IPv6 Security Considerations

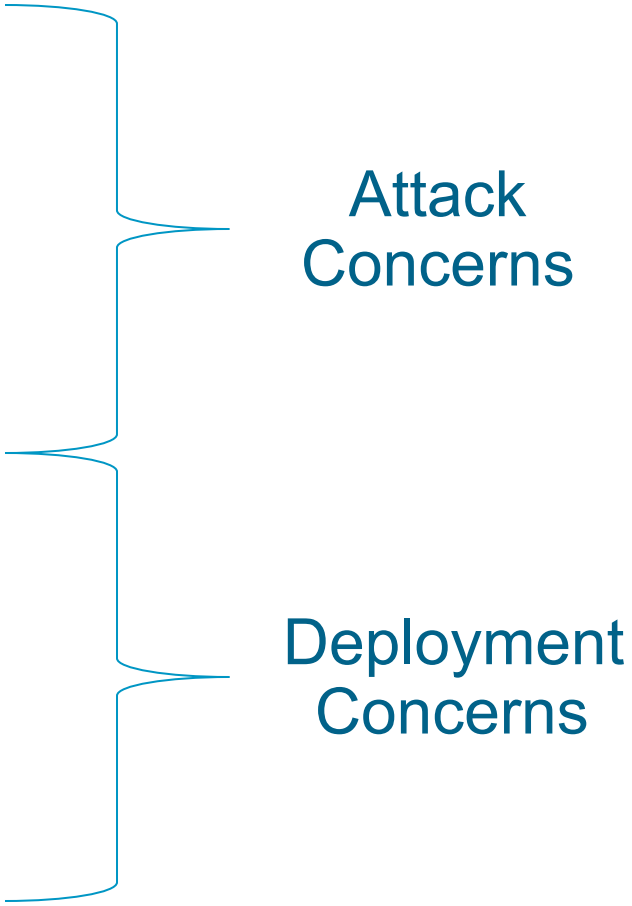
Earl Carter

Cisco Services.

Making Networks Work.
Better Together.

Agenda

- Introduction
- Threat Landscape
- IPv6 Known Attack Vectors
- Coexistence Issues
- Attacker Tools
- Host Discovery
- Identifying Known Vulnerabilities
- Identifying Malicious Traffic
- Verifying Configurations



My Background

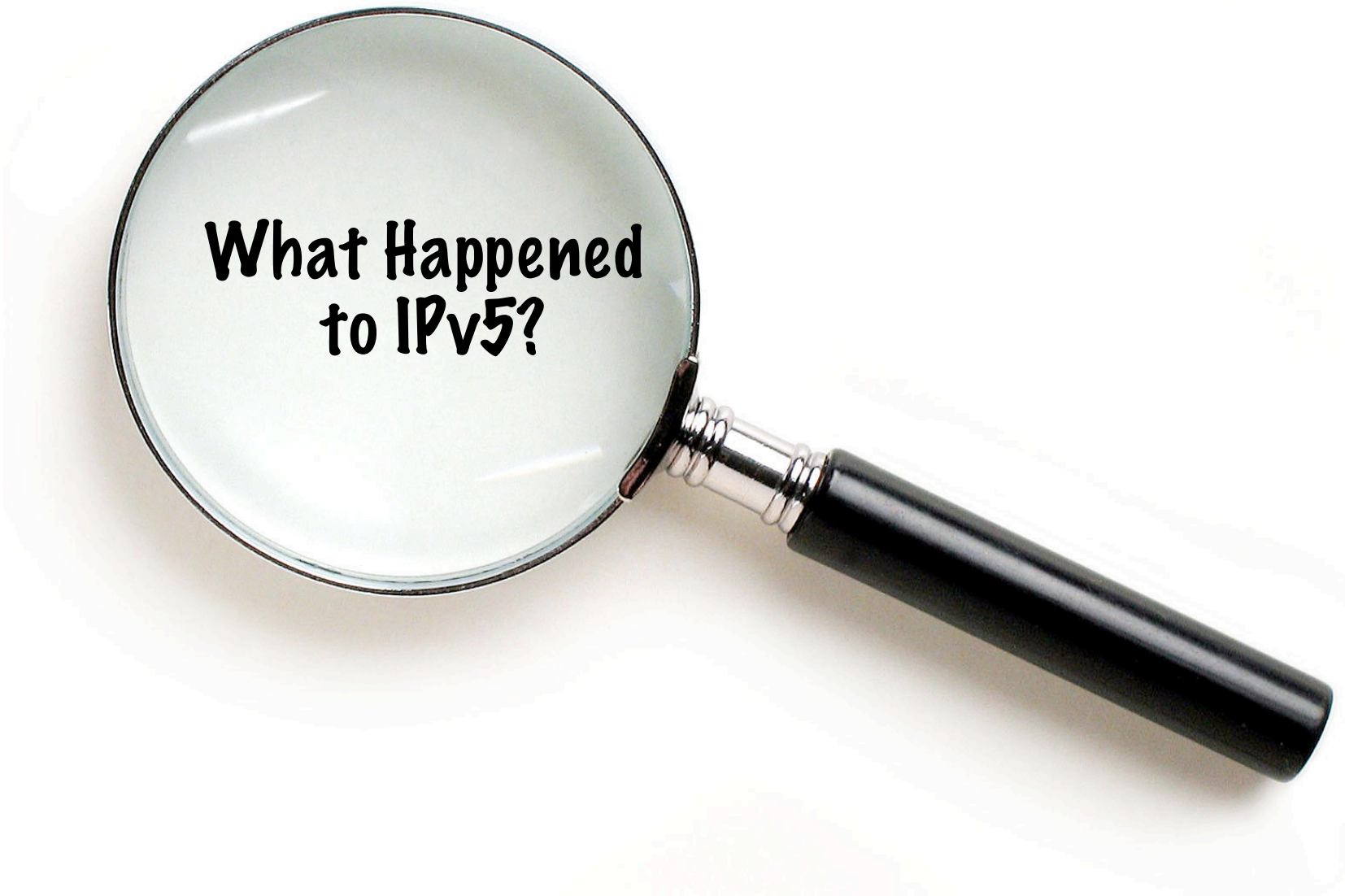
- Security Researcher for 15 years

  Security Geek not a Product Expert

- Currently Evaluate Cisco Products for Security Issues
- Written Several Security Books
- Working on IPv6 Security Training Inside Cisco
- Working on IPv6 Security Testing Inside Cisco

Agenda

- Introduction
- Threat Landscape
- IPv6 Attack Vectors
- Coexistence Issues
- Attacker Tools
- Host Discovery
- Identifying Known Vulnerabilities
- Identifying Malicious Traffic
- Verifying Configurations



Threat Landscape

November 2008

May 2009

http://advosys.ca/viewpoints/2009/05/the-coming-ipv6-security-disaster/

http://www.fiercevoip.com/story/arbor-networks-voip-ipv6-emerging-security-threats/2008-11-11?utm_medium=rss&utm_source=rss&cmp-id=OTC-RSS-FV0

Why is IPv6 Migration Slow?

- IPv6 Standards Released in 1999
- Cool Features of IPv6 Already Migrated to IPv4

  IPSec

  DHCP
- Main Reason to Migrate is No More Addresses

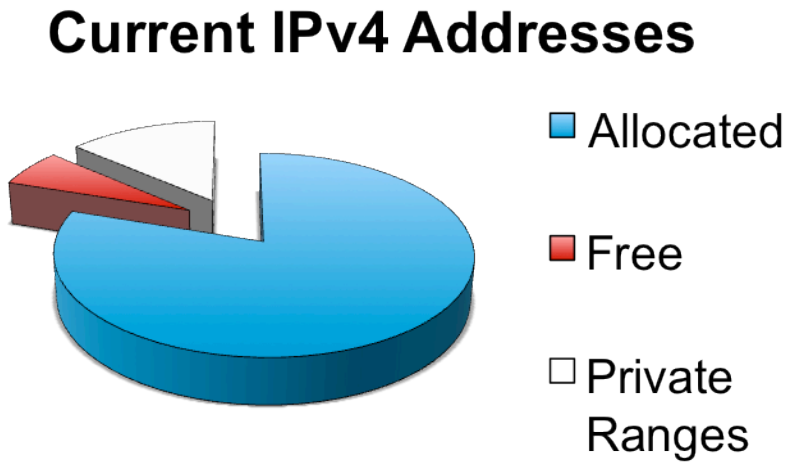
Why is IPv6 Security Important Now?

- IPv4 Addresses Expected to Run Out Next Year

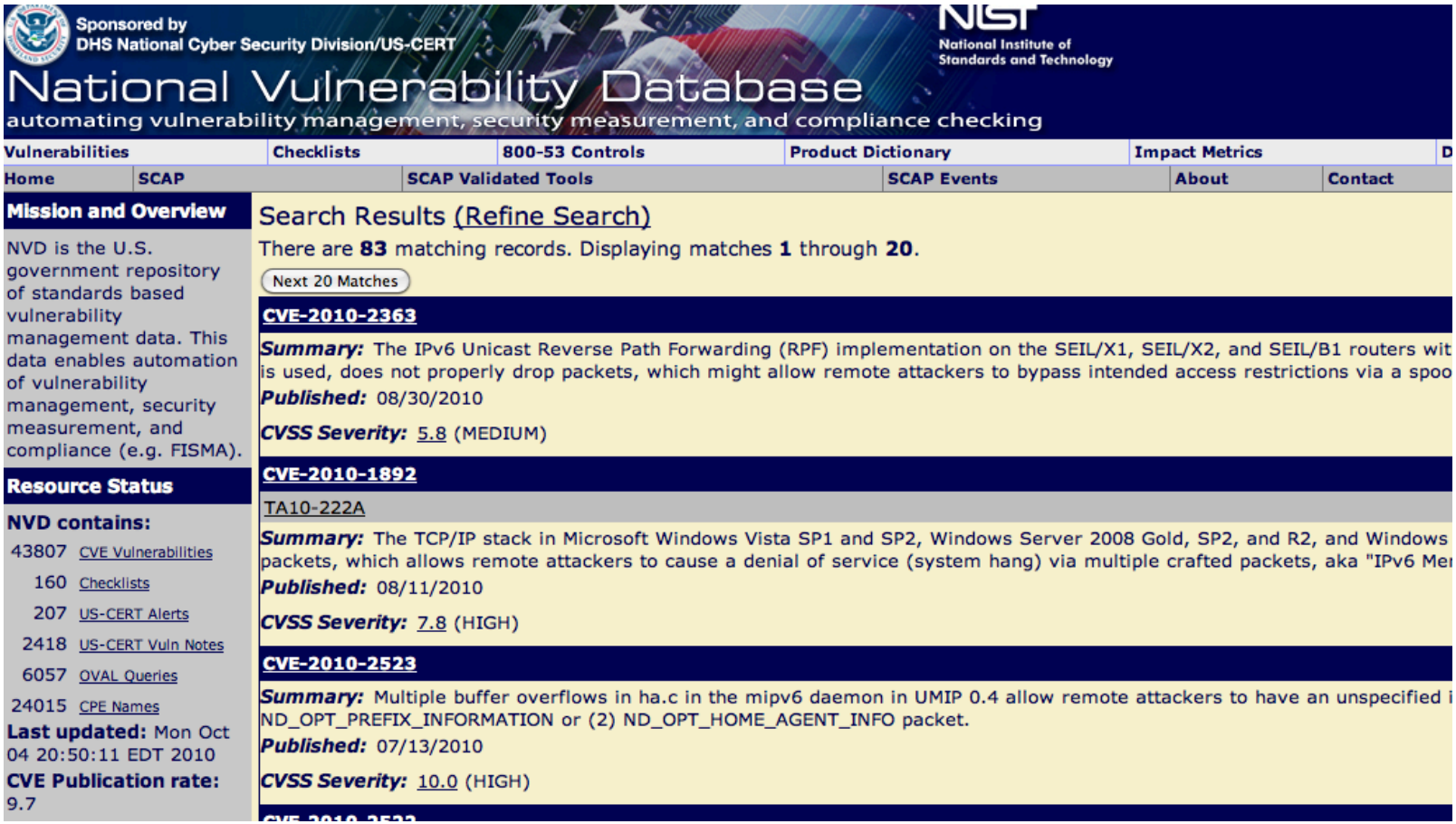
  John Curran (President of ARIN)

  Only 16 /8s left (6%)

- Still Long Transition Period



Threat Landscape



http://web.nvd.nist.gov/view/vuln/search-results?cid=2

IPv6 Security – Hype vs Fact

- Mandatory IPSec
  - Configuration Complexity
  - Key Management

IPSec Not Widely Deployed

- ARP Issues Are Gone
  - Neighbor Discovery
  - Router Discovery

Now We Have NDP Spoofing

IPv6 Security

Routing Protocol Authentication

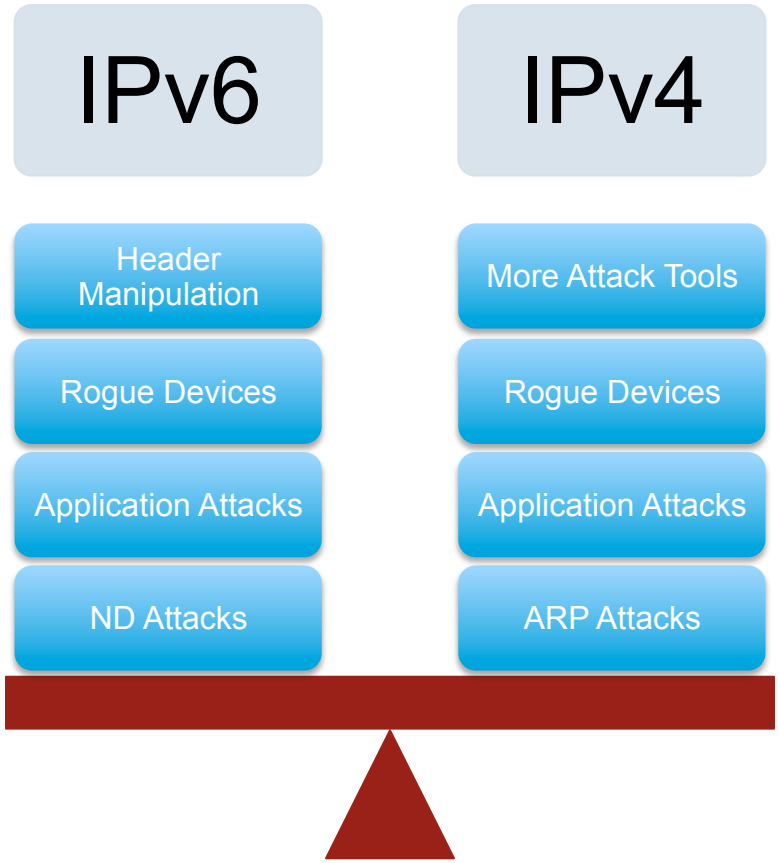
- BGP, ISIS, EIGRP no change:

  Use MD5 authentication of the routing update

- OSPFv3, RIPng and PIM have changed:

  Rely on IPSec for Authentication

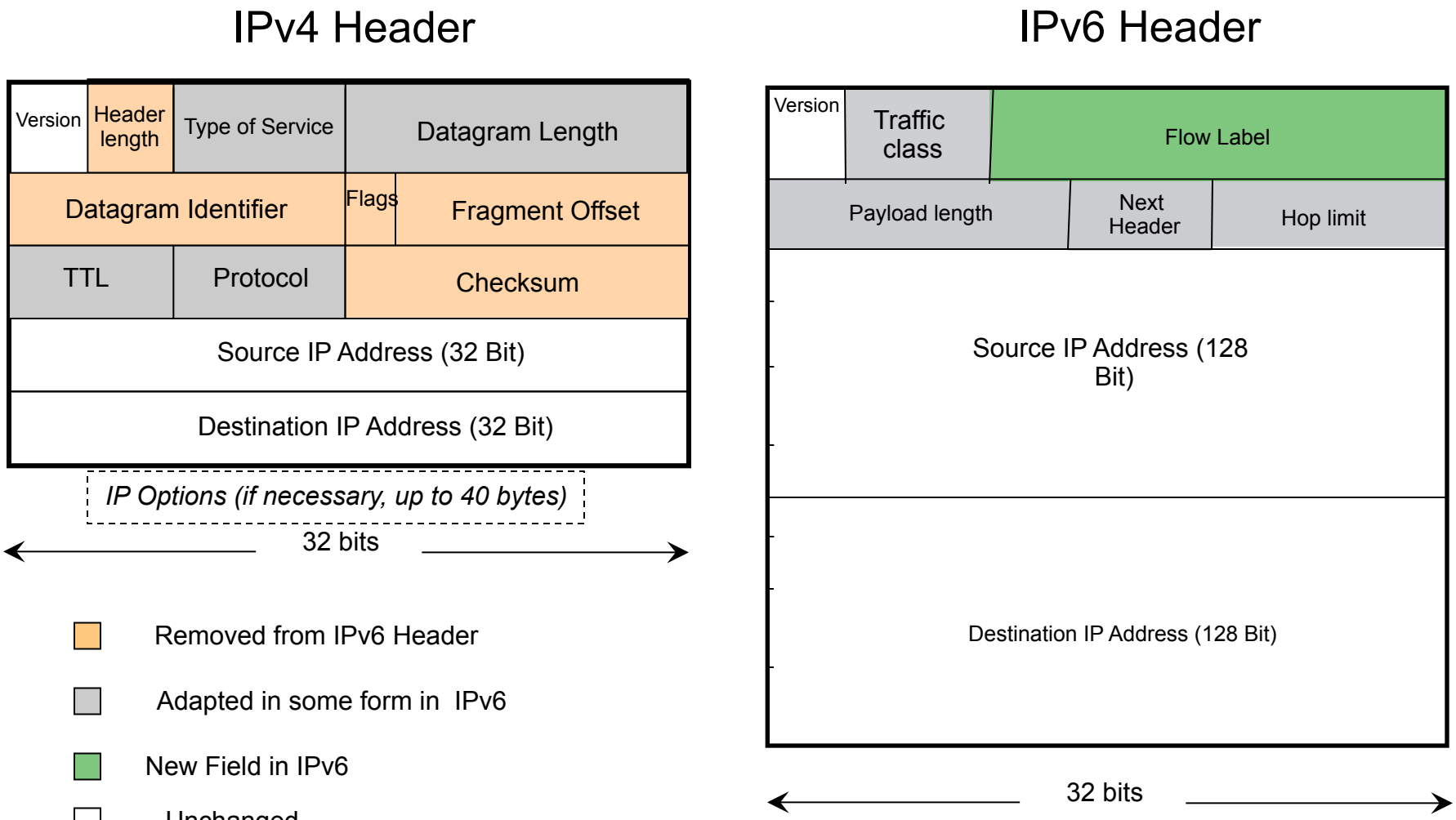
Which is more secure?



Agenda

- Introduction
- Threat Landscape
- IPv6 Known Attack Vectors
- Coexistence Issues
- Attacker Tools
- Host Discovery
- Identifying Known Vulnerabilities
- Identifying Malicious Traffic
- Verifying Configurations

IPv6 Protocol Overview



IPv6 Protocol Overview

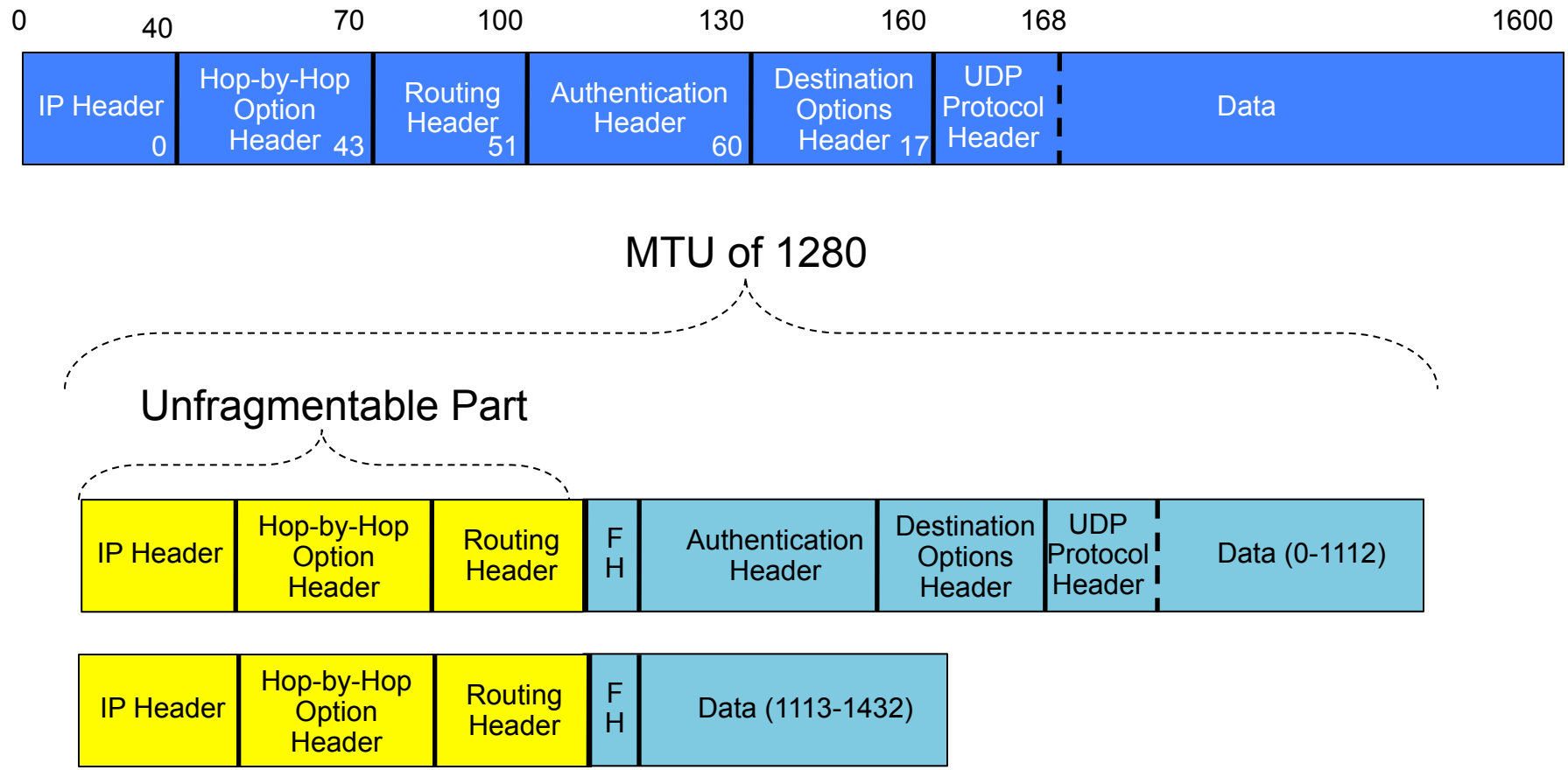
Extension Header Types

0	Hop-by-hop Option
43	Routing
44	Fragment
50	Encapsulating Security Payload (ESP)
51	Authentication Header
59	**No Next Header (null)**
60	Destination Option
62	Mobility Header

6	TCP Protocol
8	EGP Protocol
9	IGP Protocol
17	UDP Protocol
46	RSVP Protocol
47	GRE Protocol
58	ICMP Protocol

IPV6 Protocol Overview

Extension Headers & Fragmentation



Routers do not Fragment in IPv6 (Only Initiating Host)

IPv6 Protocol Overview

Recommended Extension Header Order (RFC 2460)

- IPv6 Header
- * Hop-by-Hop Options Header
- Destination Options Header
- Routing Header
- Fragment Header
- Authentication Header
- Encapsulating Security Payload Header
- Destination Options Header
- Upper Layer Header

Note: Recommended order according to RFC 2460. (Hop-by-hop Options must be 1st)

IPv6 Protocol Attacks

IPv6 Header Manipulation

- Complex Stack
  - Prone To Implementation Errors
- Unlimited size of header chain (spec-wise) can make filtering difficult
- Potential DoS
  - More boundary conditions to exploit
  - Can I overrun buffers with a lot of extension headers?
- Potential ACL Bypasses
  - Searching for Transport Header
  - Surpassing HW buffers

RFC1858 –" Security Considerations for IP Fragment Filtering" Does not Work for IPv6

IPv6 Protocol Attacks

Hop-by-Hop Extension Header and CPU

- Can it be filtered?
- Usually requires punting to CPU
- Potential DoS vector

IPv6 Protocol Overview

Types of IPv6 Addresses

- Unicast
  - One address on a single interface
  - Delivery to single interface
- Multicast
  - Address of a set of interfaces
  - Delivery to all interfaces in the set
- Anycast
  - Address of a set of interfaces
  - Delivery to a single interface in the set (*closest*)

No broadcast addresses

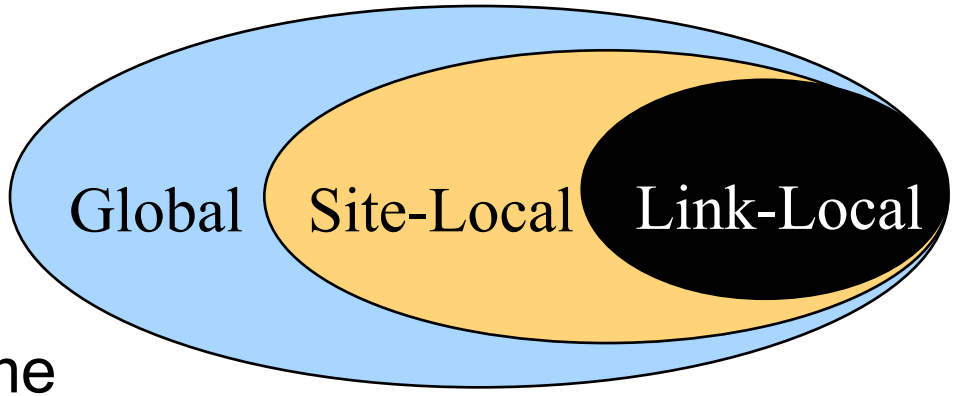
IPv6 Protocol Overview

IPv6 Address Model

Addresses are assigned to interfaces
change from IPv4 model :
Interface 'expected' to have multiple addresses

Addresses have scope
- Link Local
- Site Local (*Deprecated*)
- Global

Addresses have lifetime
- Valid and Preferred lifetime



IPv6 Protocol Overview

Address Type Prefixes

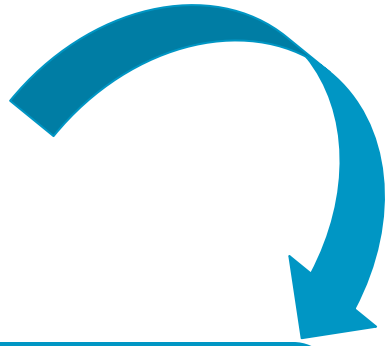
Address type	Binary prefix	
IPv4-compatible	0000...0 (96 zero bits)	
global unicast	001	(2000-3FFF)
link-local unicast	1111 1110 10	(FE80-FEBF)
site-local unicast	1111 1110 11	(FEC0-FEFF)
multicast	1111 1111	(FF)

- All other prefixes reserved (approx. 7/8ths of total)
- Anycast addresses use unicast prefixes

Traffic Filtering in IPv6

- Firewall Rules Need to Change for ICMP
- Harder to verify configuration
- Privacy Addresses Change Over Time
- More complex ACLs

IOS has implicit permit for ND



```
permit icmp any any nd-na
permit icmp any any nd-ns
deny ipv6 any any
```

IPv6 Protocol Overview

ICMPv4 vs. ICMPv6

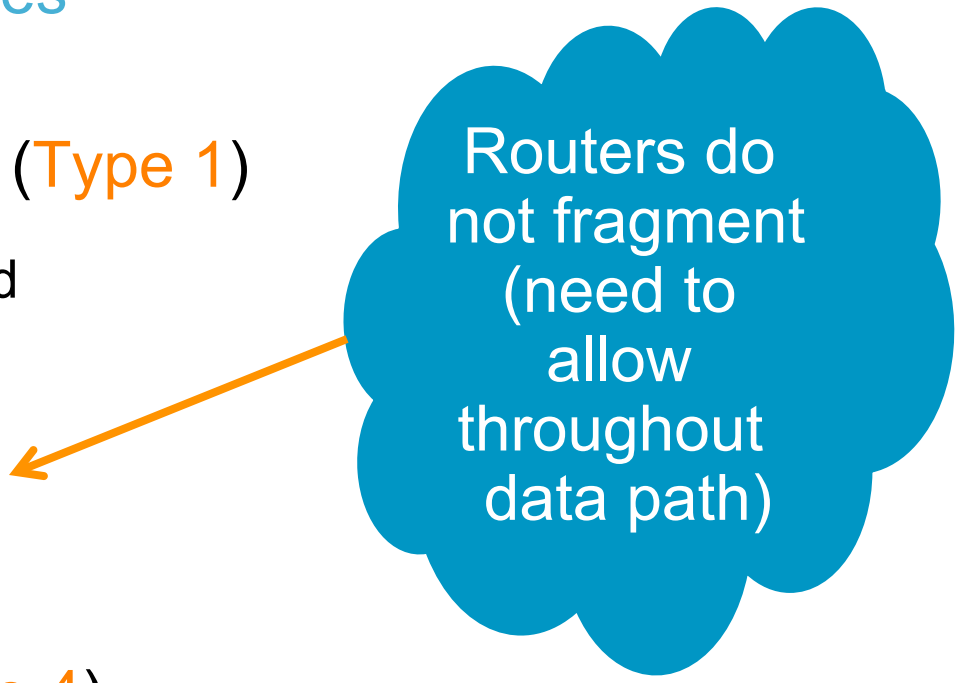
- Firewall Rules need to change
- ICMP is necessary for network operation

ICMP Message Type	ICMPv4	ICMPv6
Connectivity Checks	X	X
Informational/Error Messaging	X	X
Fragmentation Needed Notification	X	X
Address Assignment		X
Address Resolution		X
Router Discovery		X
Multicast Group Management		X
Mobile IPv6 Support		X

IPv6 Protocol Overview

ICMP Error Message Types

- Destination Unreachable (Type 1)
  - No route
  - Administratively prohibited
  - Address unreachable
  - Port unreachable
- Packet Too Big (Type 2)
- Time Exceeded (Type 3)
- Parameter Problem (Type 4)
  - Erroneous header field
  - Unrecognized next header type
  - Unrecognized option



IPv6 Protocol Attacks

ARP Spoofing is now NDP Spoofing

- All ICMP – No Authentication
- Static Host Entries Replaced by Dynamic Ones
- Route Manipulation
  - Rogue RA (Malicious or not)
  - Redirection Messages
- Local Traffic Redirection
- DoS Utilizing Duplicate Address Detection

Note: Hop Count of 255 Enforced to Limit External Attacks

IPv6 Protocol Overview

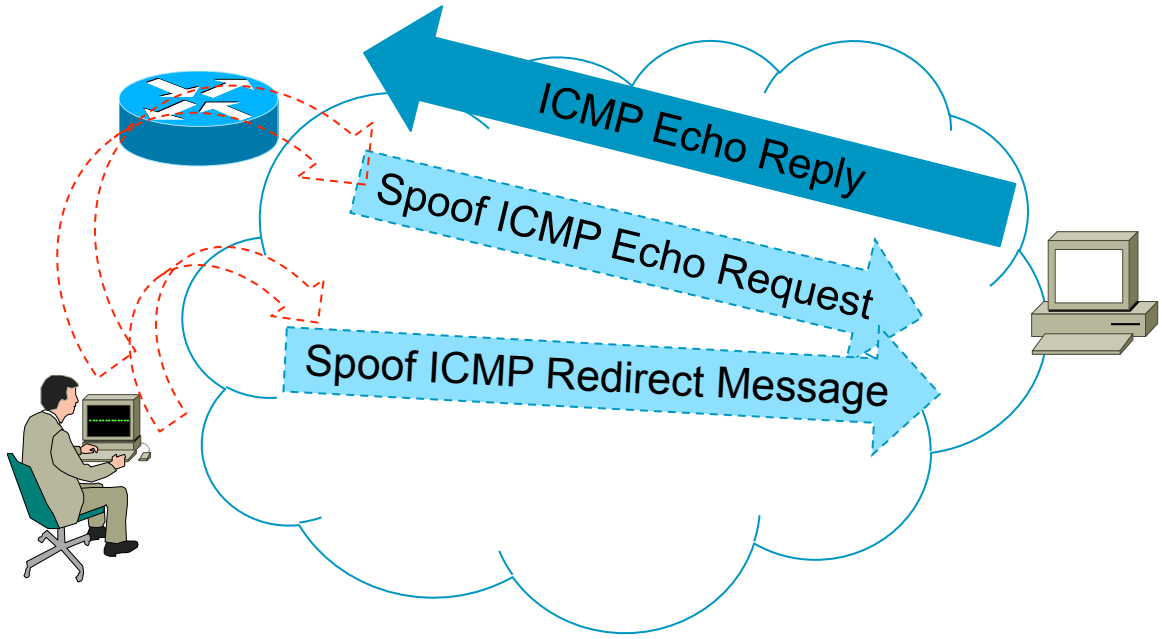
Route Redirection

- Redirection
  - ICMP Type 137
  - Redirects contain the link-layer address of the new first hop
  - Hosts learn all on-link prefixes from Router
  - Recipient of an IPv6 redirect assumes that the new next-hop is on-link
  - Inform hosts of better next-hop address

IPv6 Protocol Attacks

ICMP Redirect (ICMP Type 137)

- Requires Packet That Caused Redirect
- This Can Easily Be Bypassed



IPv6 Protocol Overview

RFC 2461 - Neighbor Discovery for IP Version 6

- Router Discovery
- Prefix Discovery
- Parameter Discovery
- Neighbor Discovery
- Automatic Address Configuration
- Duplicate Address Dedication (DAD)
- Neighbor Un-reachability Detection
- Redirection

Benefits

- No need to configure a "netmask"
- Enables Address Auto-configuration
- Routers can advertise an MTU

Note: These services depend on ICMPv6 to operate

IPv6 Protocol Overview

Router Discovery

- Router Solicitation (RS)
  - ICMP Type 133
  - Used to Request Router Advertisement
  - Sent to FF02::2 (all routers multicast address)
- Router Advertisement (RA)
  - ICMP Type 134
  - Contains prefixes, suggested hop count, MTU, etc
  - Sent to all-nodes multicast address (FF02::1) or specific host

IPv6 Protocol Overview

Neighbor Discovery

- Neighbor Solicitation (NS)

  ICMP Type 135

  Determine the link-layer address of a neighbor

  Determine if neighbor is still reachable (via cached address)

  Used for Duplicate Address Detection

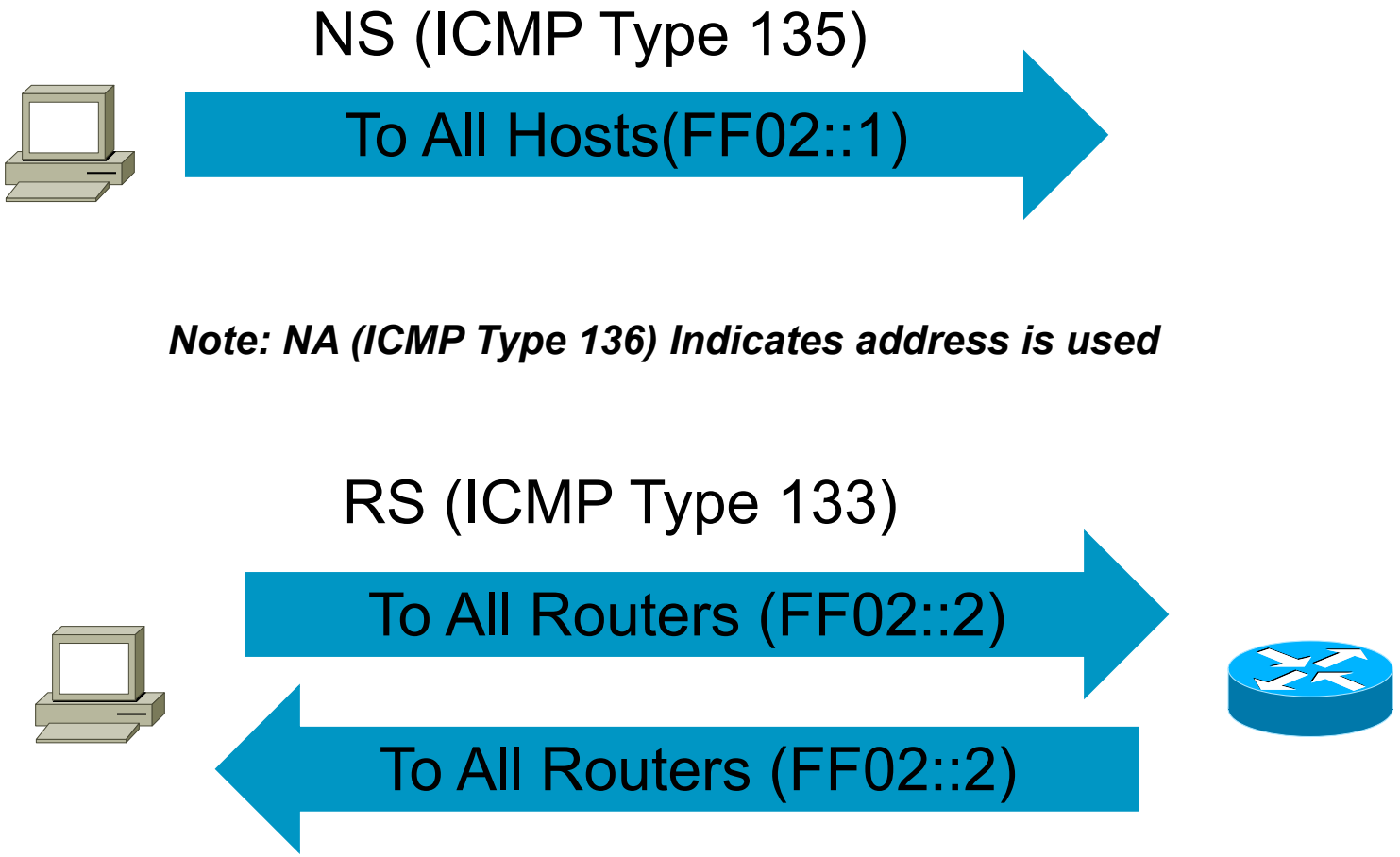
- Neighbor Advertisement (NA)

  ICMP Type 136

  Response to a NS Message

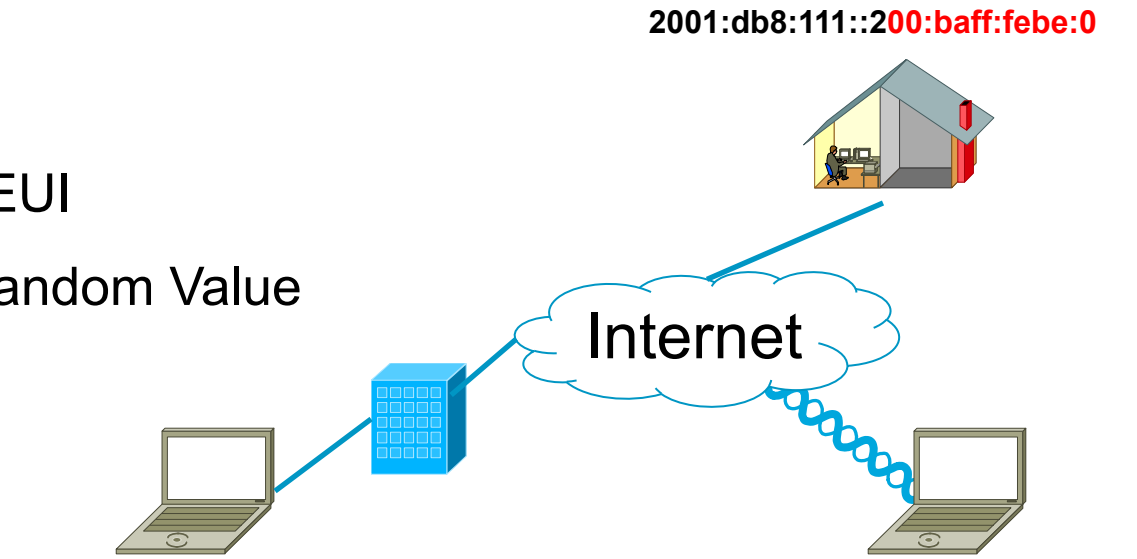
  Announce a link-layer address change

IPv6 Stateless Address Configuration



IPv6 Address Privacy Concerns

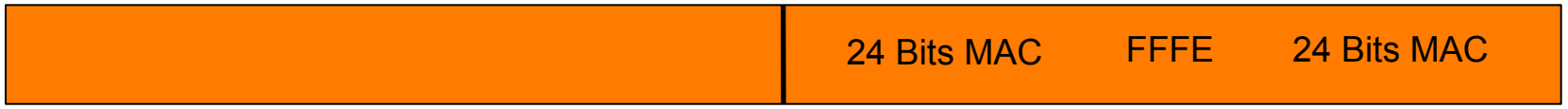
- RFC 4941
  - Message Digest of EUI
  - Concatenate with Random Value



MAC: 0000.BABE.0000

Network Identifier – 0000ba + fffe + be0000

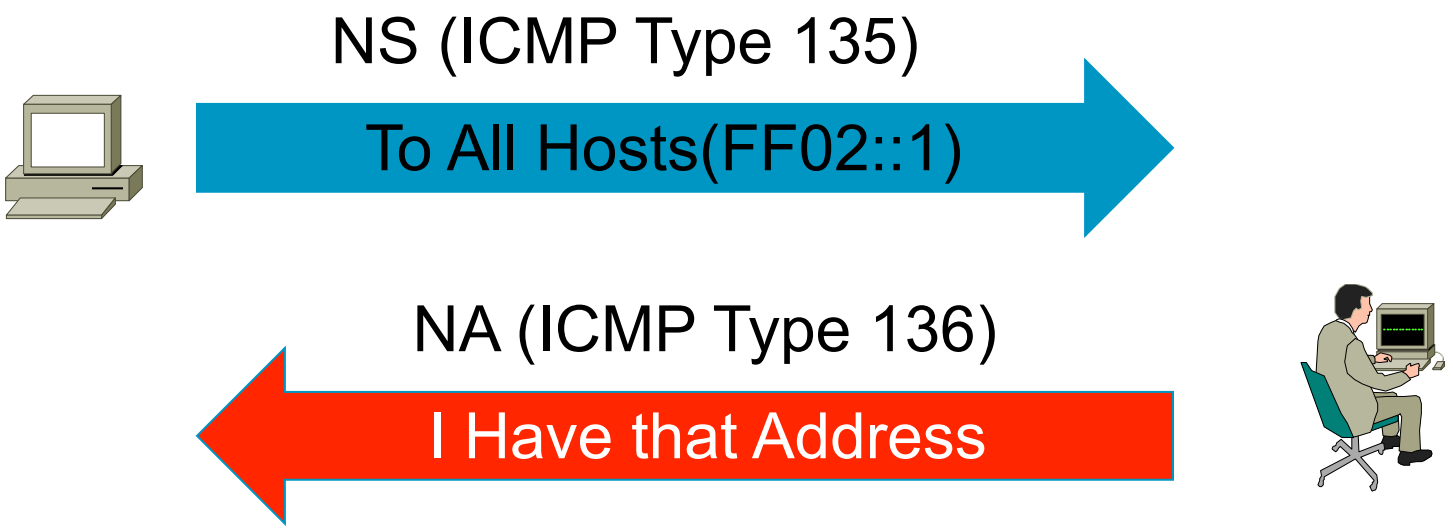
Same Regardless of Network Prefix



Network Prefix **Interface Identifier**

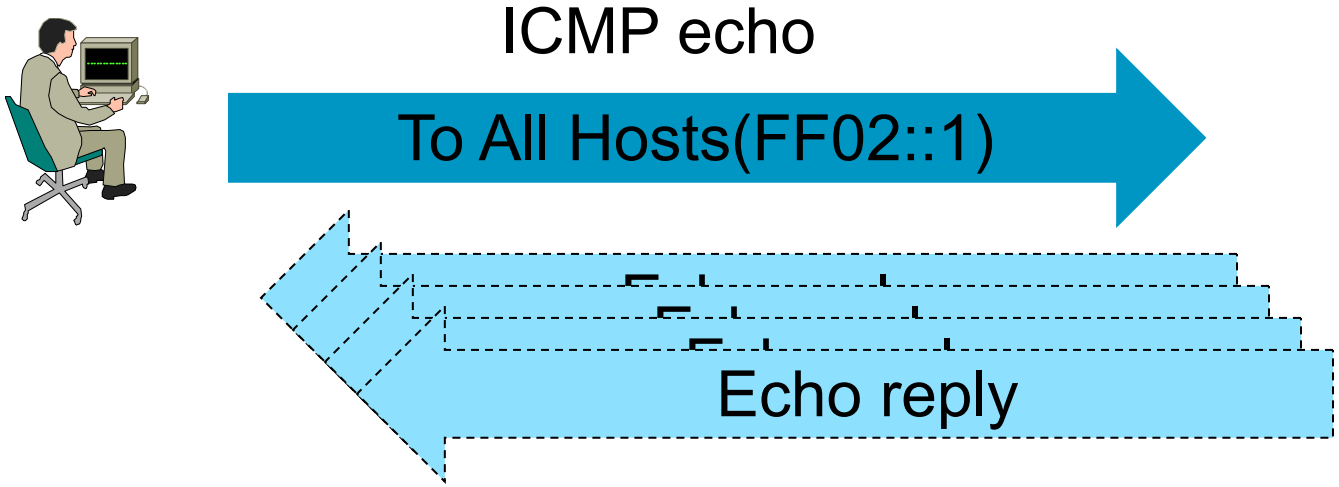
RFC 4941 – Privacy Extensions for Stateless Address Autoconfiguration

IPv6 DAD DoS Attack



Note: Duplicate Address Detection (DAD) Applies to all addresses if interface is configured for DupAddrDetectTransmits (including Stateful Addresses)

IPv6 Local Host Scan



- ICMP Echo Request

  Reply can be disabled

- IPv6 Packet with Unknown Header
- IPv6 Packet with Unknown hop-by-hop Option

IPv6 Auto-Configuration

- Stateless (RFC2462)

  Host autonomously configures its own Link-Local address

  Router solicitations are sent by booting nodes to request RAs for configuring the interfaces.

- Stateful

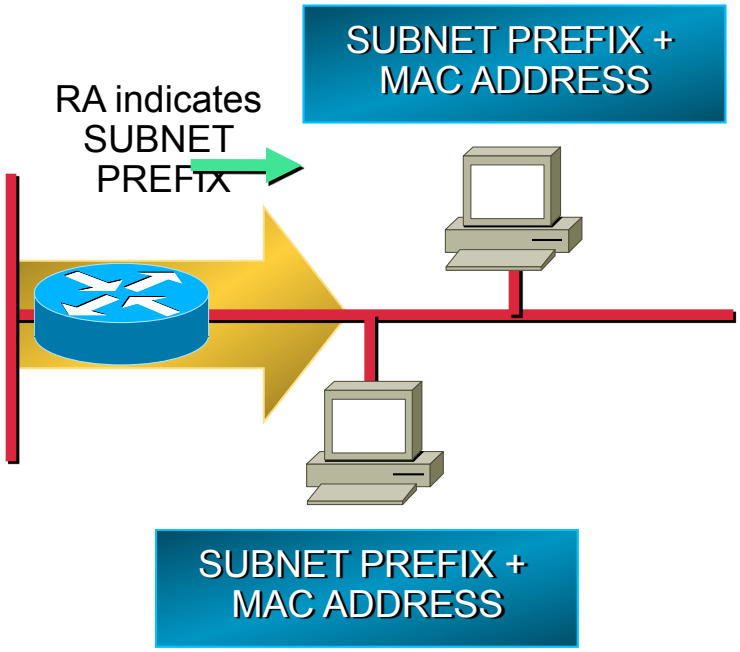
  DHCPv6

  Tighter Control of Addressing

- Renumbering

  Hosts renumbering is done by modifying the RA to announce the old prefix with a short lifetime and the new prefix.

  Router renumbering protocol (RFC 2894), to allow domain-interior routers to learn of prefix introduction / withdrawal



At boot time, an IPv6 host build a Link-Local address, then its global IPv6 address(es) from RA

IPv6 Protocol Overview

Secure Neighbor Discovery (SEND) - RFC 3971

- Certification paths

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

- Cryptographically Generated Addresses (CGA)

  IPv6 addresses whose interface identifiers are cryptographically generated

- RSA signature option

  Protect all messages relating to neighbor and router discovery

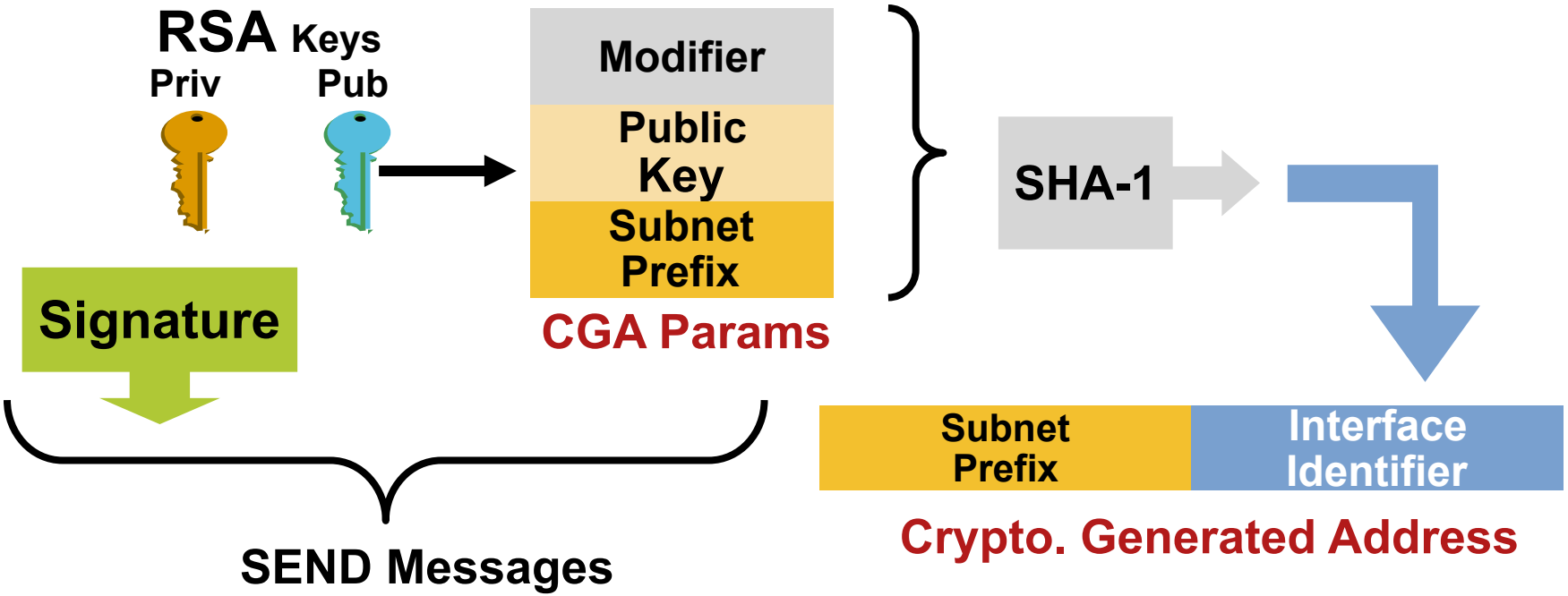
- Timestamp and nonce options

  Prevent replay attacks

IPv6 Protocol Overview

CGA RFC 3972 (Simplified)

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

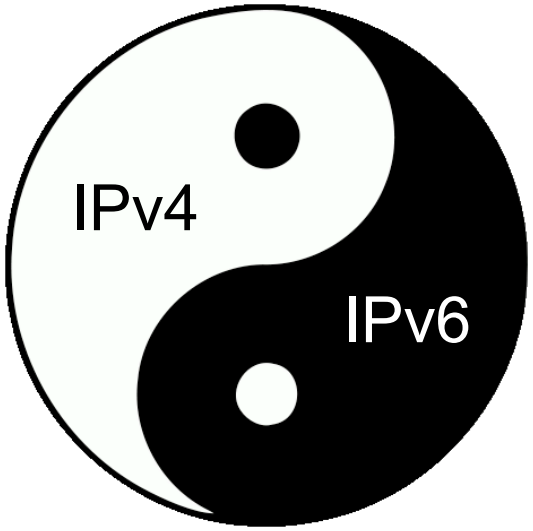


Issues With SEND

- Not Supported by All Devices
- Network Must Support All Devices on It
- Only Prevents Spoofing Already Known Hosts
- Does not Limit Who Can Generate ICMP
  - Router Advertisements (RAs)
  - Neighbor Announcements (NAs)

Agenda

- Introduction
- Threat Landscape
- IPv6 Known Attack Vectors
- Coexistence Issues
- Attacker Tools
- Host Discovery
- Identifying Known Vulnerabilities
- Identifying Malicious Traffic
- Verifying Configurations

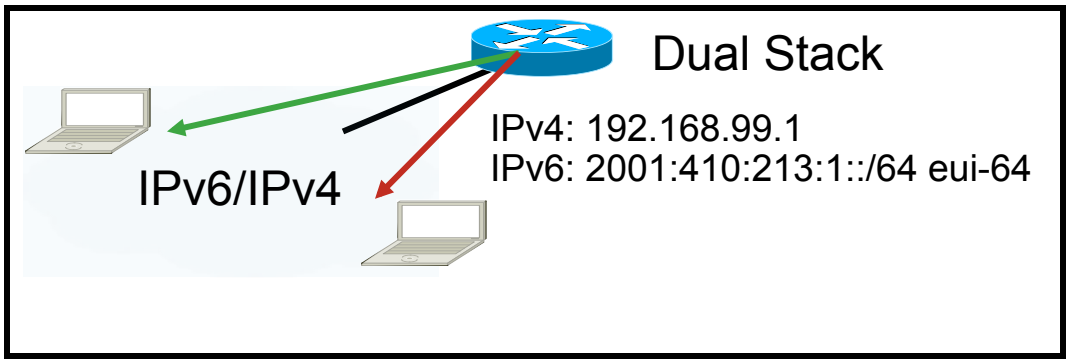


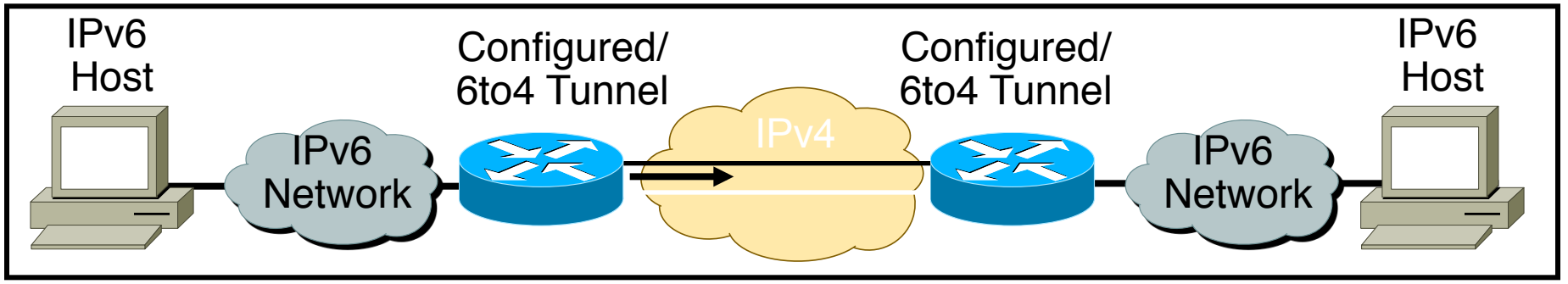
IPv6 Protocol Overview

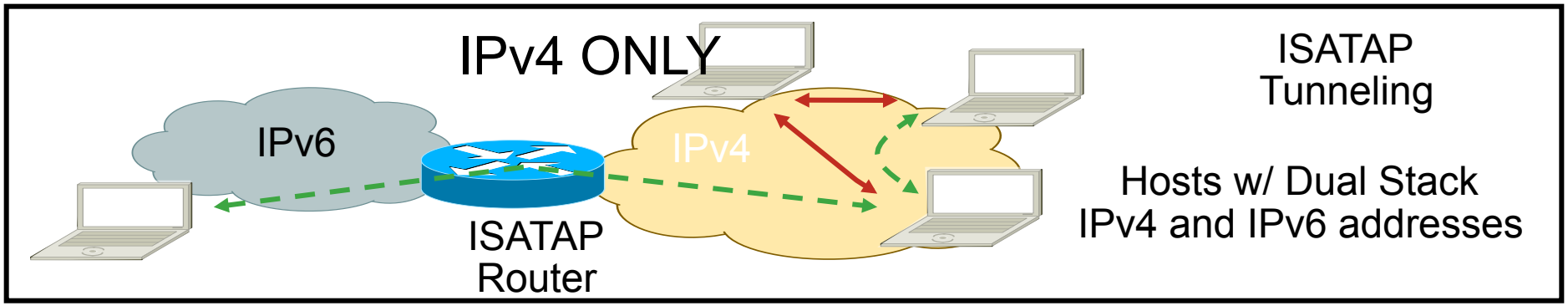
Transitioning between IPv4 & IPv6

- Numerous Methods
- Dual Stack
  - Must consider security for both protocols
  - IPv6 functionality can be automatically enabled
- Tunnels
  - Can potentially bypass firewall rules (uses protocol 41 or UDP)
  - Minimal setup

IPv6 Transition Methods







IPv6 Protocol Attacks

Dual Stack Host Considerations

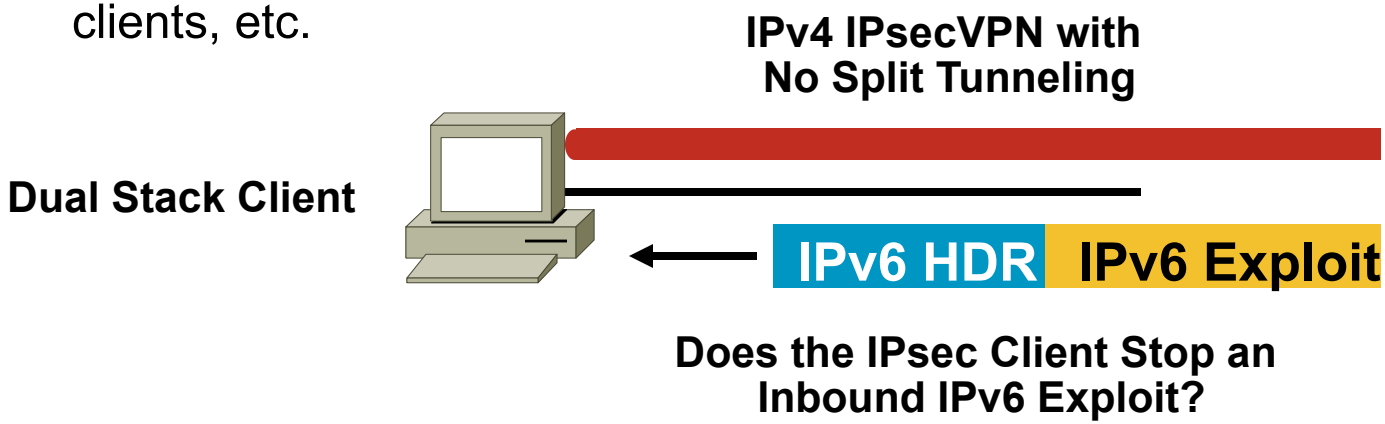
- Host security on a dual-stack device

  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.



IPv6 Protocol Attacks

Dual Stack with Enabled IPv6 by Default

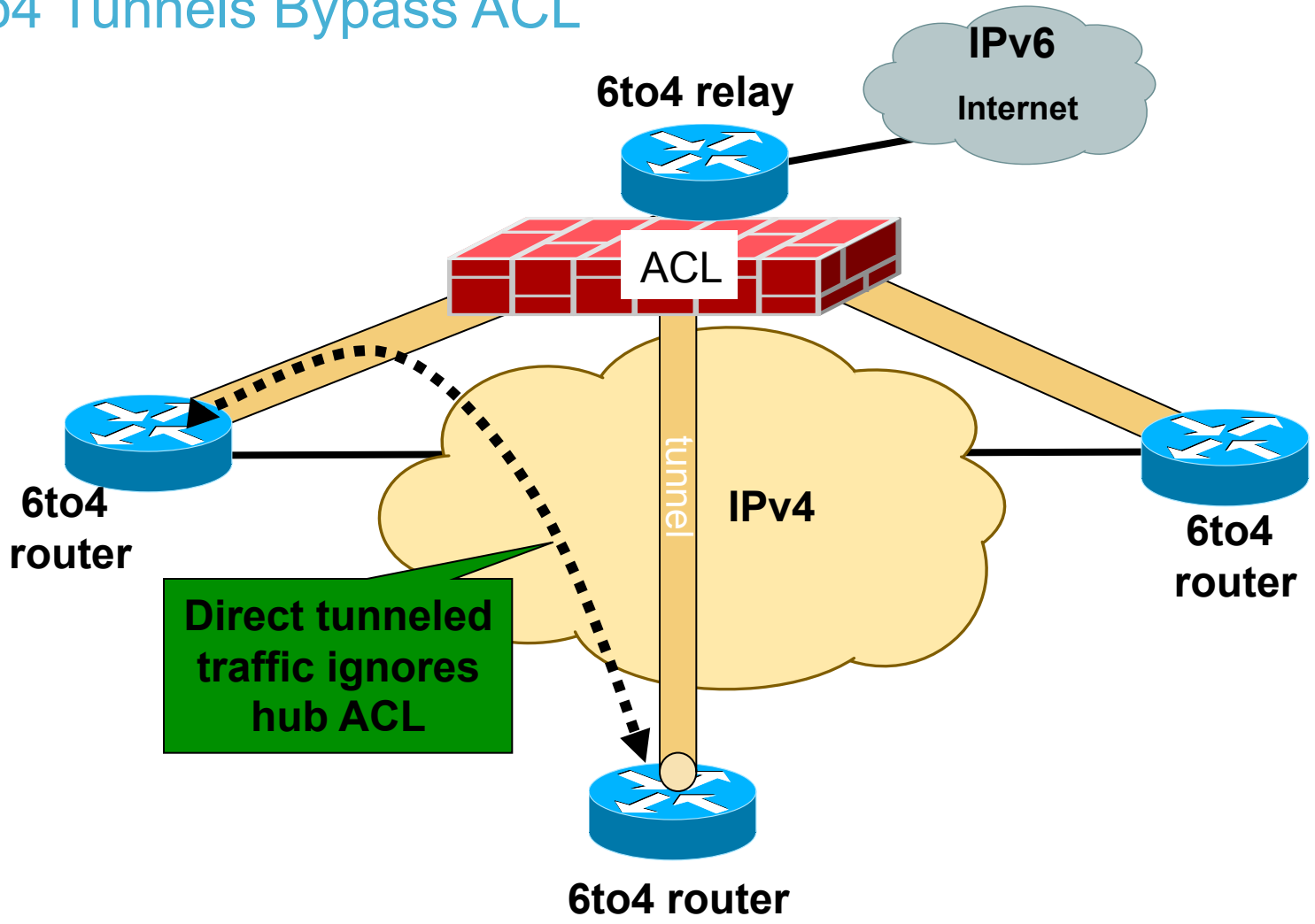
- Your host:
  - IPv4 is protected by your favorite personal firewall...
  - IPv6 is enabled by default (Vista, Linux, Mac OS/X, ...)
- Your network:
  - Does not run IPv6
- Your assumption:
  - I'm safe
- Reality (You are **not** safe)
  - Attacker sends Router Advertisements
  - Your host configures silently to IPv6
  - You are now under IPv6 attack

IPv6 Tunnel Attacks

- Tunneling Mechanisms
  - No Built-in Security
  - No Authentication
  - No Integrity Check
  - No Confidentiality
- Attacks
  - Tunnel Injection
  - Tunnel Sniffing

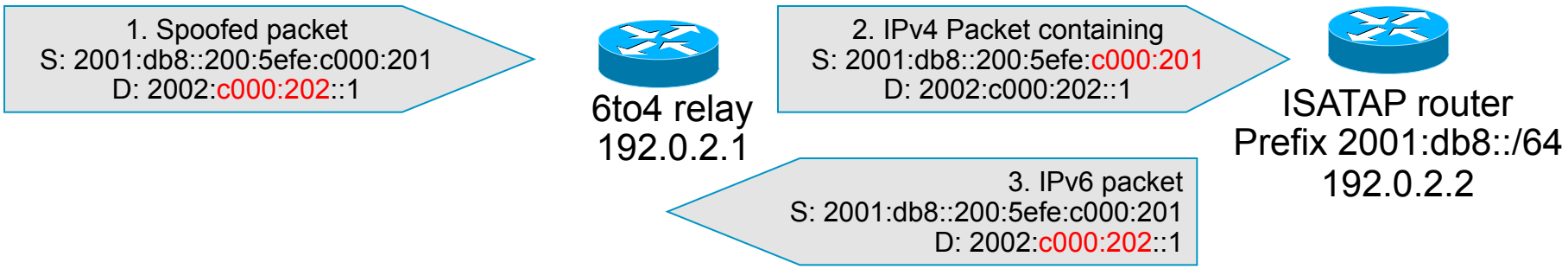
IPv6 Protocol Attacks

6to4 Tunnels Bypass ACL



IPv6 Protocol Attacks

Looping Attack Between 6to4 and ISATAP



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

Agenda

- Introduction
- Threat Landscape
- IPv6 Known Attack Vectors
- Coexistence Issues
- Attacker Tools
- Host Discovery
- Identifying Known Vulnerabilities
- Identifying Malicious Traffic
- Verifying Configurations

IPv6 Attack Tools

- Attackers Have Various Types of Tools
  - Exploit Frameworks
  - Vulnerability Scanners
  - Browser Plugins
- Some Tools Are Now Less Effective
  - Like Remote Scanners

IPv6 Attack Tools

- IPv6 Support != Same Functionality
- Network Scanners
  - Nmap Now Mainly Used for Open Ports
- Vulnerability Scanners
  - Does It Scan for IPv6 Issues

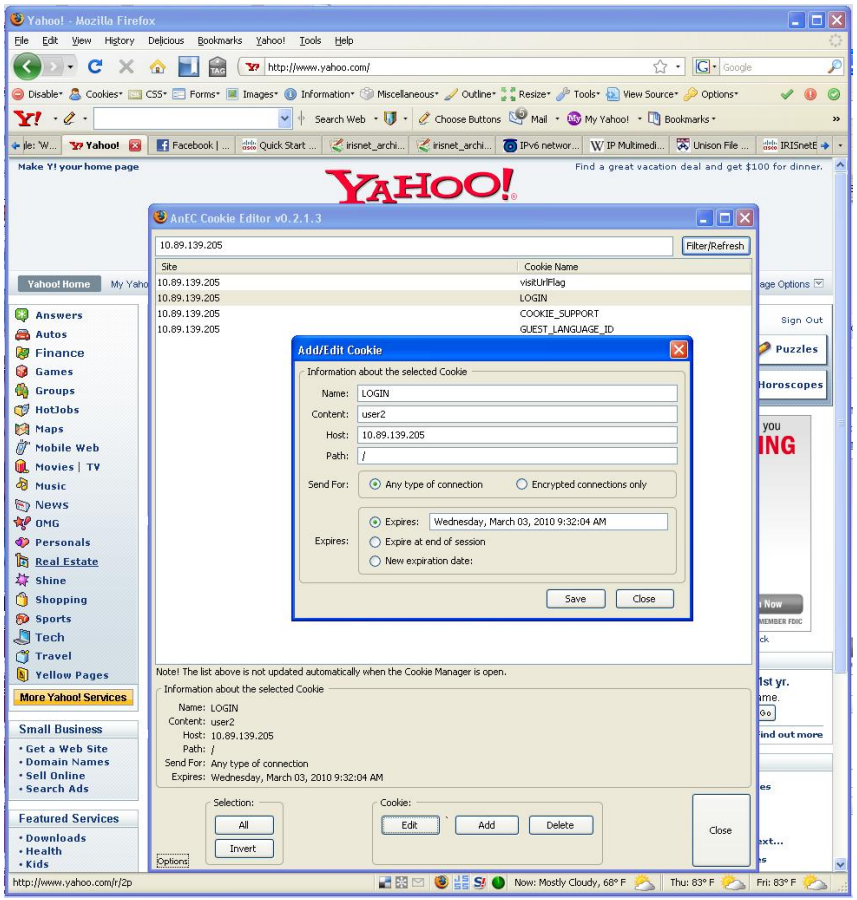
IPv6 Attack Tools

- Application Weaknesses Still the Same
- Exploit Frameworks Still a Threat
  - Metasploit
  - Core Impact

IPv6 Attack Tools

Firefox Browser Plugins

- Easy XSS, SQL Injection, etc
- Just as easy as IPv4



IPv6 Attack Tools

- Sniffers/packet capture
  - Snort
  - TCPdump
  - Sun Solaris snoop
  - COLD
  - Wireshark
  - Analyzer
  - Windump
  - WinPcap
- DoS Tools
  - 6tunneldos
  - 4to6ddos
  - Imps6-tools
- Relay Tools
  - 6tunnel
  - relay6
- Scanners
  - IPv6 security scanner
  - Halfscan6
  - Nmap
  - Strobe
  - Netcat
- Packet forgers
  - Scapy6
  - SendIP
  - Packit
  - Spak6
- Complete tool
  - THC-IPv6

IPv6 Attack Tools

THCIPv6

The Hacker's Choice

- **parasite6**: icmp neighbor solitication/advertisement spoofer, puts you as man-in-the-middle, same as ARP mitm (and parasite)
- **alive6**: an effective alive scanning, which will detect all systems listening to this address
- **fake_router6**: announce yourself as a router on the network, with the highest priority
- **redir6:** redirect traffic to you intelligently (man-in-the-middle) with a clever icmp6 redirect spoofer
- **toobig6:** mtu decreaser with the same intelligence as redir6
- **detect-new-ip6:** detect new ip6 devices which join the network, you can run a script to automatically scan these systems etc.
- **dos-new-ip6:** detect new ip6 devices and tell them that their chosen IP collides on the network (DOS).

http://www.darknet.org.uk/2010/07/thc-ipv6-toolkit-attacking-the-ipv6-protocol/

IPv6 Attack Tools

THCIPv6

- **fake_mld6:** announce yourself in a multicast group of your choice on the net
- **fake_mipv6:** steal a mobile IP to yours if IPSEC is not needed for authentication
- **fake_advertiser6:** announce yourself on the network
- **smurf6:** local smurfer
- **rsmurf6:** remote smurfer, known to work only against linux at the moment
- **sendpees6:** a tool by willdamn(ad)gmail.com, which generates a neighbor solicitation requests with a lot of CGAs (crypto stuff ;-) to keep the CPU busy. nice.

http://www.darknet.org.uk/2010/07/thc-ipv6-toolkit-attacking-the-ipv6-protocol/

IPv6 Attack Tools

THCIPv6

- **dnsdict6:** parallized dns ipv6 dictionary bruteforcer
- **trace6:** very fast traceroute6 with supports ICMP6 echo request and TCP-SYN
- **flood_router6:** flood a target with random router advertisements
- **flood_advertise6:** flood a target with random neighbor advertisements
- **fuzz_ip6:** fuzzer for ipv6
- **implementation6:** performs various implementation checks on ipv6
- **implementation6d:** listen daemon for implementation6 to check behind a FW

http://www.darknet.org.uk/2010/07/thc-ipv6-toolkit-attacking-the-ipv6-protocol/

Agenda

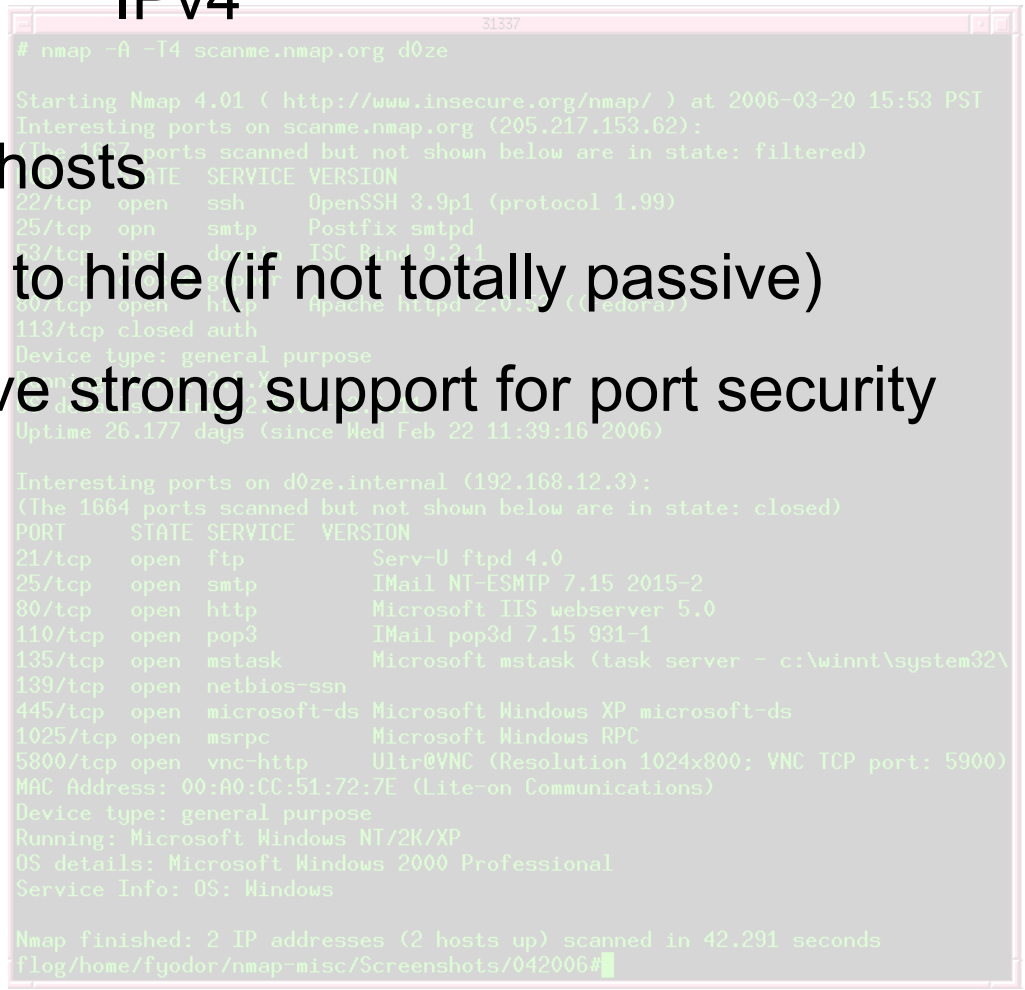
- Introduction
- Threat Landscape
- IPv6 Known Attack Vectors
- Coexistence Issues
- Attacker Tools
- Host Discovery
- Identifying Known Vulnerabilities
- Identifying Malicious Traffic
- Verifying Configurations

Host Discovery

IPv4

- Easy to identify all hosts
- Harder for attacker to hide (if not totally passive)
- Cisco Switches have strong support for port security
- Tools

  NMAP, AMAP, …



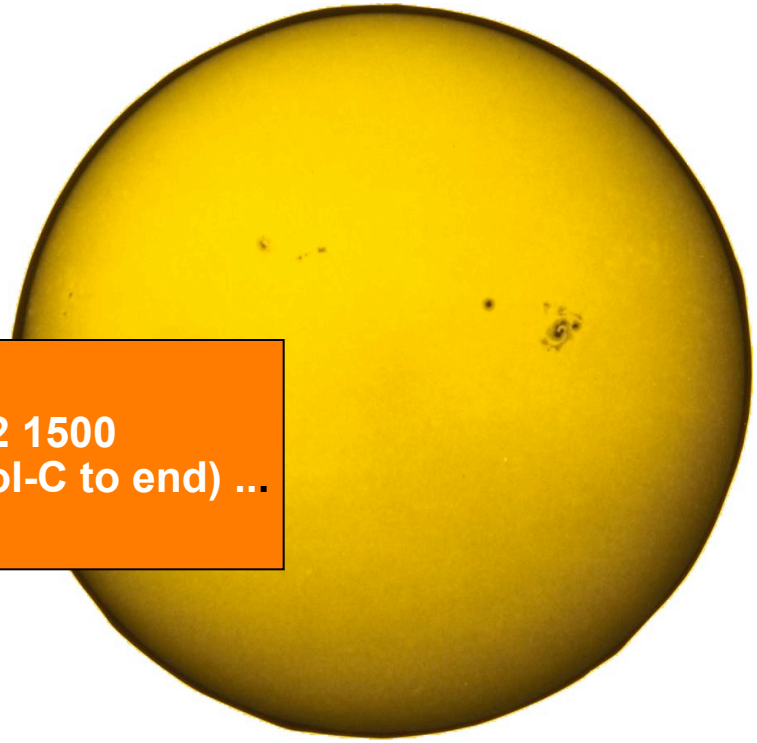
Host Discovery

IPv6

IPv4

- Traditional scanning not viable
- New Protocols
  - Neighbor Discovery Protocol
  - SEND (not fully adopted)
- Easy for host to become router

IPv6



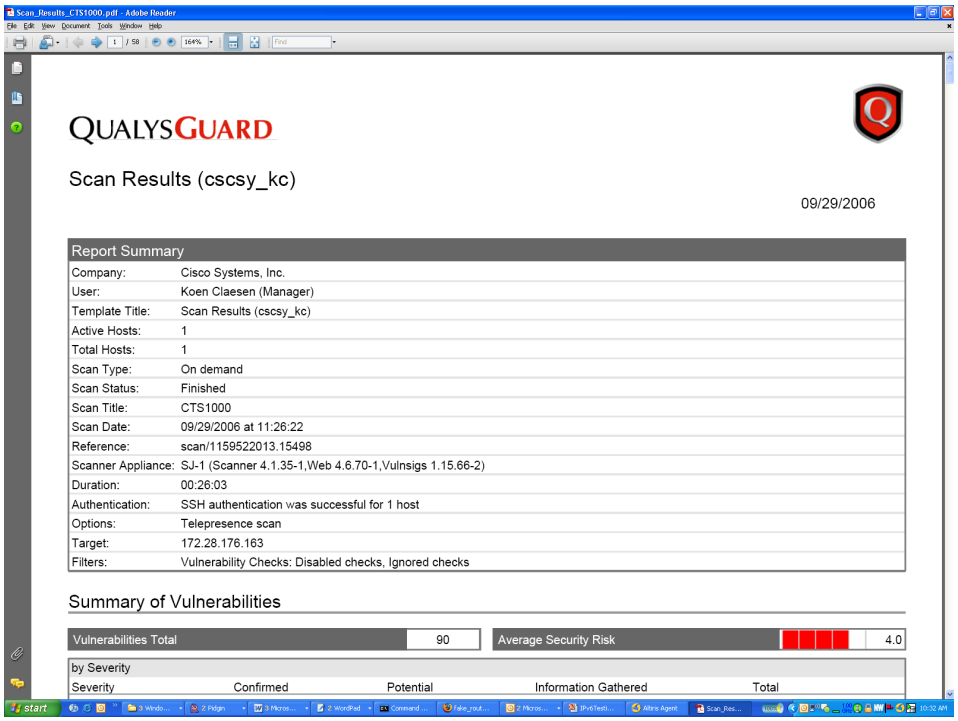
```
./fake_router6 eth0 fe80::1 2001:2001::/32 1500
Starting to advertise router fe80::1 (Press Control-C to end) ...
```

Agenda

- Introduction
- Threat Landscape
- IPv6 Known Attack Vectors
- Coexistence Issues
- Attacker Tools
- Host Discovery
- Identifying Known Vulnerabilities
- Identifying Malicious Traffic

Identifying Known Vulnerabilities

- Identify unpatched systems
- Identify misconfigurations
- Altiris
  - Patches systems regularly
- Qualys
  - Run regularly



QUALYSGUARD

Scan Results (cscsy_kc)

09/29/2006

Report Summary	
Company:	Cisco Systems, Inc.
User:	Koen Claesen (Manager)
Template Title:	Scan Results (cscsy_kc)
Active Hosts:	1
Total Hosts:	1
Scan Type:	On demand
Scan Status:	Finished
Scan Title:	CTS1000
Scan Date:	09/29/2006 at 11:26:22
Reference:	scan/1159522013.15498
Scanner Appliance:	SJ-1 (Scanner 4.1.35-1,Web 4.6.70-1,Vulnsigs 1.15.66-2)
Duration:	00:26:03
Authentication:	SSH authentication was successful for 1 host
Options:	Telepresence scan
Target:	172.28.176.163
Filters:	Vulnerability Checks: Disabled checks, Ignored checks

Summary of Vulnerabilities

Vulnerabilities Total	90	Average Security Risk	4.0

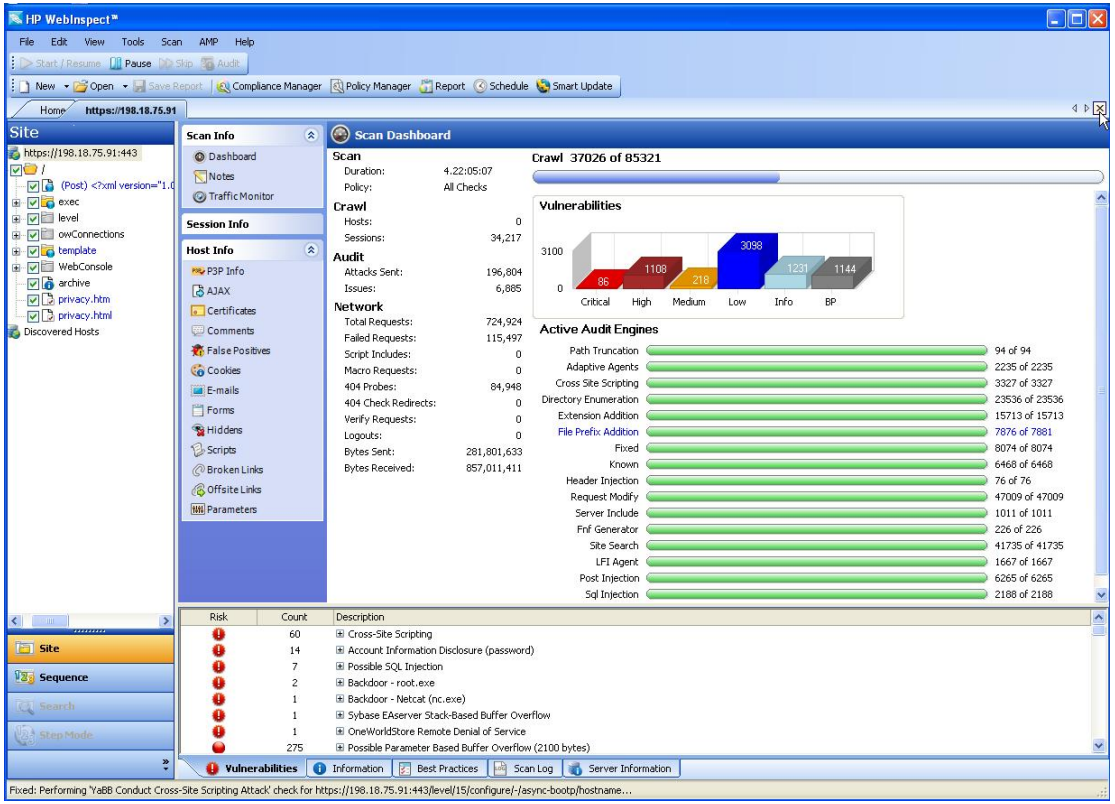
by Severity

Severity	Confirmed	Potential	Information Gathered	Total

Identifying Known Vulnerabilities

Common IPv4 Tools

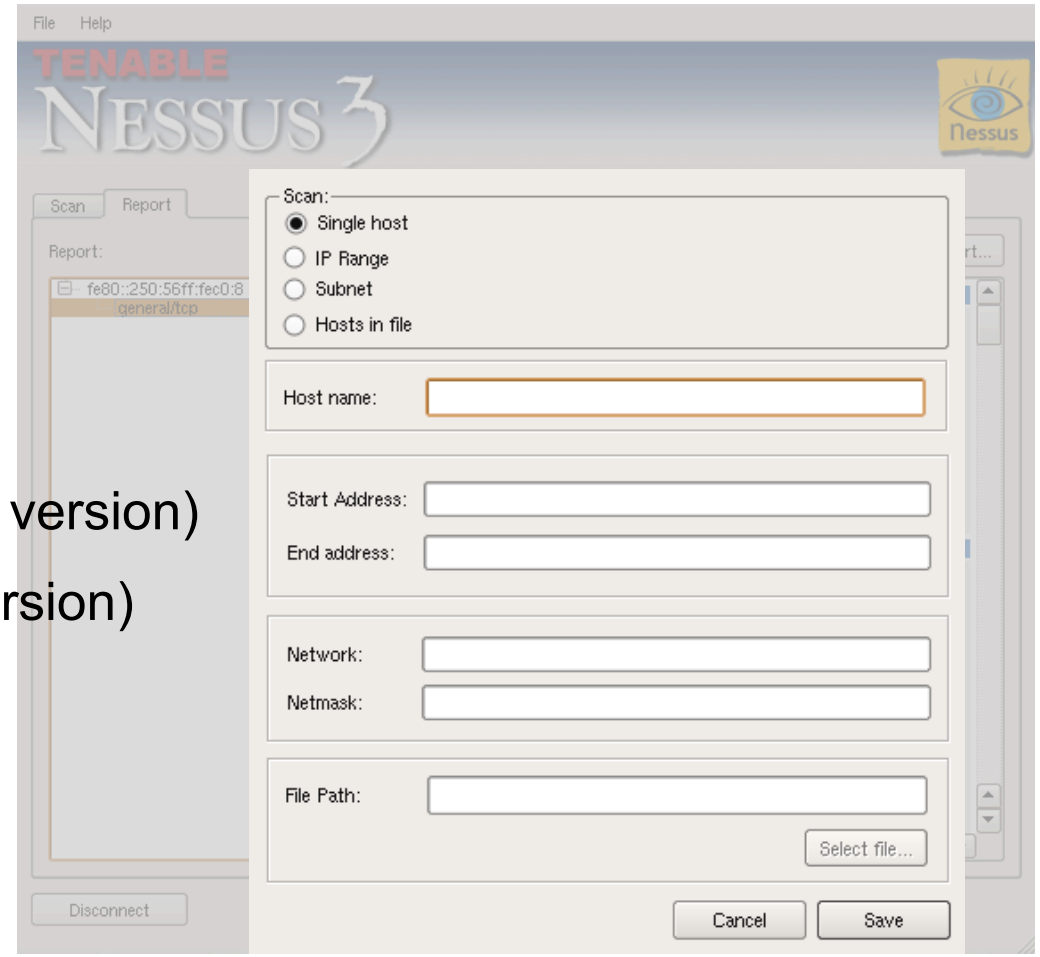
- Host Vulnerability
  - Nessus
  - Qualys
  - Saint
- Web Scanners
  - WebInspect
  - AppScan



Identifying Known Vulnerabilities

Common IPv6 Tools

- Host Vulnerability
  - Nessus (Partial)
  - Qualys (Pilot in 6.11)
  - Saint (Partial)
- Web Scanners
  - WebInspect (Yes in latest version)
  - AppScan (Yes in latest version)



Agenda

- Introduction
- Threat Landscape
- IPv6 Known Attack Vectors
- Coexistence Issues
- Attacker Tools
- Host Discovery
- Identifying Known Vulnerabilities
- Identifying Malicious Traffic
- Verifying Configurations

Identifying Malicious Traffic

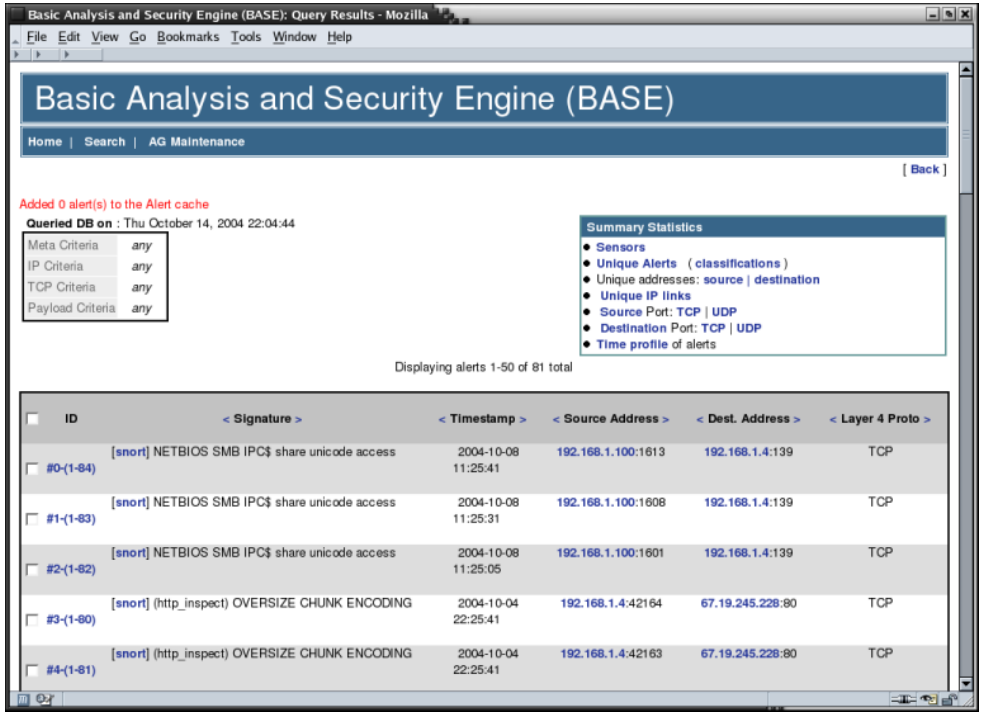
Attacks are common

- Every network experiences attacks
- Identifying attacks quickly is important
- Attackers try to avoid detection

Identifying Malicious Traffic

IPv4

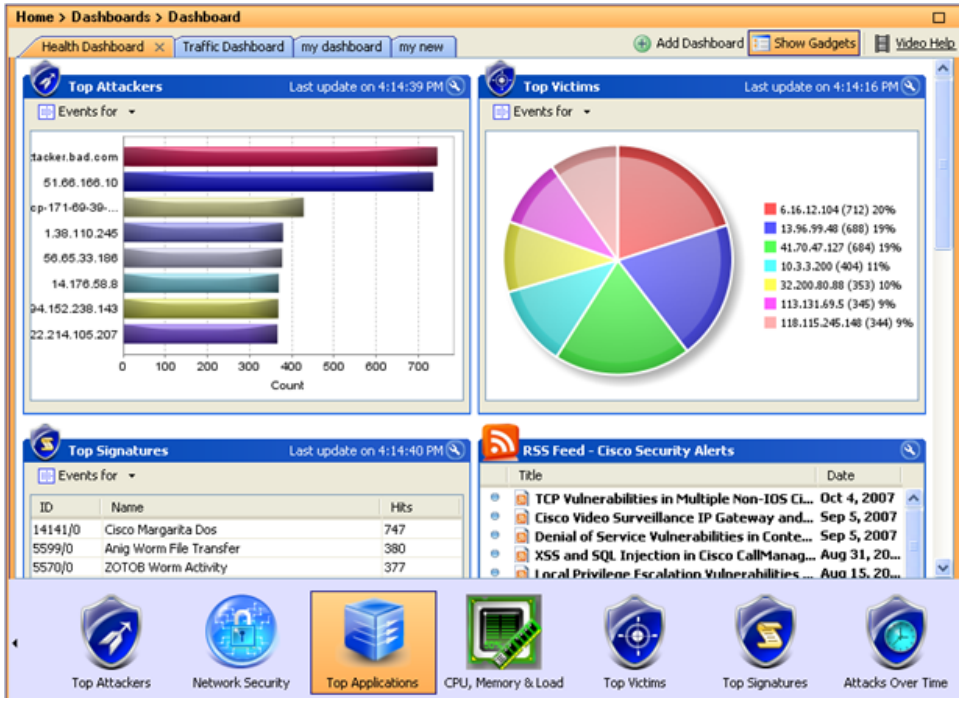
- Robust Device Support
  - Firewall Application Inspection
  - IPS
  - HIPS
  - Event Correlation
- Best Practices
  - Well Established



Identifying Malicious Traffic

IPv6

- Limited Device Testing
  - Feature Robustness?
  - Firewalls/IPS Products
- Best Practices
  - Being Developed



Agenda

- Introduction
- Threat Landscape
- IPv6 Known Attack Vectors
- Coexistence Issues
- Attacker Tools
- Host Discovery
- Identifying Known Vulnerabilities
- Identifying Malicious Traffic
- Verifying Configurations

Verifying Configurations

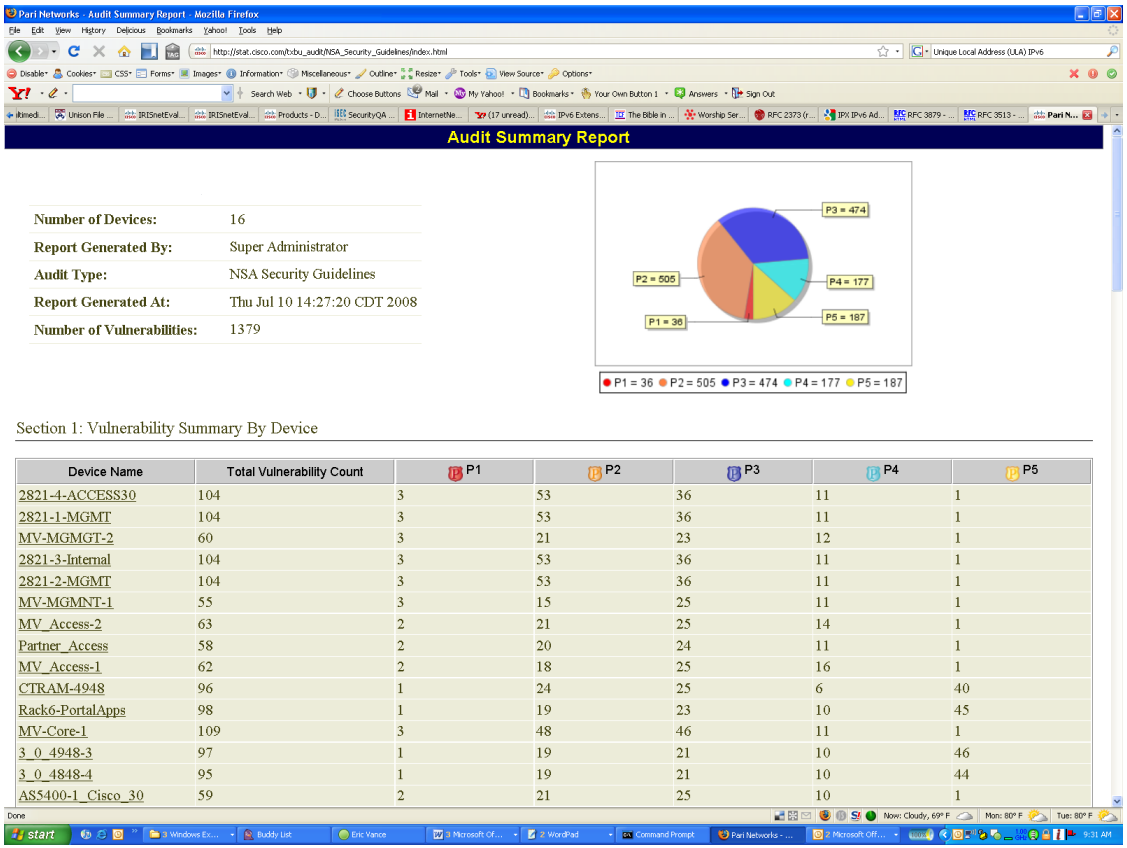
Common Practice

- Verifies configuration matches policy
- Find common configuration mistakes
- Manual can be time intensive

Verifying Configurations

IPv4

- Manual
  - Usually for smaller networks
- Automated
  - Pari
  - Redseal
- Scanning Tools
  - Limited Effectiveness

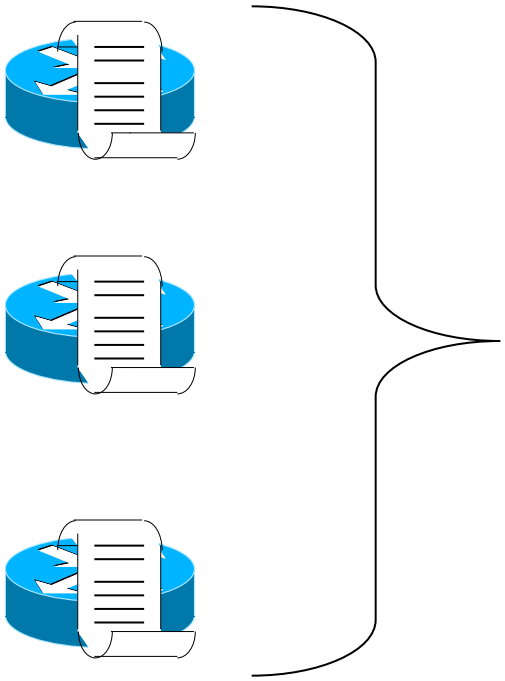


Device Name	Total Vulnerability Count	P1	P2	P3	P4	P5
2821-4-ACCESS30	104	3	53	36	11	1
2821-1-MGMT	104	3	53	36	11	1
MV-MGMGT-2	60	3	21	23	12	1
2821-3-Internal	104	3	53	36	11	1
2821-2-MGMT	104	3	53	36	11	1
MV-MGMNT-1	55	3	15	25	11	1
MV_Access-2	63	2	21	25	14	1
Partner_Access	58	2	20	24	11	1
MV_Access-1	62	2	18	25	16	1
CTRAM-4948	96	1	24	25	6	40
Rack6-PortalApps	98	1	19	23	10	45
MV-Core-1	109	3	48	46	11	1
3_0_4948-3	97	1	19	21	10	46
3_0_4848-4	95	1	19	21	10	44
AS5400-1_Cisco_30	59	2	21	25	10	1

Verifying Configurations

Pari

Configurations



Pari Software

Report Types

Cisco SAFE Suggestions
Cisco Security Advisories PSIRT
DHS Checklist
IOS IEC-27002
NSA Security Guidelines

Verifying Configurations

IPv6

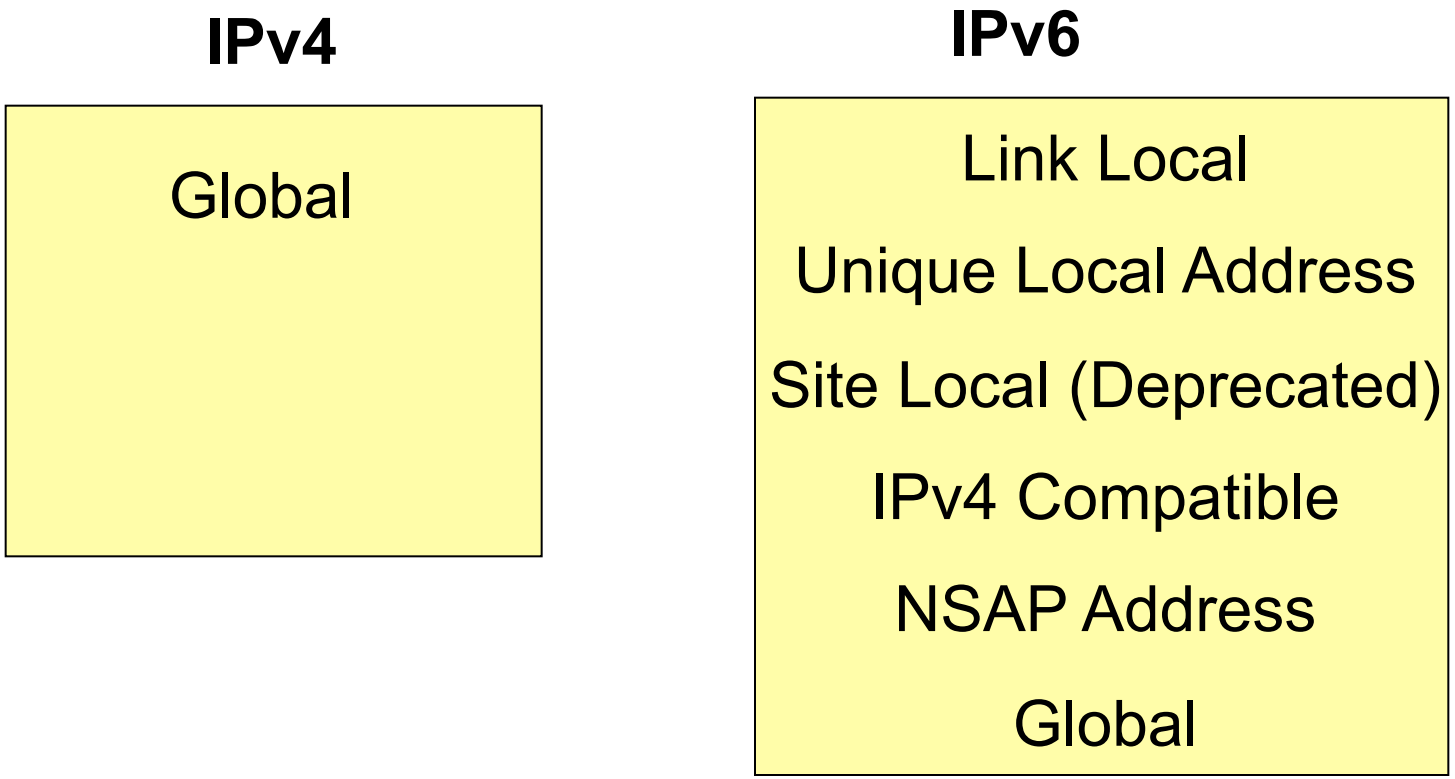
- Manual
- Scanning Tools

  Not very effective

```
Router# show running-config
Building configuration...
Current configuration : 22324 bytes
!
! Last configuration change at 14:59:38 PST Tue Jan 16 2001
! NVRAM config last updated at 04:25:39 PST Tue Jan 16 2001 by bird
!
hostname cat
!
ip cef
ipv6 unicast-routing
ipv6 cef
ipv6 cef accounting prefix-length
!
!
interface Ethernet0
ip address 10.4.9.11 255.0.0.0
media-type 10BaseT
ipv6 address 2001:yyyy:C18:1::/64 eui-64
ipv6 cef
!
```

Verifying Configurations

Unicast Addressing



References

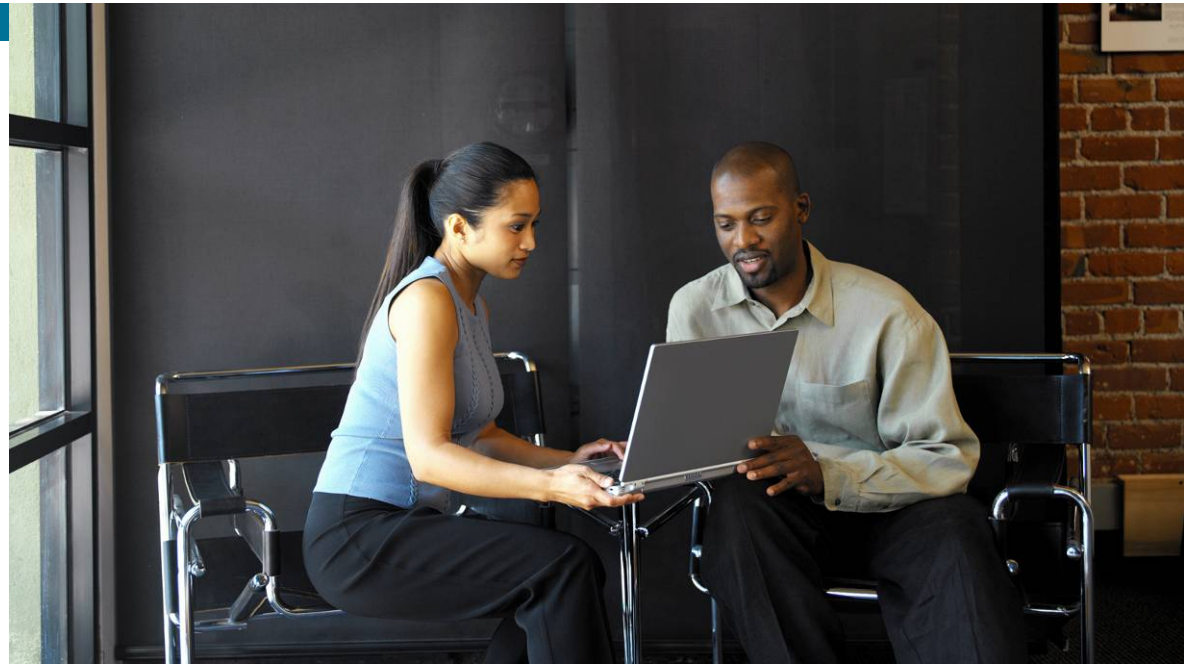
Reference Links

- http://www.codenomicon.com/
- http://www.mudynamics.com/
- http://freeworld.thc.org/thc-ipv6
- http://www.stindustries.net/IPv6/tools.html

- **IPv6 Security**

  by Scott Hogg & Eric Vyncke

Q and A



Contacts: ecarter@cisco.com


CISCO