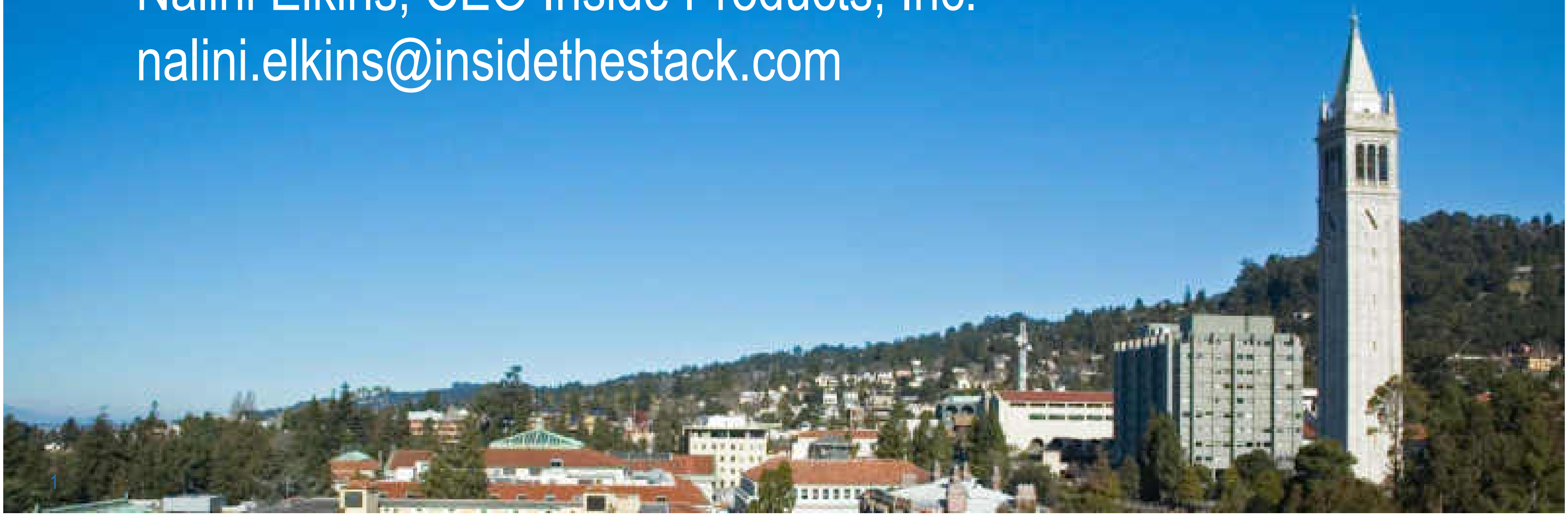
SHARKFEST ‘13

Wireshark Developer and User Conference

IPv6 Security

Nalini Elkins, CEO Inside Products, Inc.
nalini.elkins@insidethestack.com



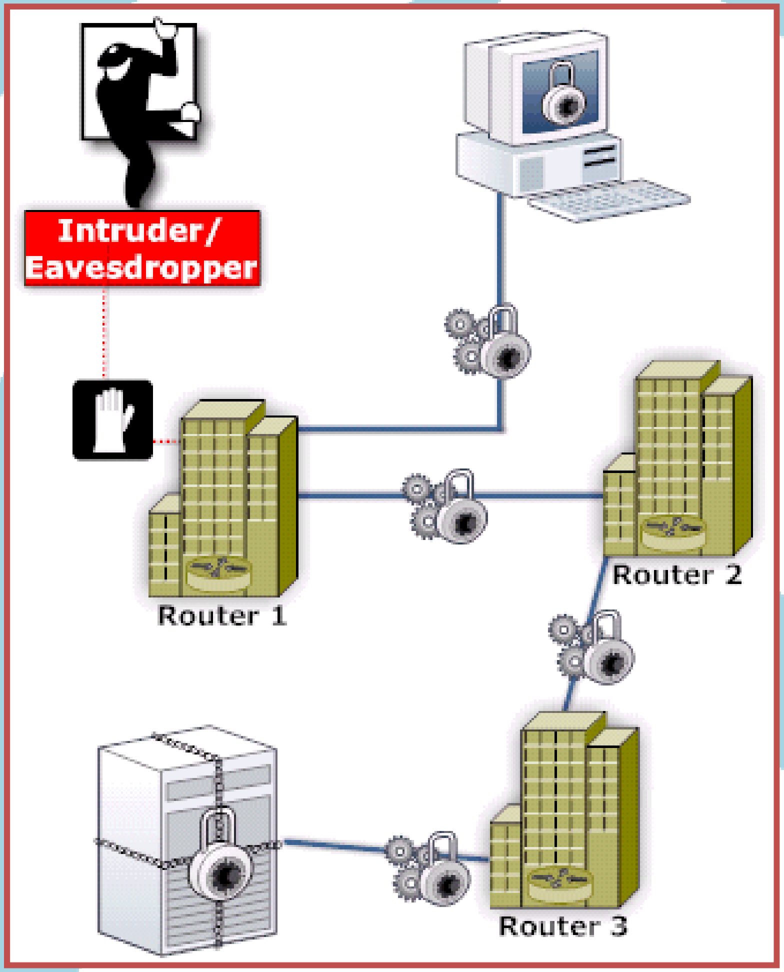
Agenda

Hackers are already aware of the security vulnerabilities in IPv6, and there are implications across all TCP-connected platforms.

- Critical vulnerabilities
- Technical and management overview
- What is more secure, and
- What is not so secure.

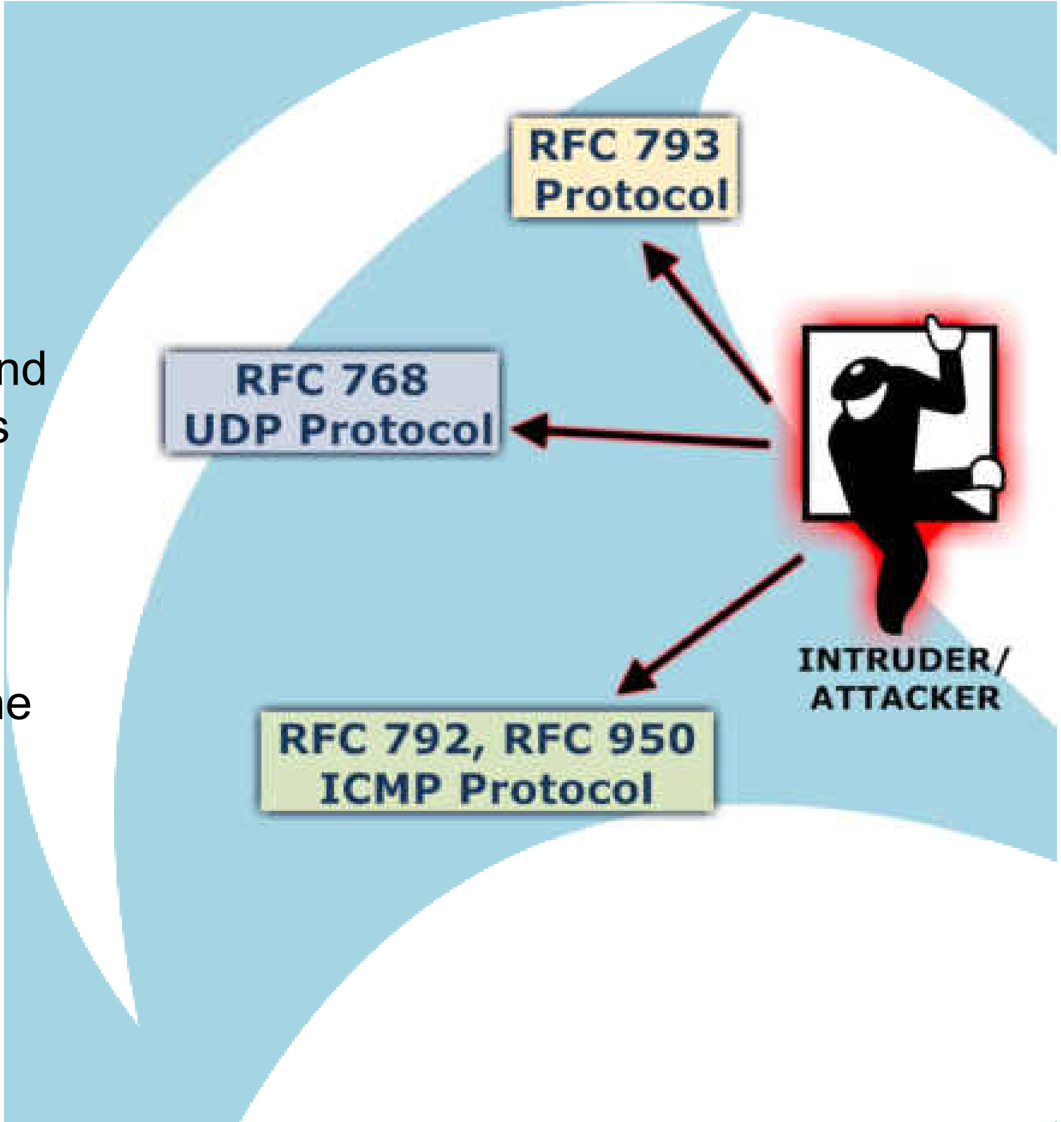
What can happen?

- Denial of service
  - High Usage (CPU or network)
  - Single device or widespread
  - Distributed Denial of Service
  - Worms
- Man in the Middle
- Service theft
  - File sharing
  - Pirated software

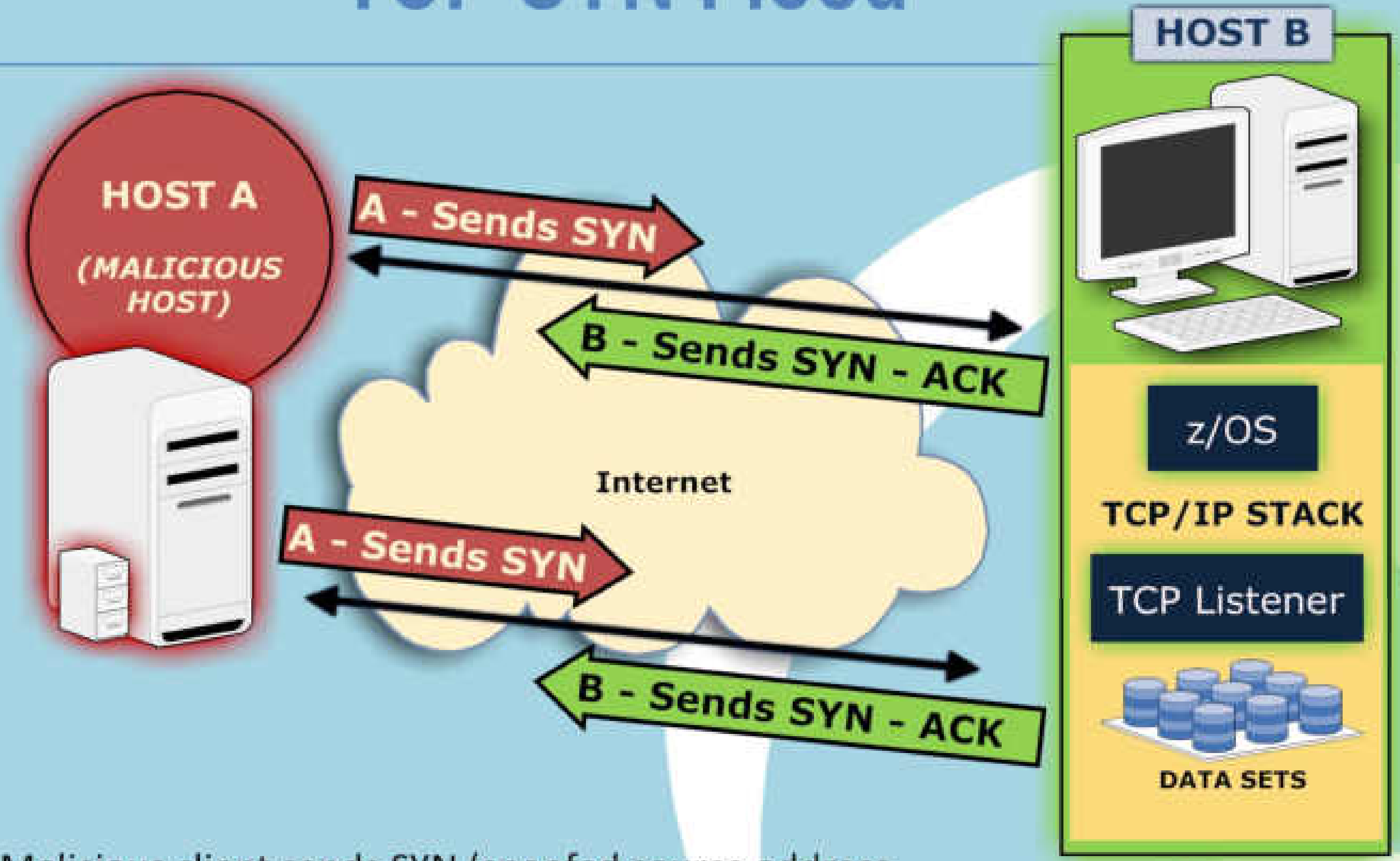


How does it happen?

- Protocol vulnerabilities
  - Reflector
    - TCP SYN flood,
    - TCP/UDP flood (Ping Pong),
    - ICMP echo (SMURF), and
    - ICMP broadcast packets
  - Spoofing
    - Address
    - Normal traffic
  - Packets which don’t follow the rules
- Application layer (same as IPv4)
  - Except DNSv6 and DHCPv6



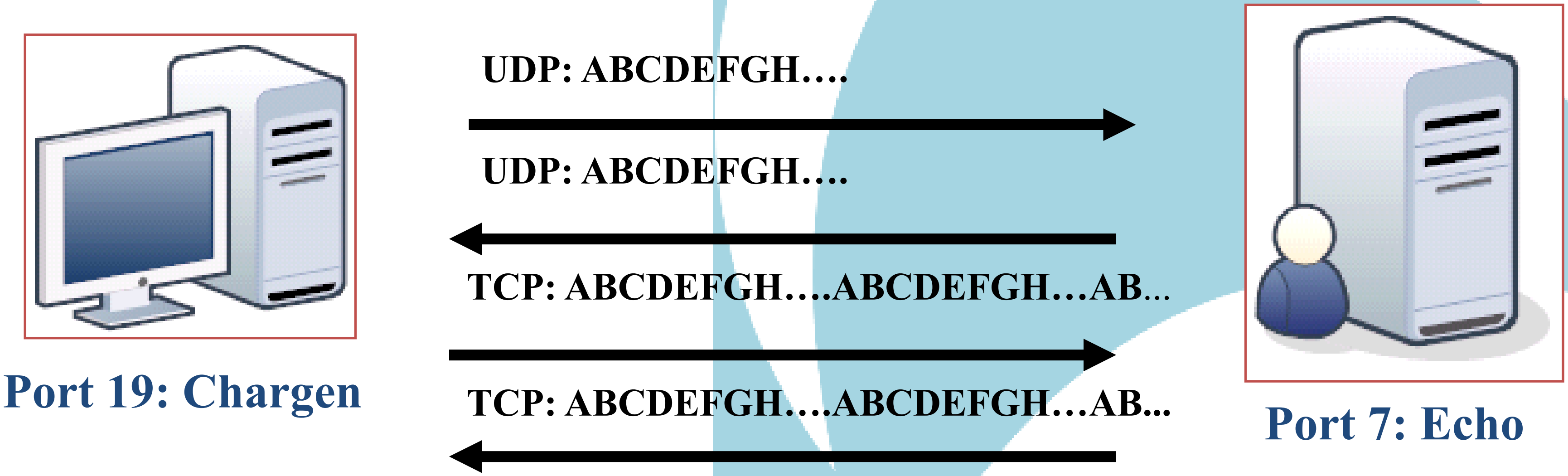
TCP SYN Flood



- Malicious client sends SYN (spoofed source address possible)
- Server responds with SYN-ACK (allocates buffers, etc.)
- Client sends another SYN…

Ping Pong or Packet Storm

- Port 19 : Character Generator
- Port 7: Echo
- Connect them and … packet storm!
- Also called ‘Ping Pong’.



UDP: ABCDEFGH….

UDP: ABCDEFGH….

TCP: ABCDEFGH….ABCDEFGH…AB...

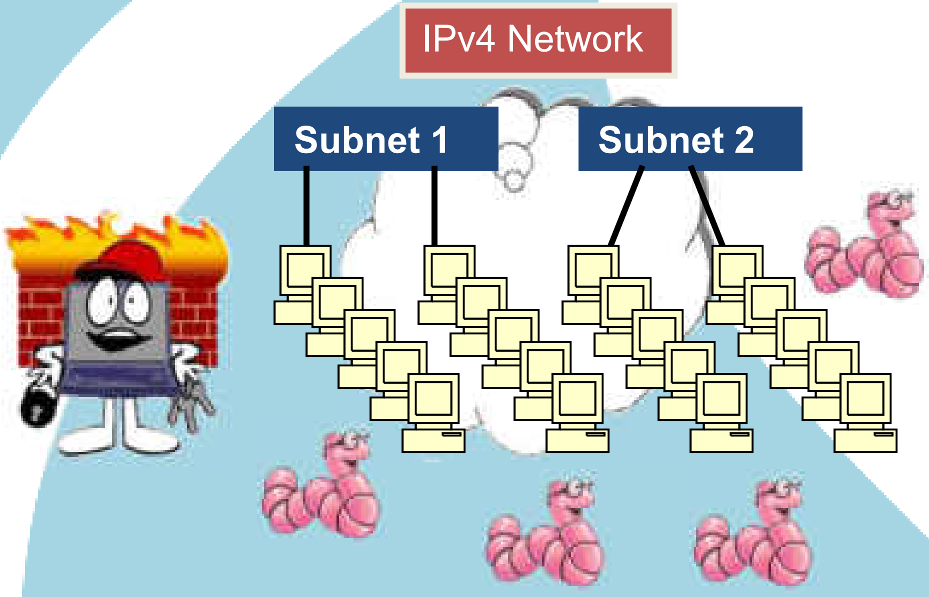
TCP: ABCDEFGH….ABCDEFGH…AB...

Port 19: Chargen

Port 7: Echo

Worms

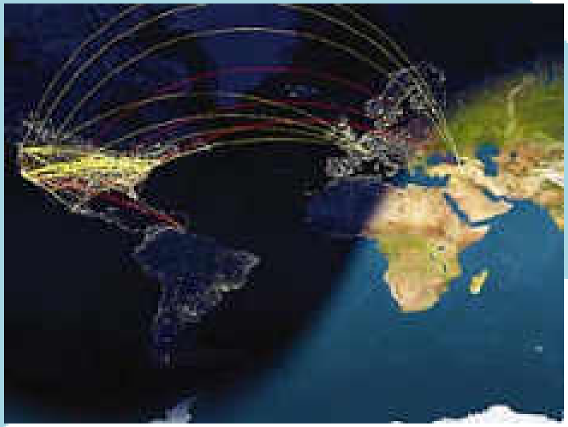
- Worms
  - Example: Slammer, Nimda, Code Red
  - A standalone malicious program
  - On TCP / UDP port or via email
- Network problems
  - Slammer worm took down internet root nameservers.
  - Routers - buffer or CPU congestion.
- Do ping sweeps or generate random IP addresses
- IPv6 : inherently more defense for worms



Slammer

- http://www.wired.com/wired/archive/11.07/slammer.html
- **Slammer: An inside view of the worm that crashed the Internet in 15 minutes.**
- On Akamai's network
- Fifty-five million database requests
- First victim at 12:30 am EST.
- Created millions of Slammer clones, targeting other computers at random.
- By 12:33 am, number of slaves doubling every 8.5 seconds. (*75,000 victims within ten minutes)*
- By 12:45 am, huge sections of Internet affected
- Net Access Corporation, a large ISP, "Nearly half our ports are in delta alarm right now."
- Emergency 911 dispatchers in Seattle resorted to paper. Continental Airlines canceled flights.
- Total cost more than $1 billion.

North America is affected.



The Akamai network polls itself continuously for trouble spots. The lines trace the escalation of jammed server-to-server connections.

How has it changed with IPv6?

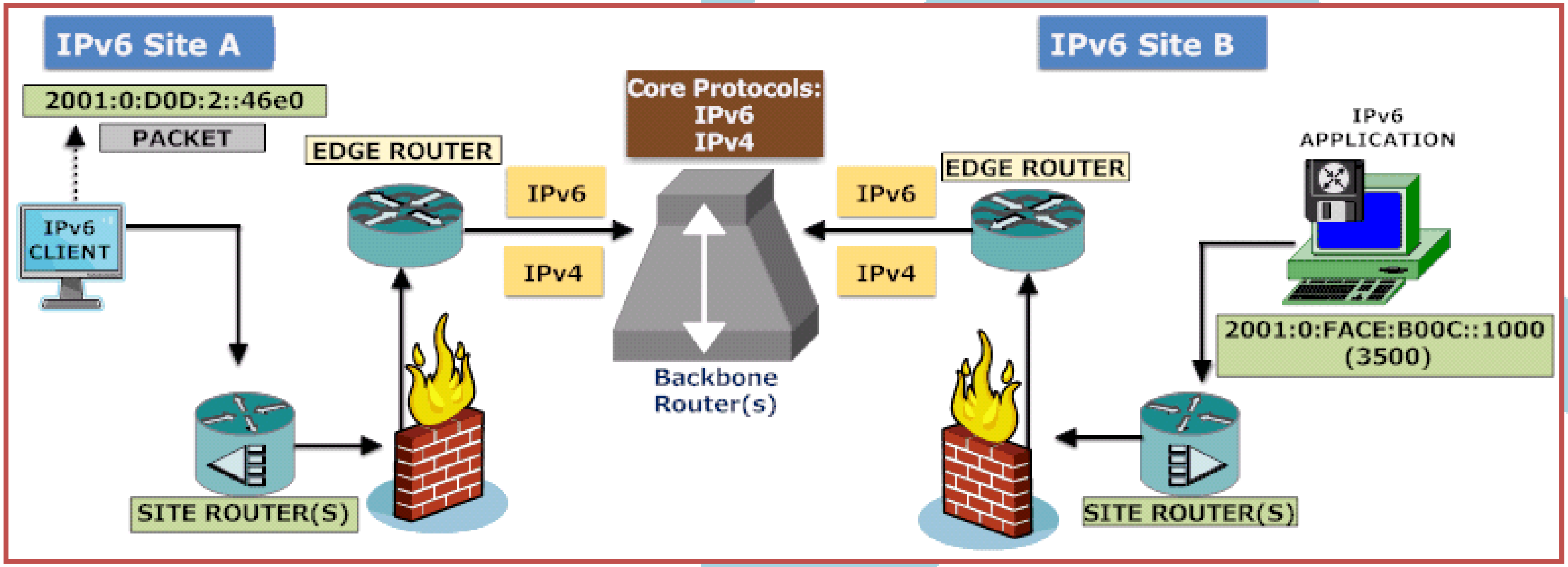
- ICMPv6 (Esp. Neighbor discovery, Router advertisement)
- Malformed / deprecated packets
  - Routing header 0 (deprecated)
  - Options
  - Site local unicast
- IPv6 Multicast
- DNSv6
- DHCPv6

New protocols = new exploits!

How do you protect yourself?

- Firewall
- IDS / IPS

- IPSec
- SSL / SSH



Reconnaissance

IPv4

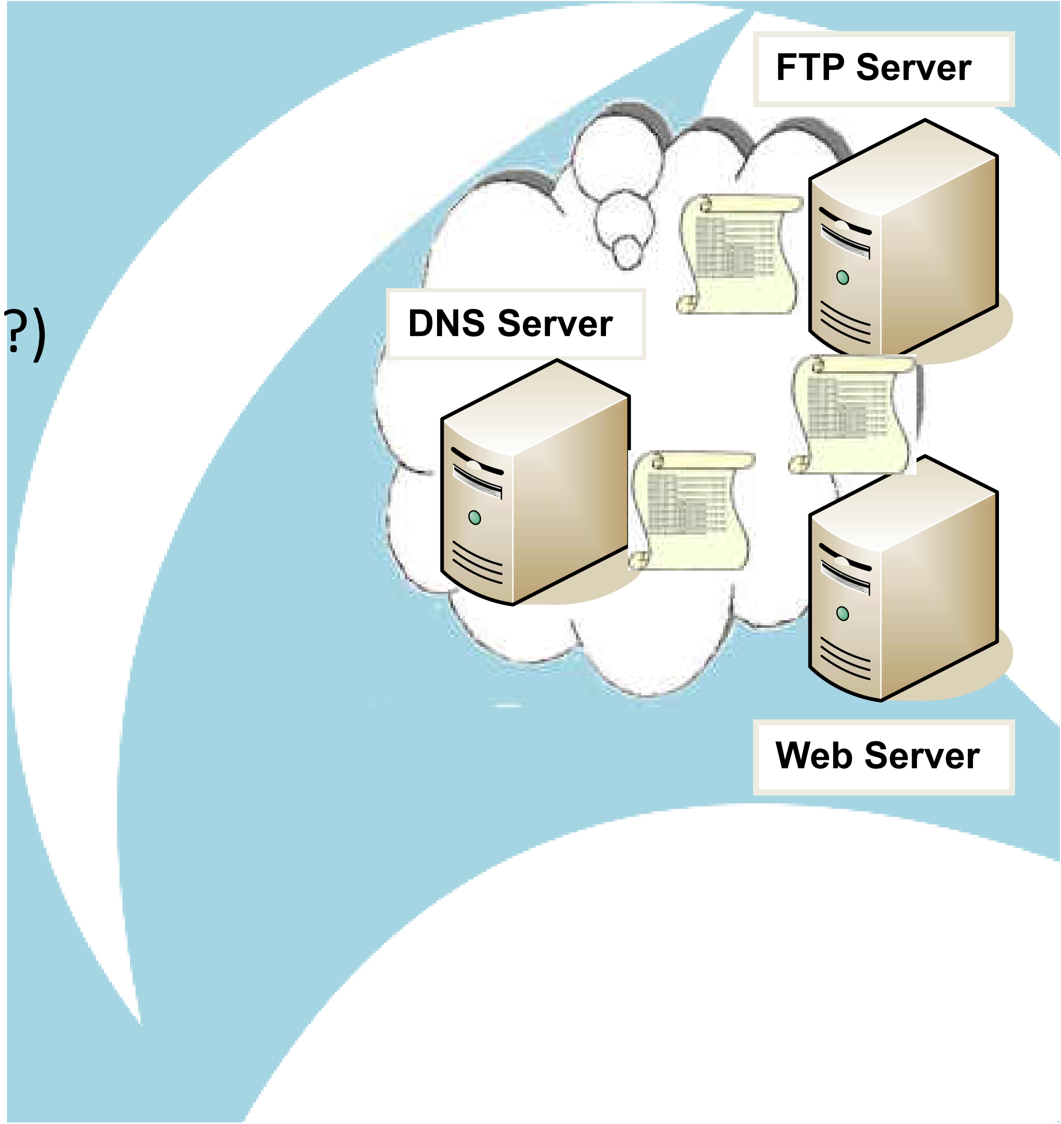
- Subnet = 2^{8} or 256
- Steps
  - Ping sweep = 5 – 30 seconds
  - Port scan live host
  - Attack active port
- Many tools available
  - Nmap
  - Amap
  - Nessus

IPv6

- Subnet = 2^{64} or 18,446,744,073,709,551,616
- Steps
  - Ping sweep = VERY LONG TIME! (assume .1 sec * 2^{64})
  - Port scan live host
  - Attack active port
- Not so many tools available

Methods To Harvest Addresses

- Find new methods!
- No NAT (translation ~= NAT?)
- Web or FTP server logs.
- Email headers

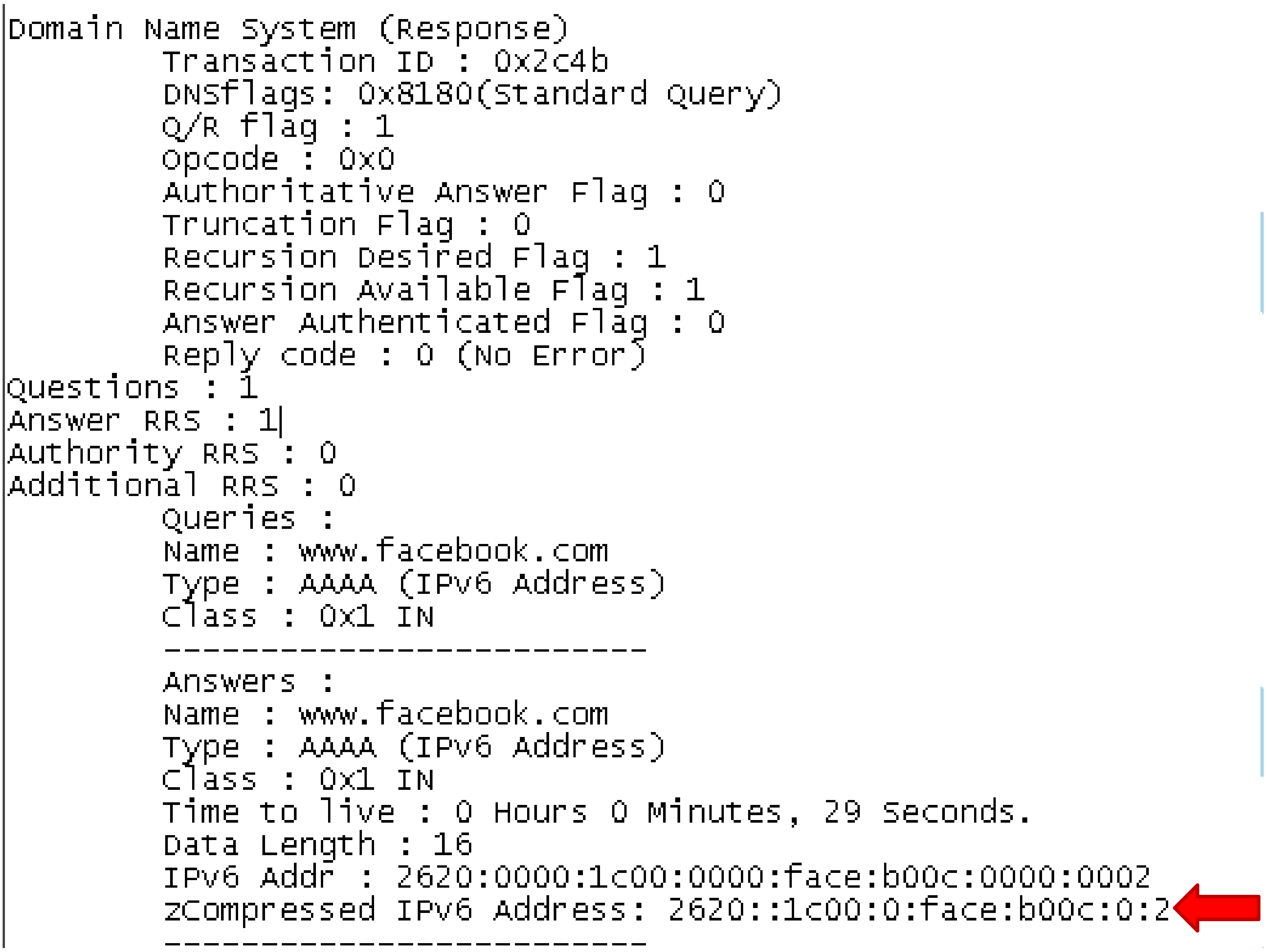


Reducing the IPv6 Search Space

- Prefixes (2001::..) at ARIN (or other RIR)
- Get inside with IPv4 – IPv6 tunnels?
- Once inside…
  - multicast address (FF02::1) all nodes
  - convention may start with ….::1

Protect Topology or Protect Resource?

What is wrong with 2620::1c00:0:face:b00c:0:2?



```
Domain Name System (Response)
        Transaction ID : 0x2c4b
        DNSflags: 0x8180(Standard Query)
        Q/R flag : 1
        Opcode : 0x0
        Authoritative Answer Flag : 0
        Truncation Flag : 0
        Recursion Desired Flag : 1
        Recursion Available Flag : 1
        Answer Authenticated Flag : 0
        Reply code : 0 (No Error)
Questions : 1
Answer RRS : 1
Authority RRS : 0
Additional RRS : 0
        Queries :
        Name : www.facebook.com
        Type : AAAA (IPv6 Address)
        Class : 0x1 IN
        -------------------------
        Answers :
        Name : www.facebook.com
        Type : AAAA (IPv6 Address)
        Class : 0x1 IN
        Time to live : 0 Hours 0 Minutes, 29 Seconds.
        Data Length : 16
        IPv6 Addr  : 2620:0000:1c00:0000:face:b00c:0000:0002
        zCompressed IPv6 Address: 2620::1c00:0:face:b00c:0:2
        -------------------------
```

Scan Protection on one IDS

ICMPv6 Event	Destination Address	Classification
Receive Echo Request	Multicast	Very suspicious
Receive Echo Request denied by QoS	Unicast	Normal
Receive Echo Request w/ Routing Header	Unicast	Possibly suspicious
Receive Echo Request without Routing Header	Unicast	Normal

- Fast / slow scans
- ICMP scans
- ICMPv6 scans
- UDP port scans
- TCP port scans

What Else?

Some IDS protect against:

- Scanning
- Floods (IPv4 and IPv6)
  - TCP SYN flood
  - Interface floods (large number of discards are occurring in proportion to the number of inbound packets

Discards (Malformed packet events)

- IPv6 incorrect or partial header
- IPv6 next header restrictions
- IPv6 destination option restrictions
- IPv6 hop-by-hop option restrictions
- IPv6 outbound raw restrictions

What is ICMPv6?

- Used by the Internet Protocol (IP)
- ICMPv4 == > ICMPv6 == Many changes!
- ICMP has:
  - Error messages
  - Informational messages

ICMPv6 error messages

•Destination unreachable
•Packet too big
•Time exceeded
•Parameter problem

ICMPv6 informational messages:

•Echo request/reply

•Multicasting messages

•Group membership query, report, done

•Neighbor discovery

•Router solicitation and advertisement

•Neighbor solicitation and advertisement

•Redirect

ICMPv6 Informational Messages

Type	Name
128	Echo Request
129	Echo Reply
130	Multicast Listener Query
131	Multicast Listener Report
132	Multicast Listener Done
133	Router Solicitation
134	Router Advertisement
135	Neighbor Solicitation
136	Neighbor Advertisement
137	Redirect Message
138	Router Renumbering
139	ICMP Node Info. Query
140	ICMP Node Info. Response
141	Inverse Neighbor Discovery Solicitation Message
142	Inverse Neighbor Discovery Advertisement Message
143	Version 2 Multicast Listener Report
144	Home Agent Address Discovery Request Message
145	Home Agent Address Discovery Reply Message
146	Mobile Prefix Solicitation
147	Mobile Prefix Advertisement
148	Certification Path Solicitation
149	Certification Path Advertisement
150	Experimental mobility protocols
151	Multicast Router Advertisement
152	Multicast Router Solicitation
153	Multicast Router Termination

Neighbor Discovery

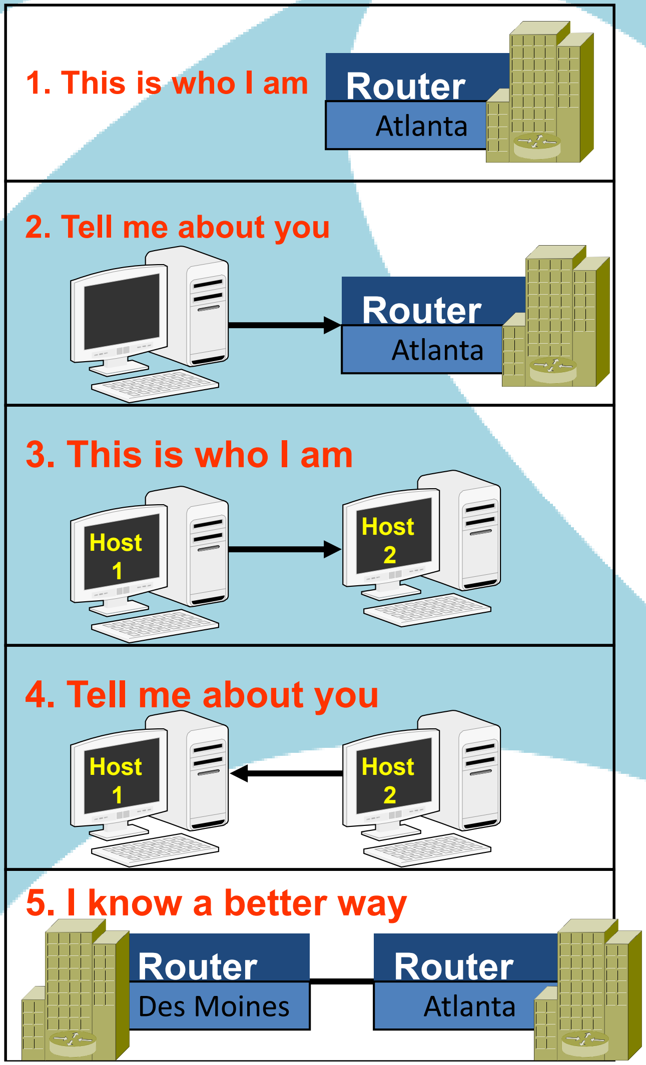
- Neighbor Discovery (ND) replaces ARP

- Very widely used

- Five ICMPv6 message types:

  1. *Router Advertisement*
  2. *Router Solicitation*
  3. *Neighbor Advertisement*
  4. *Neighbor Solicitation*
  5. *Redirect*

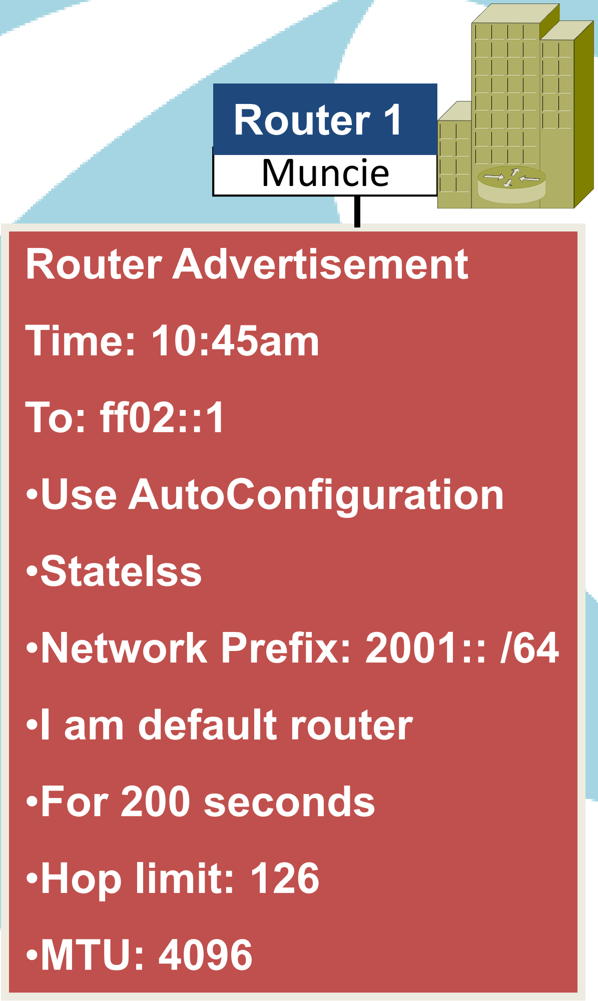
- Vast potential for misuse



Router Advertisement Contents

Router Advertisements contain:

- Stateless / stateful (DHCPv6)
- Network prefix
- Default router
- Hop limit
- MTU



Router Advertisement

Time: 10:45am

To: ff02::1

•Use AutoConfiguration

•Statelss

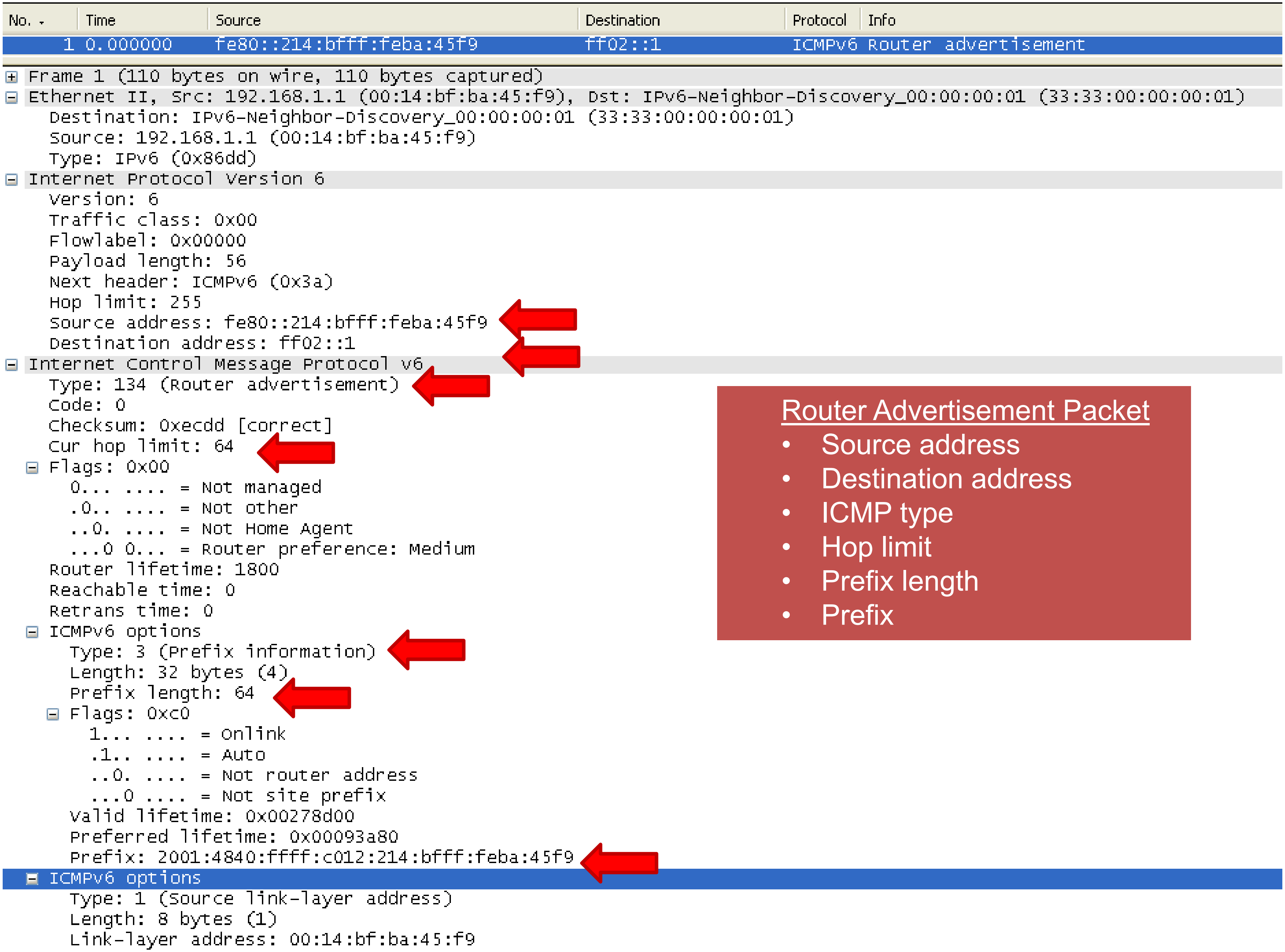
•Network Prefix: 2001:: /64

•I am default router

•For 200 seconds

•Hop limit: 126

•MTU: 4096



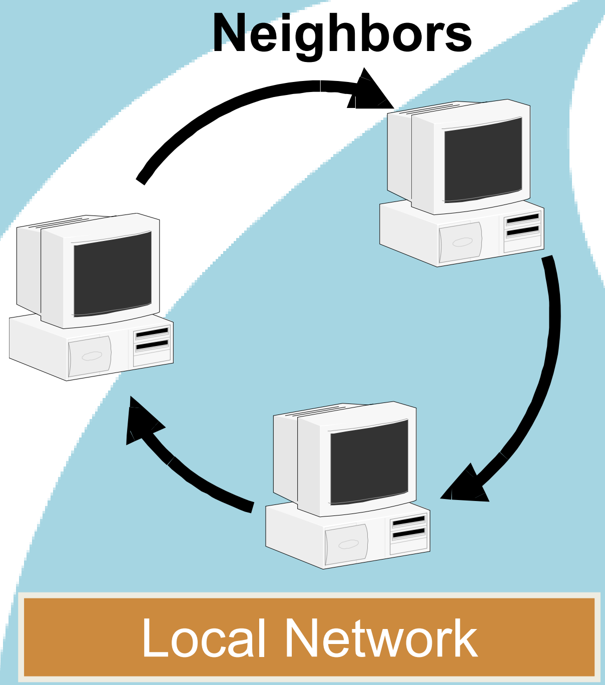
```
No. -   Time       Source                       Destination   Protocol  Info
    1 0.000000     fe80::214:bfff:feba:45f9     ff02::1       ICMPv6 Router advertisement

⊞ Frame 1 (110 bytes on wire, 110 bytes captured)
⊟ Ethernet II, Src: 192.168.1.1 (00:14:bf:ba:45:f9), Dst: IPv6-Neighbor-Discovery_00:00:00:01 (33:33:00:00:00:01)
    Destination: IPv6-Neighbor-Discovery_00:00:00:01 (33:33:00:00:00:01)
    Source: 192.168.1.1 (00:14:bf:ba:45:f9)
    Type: IPv6 (0x86dd)
⊟ Internet Protocol Version 6
    Version: 6
    Traffic class: 0x00
    Flowlabel: 0x00000
    Payload length: 56
    Next header: ICMPv6 (0x3a)
    Hop limit: 255
    Source address: fe80::214:bfff:feba:45f9
    Destination address: ff02::1
⊟ Internet Control Message Protocol v6
    Type: 134 (Router advertisement)
    Code: 0
    Checksum: 0xecdd [correct]
    Cur hop limit: 64
  ⊟ Flags: 0x00
      0... .... = Not managed
      .0.. .... = Not other
      ..0. .... = Not Home Agent
      ...0 0... = Router preference: Medium
    Router lifetime: 1800
    Reachable time: 0
    Retrans time: 0
  ⊟ ICMPv6 options
      Type: 3 (Prefix information)
      Length: 32 bytes (4)
      Prefix length: 64
    ⊟ Flags: 0xc0
        1... .... = Onlink
        .1.. .... = Auto
        ..0. .... = Not router address
        ...0 .... = Not site prefix
      Valid lifetime: 0x00278d00
      Preferred lifetime: 0x00093a80
      Prefix: 2001:4840:ffff:c012:214:bfff:feba:45f9
  ⊟ ICMPv6 options
      Type: 1 (Source link-layer address)
      Length: 8 bytes (1)
      Link-layer address: 00:14:bf:ba:45:f9
```

Router Advertisement Packet

- Source address
- Destination address
- ICMP type
- Hop limit
- Prefix length
- Prefix

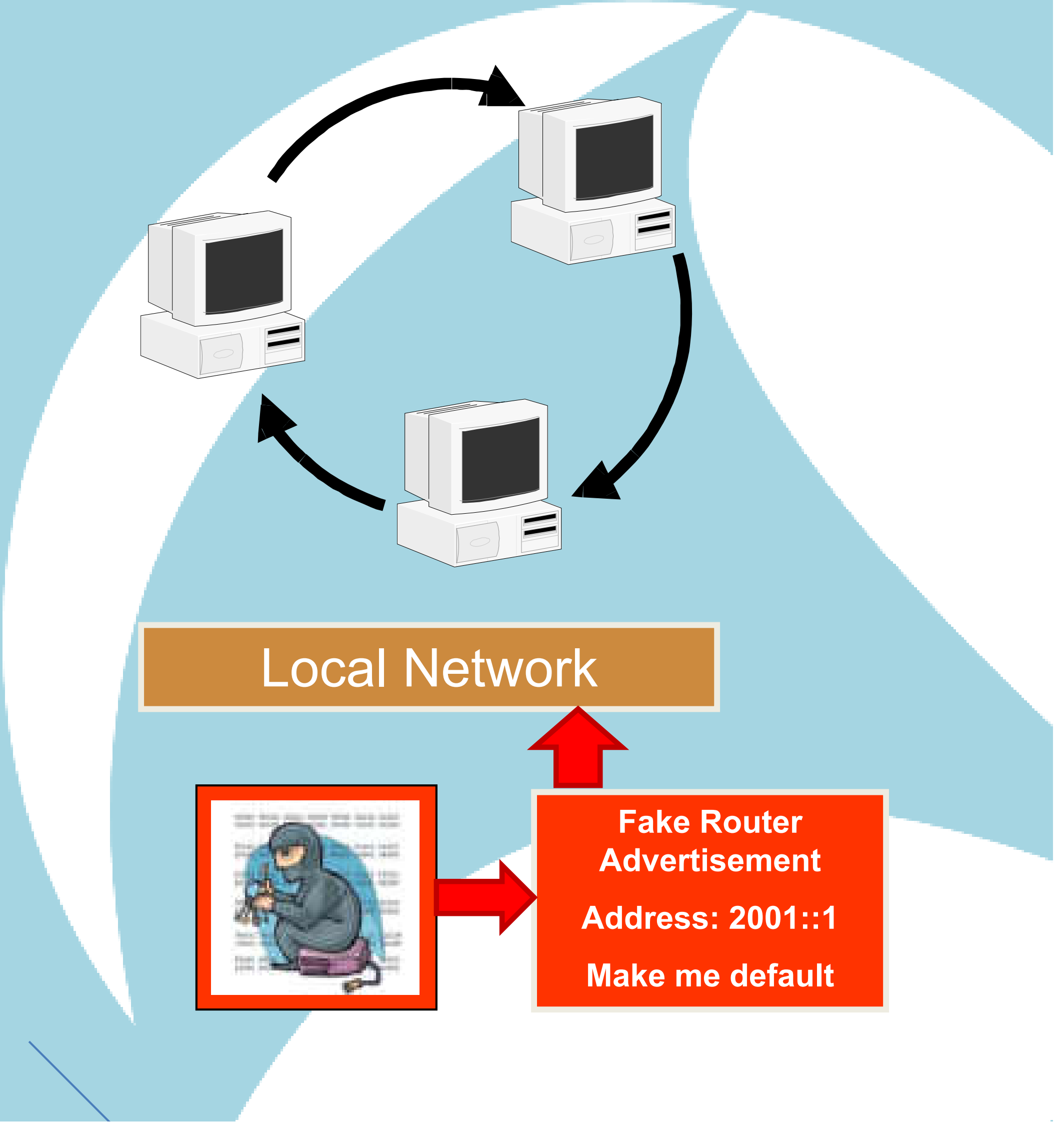
Neighbor Discovery Issues

- IPv6 first developed over 10 years ago
- Neighbors can't be trusted anymore!
- WiFi and Starbucks on every corner
- Insider attacks
- Phony WLAN base station
  - access stealing,
  - DoS, and
  - traffic snooping attacks



FakeRouter6

- Routers send Router Advertisements to well-known FF02::1
- Routing tables and network prefix reconfigured
- Any host can spoof Router Advertisement
- Malicious host becomes Default Router
- Change routing table to go via Man-in-the-Middle device



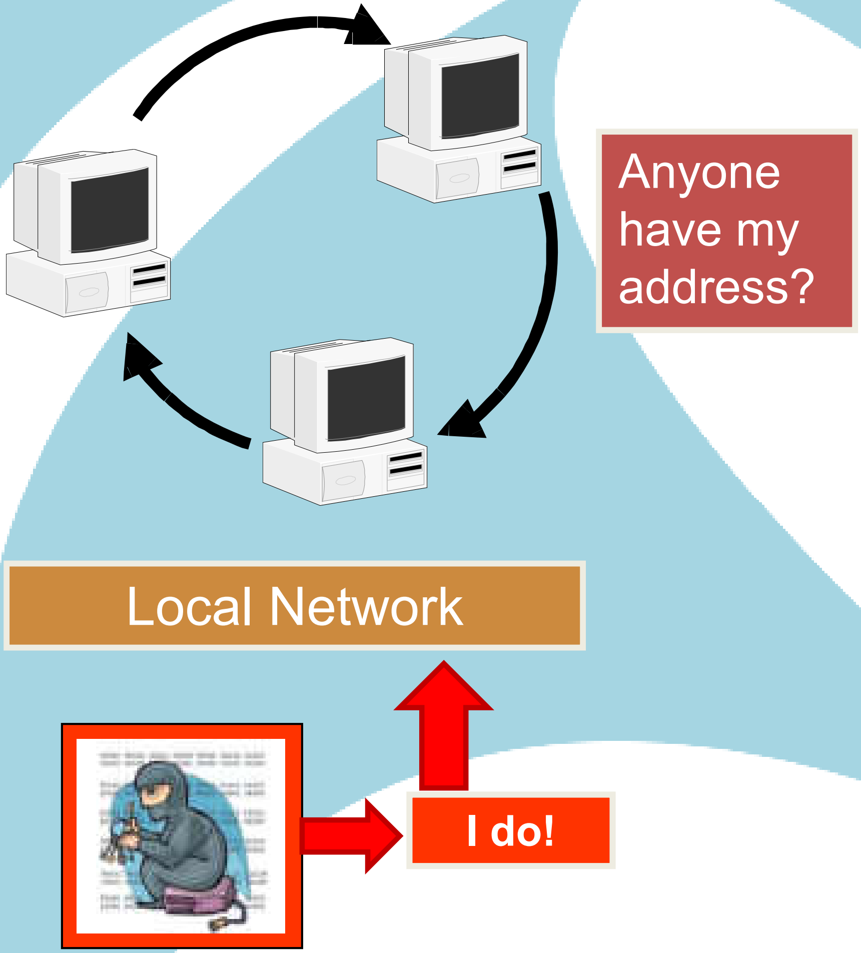
DoS New IPv6

- Denies new device network access

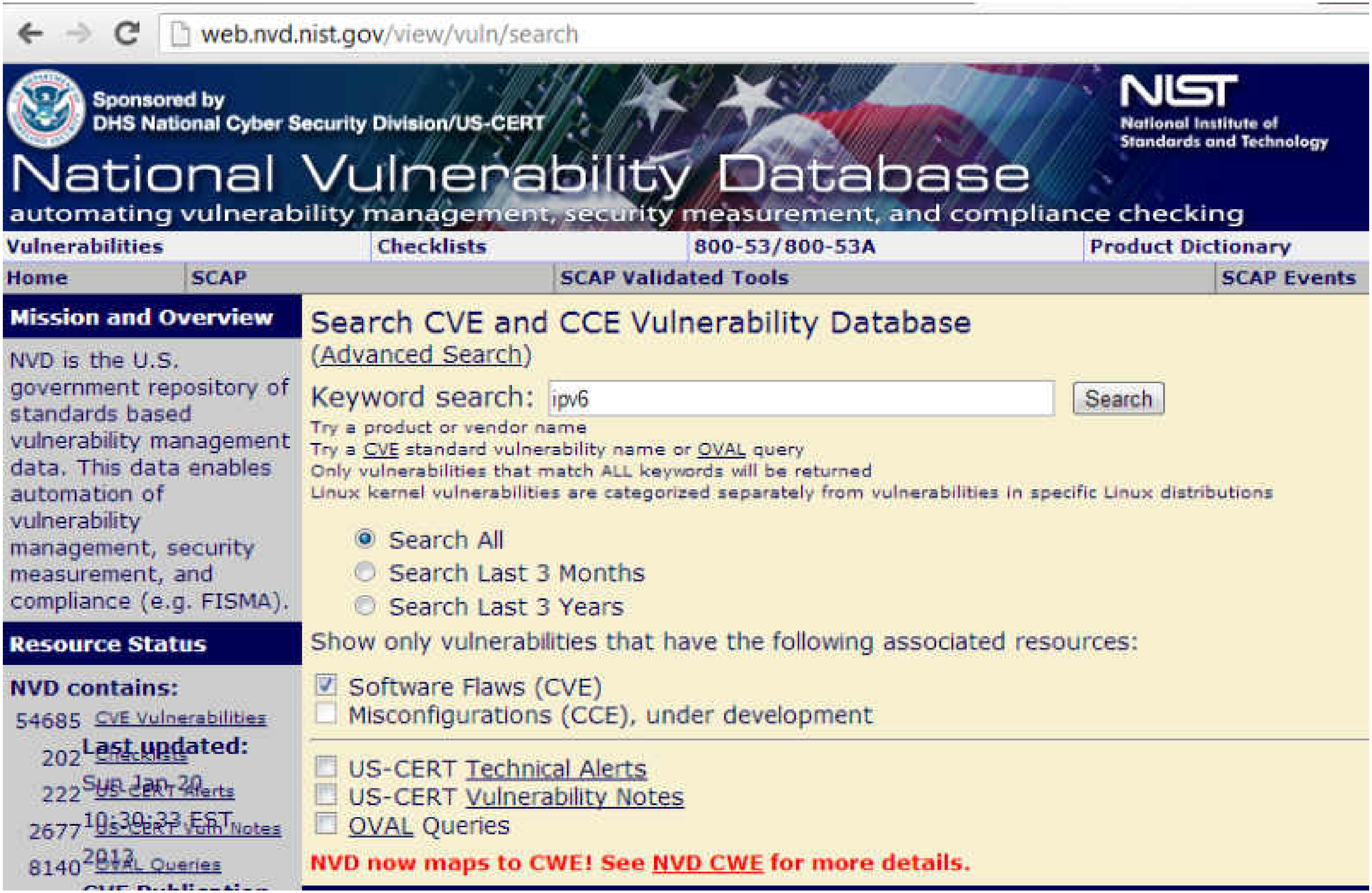
- Stateless Autoconfiguration does a Duplicate Address Detection (DAD)

- Malicious system responds to all DAD packets

- New system cannot get IPv6 address



Let's Go to CERT



web.nvd.nist.gov/view/vuln/search
Sponsored by
DHS National Cyber Security Division/US-CERT
NIST
National Institute of Standards and Technology
National Vulnerability Database
automating vulnerability management, security measurement, and compliance checking
Vulnerabilities
Checklists
800-53/800-53A
Product Dictionary
Home
SCAP
SCAP Validated Tools
SCAP Events

Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

Resource Status

NVD contains:

54685 CVE Vulnerabilities
202 Checklists
222 US-CERT Alerts
2677 US-CERT Vuln Notes
8140 OVAL Queries

Last updated:
Sun Jan 20 10:30:33 EST 2013

CVE Publication

Search CVE and CCE Vulnerability Database

(Advanced Search)

Keyword search: ipv6 [Search]

Try a product or vendor name
Try a CVE standard vulnerability name or OVAL query
Only vulnerabilities that match ALL keywords will be returned
Linux kernel vulnerabilities are categorized separately from vulnerabilities in specific Linux distributions

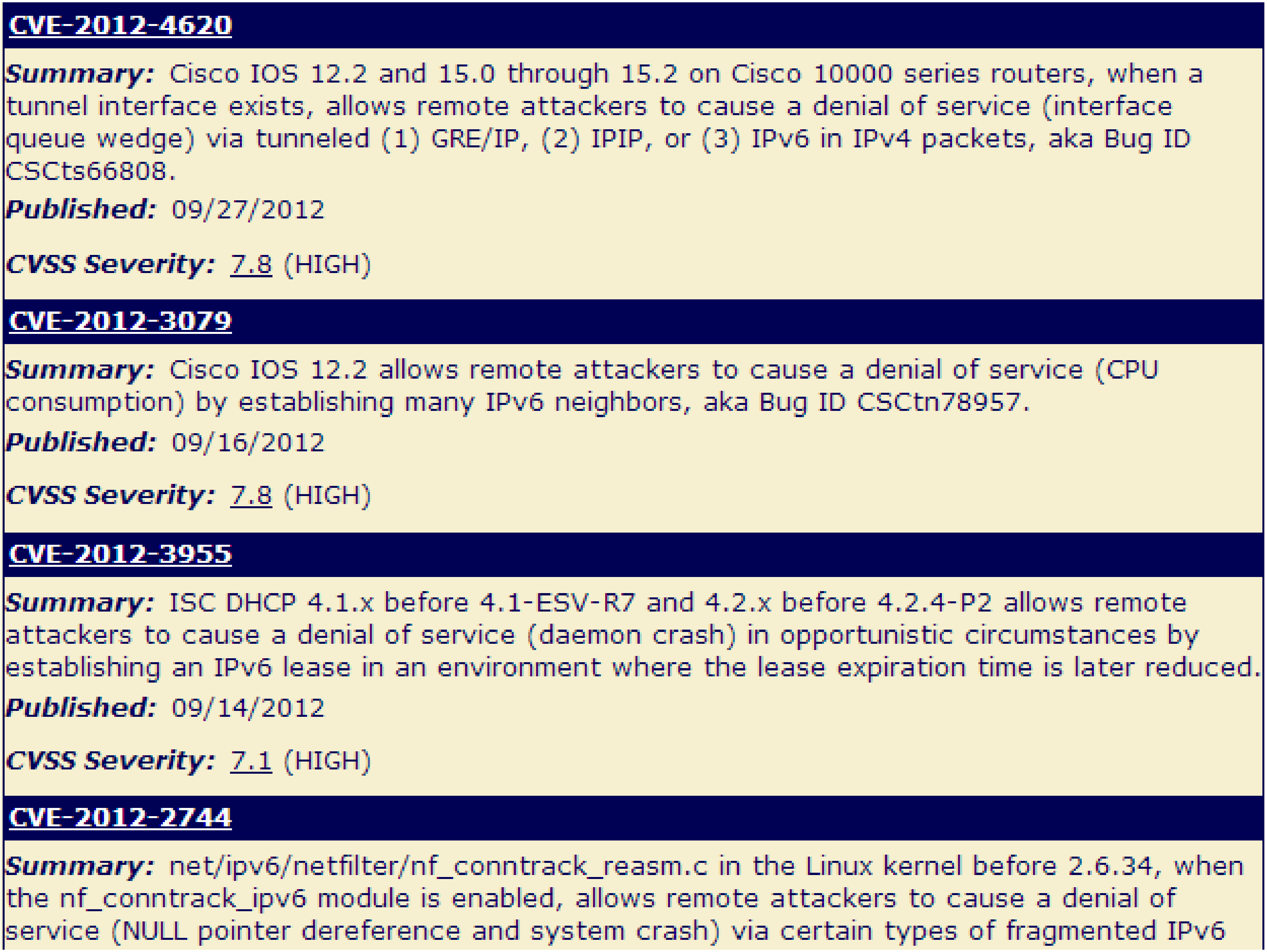
● Search All
○ Search Last 3 Months
○ Search Last 3 Years

Show only vulnerabilities that have the following associated resources:

☑ Software Flaws (CVE)
□ Misconfigurations (CCE), under development

□ US-CERT Technical Alerts
□ US-CERT Vulnerability Notes
□ OVAL Queries

NVD now maps to CWE! See NVD CWE for more details.



CVE-2012-4620

Summary: Cisco IOS 12.2 and 15.0 through 15.2 on Cisco 10000 series routers, when a tunnel interface exists, allows remote attackers to cause a denial of service (interface queue wedge) via tunneled (1) GRE/IP, (2) IPIP, or (3) IPv6 in IPv4 packets, aka Bug ID CSCts66808.

Published: 09/27/2012

CVSS Severity: 7.8 (HIGH)

CVE-2012-3079

Summary: Cisco IOS 12.2 allows remote attackers to cause a denial of service (CPU consumption) by establishing many IPv6 neighbors, aka Bug ID CSCtn78957.

Published: 09/16/2012

CVSS Severity: 7.8 (HIGH)

CVE-2012-3955

Summary: ISC DHCP 4.1.x before 4.1-ESV-R7 and 4.2.x before 4.2.4-P2 allows remote attackers to cause a denial of service (daemon crash) in opportunistic circumstances by establishing an IPv6 lease in an environment where the lease expiration time is later reduced.

Published: 09/14/2012

CVSS Severity: 7.1 (HIGH)

CVE-2012-2744

Summary: net/ipv6/netfilter/nf_conntrack_reasm.c in the Linux kernel before 2.6.34, when the nf_conntrack_ipv6 module is enabled, allows remote attackers to cause a denial of service (NULL pointer dereference and system crash) via certain types of fragmented IPv6

Flood Router 6

- http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-4669

- The Neighbor Discovery (ND) protocol implementation in the IPv6 stack in Microsoft Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7 allows remote attackers to cause a denial of service (CPU consumption and system hang) by sending many Router Advertisement (RA) messages with different source addresses, as demonstrated by the flood_router6 program in the thc-ipv6 package.

UTube of FloodRouter6

- **IPv6 DOS Attack Windows 8 Consumer Preview Release (**FloodRouter6**)**
- **http://www.youtube.com/watch?v=TfsfNWHCKK0**

Easy to get these!

- PARSITE6 : ICMP Neighbor Spoofer for Man-in-the-Middle attacks
- DOS-NEW-IPv6 : Deny any new IPv6 system access to the LAN
- REDIR6 : Redirect traffic to your host on a LAN
- FAKE Router : Become the default router, implant routes
- SMURF6 : Local SMURF tool – attack your own LAN
- RSMURF6 : Remote SMURF tool – attack a remote LAN
- TOOBIG6 : Reduce the MTU of a target

Hacker Tools

- Scanners
  - IPv6 security scanner
  - Halfscan6
  - Nmap
  - Strobe
  - Netcat

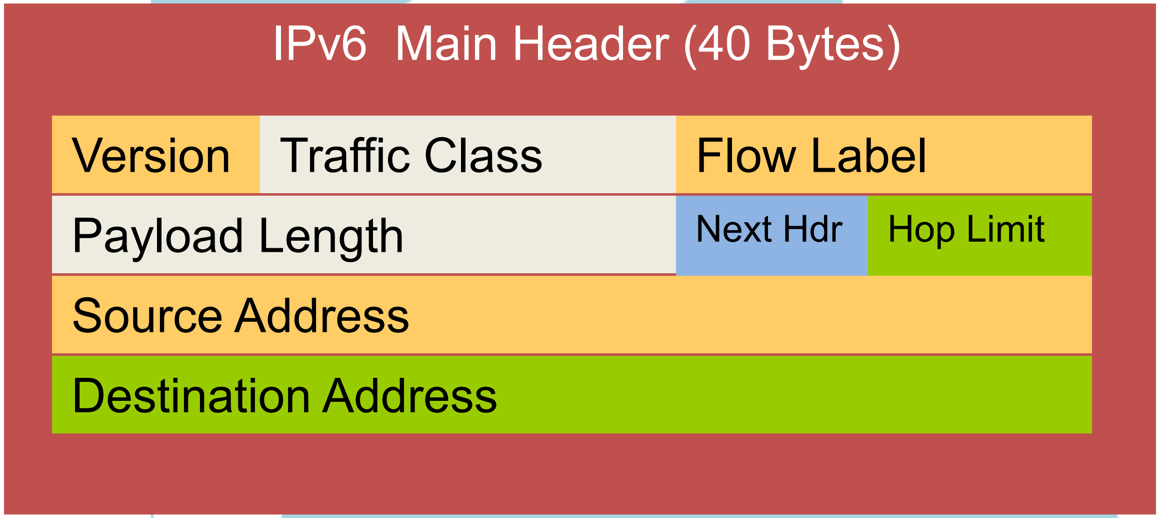
- DoS Tools
  - 6tunneldos
  - 4to6ddos
  - Imps6-tools

- Packet forgers
  - Scapy6
  - SendIP
  - Packit
  - Spak6

- Port bouncers:
  - Relay6
  - 6tunnel
  - Nt6tunnel
  - asybo

Malformed Packets

- Manipulate headers
  - IPv6 incorrect or partial header
  - Violate header order
  - Violate header option restrictions
- IPv6 Main header required
- Contains addressing and control information
- Fixed 40 bytes.



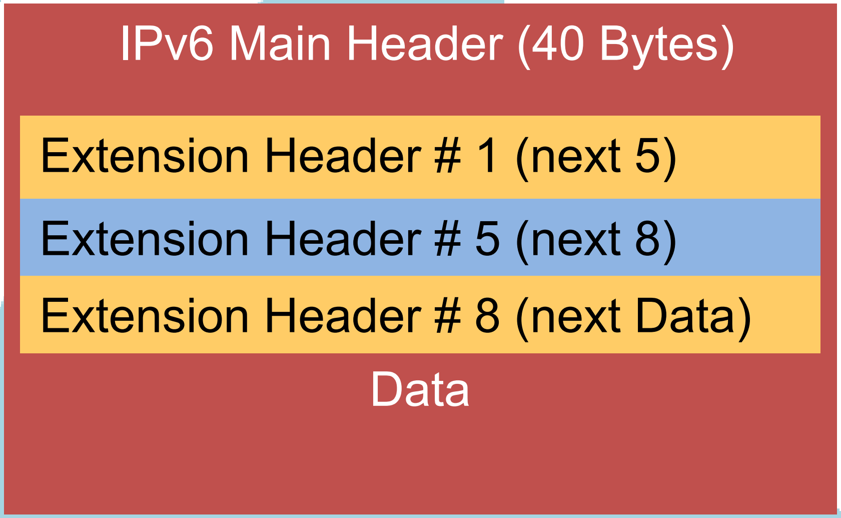
IPv6 Main Header (40 Bytes)

Version	Traffic Class	Flow Label	
Payload Length		Next Hdr	Hop Limit
Source Address			
Destination Address			

IPv6 Extension Headers

- New: IPv6 extension headers
- Next Header field chains headers

- Rules:
  - May appear only once
  - Must appear in fixed order
  - Exception: Destination Options



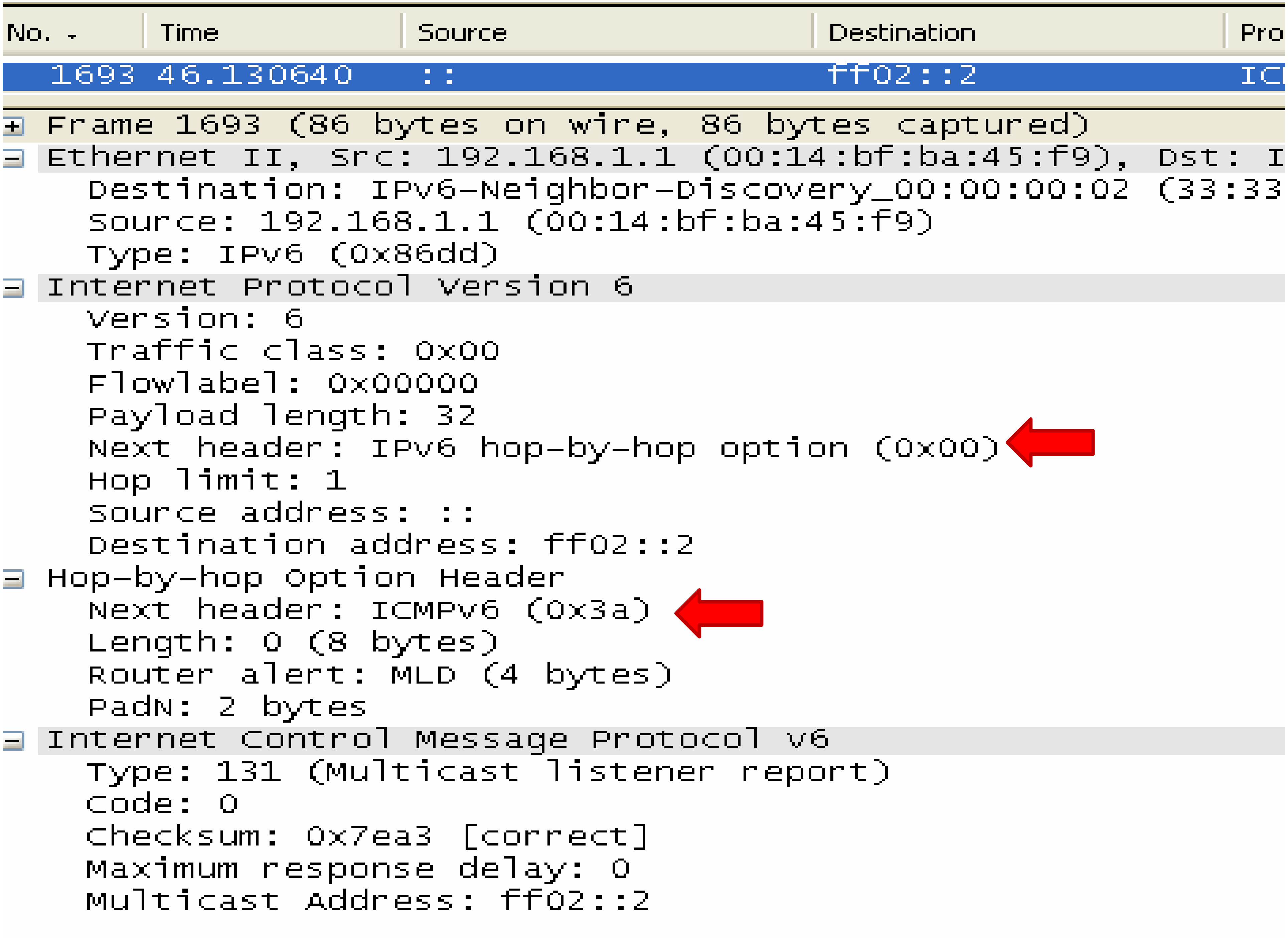
IPv6 Main Header (40 Bytes)

Extension Header # 1 (next 5)

Extension Header # 5 (next 8)

Extension Header # 8 (next Data)

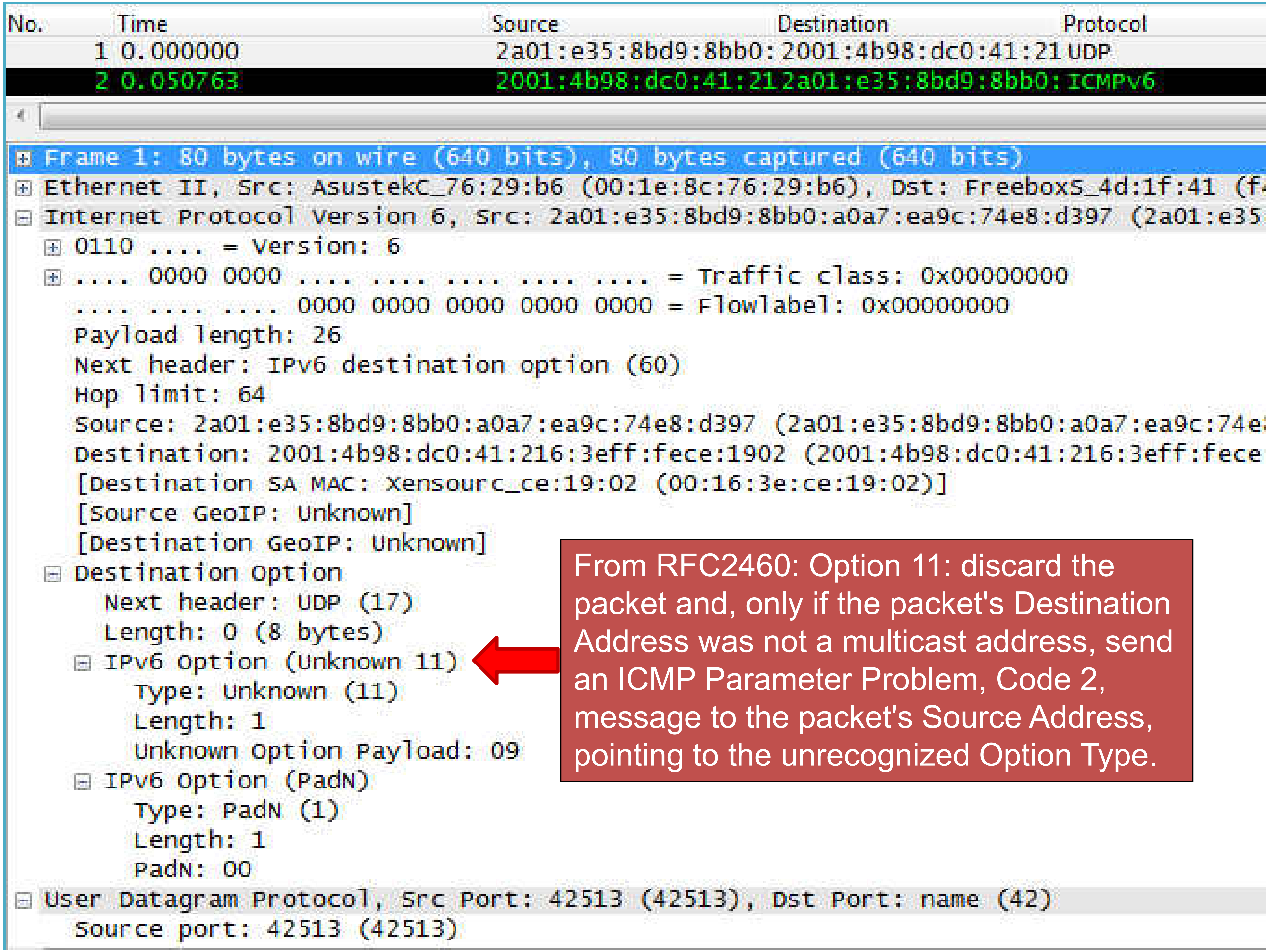
Data



```
No. -     Time            Source                         Destination                   Pro
   1693 46.130640      ::                             ff02::2                       ICI

+ Frame 1693 (86 bytes on wire, 86 bytes captured)
- Ethernet II, Src: 192.168.1.1 (00:14:bf:ba:45:f9), Dst: I
     Destination: IPv6-Neighbor-Discovery_00:00:00:02 (33:33
     Source: 192.168.1.1 (00:14:bf:ba:45:f9)
     Type: IPv6 (0x86dd)
- Internet Protocol Version 6
     Version: 6
     Traffic class: 0x00
     Flowlabel: 0x00000
     Payload length: 32
     Next header: IPv6 hop-by-hop option (0x00)
     Hop limit: 1
     Source address: ::
     Destination address: ff02::2
- Hop-by-hop Option Header
     Next header: ICMPv6 (0x3a)
     Length: 0 (8 bytes)
     Router alert: MLD (4 bytes)
     PadN: 2 bytes
- Internet Control Message Protocol v6
     Type: 131 (Multicast listener report)
     Code: 0
     Checksum: 0x7ea3 [correct]
     Maximum response delay: 0
     Multicast Address: ff02::2
```

Common IPv6 Extension Headers

Next Header (Decimal)	Header Name	Description
0	Hop-by-Hop Options	For all devices on the path
43	Routing	0 – Source Routing (deprecated) 2 – Mobile IPv6
44	Fragment	Only when packet is fragmented
50	Encapsulated Security Payload (ESP)	IPSec encrypted data
51	Authentication Header (AH)	IPSec authentication
60	Destination Options	http://www.iana.org/assignments/ipv6-parameters/ipv6-parameters.xml (Mobile IP, etc.)

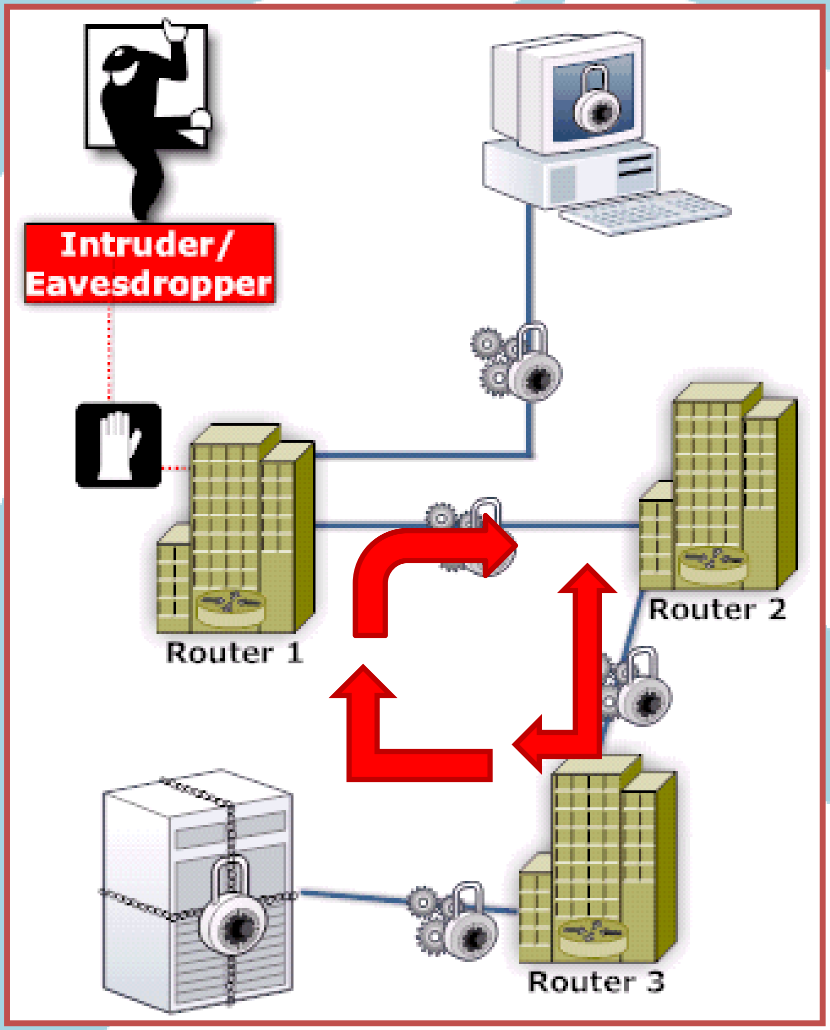


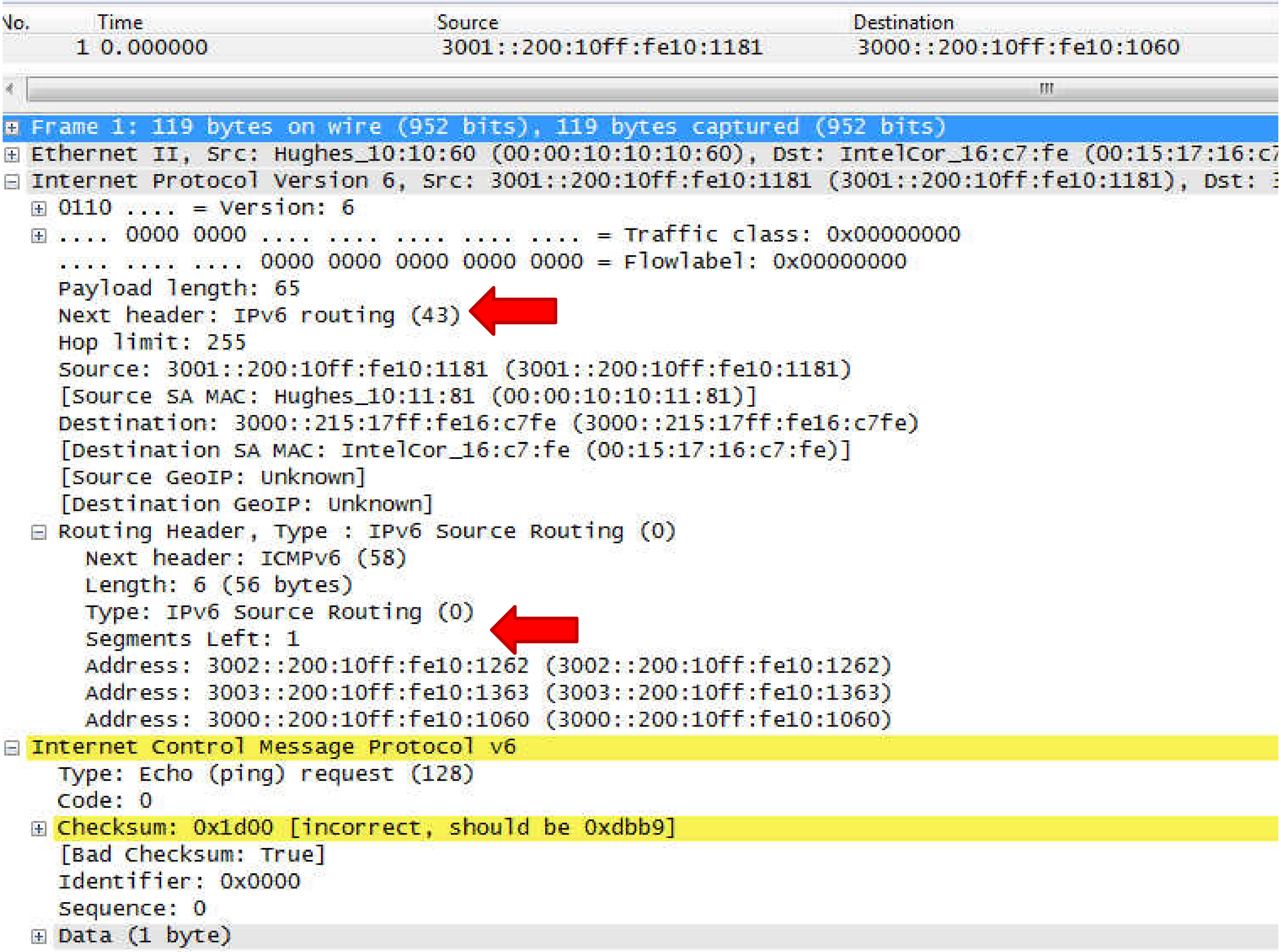
```
No.     Time                    Source                  Destination             Protocol
      1 0.000000                2a01:e35:8bd9:8bb0:2001:4b98:dc0:41:21 UDP
      2 0.050763                2001:4b98:dc0:41:21 2a01:e35:8bd9:8bb0: ICMPv6

⊞ Frame 1: 80 bytes on wire (640 bits), 80 bytes captured (640 bits)
⊞ Ethernet II, Src: AsustekC_76:29:b6 (00:1e:8c:76:29:b6), Dst: FreeboxS_4d:1f:41 (f4
⊟ Internet Protocol Version 6, Src: 2a01:e35:8bd9:8bb0:a0a7:ea9c:74e8:d397 (2a01:e35
  ⊞ 0110 .... = Version: 6
  ⊞ .... 0000 0000 .... .... .... .... .... = Traffic class: 0x00000000
    .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
    Payload length: 26
    Next header: IPv6 destination option (60)
    Hop limit: 64
    Source: 2a01:e35:8bd9:8bb0:a0a7:ea9c:74e8:d397 (2a01:e35:8bd9:8bb0:a0a7:ea9c:74e
    Destination: 2001:4b98:dc0:41:216:3eff:fece:1902 (2001:4b98:dc0:41:216:3eff:fece
    [Destination SA MAC: Xensourc_ce:19:02 (00:16:3e:ce:19:02)]
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
  ⊟ Destination Option
      Next header: UDP (17)
      Length: 0 (8 bytes)
    ⊟ IPv6 Option (Unknown 11)
        Type: Unknown (11)
        Length: 1
        Unknown Option Payload: 09
    ⊟ IPv6 Option (PadN)
        Type: PadN (1)
        Length: 1
        PadN: 00
⊟ User Datagram Protocol, Src Port: 42513 (42513), Dst Port: name (42)
    Source port: 42513 (42513)
```

From RFC2460: Option 11: discard the packet and, only if the packet's Destination Address was not a multicast address, send an ICMP Parameter Problem, Code 2, message to the packet's Source Address, pointing to the unrecognized Option Type.

RFC5095 (Deprecation of Type 0 Routing Headers in IPv6)

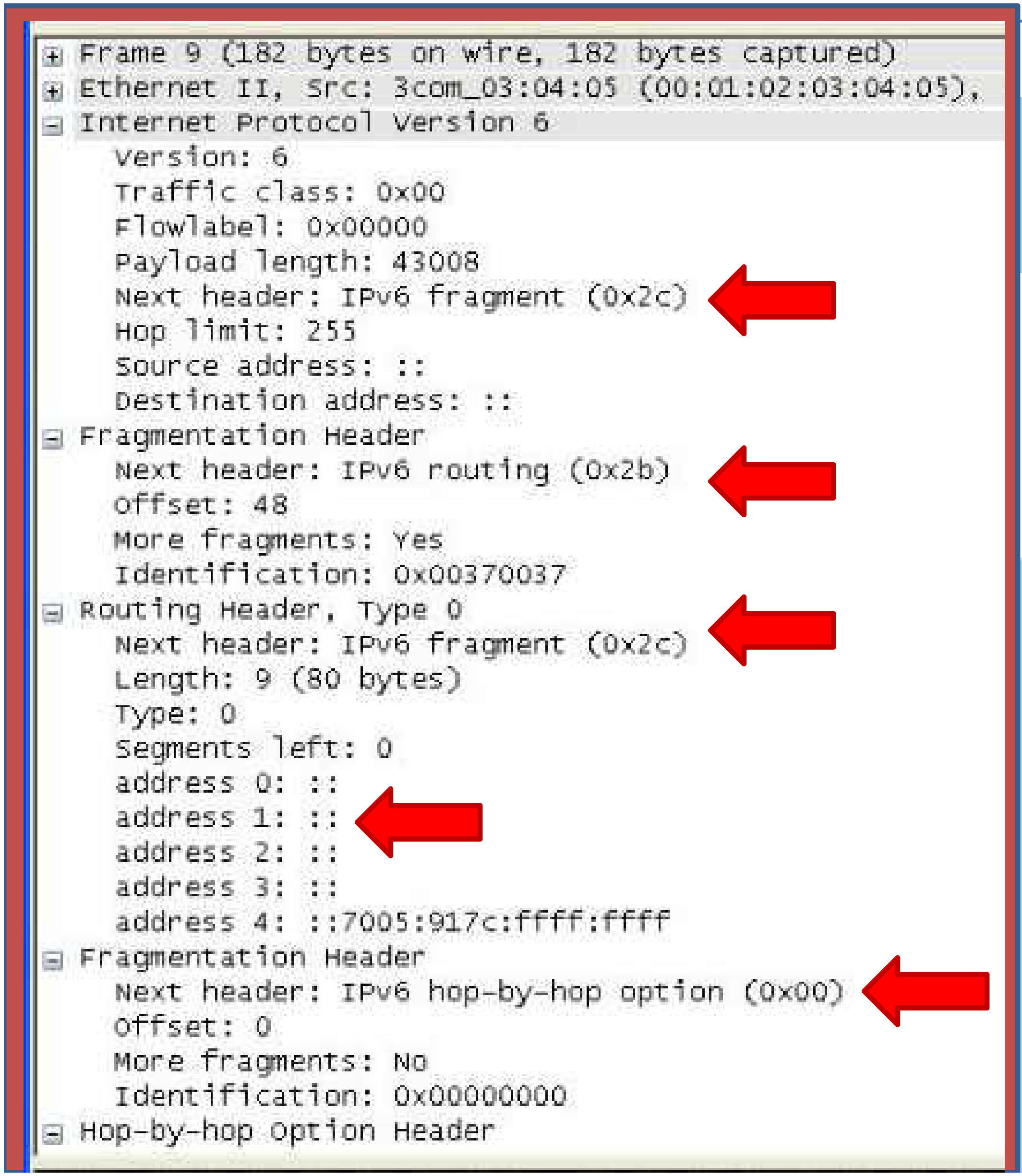
- RH0 : create routing loops.
- Deprecated
- Segments Left =zero, ignore
- Segments Left > zero, send ICMPv6





```
No.     Time                     Source                            Destination
     1 0.000000                  3001::200:10ff:fe10:1181          3000::200:10ff:fe10:1060

⊞ Frame 1: 119 bytes on wire (952 bits), 119 bytes captured (952 bits)
⊞ Ethernet II, Src: Hughes_10:10:60 (00:00:10:10:10:60), Dst: IntelCor_16:c7:fe (00:15:17:16:c7
⊟ Internet Protocol Version 6, Src: 3001::200:10ff:fe10:1181 (3001::200:10ff:fe10:1181), Dst: 3
  ⊞ 0110 .... = Version: 6
  ⊞ .... 0000 0000 .... .... .... .... .... = Traffic class: 0x00000000
    .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
    Payload length: 65
    Next header: IPv6 routing (43)
    Hop limit: 255
    Source: 3001::200:10ff:fe10:1181 (3001::200:10ff:fe10:1181)
    [Source SA MAC: Hughes_10:11:81 (00:00:10:10:11:81)]
    Destination: 3000::215:17ff:fe16:c7fe (3000::215:17ff:fe16:c7fe)
    [Destination SA MAC: IntelCor_16:c7:fe (00:15:17:16:c7:fe)]
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
  ⊟ Routing Header, Type : IPv6 Source Routing (0)
      Next header: ICMPv6 (58)
      Length: 6 (56 bytes)
      Type: IPv6 Source Routing (0)
      Segments Left: 1
      Address: 3002::200:10ff:fe10:1262 (3002::200:10ff:fe10:1262)
      Address: 3003::200:10ff:fe10:1363 (3003::200:10ff:fe10:1363)
      Address: 3000::200:10ff:fe10:1060 (3000::200:10ff:fe10:1060)
⊟ Internet Control Message Protocol v6
    Type: Echo (ping) request (128)
    Code: 0
  ⊞ Checksum: 0x1d00 [incorrect, should be 0xdbb9]
    [Bad Checksum: True]
    Identifier: 0x0000
    Sequence: 0
  ⊞ Data (1 byte)
```

Crafted Packet

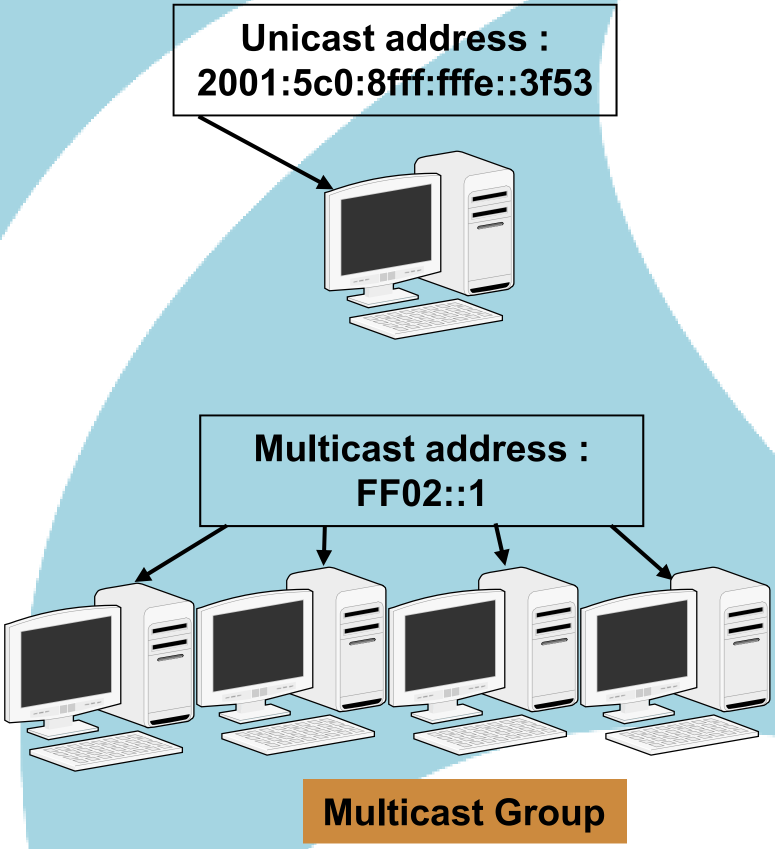


```
⊞ Frame 9 (182 bytes on wire, 182 bytes captured)
⊞ Ethernet II, Src: 3com_03:04:05 (00:01:02:03:04:05),
⊟ Internet Protocol Version 6
    Version: 6
    Traffic class: 0x00
    Flowlabel: 0x00000
    Payload length: 43008
    Next header: IPv6 fragment (0x2c)
    Hop limit: 255
    Source address: ::
    Destination address: ::
⊟ Fragmentation Header
    Next header: IPv6 routing (0x2b)
    Offset: 48
    More fragments: Yes
    Identification: 0x00370037
⊟ Routing Header, Type 0
    Next header: IPv6 fragment (0x2c)
    Length: 9 (80 bytes)
    Type: 0
    Segments left: 0
    address 0: ::
    address 1: ::
    address 2: ::
    address 3: ::
    address 4: ::7005:917c:ffff:ffff
⊟ Fragmentation Header
    Next header: IPv6 hop-by-hop option (0x00)
    Offset: 0
    More fragments: No
    Identification: 0x00000000
⊟ Hop-by-hop Option Header
```

- Crafted IPv6 packet
- Multiple headers
- Deprecated headers
- Headers out of order

IPv6 Multicast

- In IPv6, multicasting used widely
- Multicast is like a newsletter subscription.
- Devices belong to a multicast group
- IPv4 multicast uses Class D range: (224.xx.xx.xx – 239.xx.xx.xx)



Common IPv6 Multicast Groups

- IPv6 multicast addresses start with FF.
- See some common groups below.
- Multicast addresses are registered with the Internet Assigned Numbers Authority (IANA).
- For more, see: http://www.iana.org/assignments/ipv6-multicast-addresses/ipv6-multicast-addresses.xml

IPv6 multicast address	**Description**
FF02::1	**The all-nodes address**
FF02::2	**The all-routers address**
FF02::5	**The all-Open Shortest Path First (OSPF) routers address**
FF02::6	**The all-OSPF designated routers address**

IPv6 Multicast Scope

- Last 4 bits is scope. (Ex. FF01, FF02, etc.)

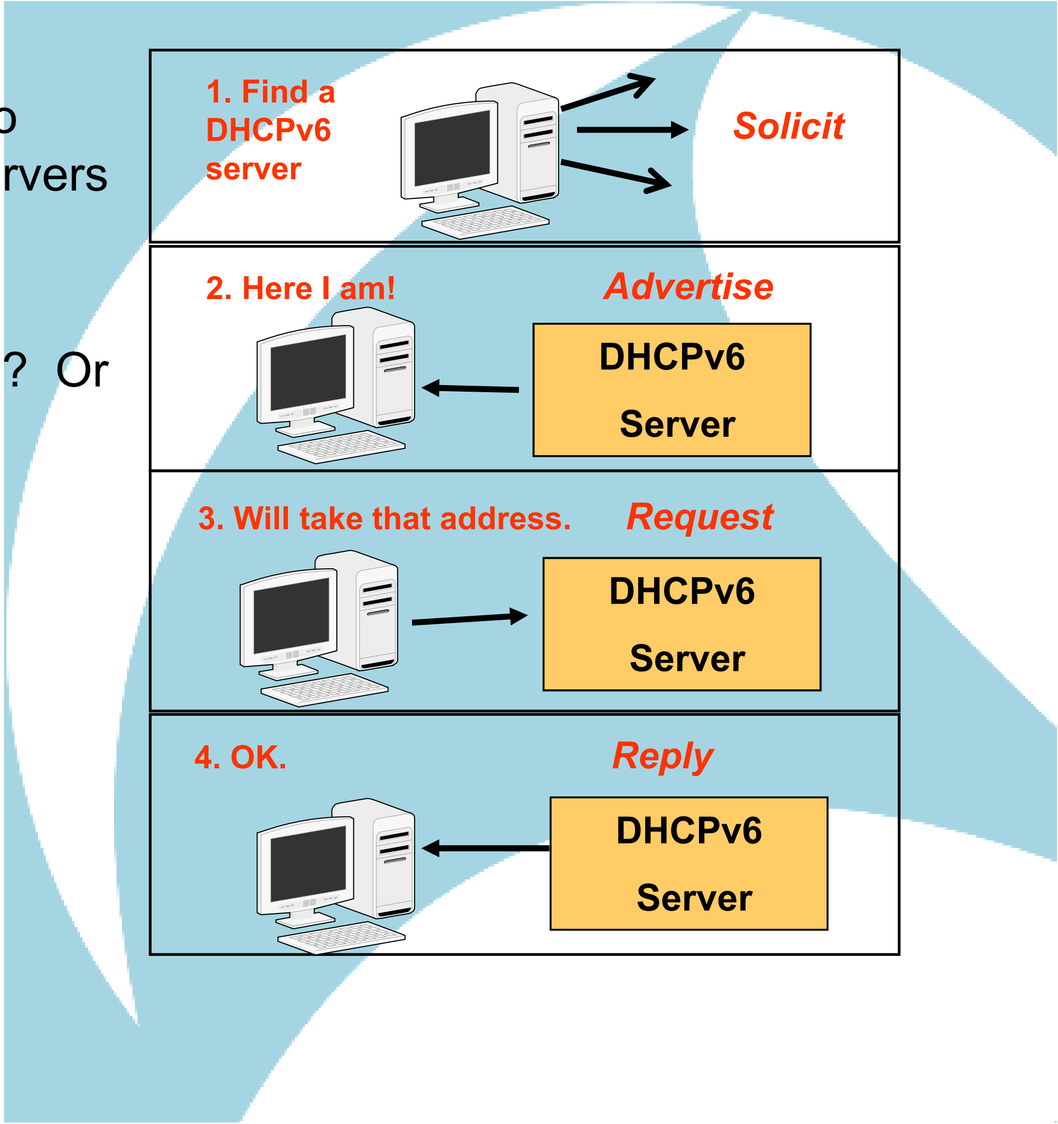
- FF01:: means on same interface
- FF02:: means on same link
- FF05:: means in the same site
- FF0E:: means in the Internet (all reachable).

(From RFC 4291)

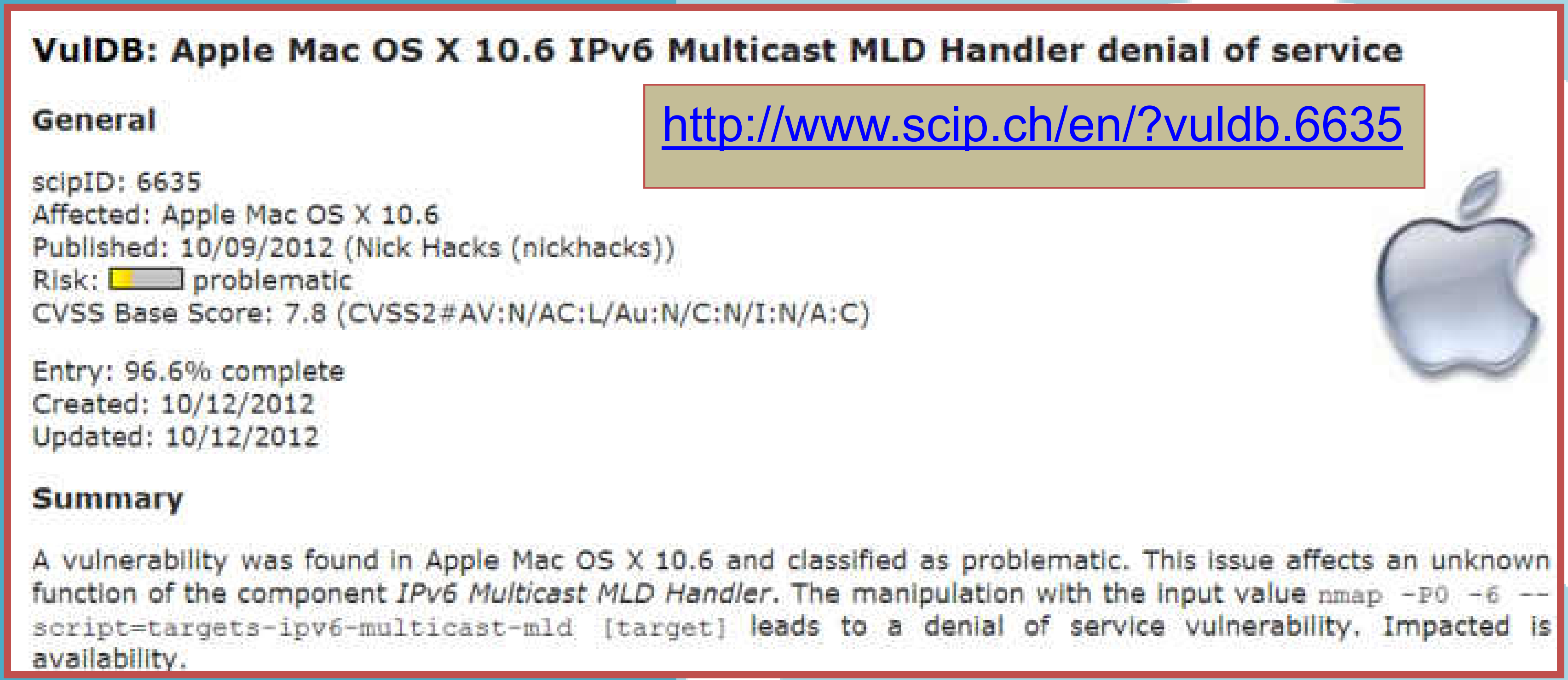
DHCPv6 Flow : Start

1. Client sends a ***Solicit*** message to All_DHCP_Relay_Agents_and_Servers (FF02::1:2)

2. How if I craft a Solicit to FF05::1:2? Or FF0E::1:2?



Multicast Storms



VulDB: Apple Mac OS X 10.6 IPv6 Multicast MLD Handler denial of service

http://www.scip.ch/en/?vuldb.6635

General

scipID: 6635
Affected: Apple Mac OS X 10.6
Published: 10/09/2012 (Nick Hacks (nickhacks))
Risk: ▨ problematic
CVSS Base Score: 7.8 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C)

Entry: 96.6% complete
Created: 10/12/2012
Updated: 10/12/2012

Summary

A vulnerability was found in Apple Mac OS X 10.6 and classified as problematic. This issue affects an unknown function of the component *IPv6 Multicast MLD Handler*. The manipulation with the input value `nmap -P0 -6 --script=targets-ipv6-multicast-mld [target]` leads to a denial of service vulnerability. Impacted is availability.

- Many hosts in a subnet
- Not filtering multicast (router or firewall)
- OS Bug

- Router-based controls
- Overrated?

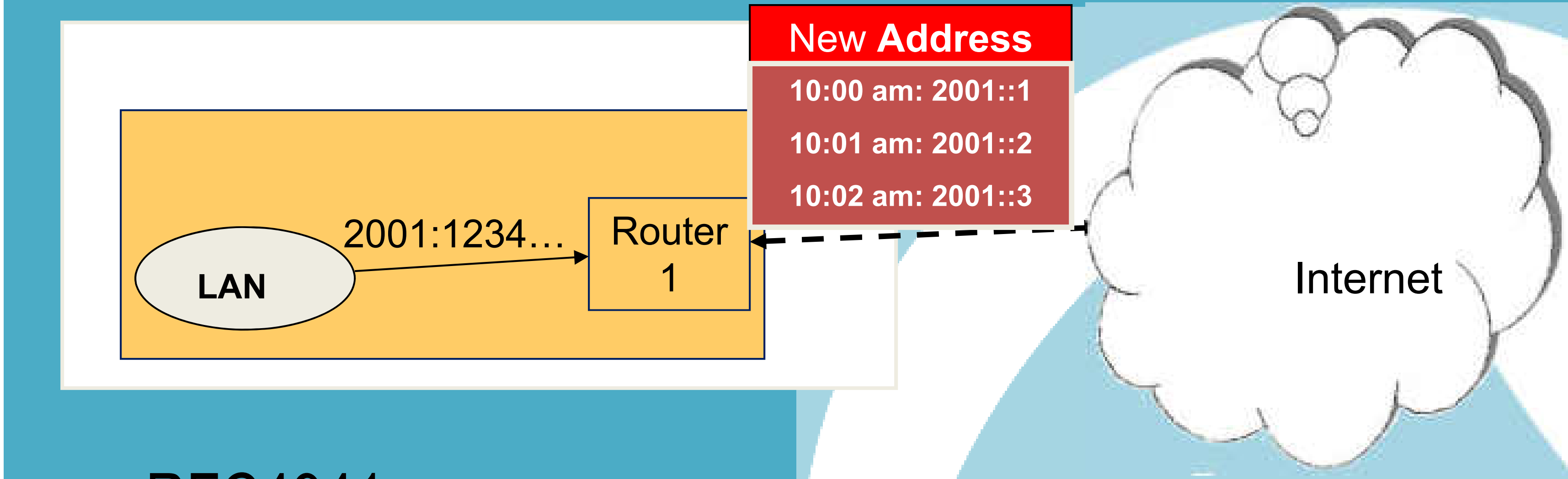
Temporary Addresses

- MAC ➔ IID
- IPv6 Address ➔ MAC

Example on Windows PC: result of IPConfig

```
Ethernet adapter Local Area Connection:
Description  : Realtek Family Fast Ethernet NIC
Physical Address : 00-11-D8-39-29-2B
Autoconfiguration Enabled . : Yes
IP Address : fe80::211:d8ff:fe39:292b%4
```

How to Create



New Address

10:00 am: 2001::1

10:01 am: 2001::2

10:02 am: 2001::3

LAN

2001:1234…

Router 1

Internet

- RFC4941
- Change address frequently
- DHCPv6 temporary addresses

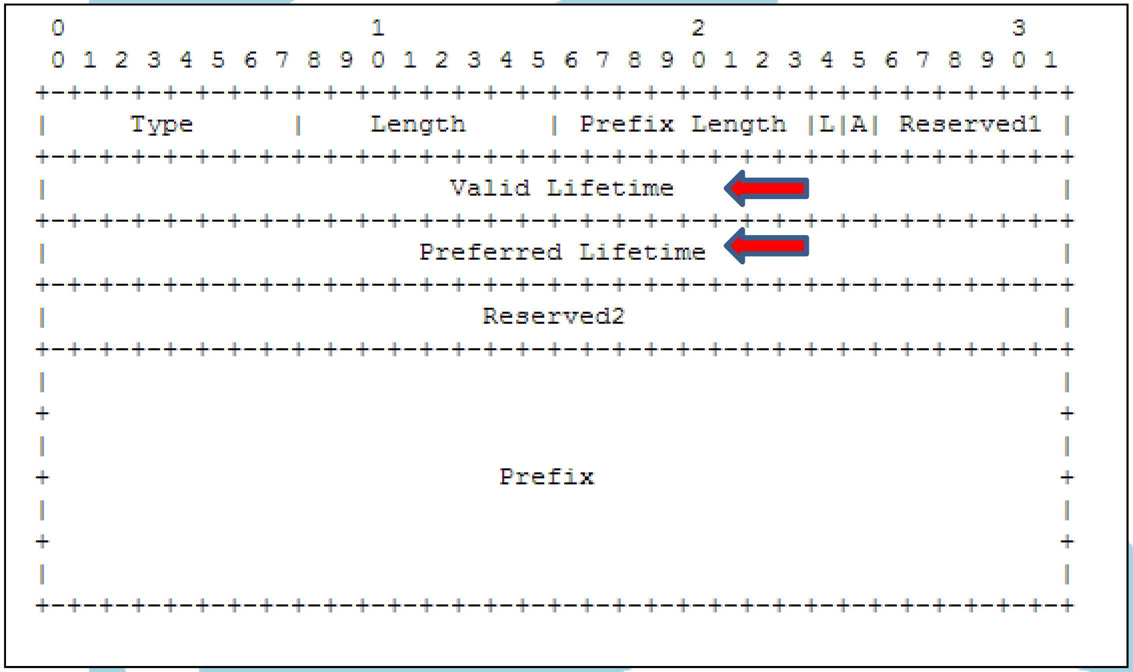
DHCPv6 Temporary Addresses

iface "Local Area Connection" { ta }

Temporary Address Guidelines

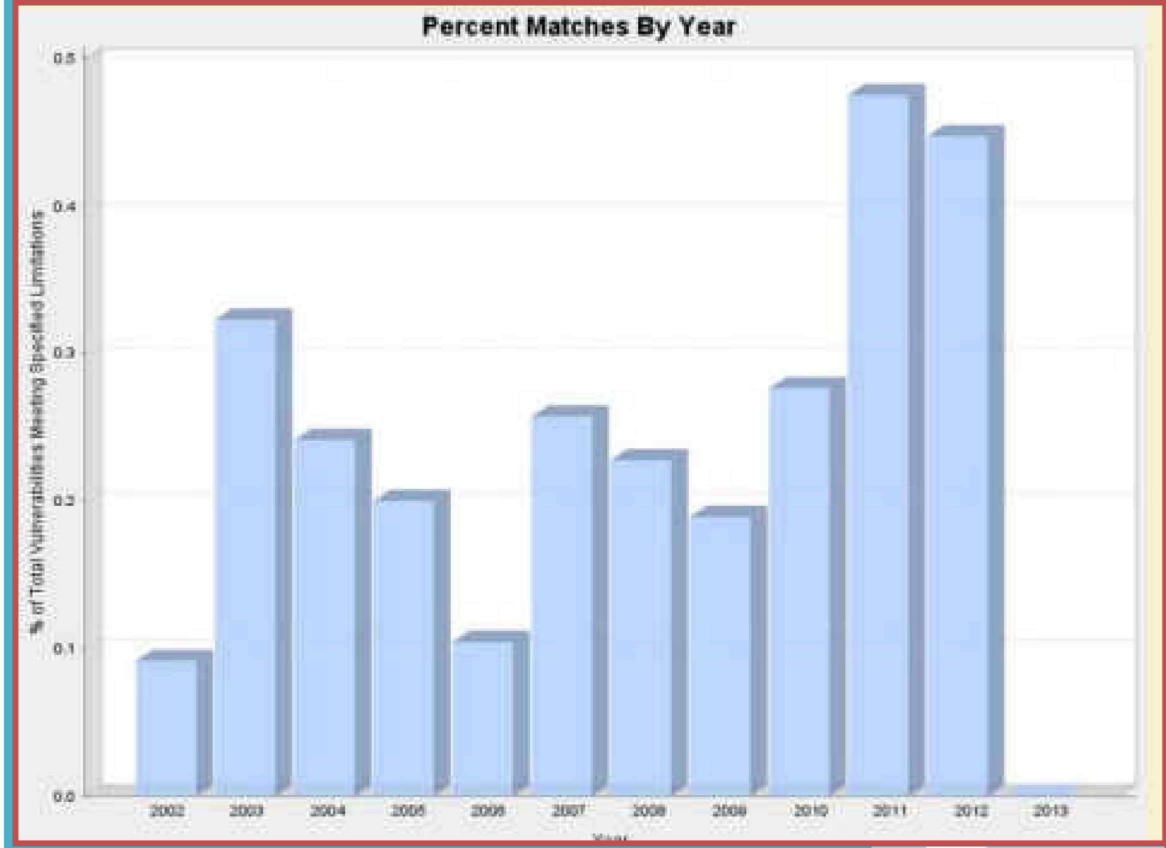
- RA can change PREFLIFETIME
- Rogue RA? Controls in OS?
- Short preferred lifetime = many new temporary addresses
- Small PREFLIFETIME with large VALIDLIFETIME can impact storage

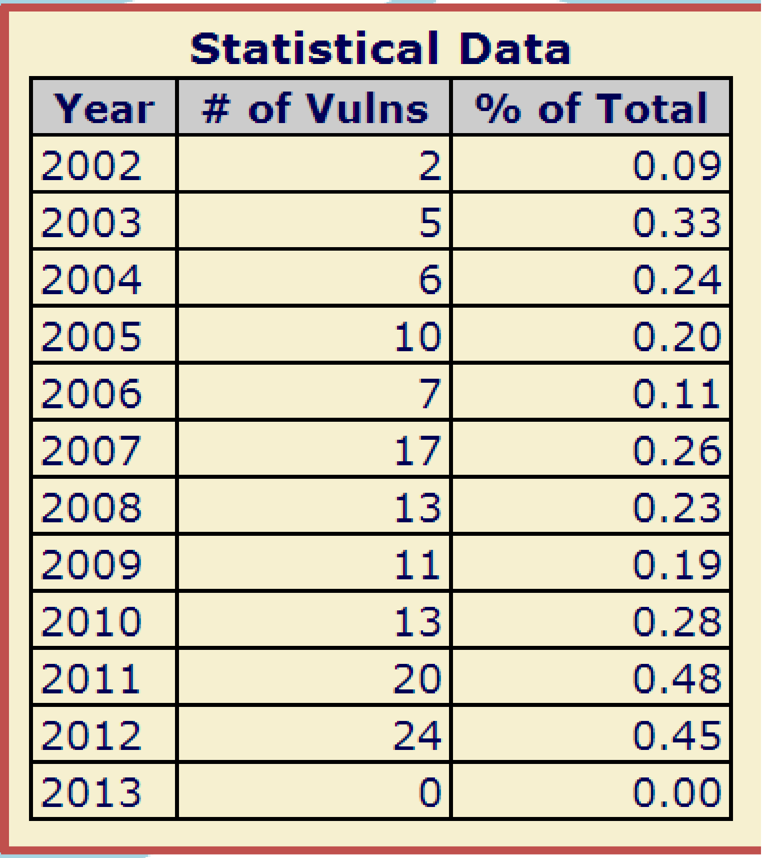
Router Advertisement Prefix Information



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     | Prefix Length |L|A| Reserved1 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Valid Lifetime                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Preferred Lifetime                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           Reserved2                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                            Prefix                             +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

CERT Database IPv6 (S/W Flaws)





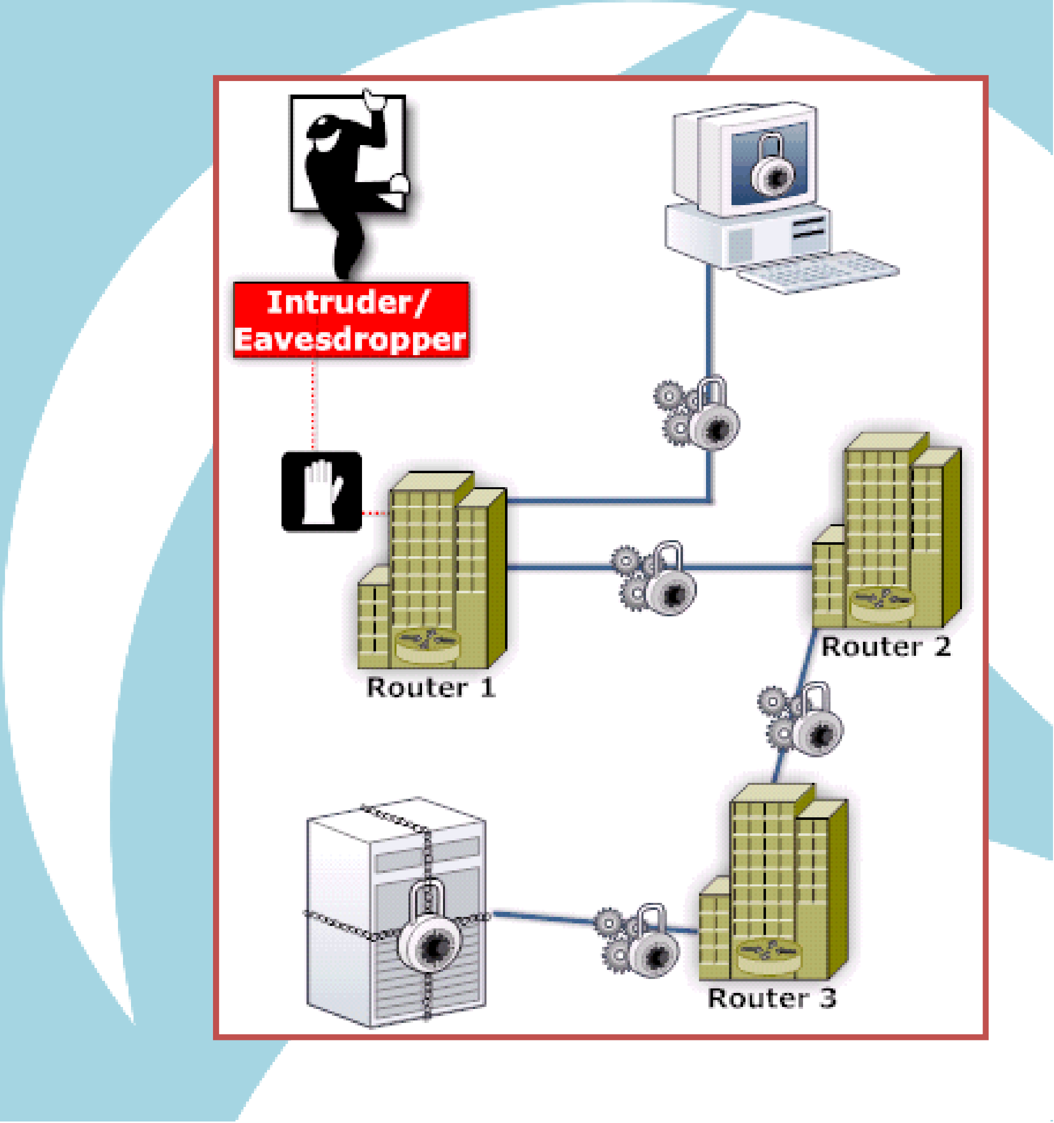
Statistical Data

Year	# of Vulns	% of Total
2002	2	0.09
2003	5	0.33
2004	6	0.24
2005	10	0.20
2006	7	0.11
2007	17	0.26
2008	13	0.23
2009	11	0.19
2010	13	0.28
2011	20	0.48
2012	24	0.45
2013	0	0.00

Summary

- What is more secure?
  - Ping sweeps
  - Hacker lack of knowledge

- What is less secure?
  - DNS / other servers targets
  - Local networks vulnerable
  - Good guys lack of knowledge (biggest!)


Intruder/
Eavesdropper
Router 1
Router 2
Router 3