GTRI
GLOBAL TECHNOLOGY RESOURCES INC.

Rocky Mountain Cisco User Groups April 16-17, 2008

IPv6 Security

Scott Hogg
GTRI - Director of Advanced Technology Services
CCIE #5133, CISSP

Agenda

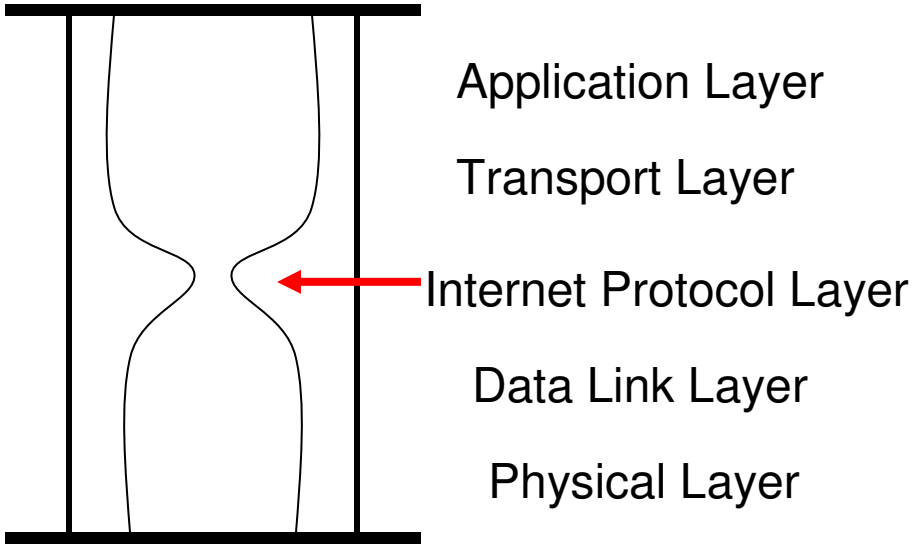
- IPv6 Threats
  - Reconnaissance
  - LAN Threats
  - ICMPv6 Threats
  - Extension Headers
  - Fragmentation
  - Transition Mechanism Threats
  - Router Threats
  - Application Threats
  - Man-In-The-Middle Threats
  - Flooding – DoS
  - Viruses and Worms
  - Mobile IPv6 Security
- IPv6 Protection Measures
  - IPv6 Firewalls
  - Intrusion Prevention Systems
  - Hardening IPv6 Network Devices
  - IPSec
  - IPv6 Privacy Addressing
- Questions and Answers

IPv6 Security

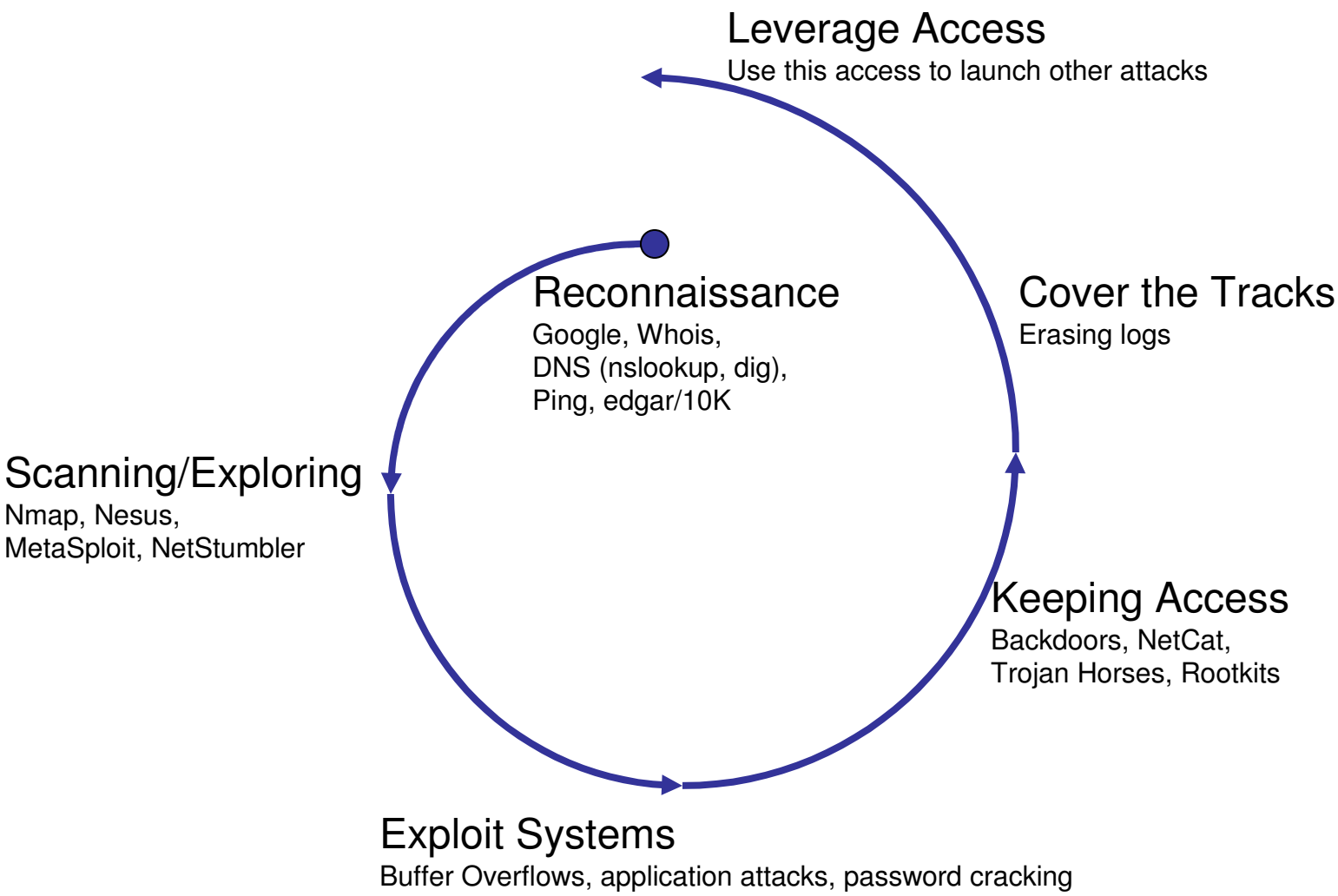
- We will all migrate eventually, but when and how remain to be seen
- I bet you have some IPv6 running on your networks already
- Do you use Linux, MacOS X, BSD, or MS Vista?
  - They all come with IPv6 capability, some even have IPv6 enabled by default (IPv6 preferred)
  - They may try to use IPv6 first and then fall-back to IPv4
  - Or they may create IPv6-in-IPv4 tunnels to Internet resources to reach IPv6 content
  - Some of these techniques take place regardless of user input or configuration
- If you are not protecting your IPv6 nodes then you have just allowed a huge back-door to exist

IPv6 Security Threats

- There isn't much of a hacker community focusing on IPv6 today but that is likely to change as IPv6 becomes more popular – IPv6 will gain the hacker's attention
- Many vendors (Cisco, Juniper, Microsoft, Sun, Open Source) have already published IPv6 bugs/vulnerabilities
- Attacks at the layers below and above the network layer are unaffected by the security of IPv6



Security Attack Lifecycle



IPv6 Security

- IPv6 Security is being considered up front in its design and deployment
- BCPs for IPv4 apply to IPv6
  - Least Privilege
  - Defense in Depth
  - Diversity of Defense
  - Choke Point
  - Weakest Link
  - Fail-Safe Stance
  - Universal Participation
- Simplicity over Complexity
- Confidentiality, Integrity, Availability (CIA)

IPv6 Threats

- There isn't much of a hacker community focusing on IPv6 today but that is likely to change as IPv6 becomes more popular (e.g. Firefox)
- IP is the most popular network-layer protocol on the planet
  - IPv6 will gain the hacker's attention
- Many vendors (Cisco, Juniper, Microsoft, Sun) have already published IPv6 bugs/vulnerabilities
- Attacks generally fall into one of these three categories.
  - Denial of Service
  - Modification of Information
  - Eavesdropping

By the Way: It Is Real ☹
IPv6 Hacking Tools

the hacker's choice

presents:

Attacking the IPv6 Protocol Suite

van Hauser, THC

vh@thc.org

http://www.thc.org

Reconnaissance

- First step of an attack
- Checking registries (whois), DNS (nslookup, dig, etc.), Google
- Ping sweeps, port scans, application vulnerability scans
- IPv6 makes the ping sweeps problematic
  - The address space is too large to scan
- Ping FF02::1 will give results
- Node Information Queries (RFC 4620)
- Attackers may find one host and leverage the neighbor cache

ICMPv6

- More powerful than ICMPv4
- ICMPv6 uses IPv6 extension header # 58 (RFC 2463)

Type	Description
1	Destination Unreachable
2	Packet to Big
3	Time exceeded
4	Parameter problem
128	Echo Request
129	Echo Reply
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)
137	Redirect message

PING

MLD

Prefix Advertisement

Router Redirection

ARP Replacement

ICMPv6 Threats

- Allow the following ICMPv6 packets inbound from the Internet
  - Type 1, <All Codes> – Destination Unreachable
  - Type 2 – Packet Too Big (PMTUD)
  - Type 3, Code 0 – Time Exceeded
  - Type 4, Codes 1 & 2 – Parameter Problem
  - Type 128 and Type 129 – Echo Request and Echo Response
- Allow the following ICMPv6 packets to and from the local LAN router
  - Type 2 – Packet Too Big (PMTUD)
  - Type 4, Code 1 & 2 – Parameter Problem
  - Type 130, 131, 132, 143 – Multicast Listener Discovery (link local source address)
  - Type 133 and Type 134 – Router Solicitation and Router Advertisement
  - Type 135 and Type 136 – Neighbor Solicitation and Neighbor Advertisement
  - Type 141 and Type 142 - Inverse Neighbor Solicitation and Advertisement
- Many of these messages should have Hop Limit = 255
- Block unallocated or experimental ICMPv6 types
  - Types 5-99, 100, 101, 102-126, 154-199, 200, 201, 202-254

LAN Threats

- IPv6 uses ICMPv6 for many LAN operations
  - Stateless auto-configuration
  - IPv6 equivalent of IPv4 ARP
- Spoofed RAs can renumber hosts or launch a MITM attack
- NA/NS – same attacks as with ARP
- DHCPv6 spoofing
- Redirects – same as ICMPv4 redirects
- Forcing nodes to believe all addresses are on-link

Secure Neighbor Discovery (SEND)

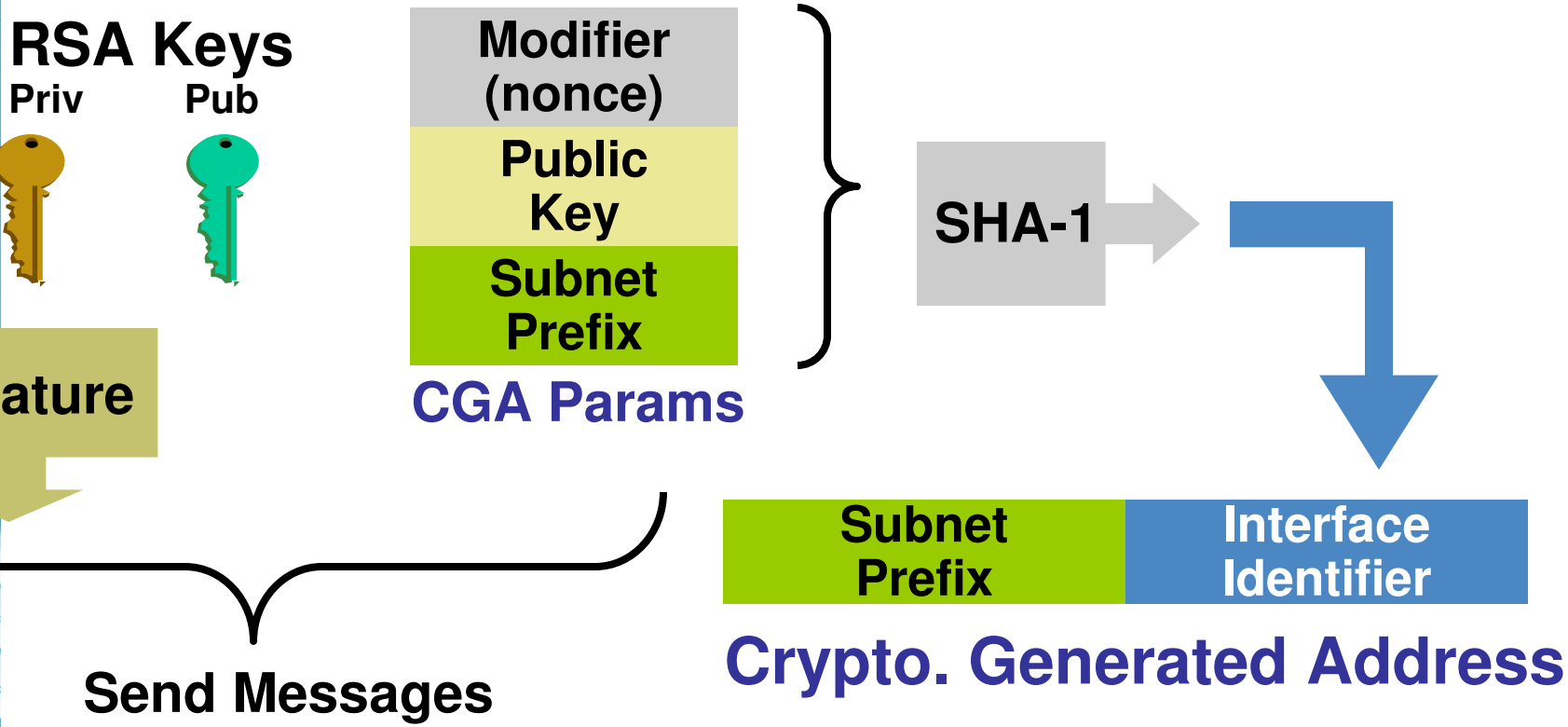
- Neighbor Discovery is vital for a network to work properly. However, it is not secure.
- Neighbor or router spoofing are possible attacks, along with rogue advertisers, redirect and unreachability attacks
- IPSec is not usable to secure NDP
- SEND (RFC 3971) defines the trust model for nodes communicating on a LAN
- Nodes use public/private key pair to create Cryptographically Generated Addresses (CGA – RFC 3972) which is the last 64 bits of address (interface ID)
- CGAs provide authentication/ownership of address
- CGAs makes it possible to prove the ownership of a
- specific address.
- “Trust Anchor” certifies that the router is legitimate

Secure Neighbor Discovery (SEND)

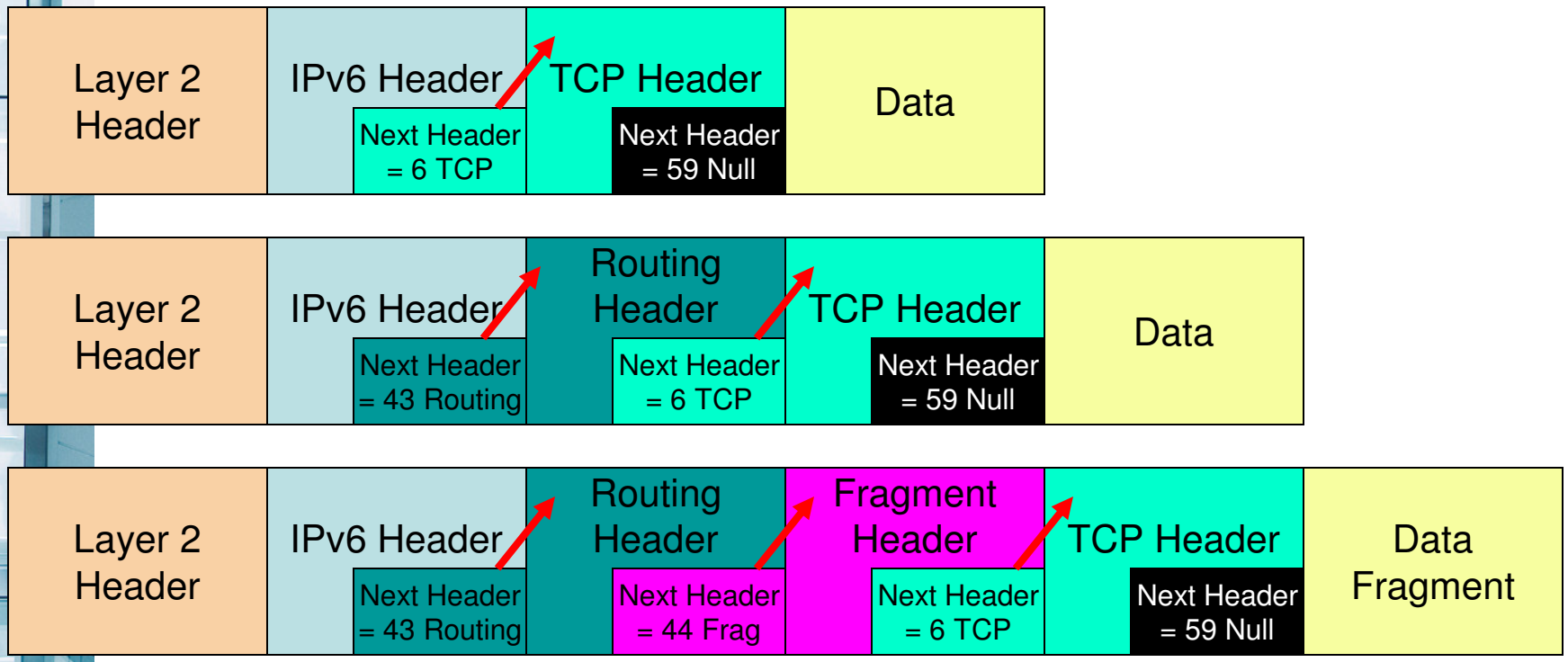
- Improvements on standard neighbor discovery:
  - Neighbor Discovery Protocol messages use RSA-based cryptography to protect their integrity
  - A timestamp and nonce are used to prevent replay attacks
  - Signed ND messages protect message integrity and
  - authenticate the sender.
  - Nonce prevent replay attacks.
  - Trust anchors may certify the authority of routers.
- Current Deployment
  - DoCoMo USA Labs - OpenSource SEND Project

Cryptographically Generated Addresses (CGA)

- Each devices has a RSA key pair (no need for cert)
- Ultra light check for validity
- Prevent spoofing a valid CGA address



IPv6 Extension Headers

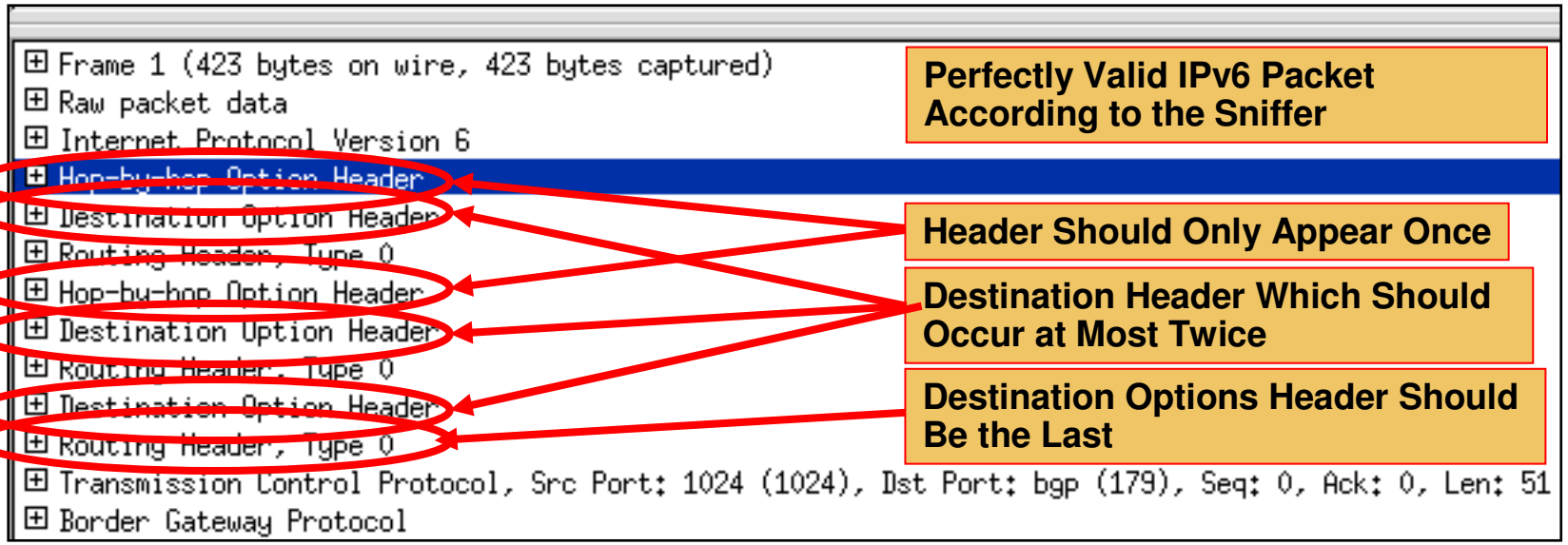


Extension Headers (EHs)

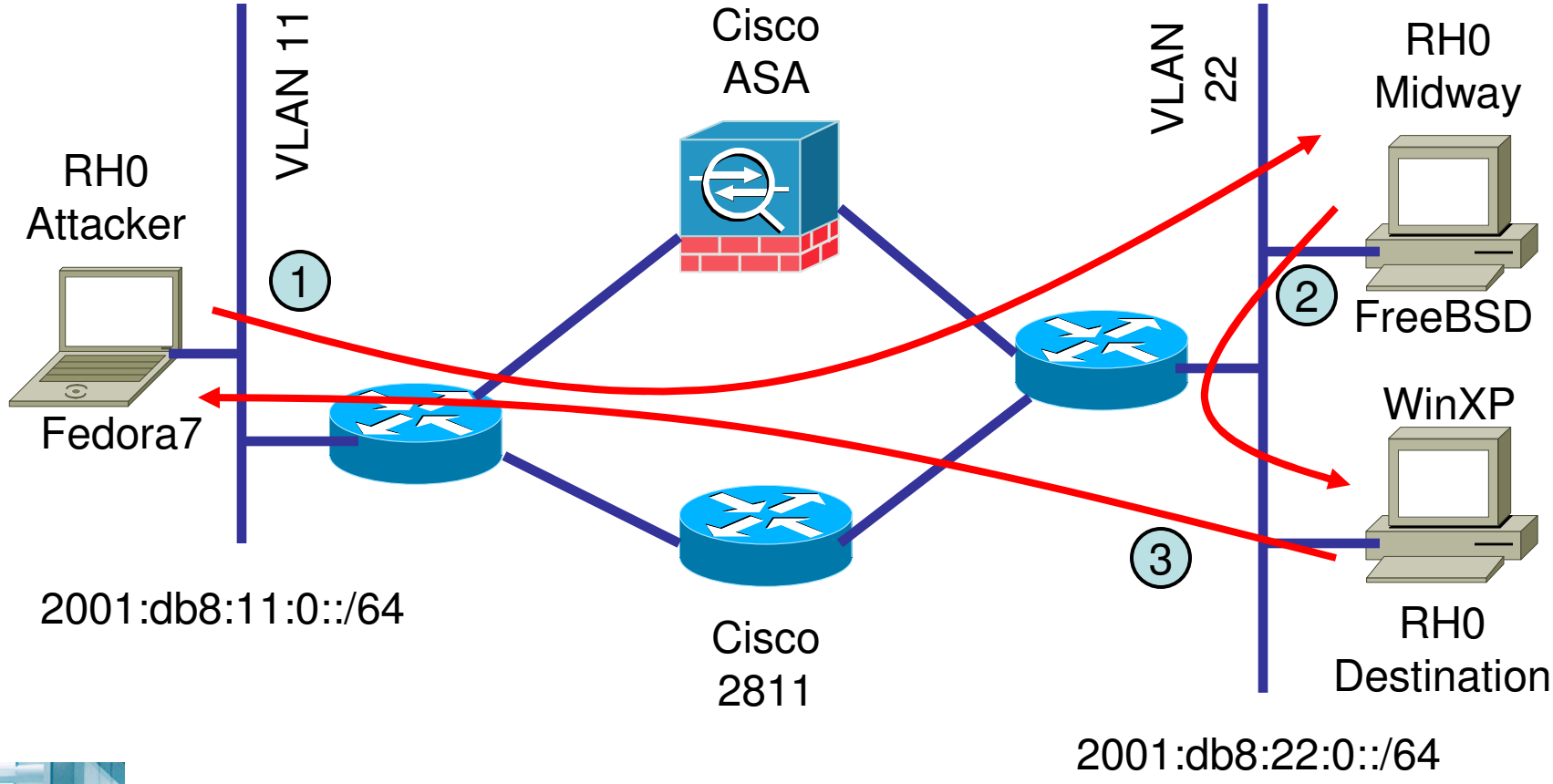
- Extension Headers
  - Each header should not appear more than once with the exception of the Destination Options header
  - Hop-by-Hop extension header should only appear once.
  - Hop-by-Hop extension header should be the first header in the list because it is examined by every node along the path.
  - Destination Options header should appear at most twice (before a Routing header and before the upper-layer header).
  - Destination Options header should be the last header in the list if it is used at all.
- Header Manipulation – Crafted Packets
- Large chains of extension headers
  - Separate payload into second fragment
  - Consume resources - DoS
- Invalid Extension Headers – DoS
- Routing Headers Type 0 – source routing

Header Manipulation

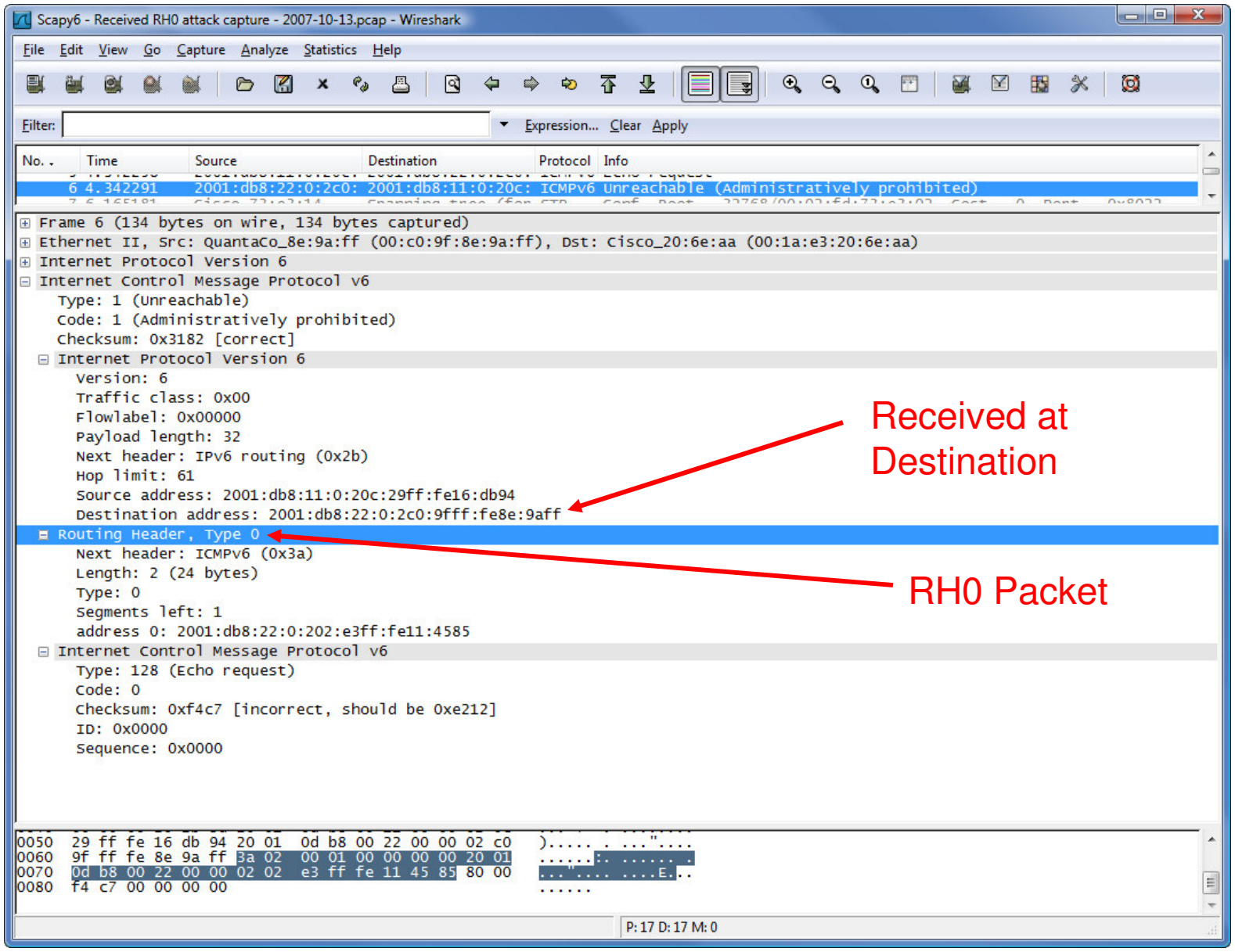
- Unlimited size of header chain (spec wise) can make filtering difficult
- DoS a possibility with poor IPv6 stack implementations
  - More boundary conditions to exploit
  - Can I overrun buffers with a lot of extension headers?



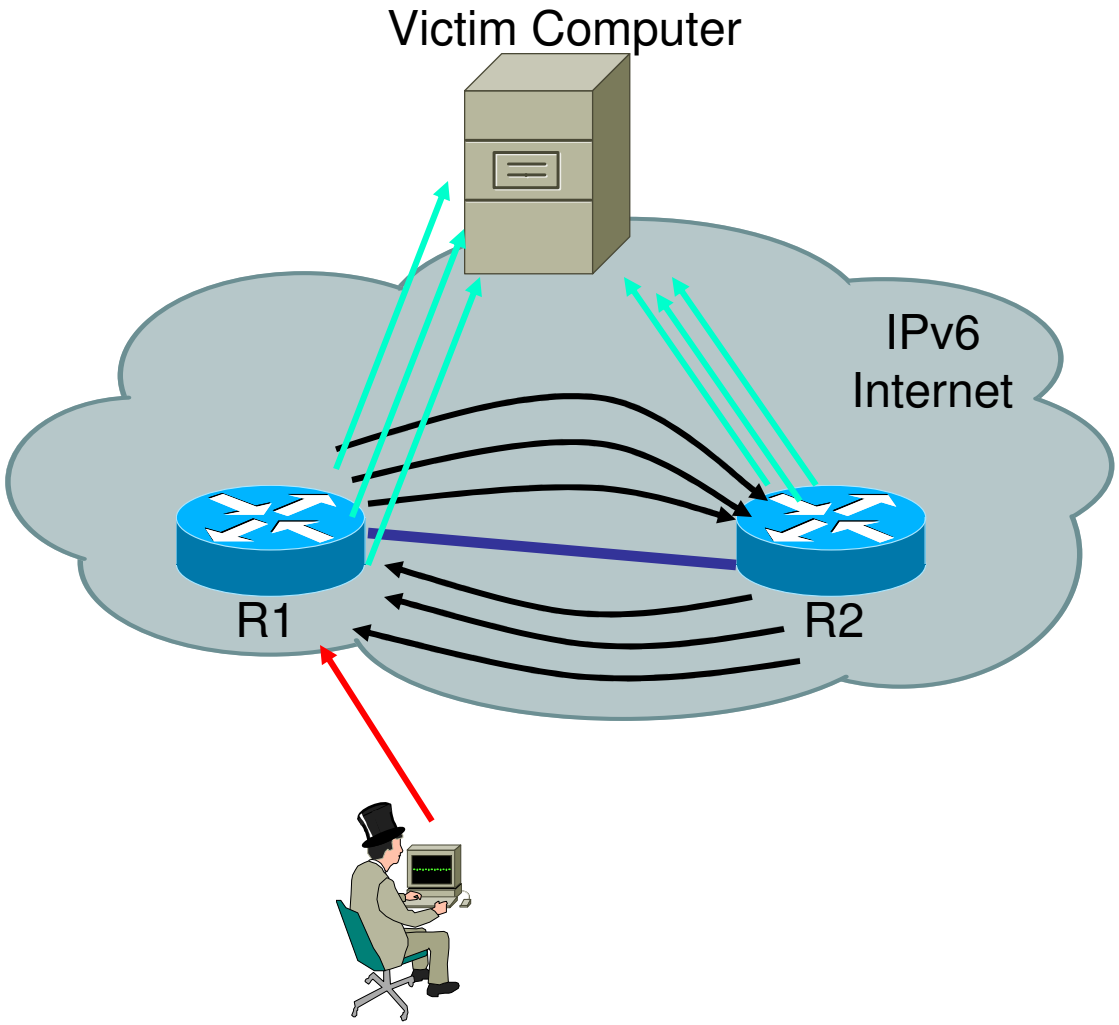
RH0 Attack



RH0 Packet Received



RHO Feedback Loop



Extension Headers (EHs)

- Cisco ACL Example
  - `! stop RH0 packets to/from router`
  - `no ipv6 source-route`
  - `! IPv6 ACL`
  - `ipv6 access-list inbound`
  - `! filter site local`
  - `deny ipv6 fec0::/10 any log-input`
  - `! filter site local`
  - `deny ipv6 any fec0::/10 log-input`
  - `! filter RH type 0, 1, and 2`
  - `deny ipv6 any any routing log-input`
  - `! filter other EHs`
  - `deny ipv6 any any undetermined-transport`
  - `! add back in NDP in order to log all drops`
  - `permit icmp any any nd-na`
  - `permit icmp any any nd-ns`
  - `deny ipv6 any any log`

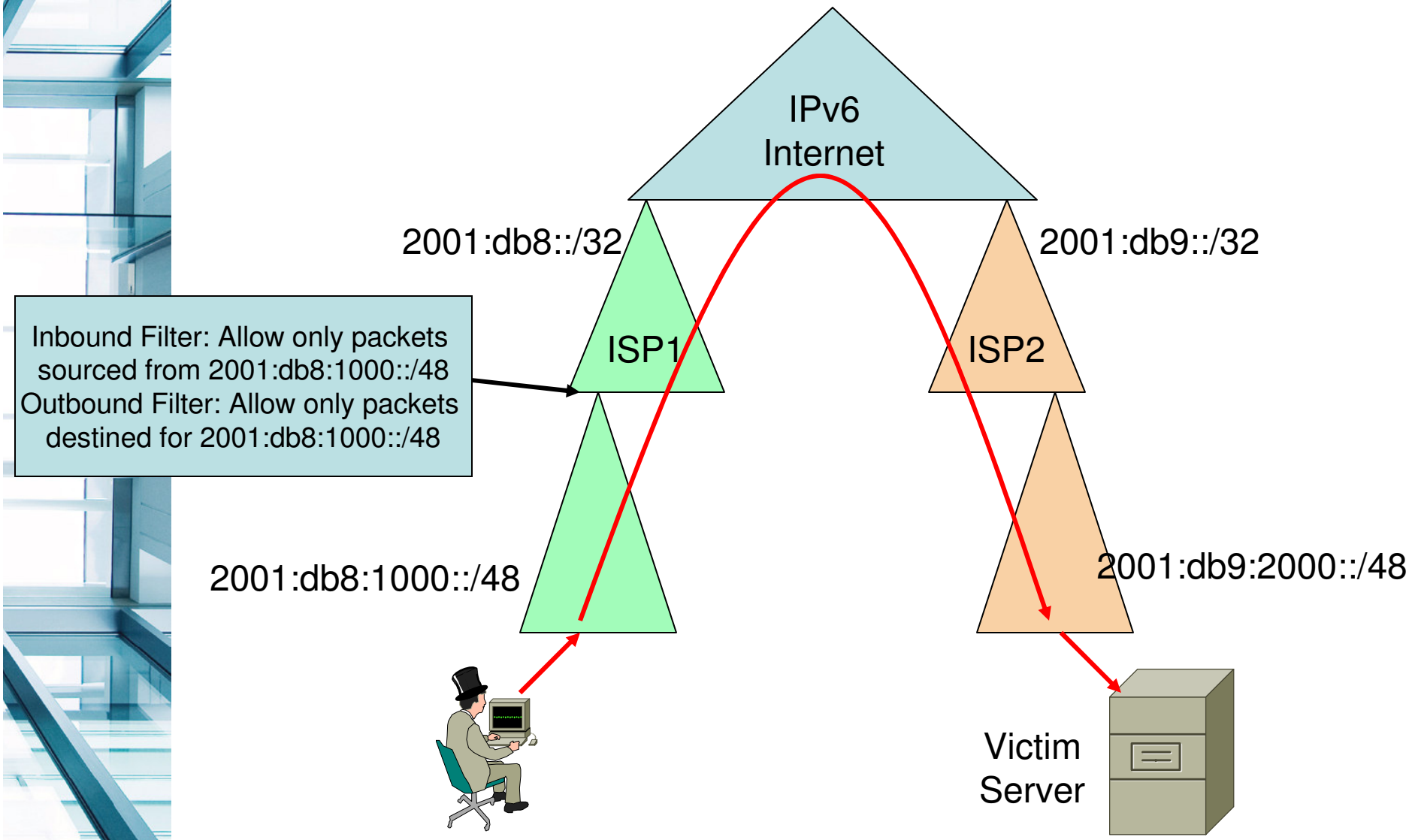
Fragmentation

- In IPv6 routers do not fragment
  - Fragments destined for network device should be dropped
- IPv6 links must have MTU >= 1280 bytes
  - Fragments with less than 1280 bytes should be dropped with the exception of the last fragment
- It is left to the end-systems to perform Path MTU Discovery (PMTUD)
  - ICMPv6 – Type 2 - Packet Too Big
- Fragmentation can hide attacks or as an attack itself on the upper layers
  - Overlapping fragments, out of order fragments, tiny fragments
- Cisco Router ACL “fragments” keyword
  - L3/L4 ACL with “fragments” the ACL action (permit/deny) is conservative

Layer-3/4 Spoofing

- Spoofing of IPv6 packets is possible (Scapy6)
- Hierarchical addressing and ingress/egress filtering
- uRPF Checks (BCP38/RFC 2827)
  - `ipv6 access-list RPFACLNAME`
  - `  permit IPv6 2001:db8:100:9::/64 any log-input`
  - `  deny IPv6 any any log-input`
  - `!`
  - `interface FastEthernet 0/0`
  - `  ipv6 address 2001:db8:100:10::1/64`
  - `  ipv6 verify unicast reverse-path RPFACLNAME`

Hierarchy and Traceback



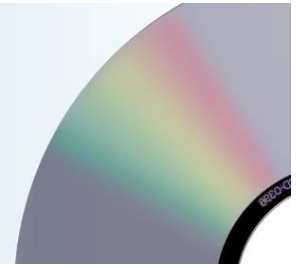
Transition Mechanism Threats

- Dual Stack - Preferred
  - You are only as strong as the weakest of the two stacks.
  - Running dual stack will give you at least twice the number of vulnerabilities
- Manual Tunnels - Preferred
  - Filter tunnel source/destination and use IPSec
  - If spoofing, return traffic is not sent to attacker
- Dynamic Tunnels
  - 6to4 Relay routers are “open relays”
  - ISATAP – potential MITM attacks
  - Attackers can spoof source/dest IPv4/v6 addresses
- Protocol Translation – Not recommended
- Deny packets for transition techniques not in use
  - Deny IPv4 protocol 41 forwarding unless that is exactly what is intended – unless using 6to4 tunneling
  - Deny UDP 3544 forwarding unless you are using Teredo-based tunneling

Router Threats

- Routing Disruption Attacks
  - Dynamic routing protocols can be exploited
  - Traffic could then be re-routed (Transitive Community Modification)
  - Routing loop, black-hole, gray-hole, detour, asymmetry, partition
- Resource Consumption/Saturation Attacks
  - Injection of extra updates, route requests, or traffic
  - Magnified by the presence of loops or detours
- Buffer Overflow Attacks
- BGP, IS-IS, and EIGRP still use MD5
- OSPFv3 and RIPng use IPSec
- “passive-interfaces” where routing is not needed
- Perform RFC2827 filtering and Unicast Reverse Path Forwarding (uRPF) checks throughout the network and at tunnel endpoints

Application Threats



- Applications for IPv4 and IPv6 are the same
- Buffer overflows, SQL Injection, cross-site scripting will all remain valid attacks on IPv6 servers
- Use of IPSec can prevent many of these attacks that exploit trust between servers
- Completely hierarchal addressing will make trace-back easier but privacy addressing and forged MAC addresses won't
- E-mail/SPAM is still a problem in IPv6 nets
- DNS servers will still be attacked

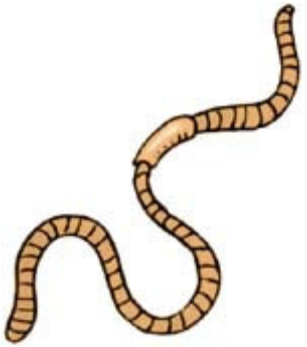
Man-In-The-Middle Threats

- MITM attacks are still possible in IPv6 networks – just like with IPv4
- LAN attacks, sniffing, spoofing the default gateway
- IPSec with both AH and ESP will help immensely
- SeND and CGAs will hopefully make these attacks less common on the LAN

Flooding – DDoS

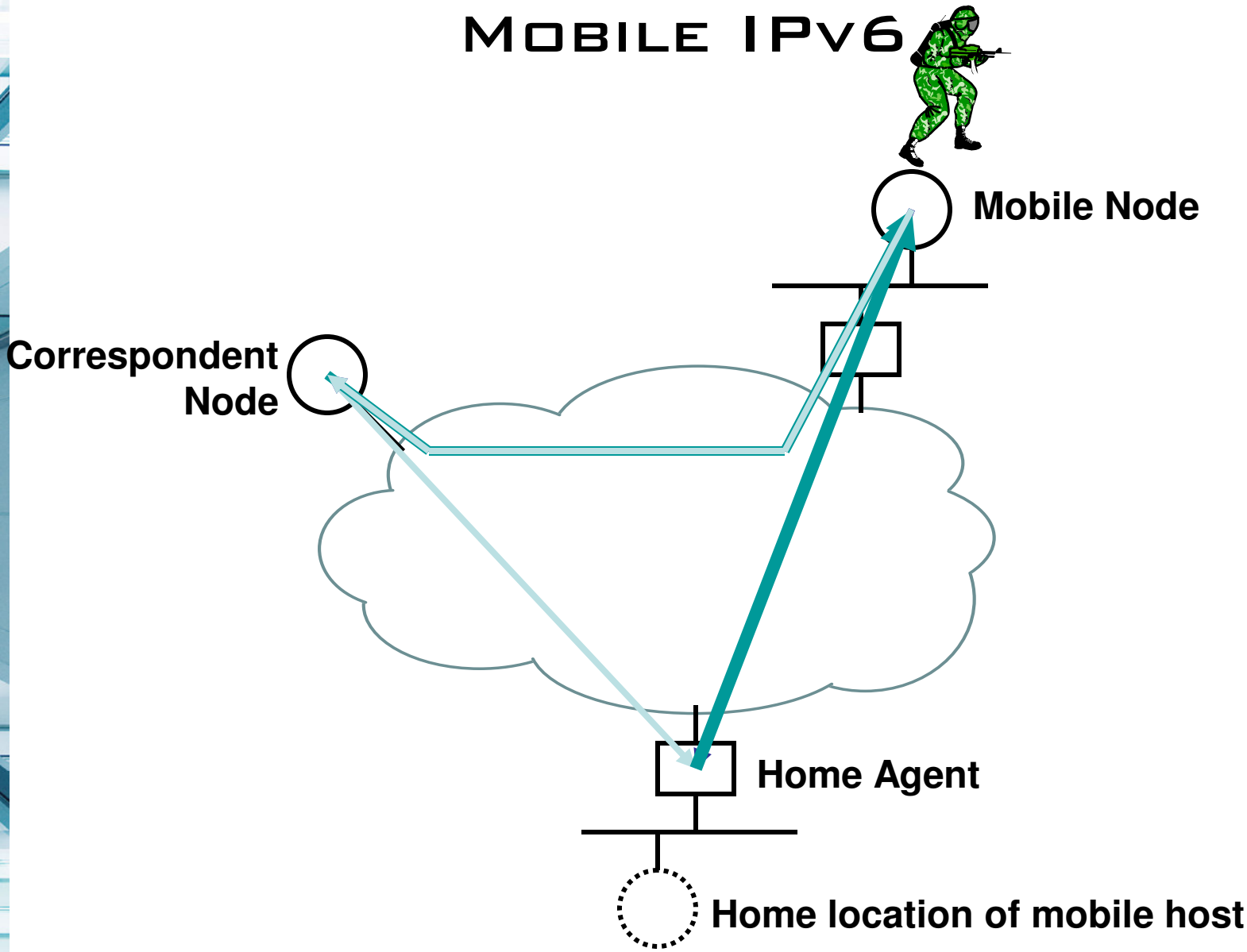
- IPv6 doesn't use broadcast only multicast – Smurf attacks more difficult
  - FF02::1 - All Nodes Address
  - FF02::2 - All Routers Address
  - FF05::1 – All Site Local Nodes
  - FF05::1:3 – All DHCPv6 servers
  - Tightly control who can send to multicast groups
- ICMPv6 error message should not be generated in response to a packet with a multicast destination address
- DDOS attacks can still exist on the IPv6 Internet just like they exist on IPv4 Internet
  - Document your procedures for "last-hop traceback" ahead of time – work with your ISP

Viruses and Worms



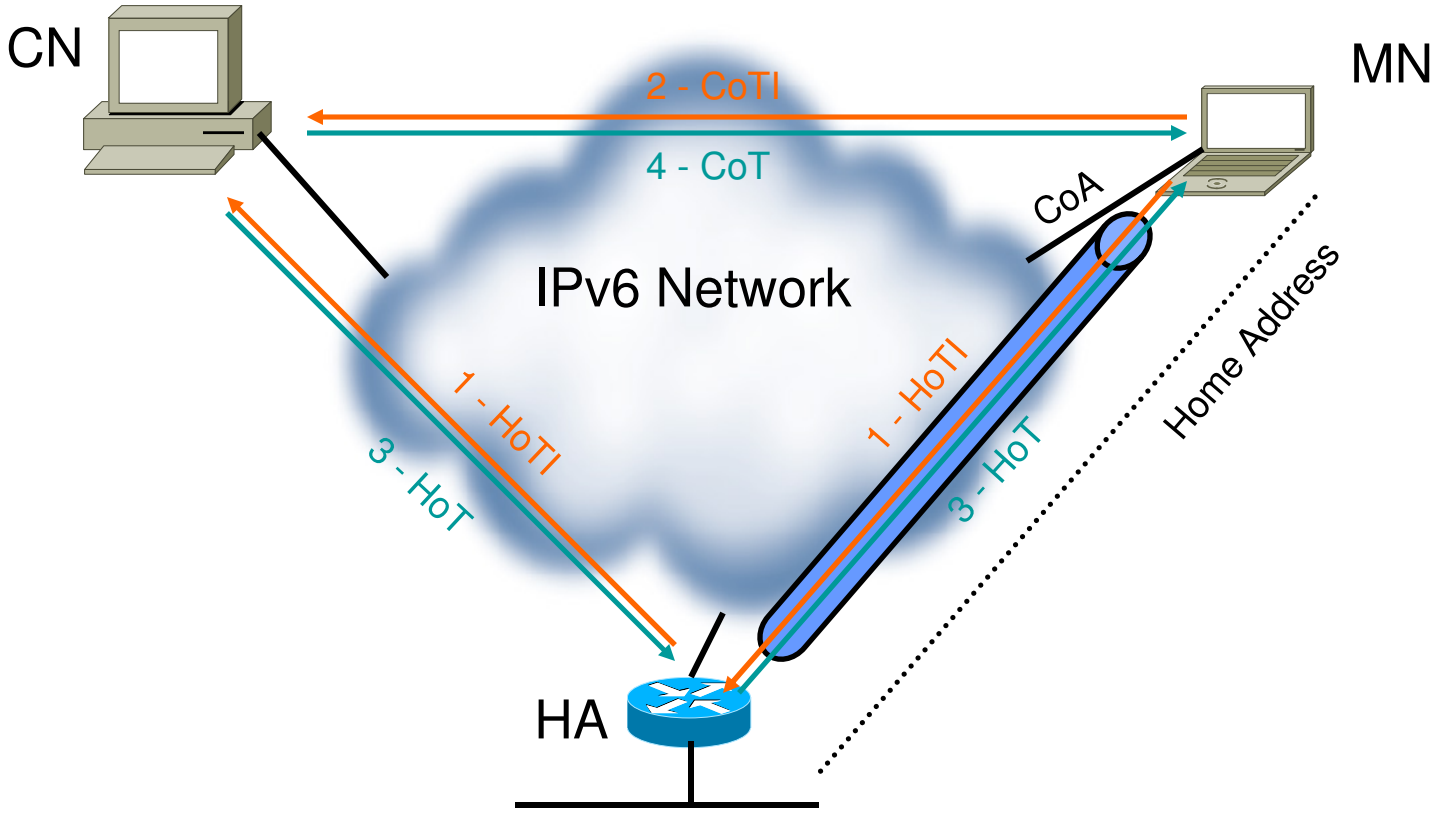
- Viruses will be the same with IPv6
- Worms like Sapphire/SQL Slammer won't spread nearly as quickly (100s of years)
- "At one million packets per second on a IPv6 subnet with 10,000 hosts it would take over 28 years to find the first host to infect"
- Scanning worms may use IPv4 and then check for IPv6 capabilities on infected host
  - IPv6 Worm – Slapper
- Perform ingress/egress filtering and uRPF checks throughout the network and at the perimeter

Mobile IPv6



Mobile IPv6

Return Routability Procedures



HoTI = Home Test Init, HoT = Home Test
CoTI = Care-of Test Init, CoT = Care-of Test

Mobile IPv6 Security

- Mobility changes the perimeter model
- Layer-3 devices need to enable MIPv6 to all hosts on the subnet
- You must allow Type 2 Routing Header for CN to MN
- Attacker could be a fake MN or a rogue Home Agent
- If you don't use MIPv6 then filter it
  - Home Agent Address Discovery Request - Type 144
  - Home Agent Address Discovery Reply - Type 145
  - Mobile Prefix Solicitation - Type 146
  - Mobile Prefix Advertisement - Type 147
- Firewalls don't have state information on who is roaming and who isn't
- Binding Update, Binding Ack filtering on the Layer-3 HAs
- IPSec can be used with MIPv6 but some mobile devices don't have the resources

IPv6 Firewalls

- Don’t just use your IPv4 firewall for IPv6 rules
- Don’t just blindly allow IPSec or IPv4 Protocol 41 through the firewall
- Procure separate firewalls for IPv6 policy
- Bogon and anti-spoofing filters are a MUST
- Look for vendor support of Extension Headers, Fragmentation, PMTUD
- Firewalls should have granular filtering of ICMPv6 and multicast
- Some hosts may have multiple IPv6 addresses so this could make firewall troubleshooting tricky
- Layer-2 firewalls are trickier with IPv6 because of ICMPv6 ND/NS/NUD/RA/RS messages

Firewalls

- Cisco Router ACLs, Reflexive ACLs, IOS-based Firewall, PIX, ASA 8.0, FWSM 3.2.5
- Full IPv6 support for interfaces
- ADSM 6.0 still doesn't recognize IPv6 commands
- Disable RAs on interfaces
  - `FWA(config-if)# ipv6 nd suppress-ra`
- Disable DAD on interfaces
  - `FWA(config-if)# ipv6 nd dad attempts 0`
- Filter Routing Header Type 0
  - `ipv6 access-list DENYV6RH0`
  - `deny ipv6 any 2001:db8:10::/48 routing`
  - `permit ipv6 any any`

ASA 8.0 ICMPv6 Filtering

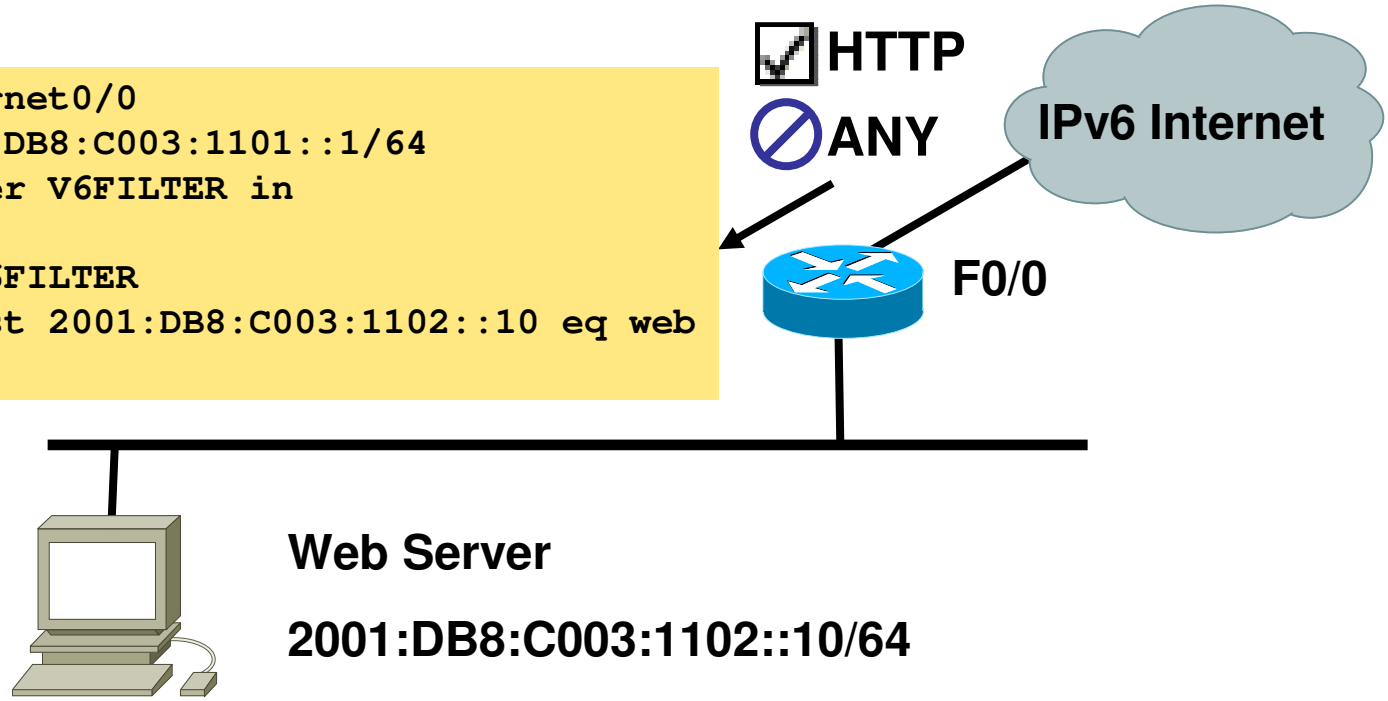
```
ASA5500(config)# ipv6 access-list TEST deny icmp6 interface inside
    any ?

configure mode commands/options:
  <0-255>          Enter ICMP type number (0 - 255)
  echo
  echo-reply
  inactive         Keyword for disabling an ACL element
  log              Keyword for enabling log option on this ACE
  membership-query
  membership-reduction
  membership-report
  neighbor-advertisement
  neighbor-redirect
  neighbor-solicitation
  object-group             ICMP object-group for destination port
  packet-too-big
  parameter-problem
  router-advertisement
  router-renumbering
  router-solicitation
  time-exceeded
  time-range       Keyword for attaching time-range option to this ACE
  unreachable
  <cr>
```

Basic IPv6 Packet Filtering

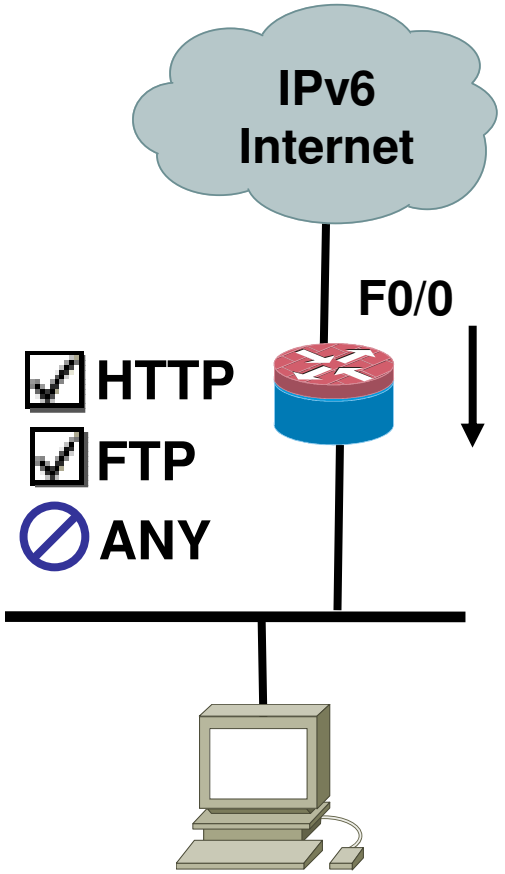
- When Used for Traffic Filtering, IPv6 Access Control Lists (ACL) Offers the Same Level of Support as in IPv4
- Every IPv6 ACL has implicit "`permit icmp any any nd-na`" and "`permit icmp any any nd-ns`"
- Implicit "`deny all`" at the end of access list

```
interface FastEthernet0/0
 ipv6 address 2001:DB8:C003:1101::1/64
 ipv6 traffic-filter V6FILTER in
!
ipv6 access-list V6FILTER
 permit tcp any host 2001:DB8:C003:1102::10 eq web
!
```



IPv6 Firewall Feature Set

```
ipv6 unicast-routing
ipv6 cef
!
ipv6 inspect audit-trail
ipv6 inspect max-incomplete low 150
ipv6 inspect max-incomplete high 250
ipv6 inspect one-minute low 100
ipv6 inspect one-minute high 200
ipv6 inspect name V6FW tcp timeout 300
ipv6 inspect name V6FW udp
ipv6 inspect name V6FW icmp
!
interface FastEthernet0/0
ipv6 address 2001:DB8:C003:1112::2/64
ipv6 cef
ipv6 traffic-filter EXAMPLE in
ipv6 inspect V6FW in
!
ipv6 access-list EXAMPLE
permit tcp any host 2001:DB8:C003:1113::2 eq www
permit tcp any host 2001:DB8:C003:1113::2 eq ftp
deny ipv6 any any log
```



Web/FTP Server
2001:DB8:C003:1113::2

PIX 7.0: ACL

```
interface Ethernet0
 nameif outside
 ipv6 address 2001:db8:c000:1051::37/64
 ipv6 enable
 ipv6 nd suppress-ra
interface Ethernet1
 nameif inside
 ipv6 address 2001:db8:c000:1052::1/64
 ipv6 enable

ipv6 unicast-routing

ipv6 route outside ::/0 2001:db8:c000:1051::1

ipv6 access-list SECURE permit tcp any host 2001:db8:c000:1052::7 eq
   telnet
ipv6 access-list SECURE permit icmp6 any 2001:db8:c000:1052::/64

access-group SECURE in interface outside
```

IPv6 Intrusion Prevention

- Old IPv6 signature
  - 1007-0 IPv6 over IPv4 ATOMIC.L3.IP
- IPS 6.0 supports IPv6 signatures
- There are 8 new Atomic IPv6 Signatures

Signature	ID Name	Description
1600	ICMPv6 zero length option	For any option type that has ZERO stated as its length
1601	ICMPv6 option type 1 violation	Violation of the valid length of 8 or 16 bytes.
1602	ICMPv6 option type 2 violation	Violation of the valid length of 8 or 16 bytes.
1603	ICMPv6 option type 3 violation	Violation of the valid length of 32 bytes.
1604	ICMPv6 option type 4 violation	Violation of the valid length of 80 bytes.
1605	ICMPv6 option type 5 violation	Violation of the valid length of 8 bytes.
1606	ICMPv6 short option data	Not enough data signature (when the packet states there is more data for an option than is available in the real packet)
1607	Multiple first fragment packets	Produces an alert when more than one first fragment is seen in a 30-second period.

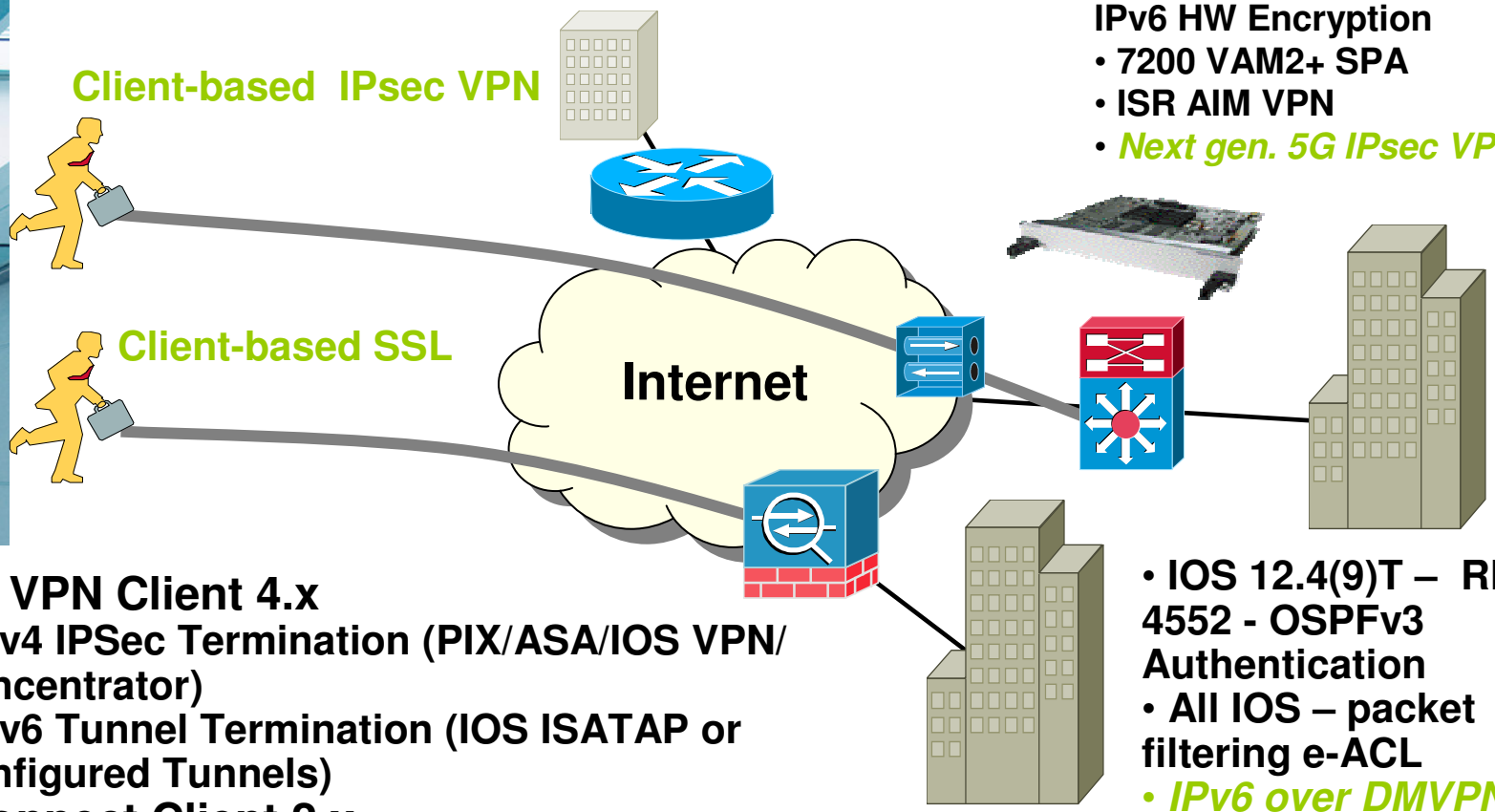
Hardening IPv6 Network Devices

- Use random bits for static host Interface ID – for router interfaces and loopbacks
  - Example: 2001:db8:100:200:ab45:92ef:7a31:7d2b
- Disable ICMPv6 Redirect messages on interfaces
  - **`no ipv6 redirect`**
- Disable ICMPv6 unreachable messages on interfaces
  - **`no ipv6 unreachables`**
- SSH works over IPv6 so use IPv6 Access-Class – Disable Telnet!
  - **`ipv6 access-list V6ACCESS`**
  - **`  permit ipv6 2001:db8:10:10::1/128 any`**
  - **`  deny IPv6 any any log-input`**
  - **`line vty 0 4`**
  - **`  ipv6 access-class V6ACCESS in`**
  - **`  transport input ssh`**
- RADIUS and TACACS+ support for IPv6
  - **`radius-server host 2001:db8:100:200::AAAA Key C1sc0123`**
  - **`tacacs-server host 2001:db8:100:200::AAAA key C1sc0123`**

IPv6 IPSec Solutions

- IPSec was first designed for IPv6 and then was added to IPv4 where it became widely deployed
- RFC 2401 mandated every IPv6 device support IPSec
- IPv6 will use more AH and ESP transport-mode implementations than IPv4/NAT
- Interoperability, global PKI, and the fact that small devices won't have the capability have stopped this from being a strict requirement
- IPSec isn't a protection against application attacks
- You may not want to allow IPSec from any to any through your firewall

Cisco IPv6 Security



IPv6 IPSec Tunnels
- **IOS 12.4(4)T**

IPv6 HW Encryption
- **7200 VAM2+ SPA**
- **ISR AIM VPN**
- ***Next gen. 5G IPsec VPN SPA***

- **Cisco VPN Client 4.x**
  - **IPv4 IPSec Termination (PIX/ASA/IOS VPN/ Concentrator)**
  - **IPv6 Tunnel Termination (IOS ISATAP or Configured Tunnels)**
- **AnyConnect Client 2.x**
  - **SSL/TLS or DTLS (datagram TLS = TLS over UDP**
  - **Tunnel transports both IPv4 and IPv6 and the packets exit the tunnel at the hub ASA as native IPv4 and IPv6.**

- **IOS 12.4(9)T – RFC 4552 - OSPFv3 Authentication**
- **All IOS – packet filtering e-ACL**
- ***IPv6 over DMVPN – 12.5T***

IPv6 Firewall
- **IOS Firewall 12.3T, 12.4, 12.4T**
- **FWSM 3.x**
- **PIX 7.x, including ASA 5500 series**

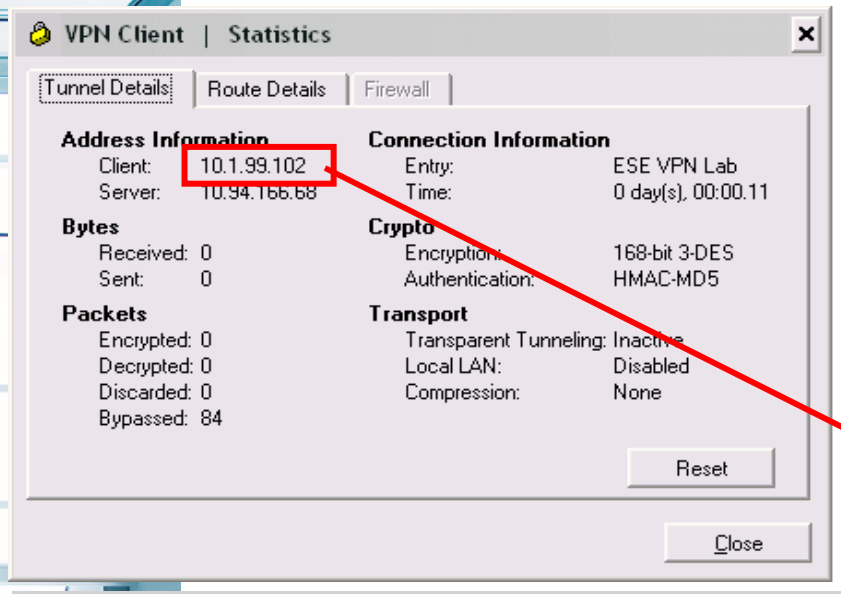
IPv6 Additional Functionality: Rel 8.2

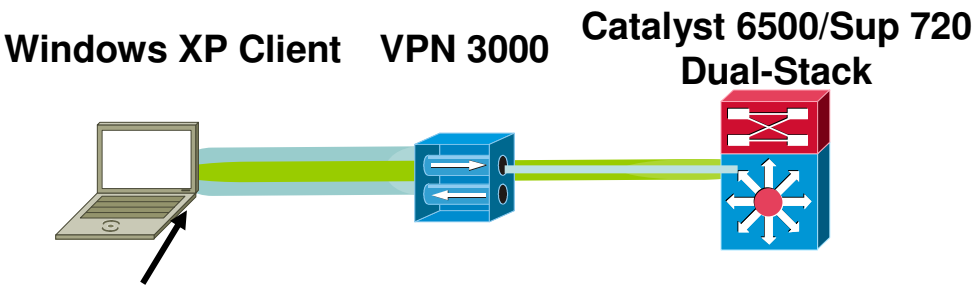
IPv6 Using Cisco VPN Client

- Microsoft Windows XP (SP1 or higher)
- IPv6 must be installed
- XP will automatically attempt to resolve the name “ISATAP”
  - Local host name
  - Hosts file—SystemRoot\system32\drivers\etc
  - DNS name query
  - NetBIOS and Lmhosts
- Manual ISATAP router entry can be made
  - **`netsh interface ipv6 isatap set router 20.1.1.1`**
- Key fact here is that NO additional configuration on the client is needed again!
- USE PREVIOUS ISATAP CONFIGURATIONS SHOWN FOR ROUTER-SIDE

Note: ISATAP is supported on some versions of Linux/BSD (manual router entry is required)

Does It Work?





10.1.99.102—VPN Address

2001:DB8:c003:1101:0:5efe:10.1.99.102—IPv6 address

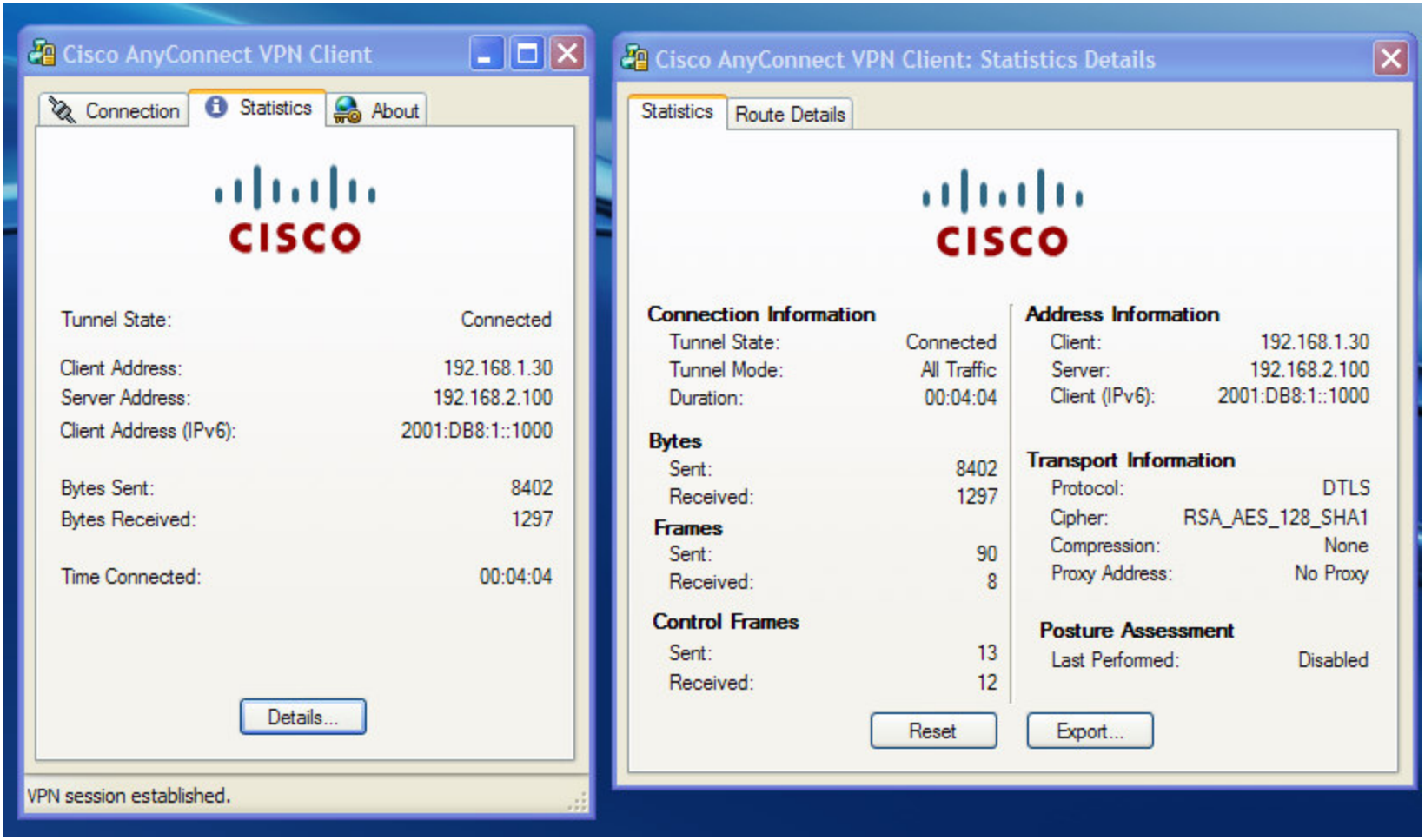
```
Interface 2: Automatic Tunneling Pseudo-Interface

Addr Type  DAD State  Valid Life   Pref. Life   Address
---------  ---------- ------------ ------------ ----------------------------
Public     Preferred   29d23h56m5s  6d23h56m5s 2001:db8:c003:1101:0:5efe:10.1.99.102
Link       Preferred   infinite     infinite   fe80::5efe:10.1.99.102
```

```
netsh interface ipv6>show route
Querying active state...

Publish  Type       Met  Prefix                    Idx  Gateway/Interface Name
-------  --------  ----  ------------------------  ---  --------------------
no       Autoconf     9  2001:db8:c003:1101::/64     2  Automatic Tunneling Pseudo-Interface
no       Manual       1  ::/0                        2  fe80::5efe:20.1.1.1
```

AnyConnect with IPv6



IPv6 Privacy Addressing

- Privacy of addresses in an issue with IPv6
  - EUI-64 addresses are derived from the host's MAC
  - That could be used to track user's activity and thus identity
- Temporary host portions of an IPv6 address intended to protect the identity of the end-user
  - MD5 hash of the EUI-64 concatenated with a random number that can change over time
  - Different implementations rotate the address at different frequencies – can be disabled
- Forensics and troubleshooting are difficult with privacy addresses
- Dynamic DNS and Firewall state will also need to update
- Difficulty creating granular firewall policy when IP addresses change often

Security for Service Providers

- Ingress/Egress Filtering - BOGON filtering
- DDOS traceback in IPv6 networks
- BlackHoles – Darknet – understanding hacker behavior with the use of a honeypot/sniffer
- 6PE is like having one large single routing table
  - Customers are not separated from each other like with IPv6 MPLS-based VPNs
  - 6PE is more like a big MPLS Internet service
- 6VPE is more like the MPLS-Based VPNs that are used with IPv4.
- Separate Routing Registry for IPv4 and IPv6

IPv6 BOGON Filtering

- Filter traffic from unallocated space and filter router advertisements of bogus prefixes
- Permit Legitimate Global Unicast Addresses
  - 2001::/16—IPv6 Unicast Addresses
  - 2002::/16 - 6to4
  - 2003::/18 - RIPE NCC
  - 2400::/12 - APNIC
  - 2600::/12 - ARIN(US DoD)
  - 2610::/23 - ARIN
  - 2620::/23 - ARIN
  - 2800::/12 - LACNIC
  - 2A00::/12 - RIPE NCC
  - 2C00::/12 – AfriNIC

Team Cymru

IPv6 BOGON Filtering

- Deny Teredo (or UDP 3544)
  - 2001:0000::/32
- Deny 6Bone
  - 3ffe::/16
- Deny Unspecified and Loopback
  - ::/128 (::/0) , ::1
- Deny Site-local Multicast or Deny All Multicasts
  - ff05::/16 or ff00::/8
- Deny Link Local Addresses
  - fe80::/10
- Deny IETF Reserved Address
  - fec0::/10
- Deny Unique-local Address
  - fc00::/7
- Deny Documentation Address
  - 2001:db8::/32
- Deny IPv4 Mapped Addresses
  - ::ffff:0.0.0.0/96
- Deny IPv4-compatible IPv6 Address
  - ::0.0.0.0/96
- Deny Other Compatible Addresses
  - ::224.0.0.0/100
  - ::127.0.0.0/104
  - ::0.0.0.0/104
  - ::255.0.0.0/104
- Deny False 6to4 Packets
  - 2002:e000::/20
  - 2002:7f00::/24
  - 2002:0000::/24
  - 2002:ff00::/24
  - 2002:0a00::/24
  - 2002:ac10::/28
  - 2002:c0a8::/32

IPv6 Security Summary

- IPv6 is no more or less secure than IPv4
  - Lack of knowledge of IPv6 is an issue
- There aren't as many security products that support IPv6 yet
- IPv6 will change traffic patterns (p2p, MIPv6)
- IPv6 larger addresses makes worms and scanning less effective but there are still ways to find hosts
- IPv6 hierarchical addressing and no NAT should reduce the anonymity of hackers and allow for full IPSec
- LAN-based attacks exist in IPv6, Physical Security, Ethernet port security, NAC, 802.1X, SEND can help
- Perform IPv6 filtering at the perimeter
- Use RFC2827 filtering and Unicast Reverse Path Forwarding (uRPF) checks throughout the network
- Use manual tunnels instead of dynamic tunnels

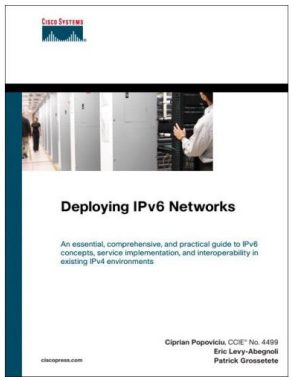
Summary of BCPs

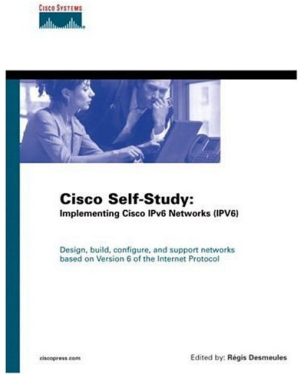
- Remember physical security
- Use a NAC/802.1X solution, disable unused switch ports, Ethernet port security
- Perform IPv6 filtering at the perimeter
- Use RFC2827 filtering and Unicast Reverse Path Forwarding (uRPF) checks throughout the network
- Use manual tunnels instead of dynamic tunnels
- Deny packets for transition techniques not in use
  - Deny IPv4 protocol 41 forwarding unless that is exactly what is intended – unless using 6to4 tunneling
  - Deny UDP 3544 forwarding unless you are using Teredo-based tunneling
- Leverage IPSec for everything possible
- Try to achieve equal protections for IPv6 as with IPv4

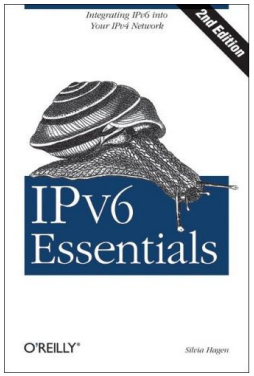
Summary

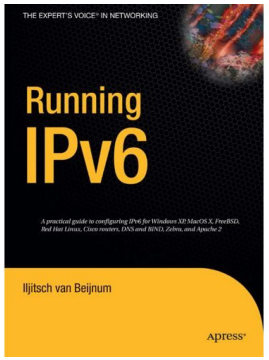
- An IPv6 transition is already underway in the Federal Government and other parts of the world.
- IPv6 infrastructure and Host OSs are ready now!
- Cisco is a leader in IPv6 and has a full-set of IPv6 products
- Much of the infrastructure you have already purchased is IPv6 capable, it's just a matter of enabling (software upgrade)
- GTRI can assist with transition planning
  - Perform your assessment
  - Create a migration strategy
  - Create a test lab or leverage other test labs and start experimenting.
  - Dual Stack some of your systems
  - Test DNS and focus on your other applications
- The sooner we begin the transition, the sooner we will be done.

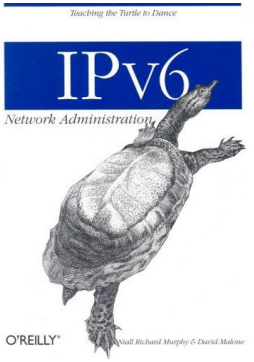
IPv6 Books

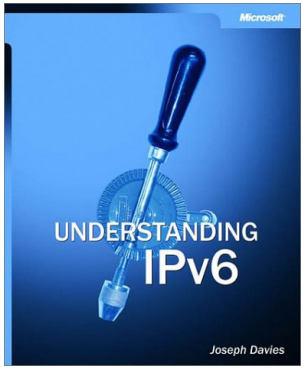












Resources

- IETF v6ops Working Group
  - http://www.ietf.org/html.charters/v6ops-charter.html
- Microsoft
  - http://www.microsoft.com/ipv6
- Cisco IPv6 SRND Guides for Branch and WAN
  - http://www.cisco.com/go/srnd
- S. Convery & D. Miller, “IPv6 and IPv4 Threat Comparison and Best-Practice Evaluation”, v1.0, Cisco Systems Technical Report, March 2004
  - http://www.cisco.com/security_services/ciag/documents/v6-v4-threats.pdf
- North American IPv6 Task Force (NAv6TF) Technology Report, “IPv6 Security Technology Paper”, by Merike Kaeo, David Green, Jim Bound, Yanick Pouffary
  - http://www.nav6tf.org/documents/nav6tf.security_report.pdf
- NSA SNAC Guide for IPv6
  - http://www.nsa.gov/snac/downloads_cisco.cfm?MenuID=scg10.3.1

Rocky Mountain IPv6 Task Force

- Regional “chapter” of North American IPv6 Task Force
- Our Charter
  - Provide Education on IPv6 and its benefits
  - Promotion of IPv6 technology
  - Research and Development and showcase IPv6 technology and services
  - Put on local IPv6-focused events
  - Work to further the use of IPv6 with a regional focus
- Get involved in your regional/national IPv6 organizations
  - www.RMv6TF.org
  - www.MidAtlanticv6tf.org
  - www.cav6tf.org

Question and Answer

Q:

&

A:

SHogg@GTRI.com
Scott@HoggNet.com
Mobile: 303-949-4865