IPv6 Security Threats and Mitigations

Rohit Bothra (rbothra@cisco.com)
Dilip Sai Chandar(dipasupu@cisco.com)

Network Consulting Engineer, Cisco

APRICOT Feb-March 2012

Agenda

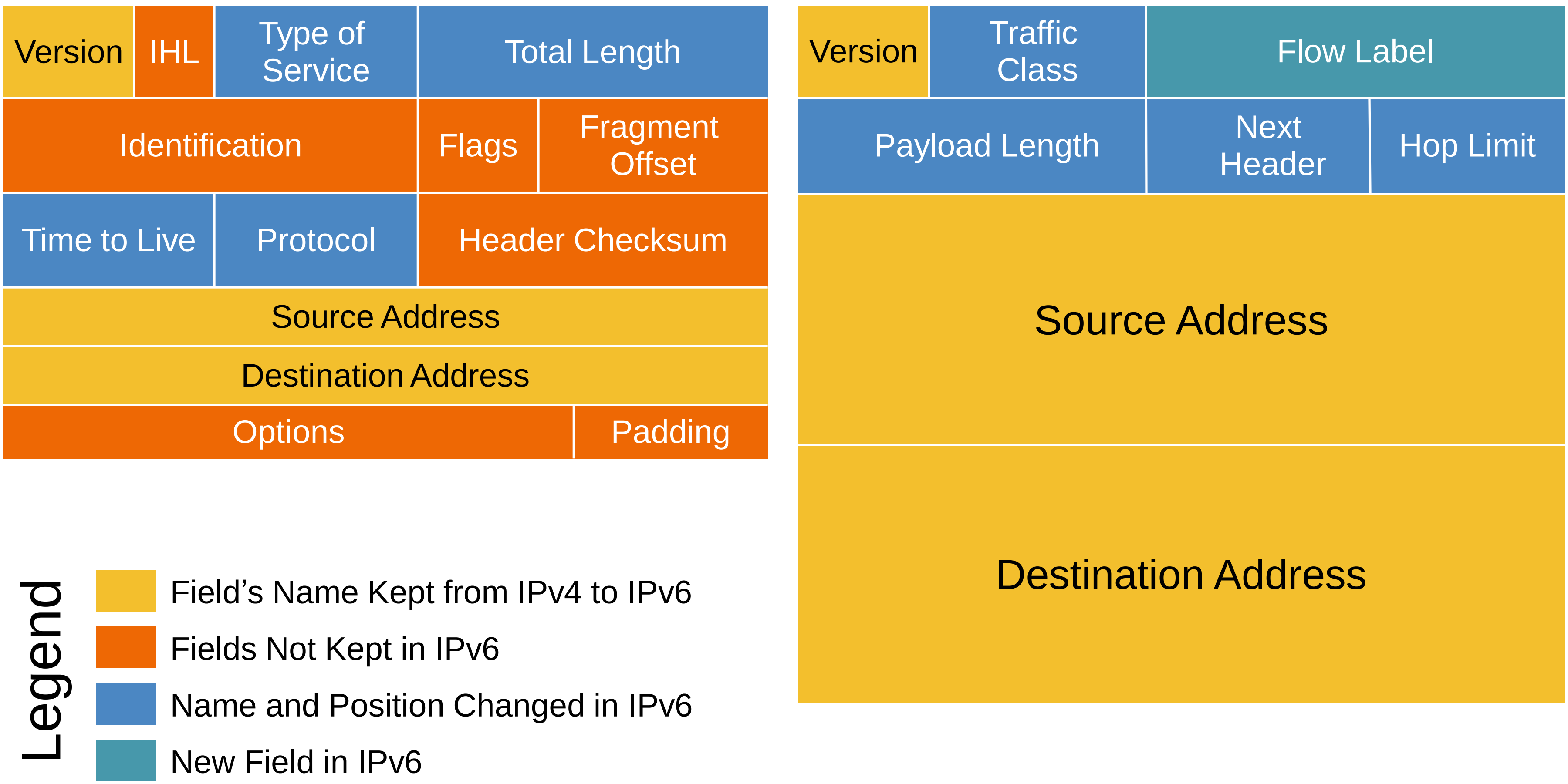
- IPv6 Primer
- Security Issues Shared by IPv4 and IPv6
- Security Issues Specific to IPv6
- Enforcing Security policies
- Cisco IPv6 Products
- Demo: IPv6 DoS attack
- References

IPv6 Primer

IPv4 and IPv6 Header Comparison

IPv4 Header

IPv6 Header



IPv6 Address Types

- Three types of unicast address scopes

Link-Local – Non routable exists on single layer 2 domain (FE80::/64)

FE80:0000:0000:0000: xxxx:xxxx:xxxx:xxxx

Unique-Local (ULA) – Routable with an administrative domain (FC00::/7)

FC00:gggg:gggg: ssss: xxxx:xxxx:xxxx:xxxx

Global – Routable across the Internet (2000::/3)

2000:GGGG:GGGG: ssss: xxxx:xxxx:xxxx:xxxx

- Interface “expected” to have multiple addresses

- Multicast addresses begin with FF00::/8

FFfs: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx

IPv6 Addresses – Unicast and Multicast
Examples

```
Router#sh ipv6 int Ethernet0
Ethernet0 is up, line protocol is up
  IPv6 is enabled, link-local address is
FE80::2D0:D3FF:FE81:9000

  Global unicast address(es):
          2001:DB8:12::1, subnet is 2001:DB8:12::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::5
    FF02::D
    FF02::16
    FF02::1:FF00:1
    FF02::1:FF81:9000
```

- **Link-Local** — FE80::2D0:D3FF:FE81:9000
- **Global** — 2001:DB8:12::/64
- **All nodes** — FF02::1
- **All routers** — FF02::2
- **OSPF Routers** — FF02::5
- **All PIM Routers** — FF02::D
- **All MLDv2 capable Routers** — FF02::16

ICMPv4 vs. ICMPv6

Covers ICMP (v4) features: Error control, Administration, …

Transports ND messages: NS, NA, RS, RA
Transports MLD messages: Queries, Reports, …

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

IPv6 is not that different than IPv4

- Layer2 remains unchanged
- Layer4 (TCP, UDP..) and above unchanged
- Same routing protocols: BGP, OSPF, RIP
- Only Four major changes
  - Larger Addresses (128 bits compared to 32 bits)
  - Multiple addresses per host.
  - Fixed length header.
  - ARP is replaced with ND protocol.
- But lot of security implications.

Security Issues Shared by IPv4 and IPv6

Reconnaissance in IPv6

- Default subnets in IPv6 have 2^{64} addresses

  10 Mpps = more than 50 000 years

- Public servers will still need to be DNS reachable
- Administrators may adopt easy-to-remember addresses (::10,::20,::F00D, ::C5C0, :d09:f00d or simply IPv4 last octet for dual stack)
- By compromising hosts in a network, an attacker can learn new addresses to scan
- Transition techniques derive IPv6 address from IPv4 address

Reconnaissance in IPv6? Easy with Multicast!

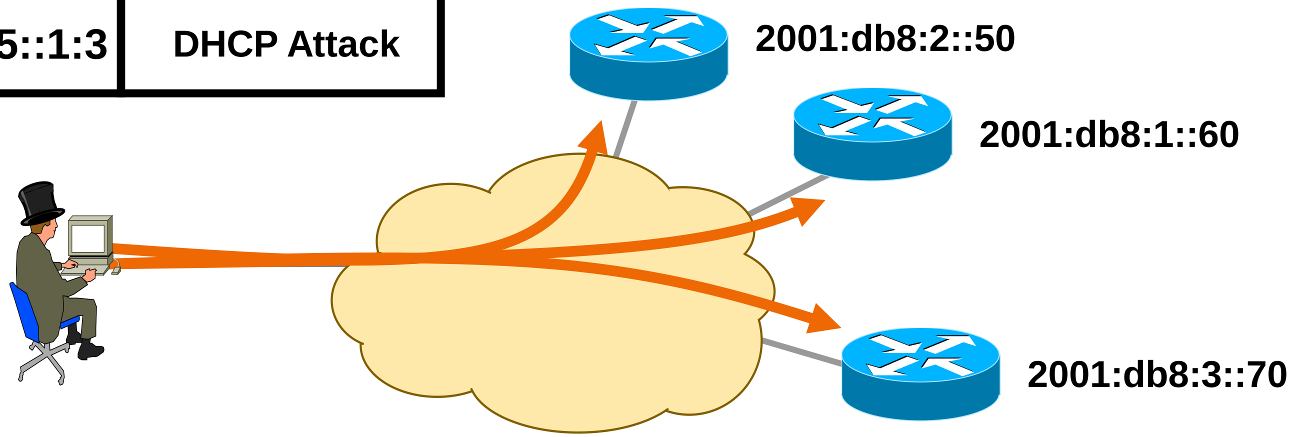
- No need for reconnaissance anymore
- 3 site-local multicast addresses

  FF05::2 all-routers, FF05::FB mDNSv6, FF05::1:3 all DHCP servers

- Several link-local multicast addresses

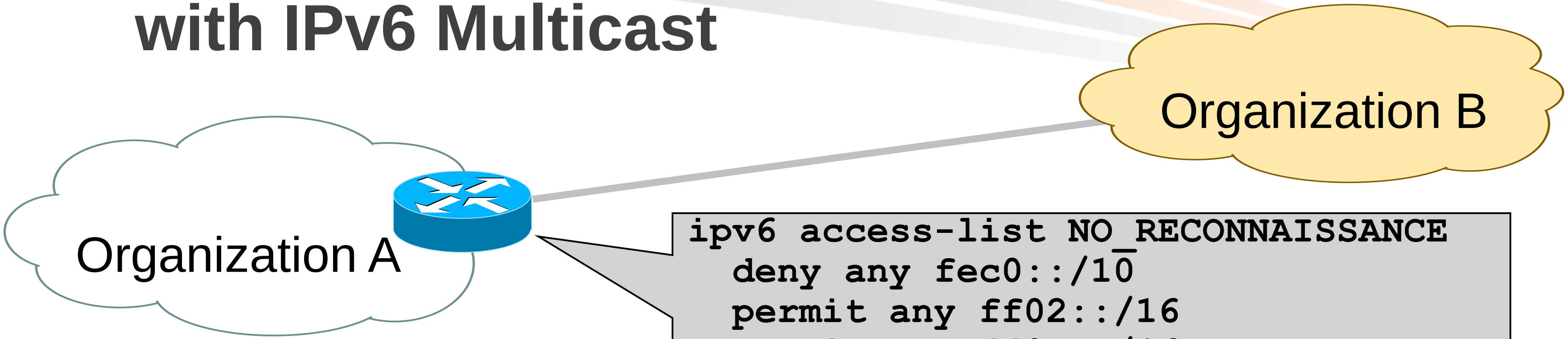
  FF02::1 all nodes, FF02::2 all routers

Source	Destination	Payload
Attacker	FF05::1:3	DHCP Attack



http://www.iana.org/assignments/ipv6-multicast-addresses/

Preventing Reconnaissance with IPv6 Multicast




```
ipv6 access-list NO_RECONNAISSANCE
  deny any fec0::/10
  permit any ff02::/16
  permit any ff0e::/16
  deny any ff00::/8
  permit any any
```

- The site-local/anycast addresses must be filtered at the border in order to make them unreachable from the outside
- ACL block ingress/egress traffic to

  Block FEC0::/10 (deprecated site-local addresses)

  Permit mcast to FF02::/16 (link-local scope)

  Permit mcast to FF0E::/16 (global scope)

  Block all mcast

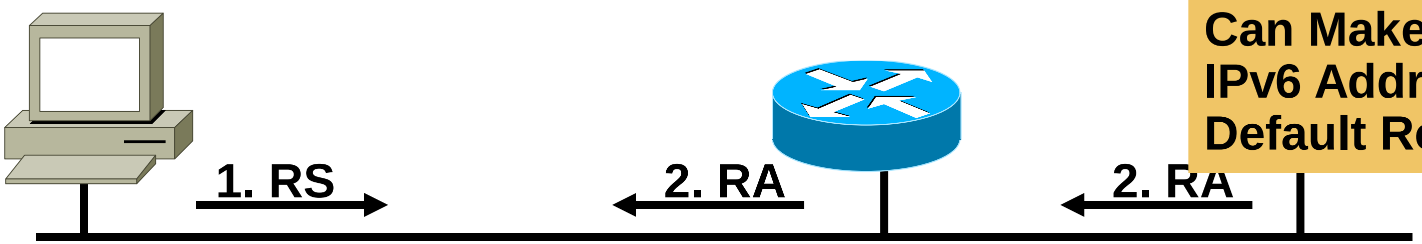
Neighbor Discovery Issue#1 Stateless Autoconfiguration

Router Solicitations Are Sent by Booting Nodes to Request Router Advertisements for Stateless Address Auto-Configuring

RA/RS w/o Any Authentication Gives Exactly Same Level of Security as ARP for IPv4 (None)

Attack Tool: fake_router6

Can Make Any IPv6 Address the Default Router



1. RS:
   - Src = ::
   - Dst = All-Routers multicast Address
   - ICMP Type = 133
   - Data = Query: please send RA
2. RA:
   - Src = Router Link-local Address
   - Dst = All-nodes multicast address
   - ICMP Type = 134
   - Data= options, prefix, lifetime, etc

Neighbor Discovery Issue#2
Neighbor Solicitation

Src = A
Dst = Solicited-node multicast of B
ICMP type = 135
Data = link-layer address of A
Query: what is your link address?

Src = B
Dst = A
ICMP type = 136
Data = link-layer address of B

A and B Can Now Exchange

Packets on This Link

Security Mechanisms Built into Discovery Protocol = None

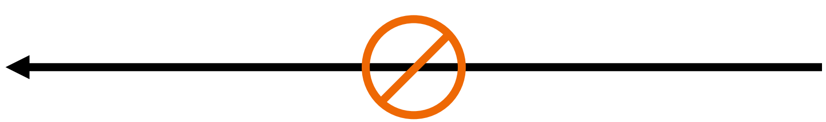
=> Very similar to ARP

Attack Tool:
Parasite6
Answer to all NS, Claiming to Be All Systems in the LAN...

Neighbor Discovery Issue#3 Duplicate Address Detection

Duplicate Address Detection (DAD) Uses neighbor solicitation to verify the existence of an address to be configured

Src = ::
Dst = Solicited-node multicast of A
ICMP type = 135
Data = link-layer address of A
Query = what is your link address?



From RFC 2462:
« If a Duplicate @ Is Discovered… the Address Cannot Be Assigned to the Interface»
⇔What If: Use MAC@ of the Node You Want to DoS and Claim Its IPv6 @

Attack Tool:
Dos-new-ipv6

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

ND threat Mitigation using SEND

Threats	How SEND counters?
Neighbor Solicitation/Advertisement Spoofing	SEND requires the RSA Signature and CGA options to be present in solicitations
Neighbor Unreachability Detection Failure	SEND requires a node responding to Neighbor Solicitations probes to include an RSA Signature option and proof of authorization to use the interface identifier in the address being probed.
Duplicate Address Detection DoS Attack	SEND requires to include an RSA Signature option and proof of authorization in the Neighbor Advertisements sent as responses to DAD
Router Solicitation and Advertisement Attacks	SEND requires Router Advertisements to contain an RSA Signature option and proof of authorization.
Replay Attacks	SEND includes a Nonce option in the solicitation and requires the advertisement to include a matching option.

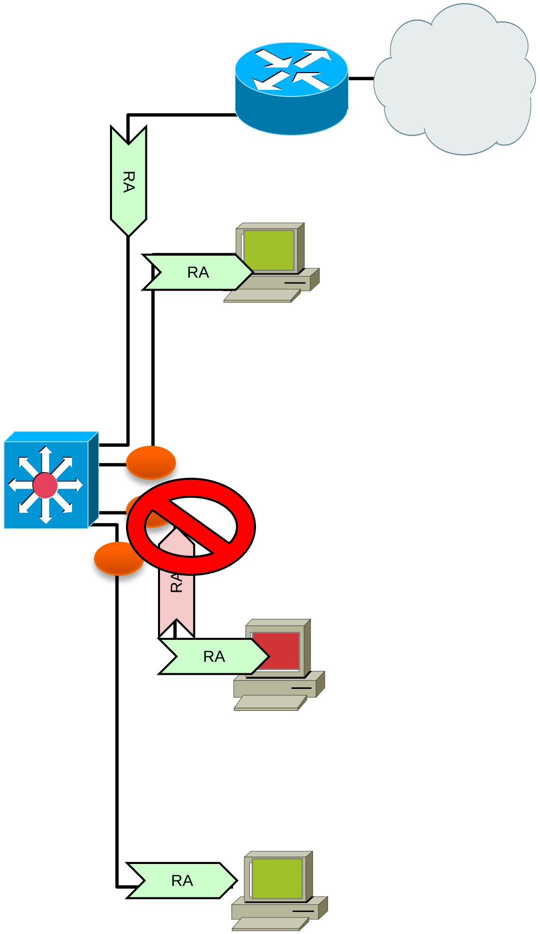
Protecting Against Rogue RA

- Port ACL (see later) blocks all ICMPv6 Router Advertisements from hosts

```
interface FastEthernet3/13
  switchport mode access
  ipv6 traffic-filter ACCESS_PORT in
  access-group mode prefer port
```

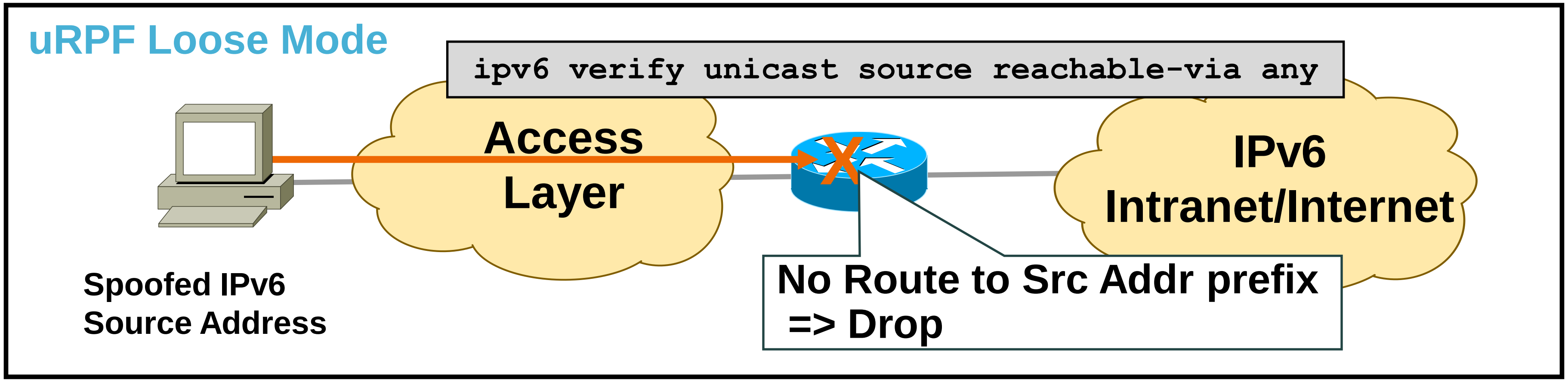
- RA-guard feature in host mode (12.2(33)SXI4 & 12.2(54)SG): also dropping all RA received on this port

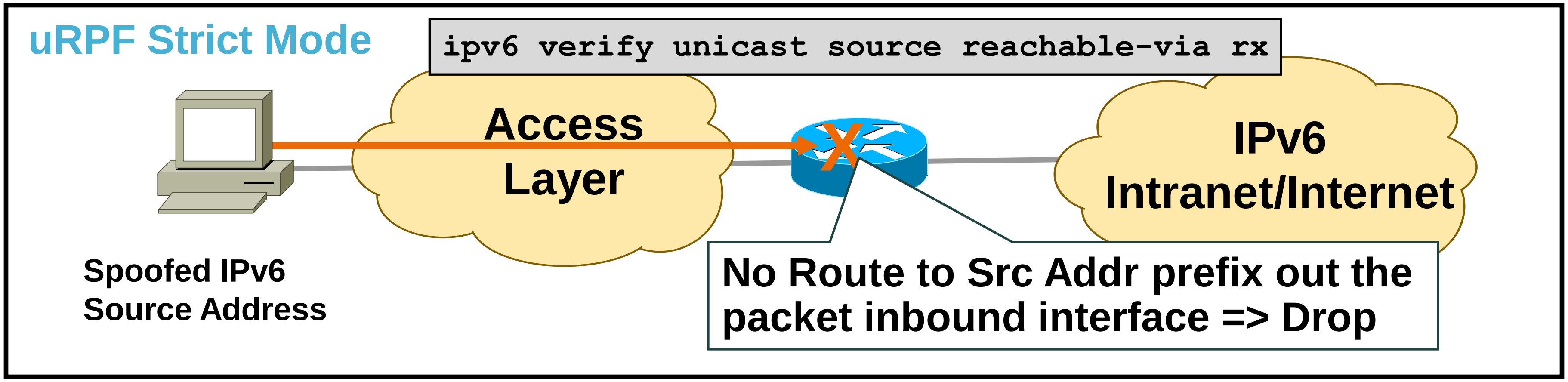
```
interface FastEthernet3/13
  switchport mode access
  ipv6 nd raguard
  access-group mode prefer port
```



L3 Spoofing in IPv6

uRPF Remains the Primary Tool for Protecting Against L3 Spoofing





DHCPv6 Threats

- Note: use of DHCP is announced in Router Advertisements
- Rogue devices on the network giving misleading information or consuming resources (DoS)
  - Rogue DHCPv6 client and servers on the link-local multicast address (FF02::1:2): same threat as IPv4
  - Rogue DHCPv6 servers on the site-local multicast address (FF05::1:3): new threat in IPv6
- Scanning possible if leased addresses are consecutive

DHCPv6 Threat Mitigation

- Rogue clients and servers can be mitigated by using the authentication option in DHCPv6
  - There are not many DHCPv6 client or server implementations using this today
- Port ACL can block DHCPv6 traffic from client ports

```
deny udp any eq 547 any eq 546
```

IPv6 Attacks with Strong IPv4 Similarities

- Sniffing

  IPv6 is no more or less likely to fall victim to a sniffing attack than IPv4

- Application layer attacks

  The majority of vulnerabilities on the Internet today are at the application layer, something that IPSec will do nothing to prevent.

- Rogue devices

  Rogue devices will be as easy to insert into an IPv6 network as in IPv4

- Man-in-the-Middle Attacks (MITM)

  Without strong mutual authentication, any attacks utilizing MITM will have the same likelihood in IPv6 as in IPv4

- Flooding

  Flooding attacks are identical between IPv4 and IPv6

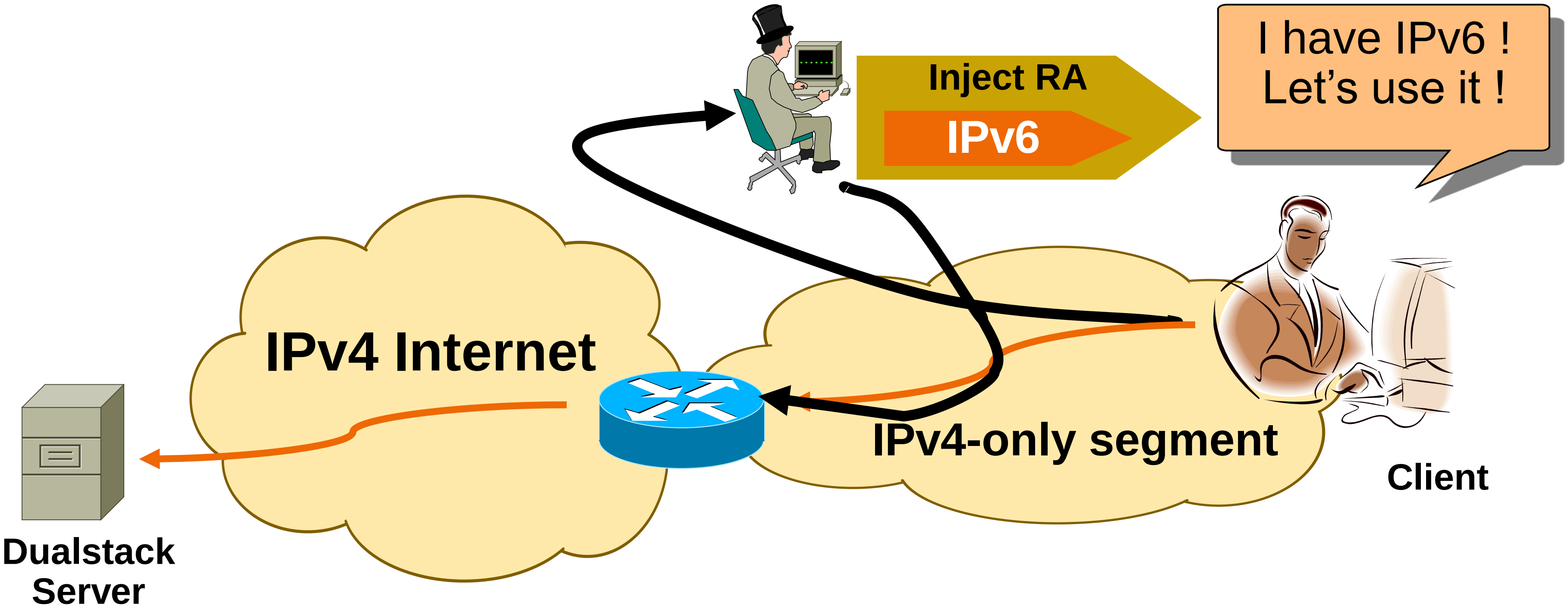
Security Issues Specific to IPv6

IPSec is not deployed as the IPv6 Security panacea

- “*IPv6 has improved security as a result of its mandatory Ipsec support” -myth*
- IPsec already existed for IPv4
- The mandatory-ness of IPsec for IPv6 is just words on paper.
- There are problems with its deployment as a general end-to-end security mechanism.
- Deployment of IPsec(v6) has similar problems as those of IPsec(4). As a result, IPsec(v6) is not deployed as a general end-to-end security mechanism.

No IPv6 network = no problem ? Wrong !

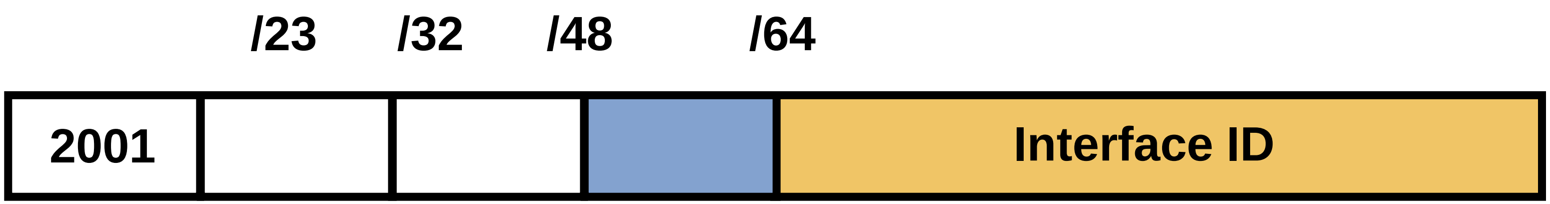
- IPv6 enabled by default on all modern OSes
- Applications prefer IPv6 addresses
- "Blackhat" may not be malicious (Windows with ICS)
- Time to think about deploying IPv6



Dual Stack with Enabled IPv6 by Default

- Your host:
  - IPv4 is protected by your favorite personal firewall...
  - IPv6 is enabled by default (Win7, 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
- => Probably time to think about IPv6 in your network

IPv6 Privacy Extensions (RFC 3041)



- Temporary addresses for IPv6 host client application, e.g. web browser
  - Inhibit device/user tracking
  - Random 64 bit interface ID, then run Duplicate Address Detection before using it. Rate of change based on local policy
- supported in Windows and MacOS (choice isn't available to end user)

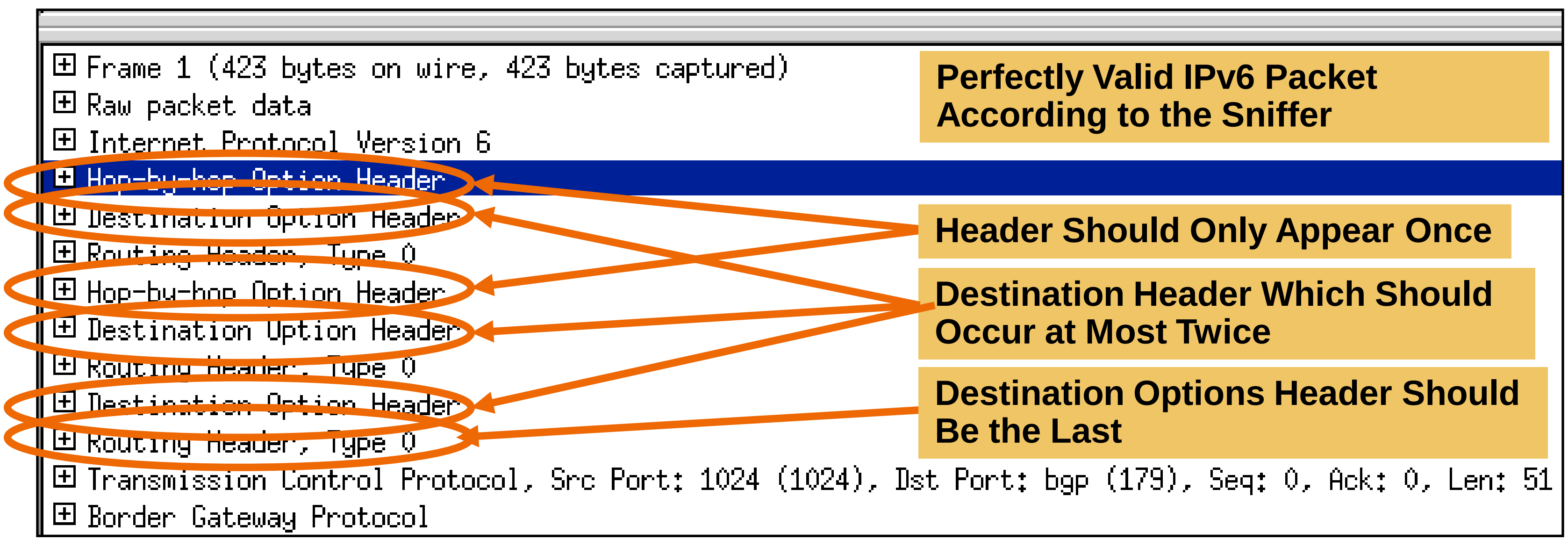
Recommendation: Use Privacy Extensions for External Communication but not for Internal Networks (Troubleshooting and Attack Trace Back)

IPv6 Header Manipulation

- Unlimited size of header chain (spec-wise) can make filtering difficult
- Potential DoS with poor IPv6 stack implementations

  More boundary conditions to exploit

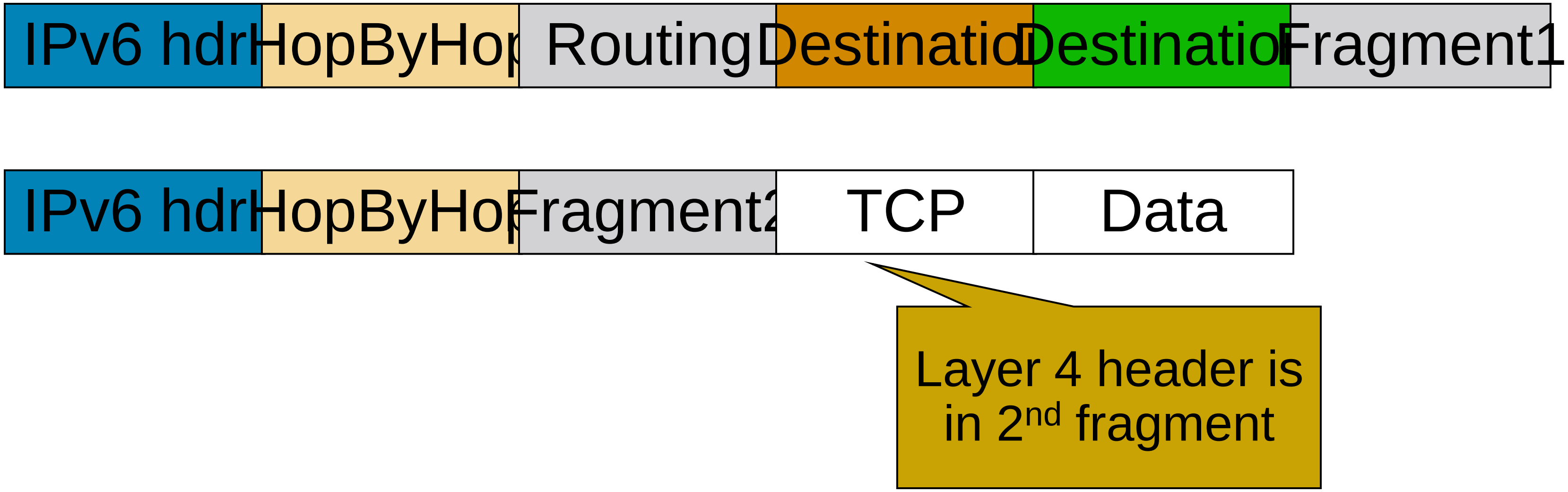
  Can I overrun buffers with a lot of extension headers?



See also: http://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8054d37d.html

Parsing the Extension Header Chain Fragmentation Matters!

- Extension headers chain can be so large than it is fragmented!
- Finding the layer 4 information is not trivial in IPv6
  - Skip all known extension header
  - Until either known layer 4 header found => **SUCCESS**
  - Or unknown extension header/layer 4 header found... => **FAILURE**
  - Or end of extension header => **FAILURE**

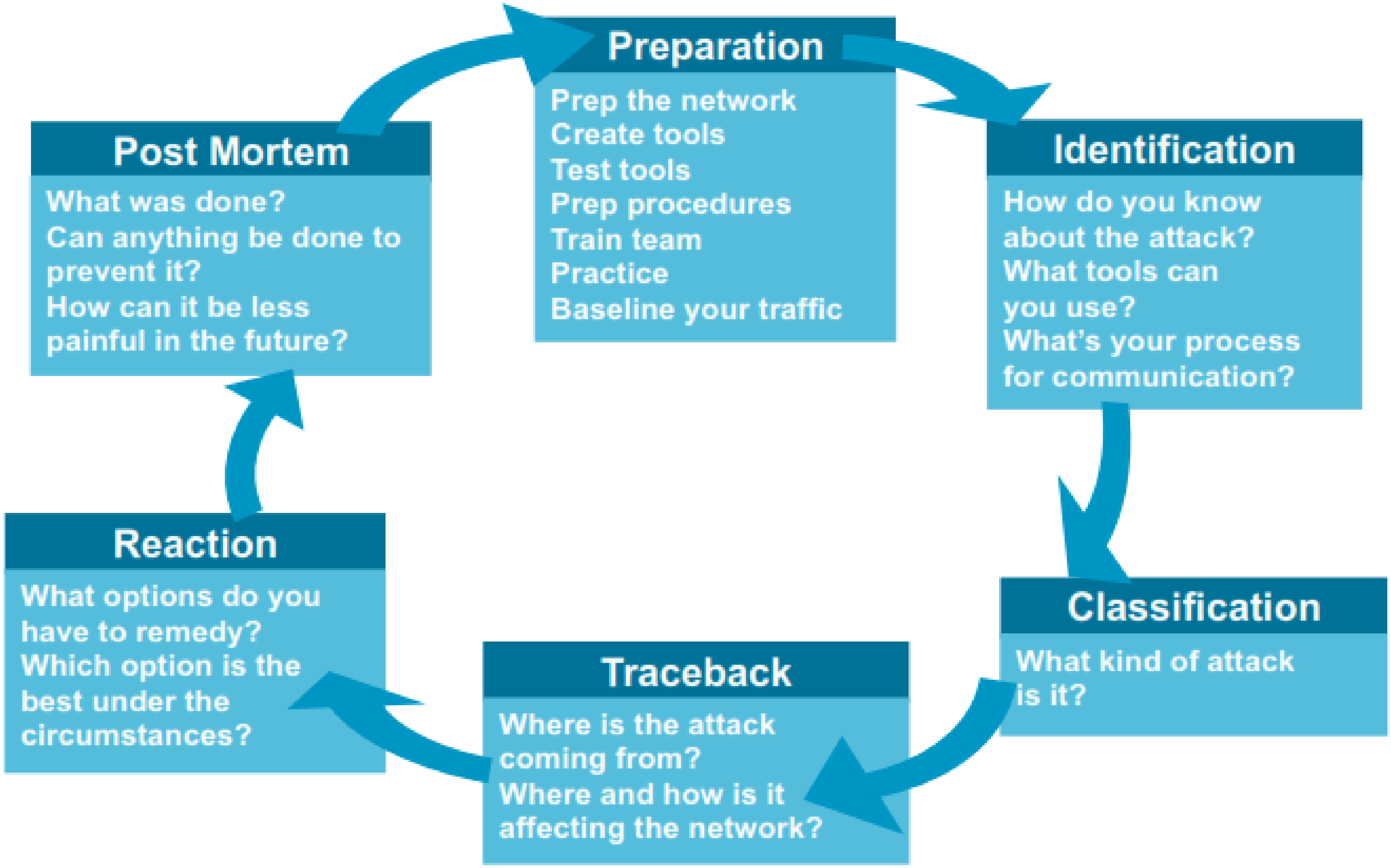


Filtering Extension Headers

- Determine what extension headers will be allowed through the access control device
- IPv6 headers and optional extensions need to be scanned to access the upper layer protocols (UPL)
- May require searching through several extensions headers
- Known extension headers (HbH, AH, RH, MH, destination) are scanned until:
  - Layer 4 header found
  - Unknown extension header is found
- Important: a router must be able to filter both option header and L4 at the same time

Enforcing Security Policies

Designing Security Policy



Cisco IOS IPv6 ACL
A Trivial Example

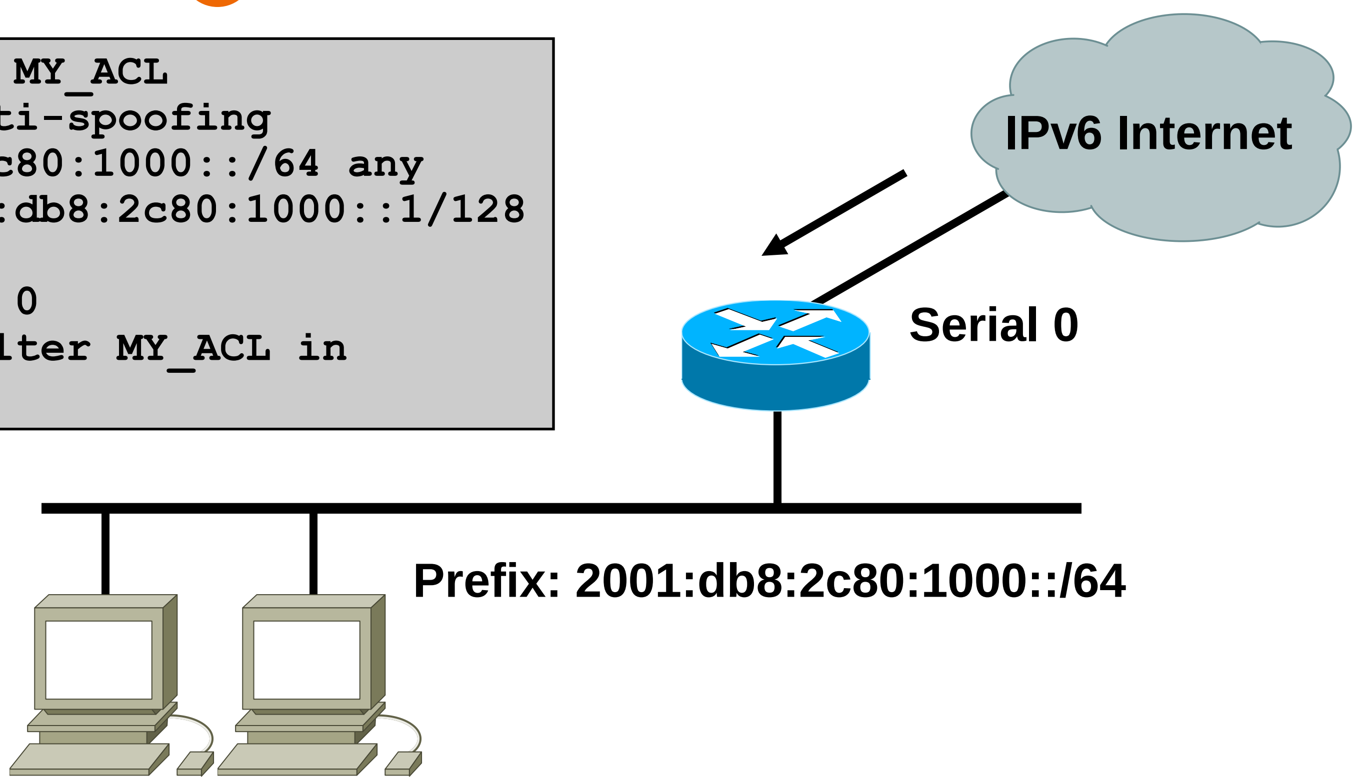
Filtering inbound traffic to one specific destination address

☑ 2001:db8:2c80:1000::1

⊘ others

```
ipv6 access-list MY_ACL
 remark basic anti-spoofing
 deny 2001:db8:2c80:1000::/64 any
 permit any 2001:db8:2c80:1000::1/128

interface Serial 0
 ipv6 traffic-filter MY_ACL in
```



CoPP: Control Plane Policing

- A router can be logically divided into three functional components or planes:

  1. Data plane—packets going through the router
  2. Control plane—routing protocols gluing the network together
  3. Management plane—tools and protocols used to manage the device

- Route Processor contains control and management planes

Problem Definition

- Network uptime is increasingly becoming more vital to companies.
- Denial of Service (DoS) attacks are just one example of a network assault on the control plane.
- DoS attacks target the network infrastructure by generating IP traffic streams to the control plane at very high rates.
- A DoS attack targeting a Route Processor (RP) can cause high Route Processor CPU utilization.

Solution - Control Plane Policing

- Protects the Control Plane from DoS attacks
- Uses QoS to identify and rate limit traffic.
- Allows specification of **types** of packets (traffic-classes) & the desired **rate** to be sent to CPU.
- CPU cycles are used only for packets matching the criteria, availability of the network is greatly increased.
- Control plane treated as a separate entity
- CoPP protects control / management planes:

    1. Ensures routing stability
    2. Reachability
    3. Packet delivery
    4. CP policies are separate from DP and don’t impact data plane.

Which packets are we talking about?

- CPU bound packets that will be policed :
  - L2 Fwd Packets (ARP, IPX, Broadcast, etc)
  - L2 Control: Keepalives and control packets for HDLC, PPP, FR LMI, ATM control ILMI, X.25 and ISDN call setup, STP BPDUs
  - L3 Control: Routing protocol control packets
  - L3 Fwd Packets (telnet, SNMP, HTTP, ICMP, etc)
  - Control Packet (BPDU, CDP, IGMP, DHCP, etc)
  - L3 and L2 Miscellaneous:

Configuring CoPP

- **4 step process:**

  1. Enable global QoS
  2. Classify the traffic
  3. Define the QoS policy
  4. Apply the policy to control plane “interface”

Sample Traffic Classification

1. Critical Traffic—routing protocols, control plane no rate-limit
2. Important Traffic—SNMP, SSH, AAA, NTP, management plane, maybe rate-limit
3. Normal Traffic—other expected non-malicious traffic, ping and other ICMP, rate-limit
4. Undesirable—handling of potentially malicious traffic we expect to see, fragments and the like, drop this traffic
5. Default—non-IP traffic or any other non identified IP traffic, maybe rate-limit

Cisco Security Products and Features

Broad Platform Support

Cisco IOS 12.0S

Cisco 12000 Series Routers

Cisco 10720 Series

Cisco IOS 12.4/12.4T

Cisco 800 Series Routers

Cisco 1700 Series Routers

Cisco 1800 Series Routers

Cisco 2600 Series Routers

Cisco 2800 Series Routers

Cisco 3600 Series Routers

Cisco 3700 Series Routers

Cisco 3800 Series Routers

Cisco 7200 Series Routers

Cisco 7301 Series Routers

Cisco 7500 Series Routers (EoL)

Cisco IOS-XR

CRS-1, Cisco 12000

Cisco IOS 12.2S family

Cisco ASR1000 series

Cisco 72/7300 Series Routers

Cisco 75/7600 Series Routers

Cisco 10000 Series Routers

Catalyst 3750/3560/2960 Series

Catalyst 4500 Series

Catalyst 6500 Series

Cisco Product Portfolio

ASA Firewall (7.x), FWSM 3.1,

LMS 2.5, CNR 6.2, NFC 5.x, NAM 3.x,

MDS9500 series, GGSN 7.0

Nexus 7000

Key Take Away

- So, nothing much new in IPv6
  - Reconnaissance: address enumeration replaced by DNS enumeration
  - Spoofing & bogons: uRPF is our IP-agnostic friend
  - NDP spoofing: RA guard and more feature coming
  - ICMPv6 firewalls need to change policy to allow NDP
  - Extension headers: firewall & ACL can process them
  - Amplification attacks by multicast mostly impossible
- Lack of operation experience may hinder security for a while: **training is required**
- Security enforcement is possible
  - Control your IPv6 traffic as you do for IPv4
- Leverage IPsec to secure IPv6 wherever suitable

Summary: Key take away

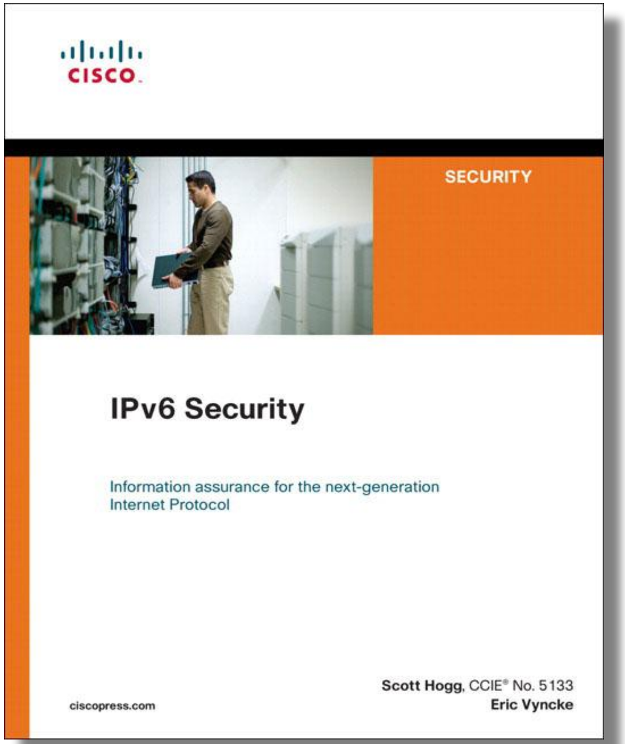
Threat	IPv6 Characteristics	Mitigation
Threats with New Considerations in IPv6		
Reconnaissance	Scanning for hosts is not feasible because of large address space. Well-known addresses, in particular multicast, are vulnerable.	Same as IPv4. Privacy extensions can make reconnaissance less effective.
Unauthorized access	End-to-end security reduces the exposure. Extension headers (EH) open new attack venues.	Use privacy extensions to reduce a host's exposure. Use multiple addresses with different scopes. Manage EH use.
Header manipulation	IPv6 can take advantage of chained and large-size EHs. EHs that must be processed by all stacks are particularly useful to an attacker.	The EHs usage should be strictly controlled based on deployed services.
Fragmentation	No fragment overlap should be allowed in IPv6, but some stacks do reassemble overlapping fragments. The impact of tiny fragments is minimal in IPv6.	Use properly implemented stacks that do not allow fragment overlap.
Layer 3/layer 4 spoofing	The use of tunneling offers more spoofing opportunities even though they are not different from IPv4 tunneling.	Same mitigation techniques as with IPv4.

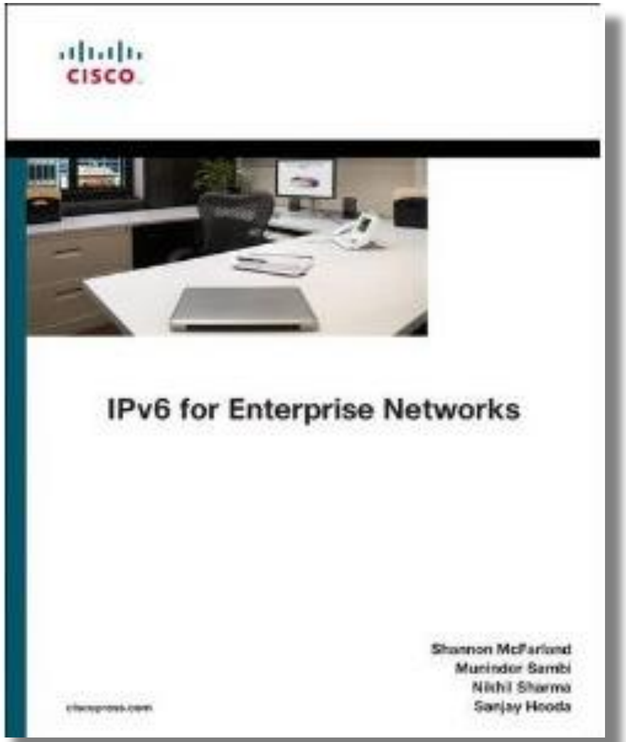
Summary: Key take away

Threat	IPv6 Characteristics	Mitigation
Threats with New Considerations in IPv6		
Host initialization and address-resolution attacks	DHCP has similar vulnerabilities for the two protocols. Neighbor Discovery has similar vulnerabilities as ARP. Stateless autoconfiguration and renumbering offer new attack options.	Use an interim solution such as static neighbors; the SEND recommendations are adopted by the IPv6 stacks.
Broadcast-amplification attacks (Smurf)	No concept of broadcast in IPv6, and that reduces the amplification options.	Use filtering for multicast traffic, in particular, because it is the only amplification option.
Routing attacks	IPsec provides additional peering security for some protocols. From a threat perspective, it is similar to IPv4.	Same as IPv4. Wherever possible, implement IPsec.
Viruses and worms	Same as IPv4. Random scanning used by worms to propagate is impractical in IPv6 because of the large address space.	Same as IPv4.

Reference & Recommended Reading

www.cisco.com/go/ipv6





Source: Cisco Press

Demo: DoS Attack

Attack Type: MLDv2

Solution Applied: CoPP

Thank you.