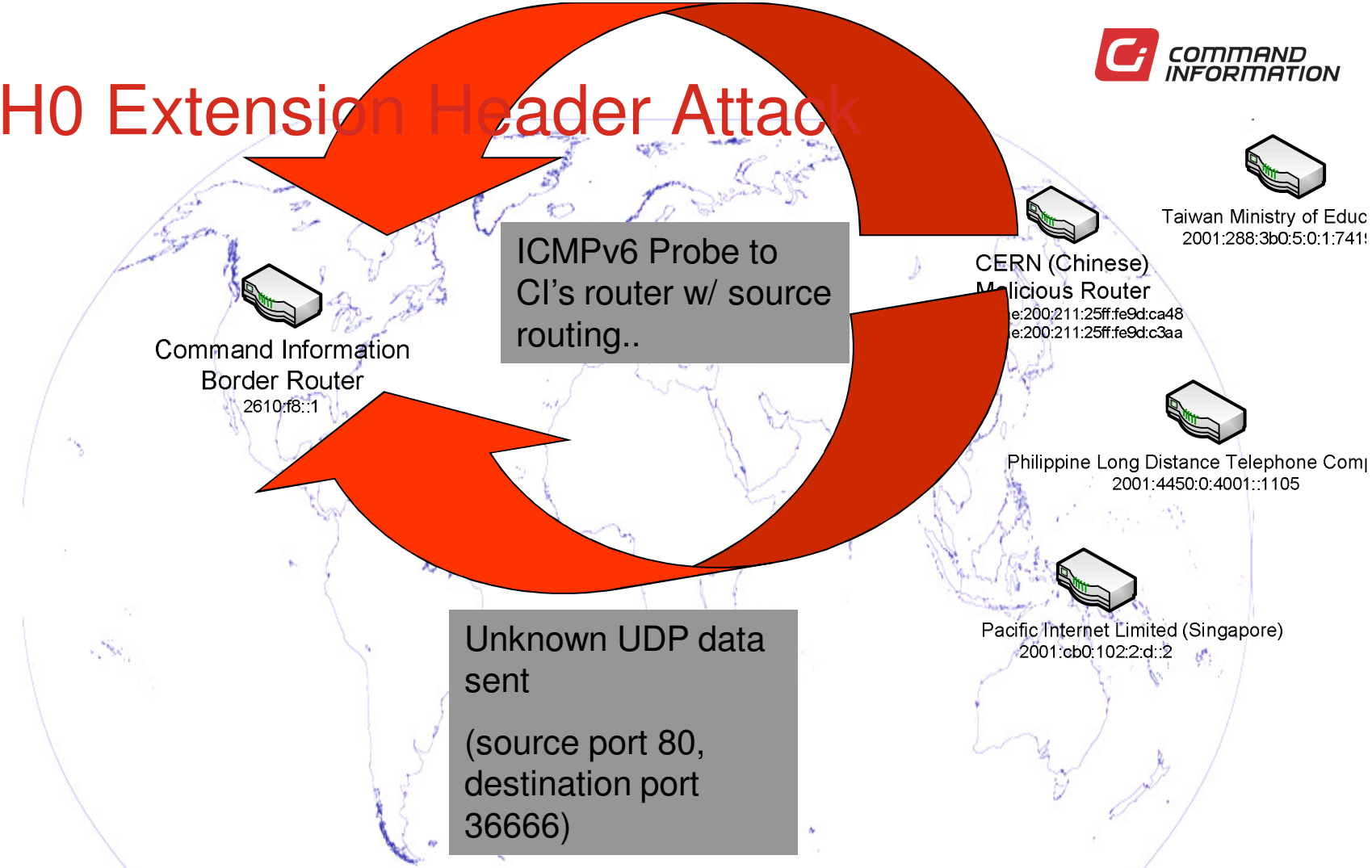
- Fewer fields (8 vs. 13 for IPv4)
- No checksums
- Streamlined, efficient
- Options aligned on 64 bit boundaries

IPv6 Extension Headers can be Indefinite



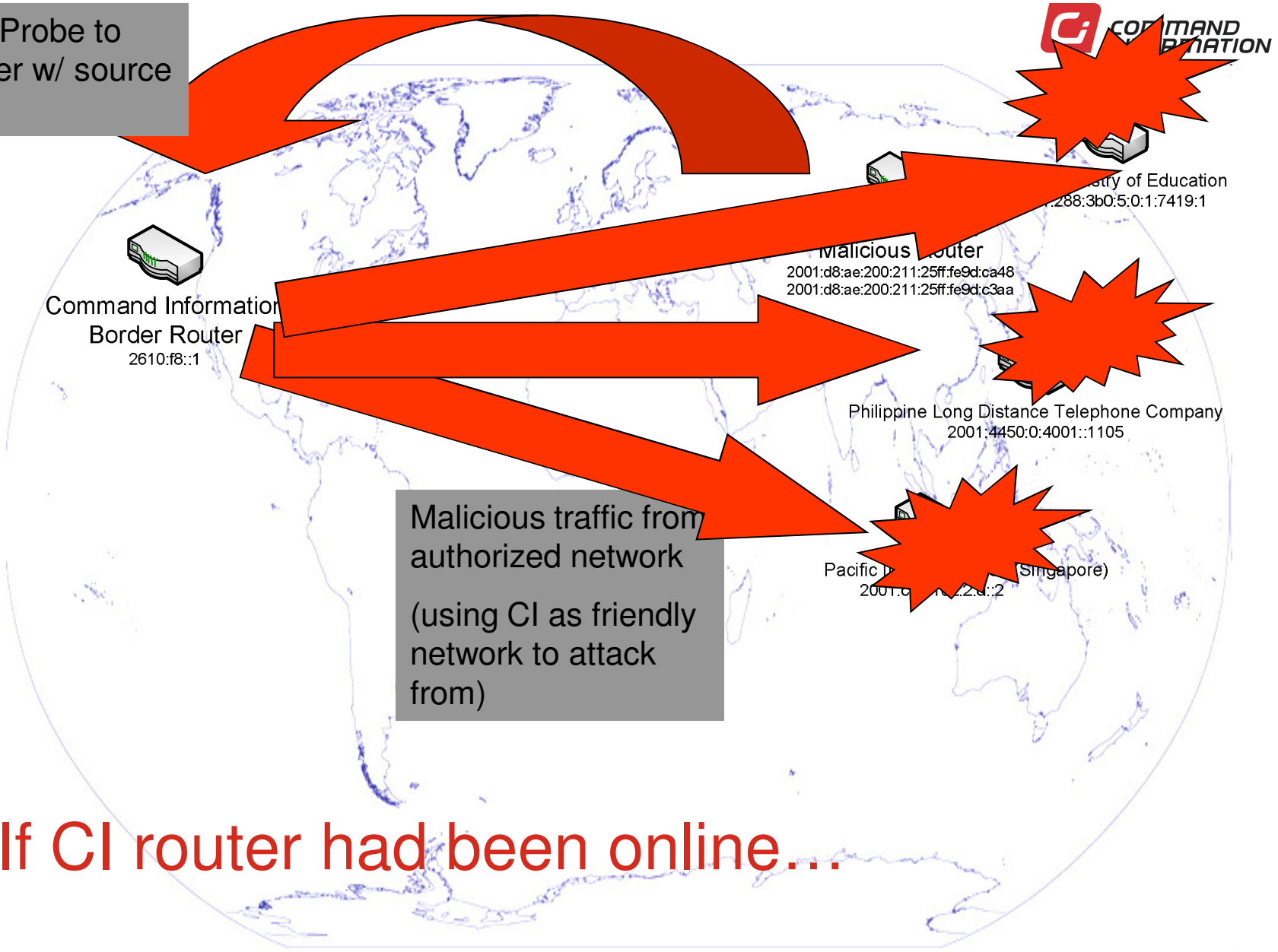
How many combinations are there?

RH0 Extension Header Attack



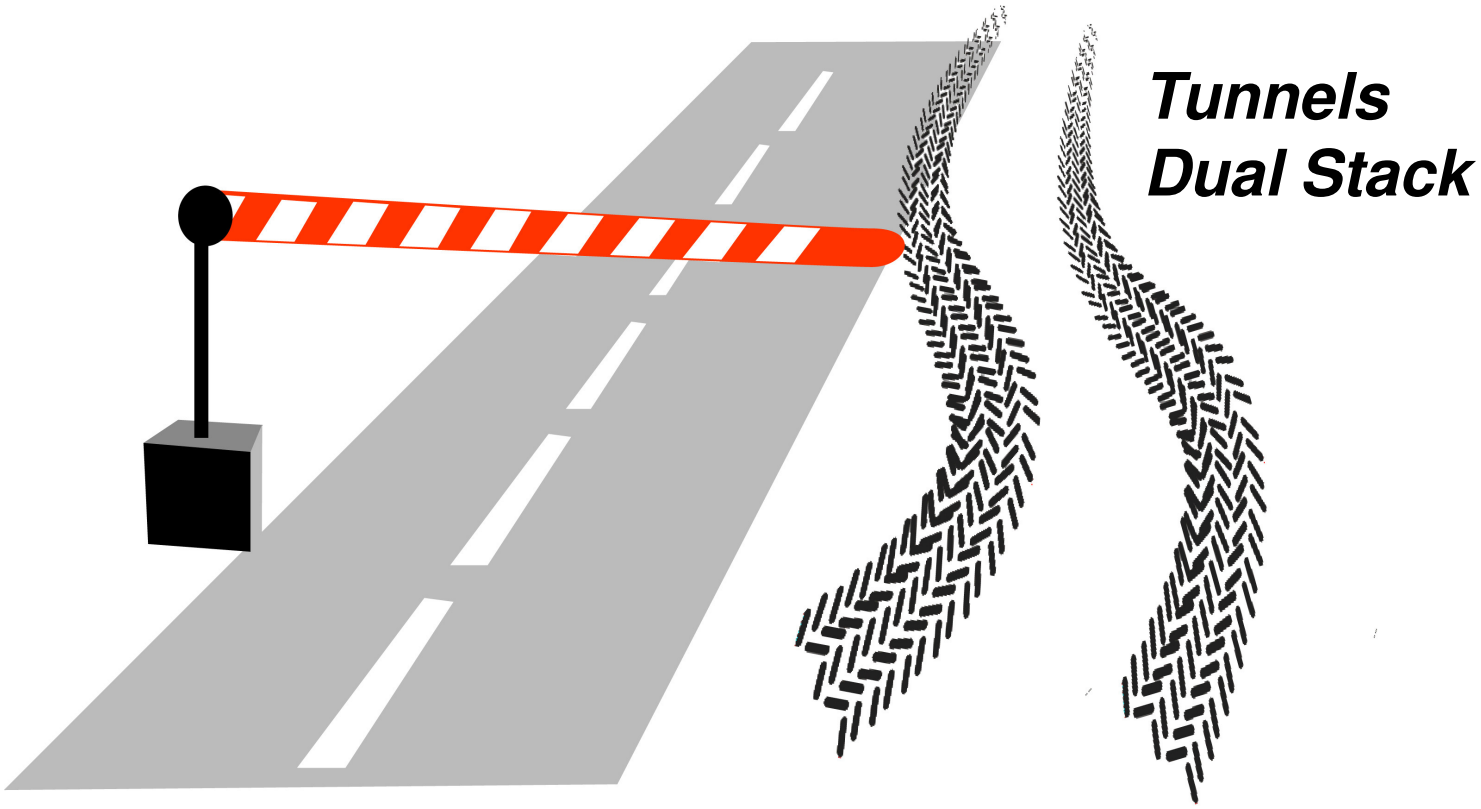
Because CI Router was not online

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



If CI router had been online…

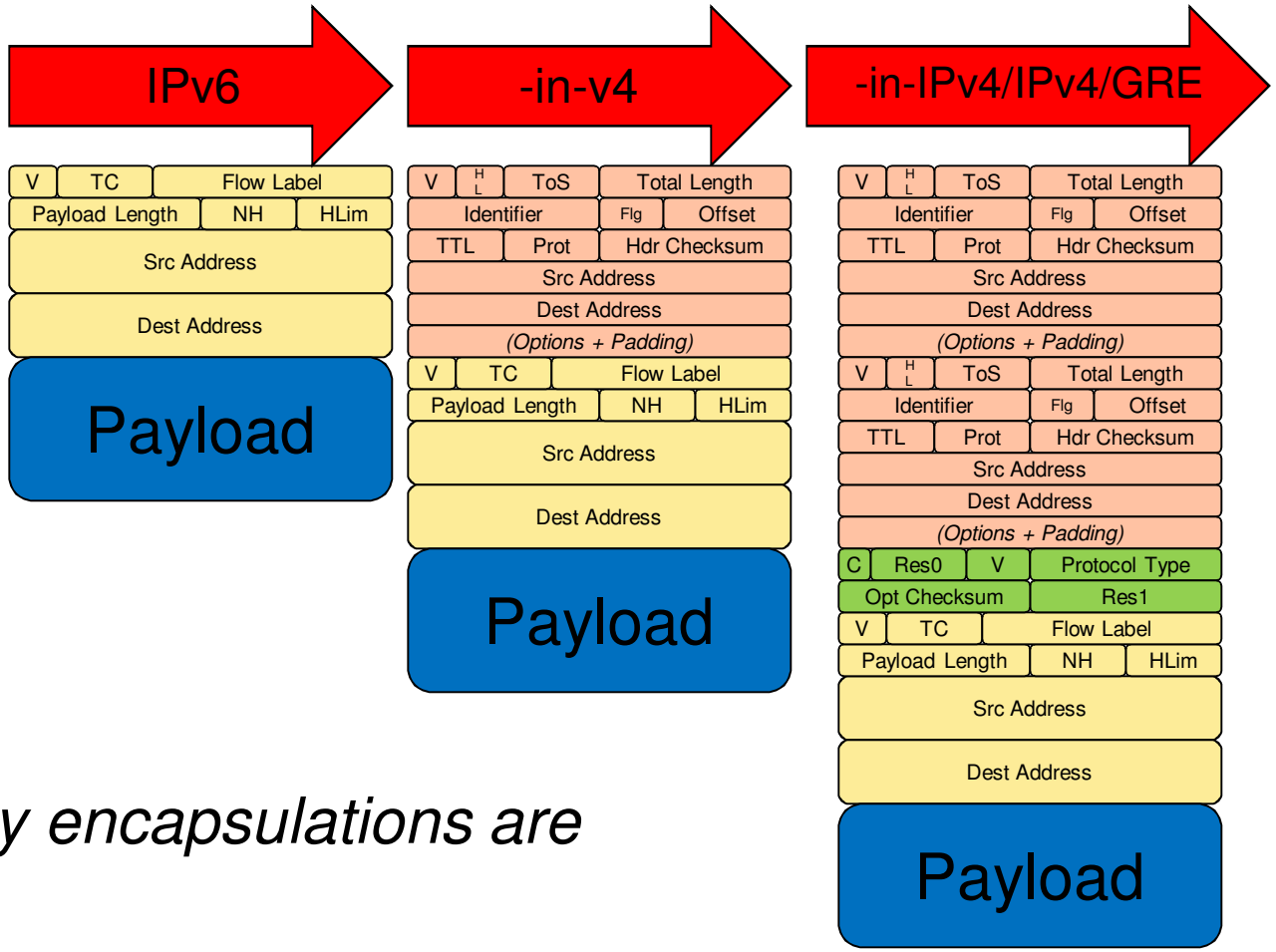
IPv4 Security Must Account For IPv6!



IPv6 Tunnels are a Transition Mechanism

- Protocol 41 and 47 Tunnels
  - 6in4
  - 6to4
  - 6RD
  - IPv6 in GRE
- IPSec Tunnels
  - AH
  - ESP Null
- UDP Based Tunnels
  - Teredo (Port 3544)
  - AYIYA (Port 5072)
  - Heartbeat (Port 3740)
  - TIC (Port 3874)
  - TSP (Port 3653)

Tunneled Packet Processing is *Complex*



How many encapsulations are there?

Tunnels Need to be Protected

ACL's can protect against Protocol 41, 47, IPSec and port specific UDP traffic

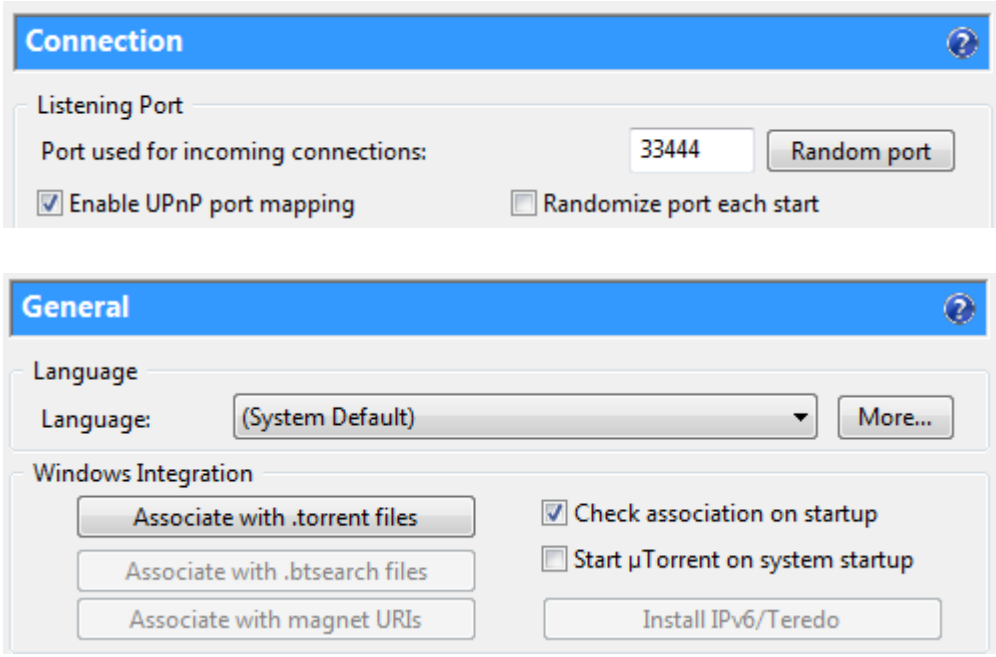
What if you don't know the Port?

Miredo: Teredo configured to run on any port

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

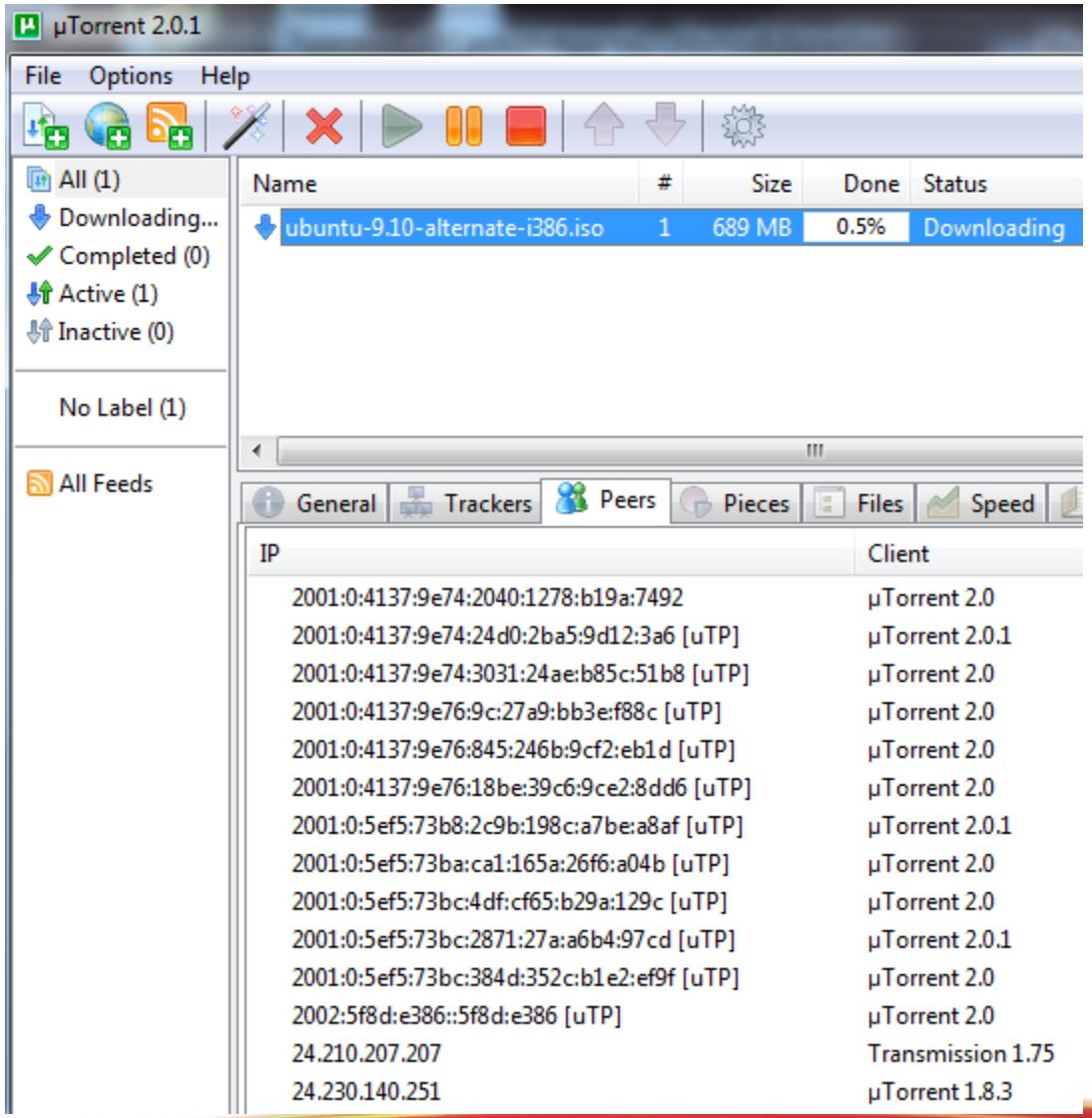
uTorrent – Teredo and IPv6-Capable

- Uses ephemeral port for connections
- User may randomly choose port
- Port may be randomly chosen on restart
- IPv6 support “on by default”



uTorrent – Teredo Peers

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



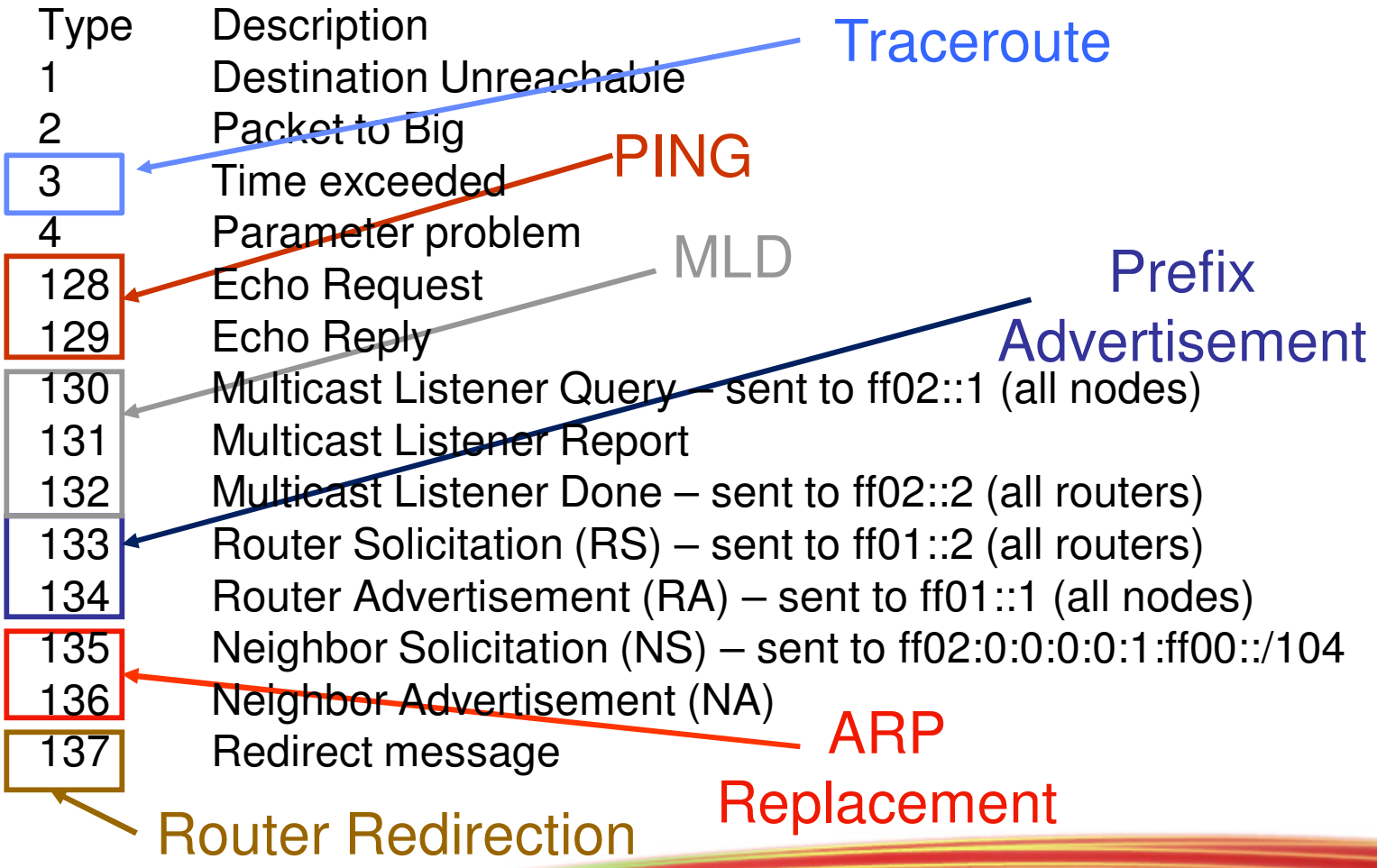
IPv4 “AAAA” DNS Queries Broadcast IPv6

- Microsoft Dual Stack enabled on ALL Vista / Windows 7 systems
- AAAA Queries present on every network we monitored.
- Considered ‘harmless’ by Security and Network Personal
- Must be disabled by DoD MO2 guidelines

IPv4 “AAAA” DNS– 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
- 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

ICMPv6 is Required for IPv6



Malevolent RAs: the threat inside

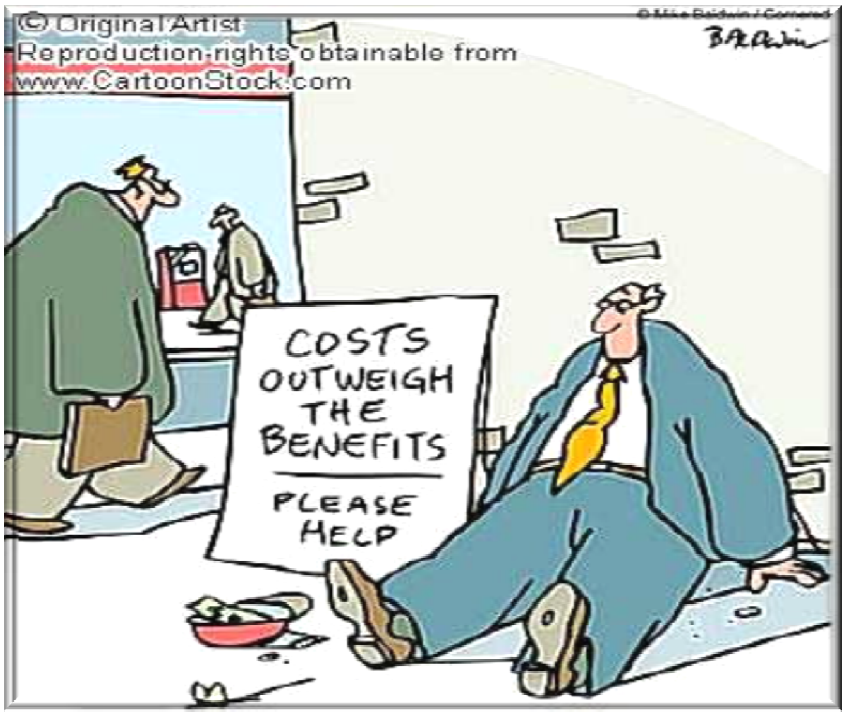
- IPv6-enabled workstations (untouched Vista, 7, Linux, Mac, etc) always listen for Router Advertisements
- User A downloads that pesky malware
  - Sets up tunnel like the non-standard UDP port example (or port 53)
  - Installs basic router advertisement daemon & IPv6 forwarding
- It sends RAs out to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

Summary

- IPv6 Threats are Real – both native and tunneled
- Hackers are using IPv6 to tunnel into networks undetected by current security tools
- Companies must develop a security policy to address IPv6.

IPv6 Cyber Security War Plan

- Knowledge
- Analysis
- Planning
- Securing
- Monitoring
- Lifecycle Management



Thank You

Ron Hulen

Command Information

ron.hulen@commandinformation.com

703-234-9363