Can we enforce a Security Policy in an IPv6 World?

Eric Vyncke, Distinguished Engineer, evyncke@cisco.com

Security Myths

IPv6 Myths: Better, Faster, More Secure

Sometimes, newer means better and more secure

Sometimes, experience IS better and safer!

Reconnaissance in IPv6
Subnet Size Difference

- Default subnets in IPv6 have 2^{64} addresses
  - 10 Mpps = more than 50 000 years
- NMAP doesn't even support ping sweeps on IPv6 networks

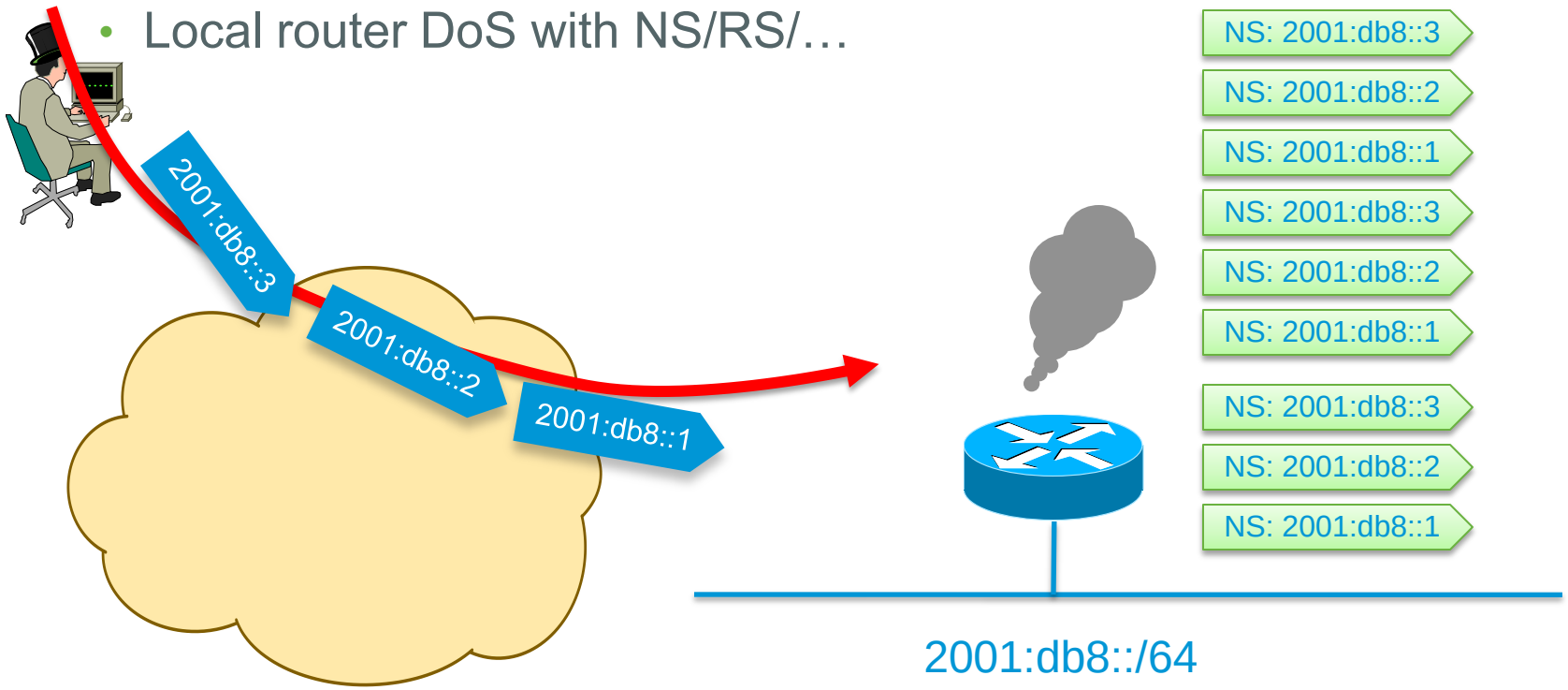
- But, attackers can still find potential targets:
  - DNS enumeration
  - Log files, connection tables on cracked nodes
  - P2P registration
  - ....

Scanning Can be Good

- Multiple organizations scan their network for inventory and compliance checks...
- Doable in IPv6 but with different techniques:
  - Gather addresses from Netflow
  - Gather addresses from neighbor cache in all routers (SNMP, ssh, ...)

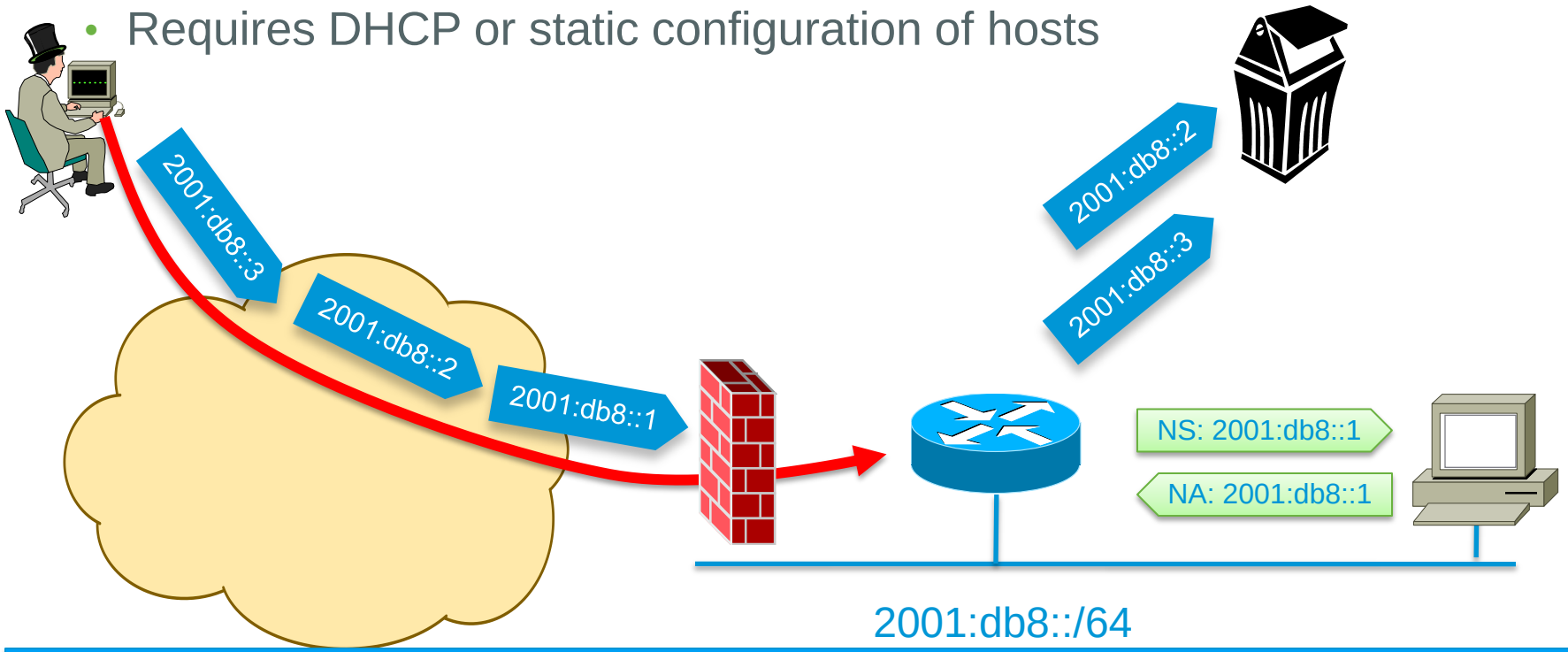
Scanning Made Bad for CPU
Remote Neighbor Cache Exhaustion

- Remote router CPU/memory DoS attack if aggressive scanning
  - Router will do Neighbor Discovery... And waste CPU and memory
- Local router DoS with NS/RS/…



Simple Fix for Remote Neighbor Cache Exhaustion

- Ingress ACL allowing only valid destination and dropping the rest
- NDP cache & process are safe
- Requires DHCP or static configuration of hosts



More complex cases (users LAN) require good implementation

The IPsec Myth: IPsec End-to-End will Save the World

- "IPv6 mandates the implementation of IPsec"
- Some organizations believe that IPsec should be used to secure all flows…

"Security expert, W., a professor at the University of <foo> in the UK, told <newspaper> the new protocol system – IPv6 – comes with a security code known as IPSEC that would do away with anonymity on the web.

If enacted globally, this would make it easier to catch cyber criminals, Prof W. said."

The IPsec Myth: IPsec End-to-End will Save the World

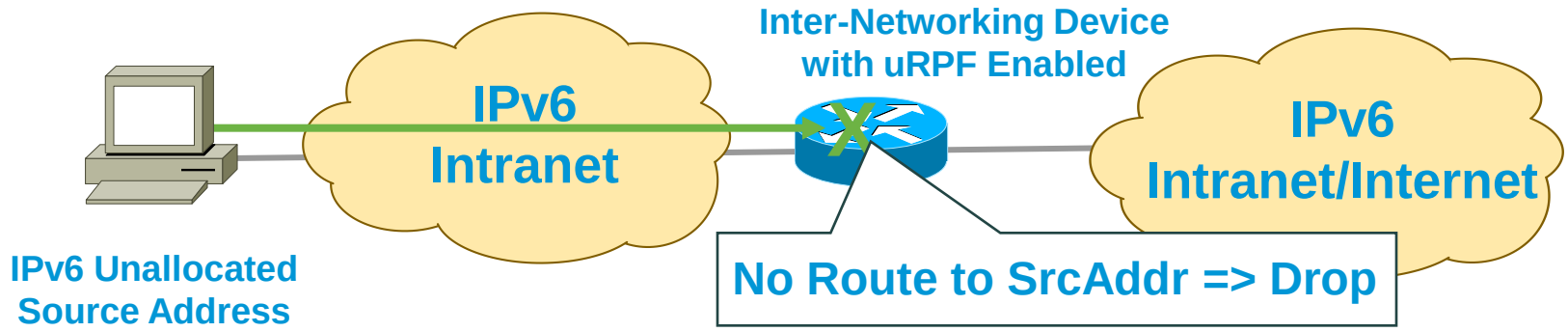
- IPv6 originally mandated the implementation of IPsec (but not its use)
- Now, RFC 6434 "*IPsec SHOULD be supported by all IPv6 nodes*"
- Some organizations still believe that IPsec should be used to secure all flows...
  - Interesting **scalability** issue (n^2 issue with IPsec)
  - Need to **trust endpoints and end-users** because the network cannot secure the traffic: no IPS, no ACL, no firewall
    - IOS 12.4(20)T can parse the AH
  - Network **telemetry is blinded**: NetFlow of little use
  - Network **services hindered**: what about QoS?

Recommendation: do not use IPsec end to end within an administrative domain.
Suggestion: Reserve IPsec for residential or hostile environment or high profile targets EXACTLY as for IPv4

Shared Issues

IPv6 Bogon and Anti-Spoofing Filtering

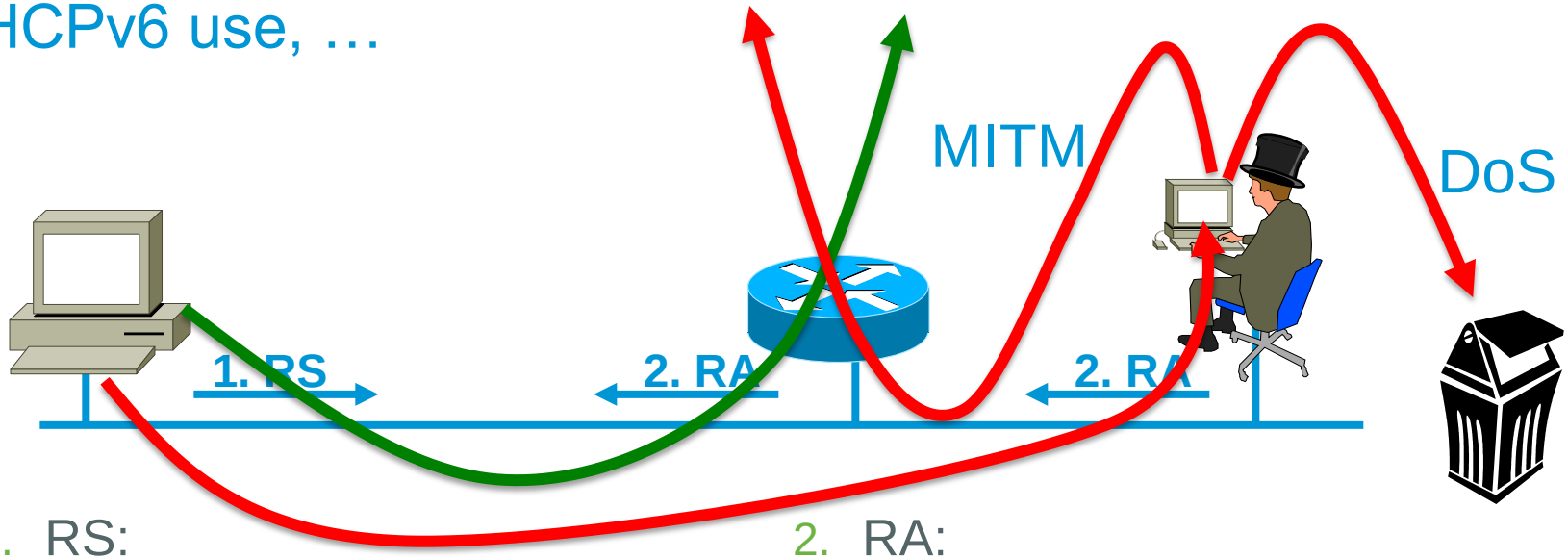
- Same as in IPv4
- Bogon filtering (data plane & BGP route map): http://www.cymru.com/Bogons/ipv6.txt
- Anti-spoofing: uRPF



Rogue Router Advertisement

Router Advertisements contains:
-Prefix to be used by hosts
-Data-link layer address of the router
-Miscellaneous options: MTU, DHCPv6 use, …

RA w/o Any Authentication Gives Exactly Same Level of Security as DHCPv4 (None)



1. RS:
   Data = Query: please send RA
2. RA:
   Data= options, **prefix**, lifetime, A+M+O flags

Effect of Rogue Router Advertisements

- Devastating:
  - Denial of service: all traffic sent to a black hole
  - Man in the Middle attack: attacker can intercept, listen, modify unprotected data
- Also affects legacy IPv4-only network with IPv6-enabled hosts
- Most of the time from non-malicious users
- Requires layer-2 adjacency (some relief…)
- The major blocking factor for enterprise IPv6 deployment

ARP Spoofing is now NDP Spoofing: Threats

- ARP is replaced by Neighbor Discovery Protocol
  - Nothing authenticated
  - Static entries overwritten by dynamic ones
- Stateless Address Autoconfiguration
  - rogue RA (malicious or not)
  - All nodes badly configured
    - DoS
    - Traffic interception (Man In the Middle Attack)
- Attack tools exist (from THC – The Hacker Choice)
  - Parasit6
  - Fakerouter6
  - ...

The Hacker's Choice

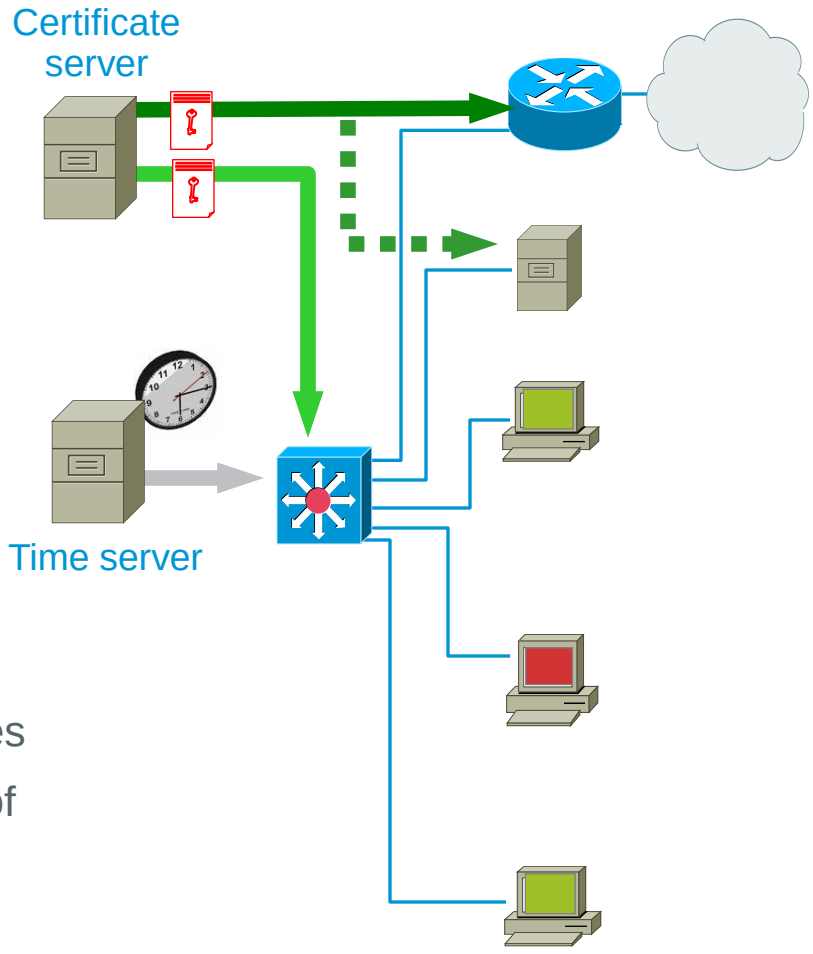
ARP Spoofing is now NDP Spoofing: Mitigation

- **MOSTLY GOOD NEWS**: dynamic ARP inspection for IPv6 is available (but not yet on all platforms)
  - First phase (Port ACL & RA Guard) available since Summer 2010
  - Second phase (NDP & DHCP snooping) starting to be available since Summer 2011
  - http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-first_hop_security.html
- **GOOD NEWS**: Secure Neighbor Discovery
  - SeND = NDP + crypto
  - IOS 12.4(24)T
  - But not in Windows Vista, 2008 and 7, Mac OS/X, iOS, Android
  - Crypto means slower...
- Other **GOOD NEWS**:
  - Private VLAN works with IPv6
  - Port security works with IPv6
  - IEEE 801.X works with IPv6 (except downloadable ACL)

Securing Link Operations: First Hop Trusted Device

Cisco Short Term Roadmap IETF SAVI WG

- **Advantages**
  - central administration, central operation
  - Complexity limited to first hop
  - Transitioning lot easier
  - Efficient for threats coming from the link
  - Efficient for threats coming from outside
- **Disadvantages**
  - Applicable only to certain topologies
  - Requires first-hop to learn about end-nodes
  - First-hop is a bottleneck and single-point of failure



Mitigating Rogue RA: RFC 6101

- **Port ACL** blocks all ICMPv6 RA from hosts

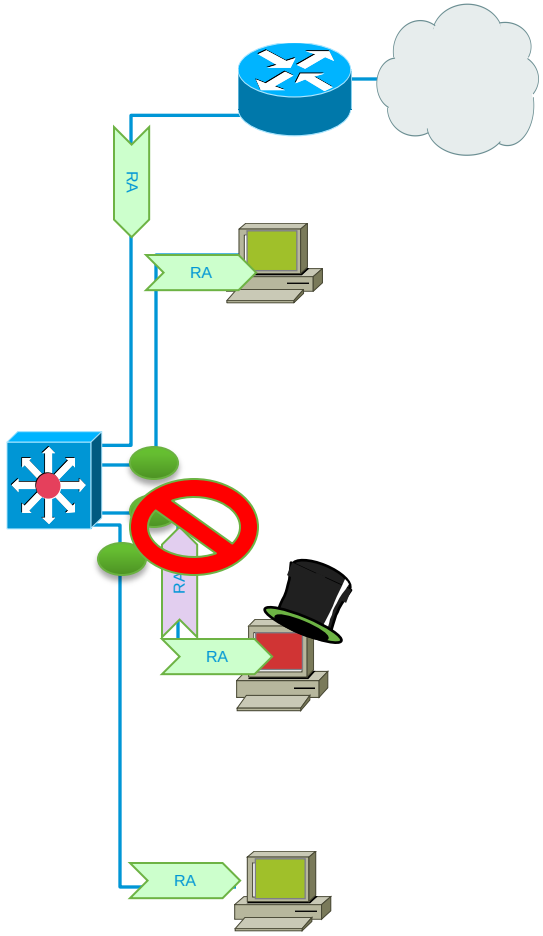
```
interface FastEthernet0/2
  ipv6 traffic-filter ACCESS_PORT in
  access-group mode prefer port
```

- **RA-guard lite** (12.2(33)SXI4 & 12.2(54)SG): also dropping all RA received on this port

```
interface FastEthernet0/2
  ipv6 nd raguard
  access-group mode prefer port
```

- **RA-guard** (12.2(50)SY)

```
ipv6 nd raguard policy HOST device-role host
ipv6 nd raguard policy ROUTER device-role router
ipv6 nd raguard attach-policy HOST vlan 100
interface FastEthernet0/0
  ipv6 nd raguard attach-policy ROUTER
```



IPv6 Attacks with Strong IPv4 Similarities

Good news
IPv4 IPS signatures can be re-used

- 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

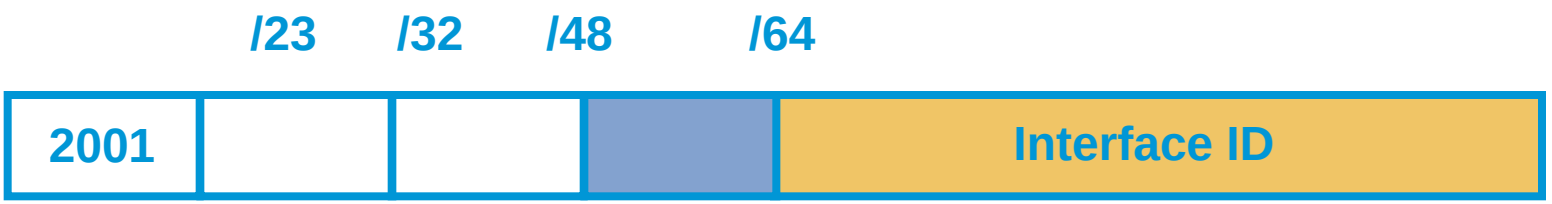
  Flooding attacks are identical between IPv4 and IPv6

- Sniffing

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

Specific IPv6 Issues

IPv6 Privacy Extensions (RFC 4941)



- 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
- Enabled by default in Windows, Android, iOS 4.3, Mac OS/X 10.7

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

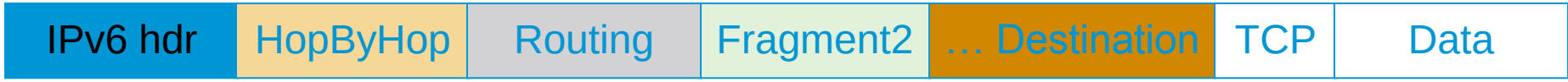
IETF Work in progress: unpredictable and stable addresses

Parsing the Extension Header Chain

- Finding the layer 4 information is not trivial in IPv6
  - Skip all known extension header
  - Until either known layer 4 header found => **MATCH**
  - Or unknown extension header/layer 4 header found... => **NO MATCH**

Parsing the Extension Header Chain Fragments and Stateless Filters

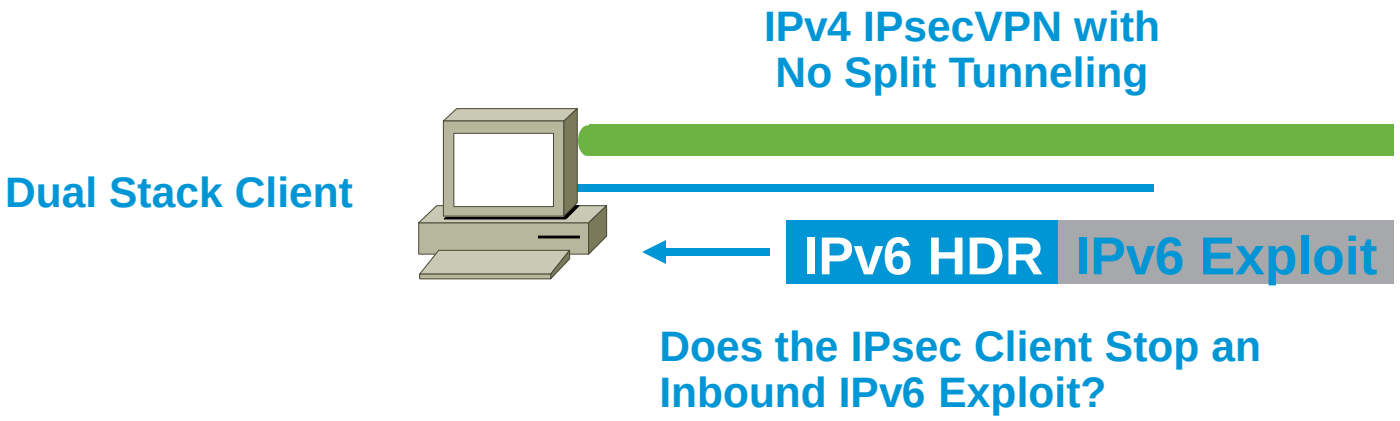
- RFC 3128 is not applicable to IPv6
- Layer 4 information could be in 2nd fragment
- But, stateless firewalls could not find it if a previous extension header is fragmented
- **Important to have ACL able to drop those fragmented packets (even if valid)**
  - Undetermined-transport in Cisco ACL



Layer 4 header is in 2nd fragment, Stateless filters have no clue where to find it!

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.

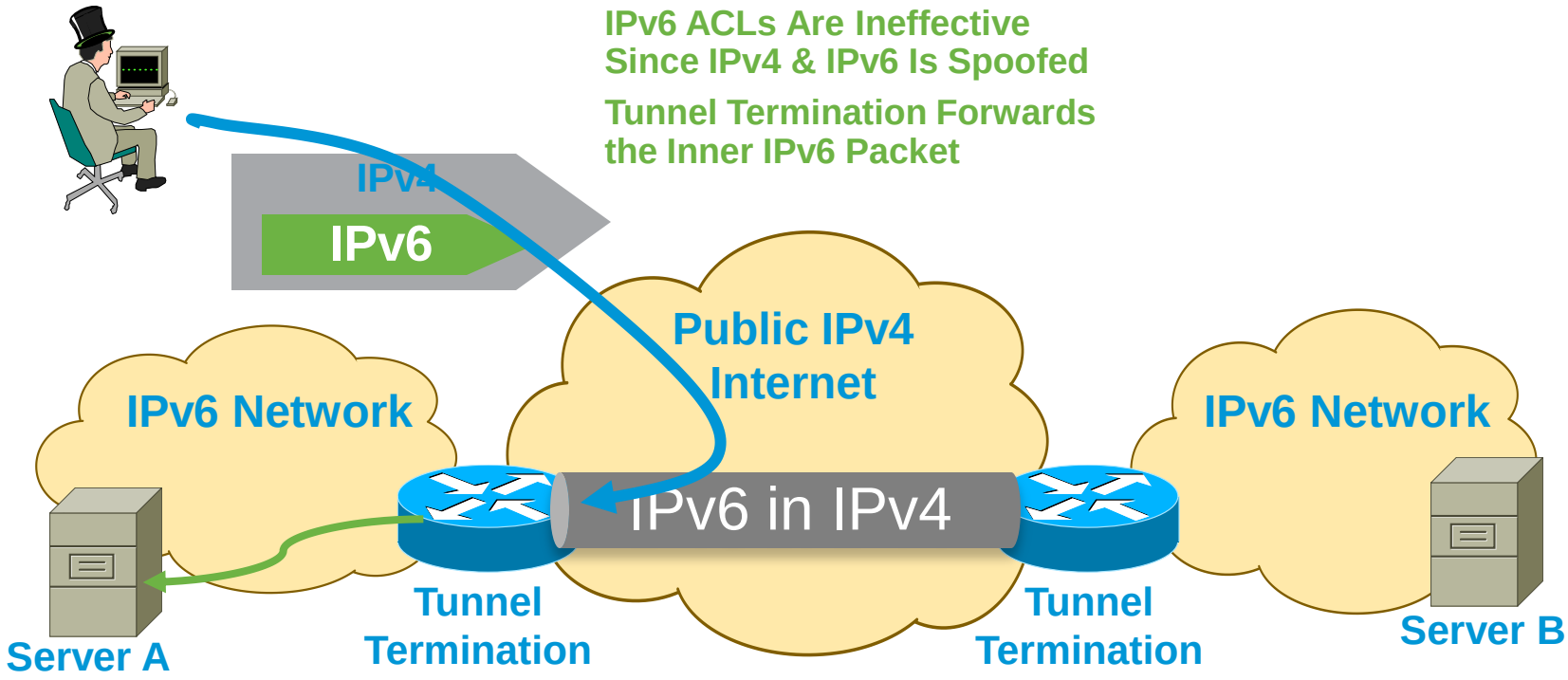


Dual Stack with Enabled IPv6 by Default

- 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
- => Probably time to think about IPv6 in your network

L3-L4 Spoofing in IPv6 When Using IPv6 over IPv4 Tunnels

- Most IPv4/IPv6 transition mechanisms have no authentication built in
- => an IPv4 attacker can inject traffic if spoofing on IPv4 and IPv6 addresses



TEREDO?

- Teredo navalis

  A shipworm drilling holes in boat hulls

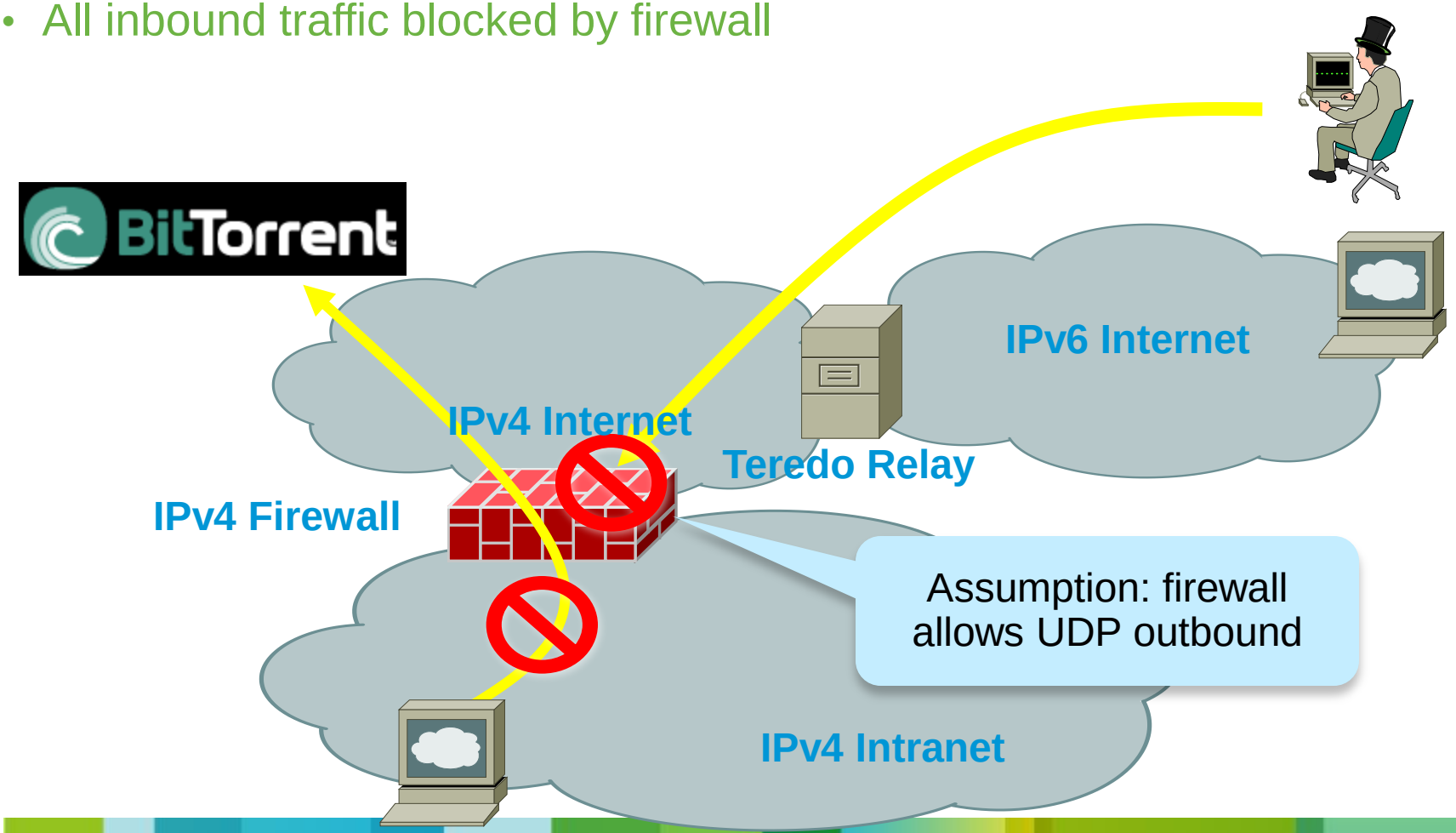
- Teredo Microsoftis

  IPv6 in IPv4 punching holes in NAT devices

Source: United States Geological Survey

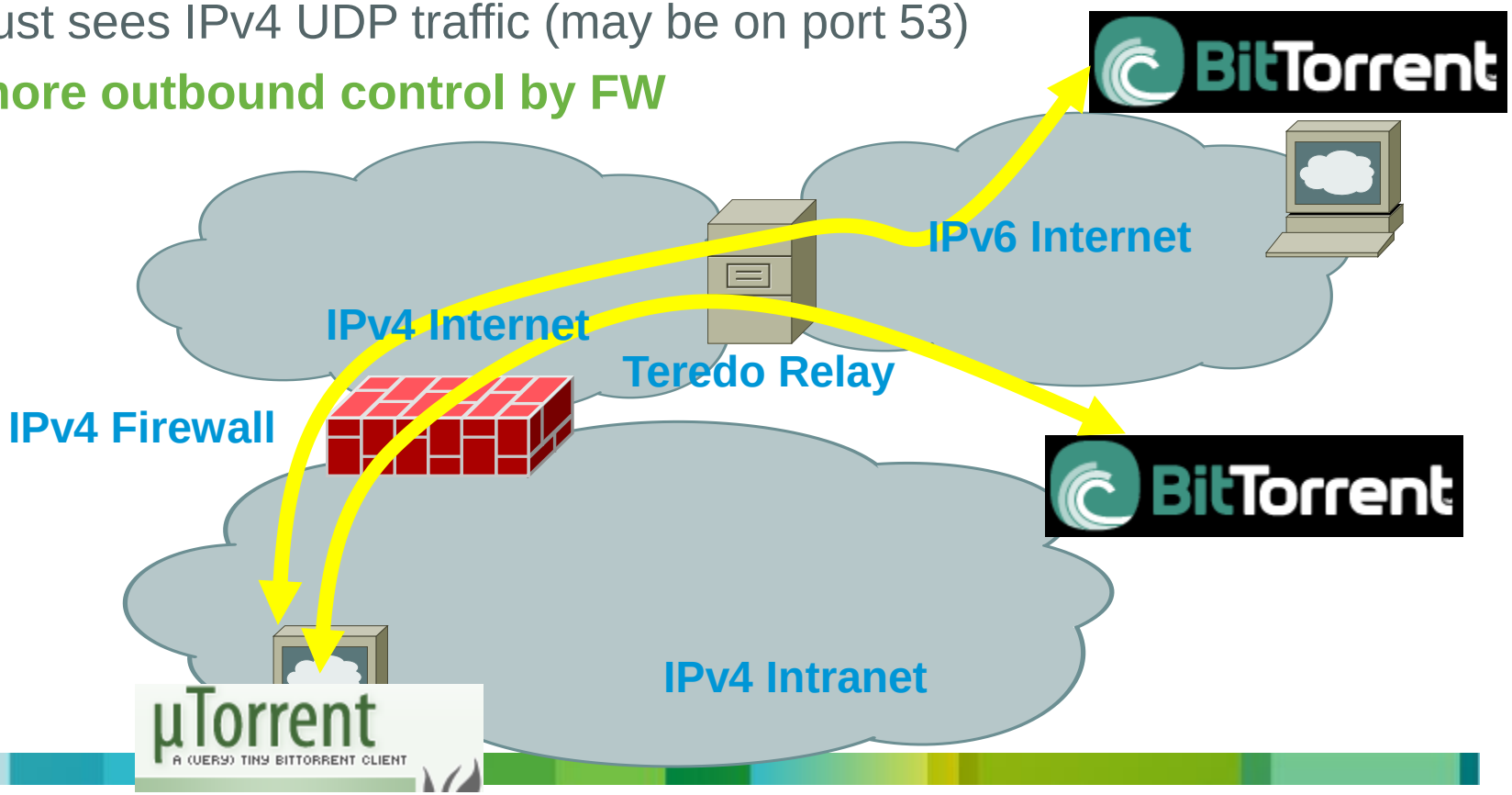
Teredo Tunnels (1/3)
Without Teredo: Controls Are in Place

- All outbound traffic inspected: e.g., P2P is blocked
- All inbound traffic blocked by firewall



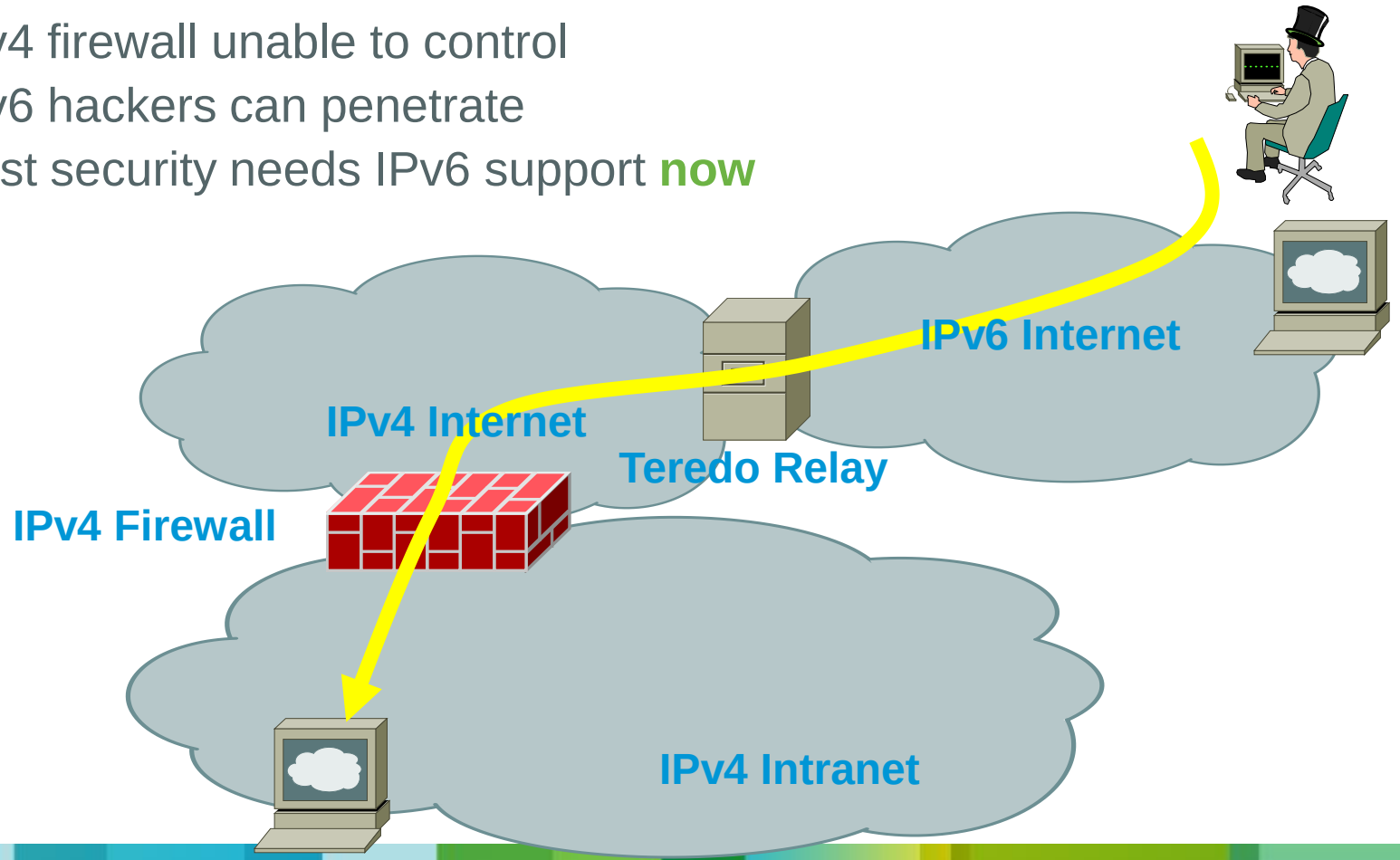
Teredo Tunnels (2/3)
No More Outbound Control
Teredo threats—IPv6 over UDP (port 3544)

- Internal users wants to get P2P over IPv6
- Configure the Teredo tunnel (already enabled by default!)
- FW just sees IPv4 UDP traffic (may be on port 53)
- **No more outbound control by FW**



Teredo Tunnels (3/3)
No More Outbound Control
Once Teredo Configured

- **Inbound** connections are allowed
- IPv4 firewall unable to control
- IPv6 hackers can penetrate
- Host security needs IPv6 support **now**

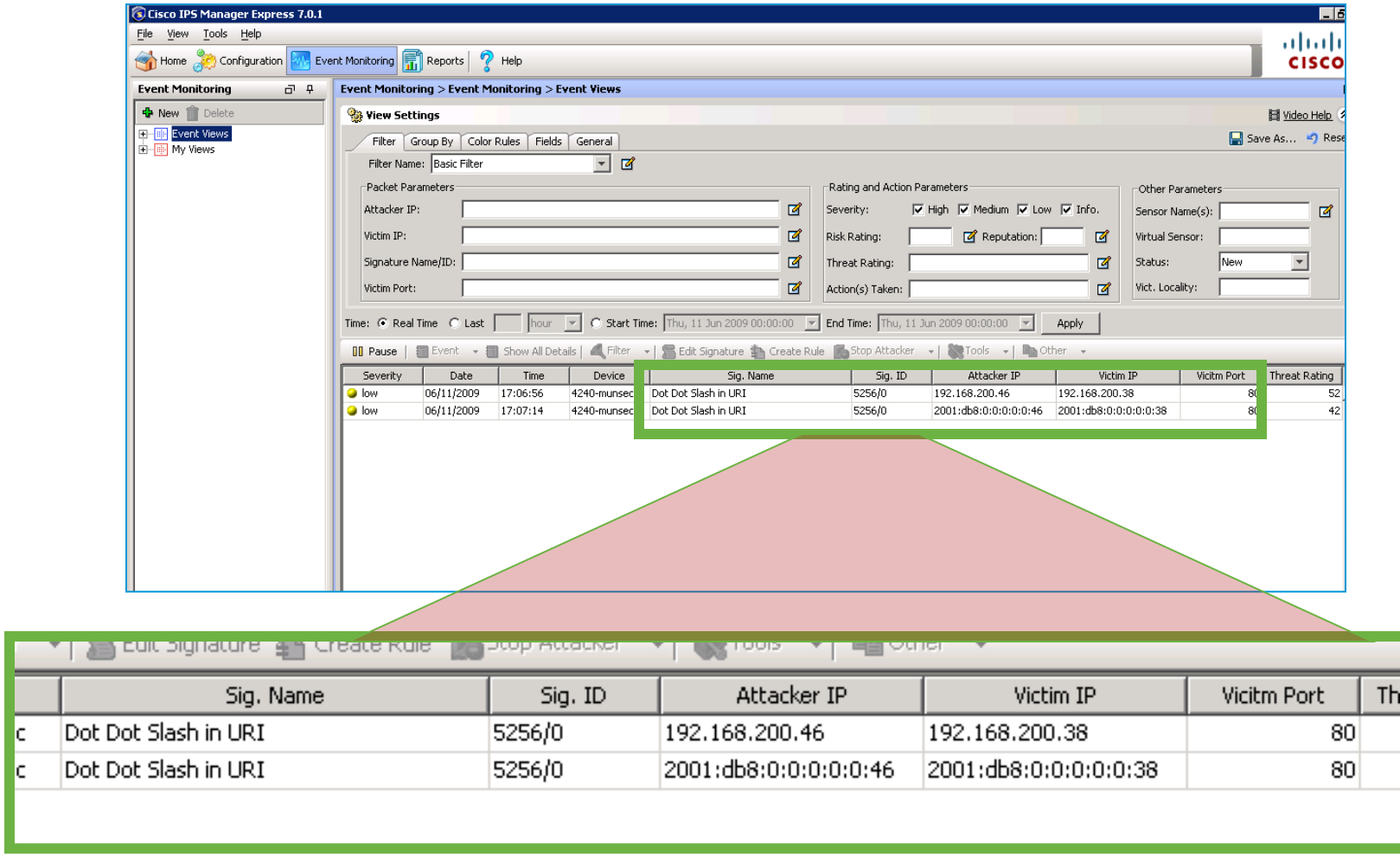


Enforcing a Security Policy

Firewall Policies

- CONGRUENCE between IPv4 and IPv6 is paramount
  - Same policy whether IPv4 or IPv6
    - except RFC 4890 for ICMP
  - Easier if ACLs are dual-stack or use DNS or use object grouping
  - Privacy extension MUST be disabled for servers (usually ACE per host)
  - Privacy extension MAY be used for clients (usually ACE per LAN)
  - IEEE 802.1X or VPN downloadable per-user ACL are useful
- Stateful firewalls MUST understand extension headers & fragments
- Stateless firewalls CANNOT handle fragments
  - If possible, drop all ‘undetermined transport’ fragments
- Usually, Security Incident and Event Managers (SIEM) do not understand the ‘multiple addresses per host’ ...

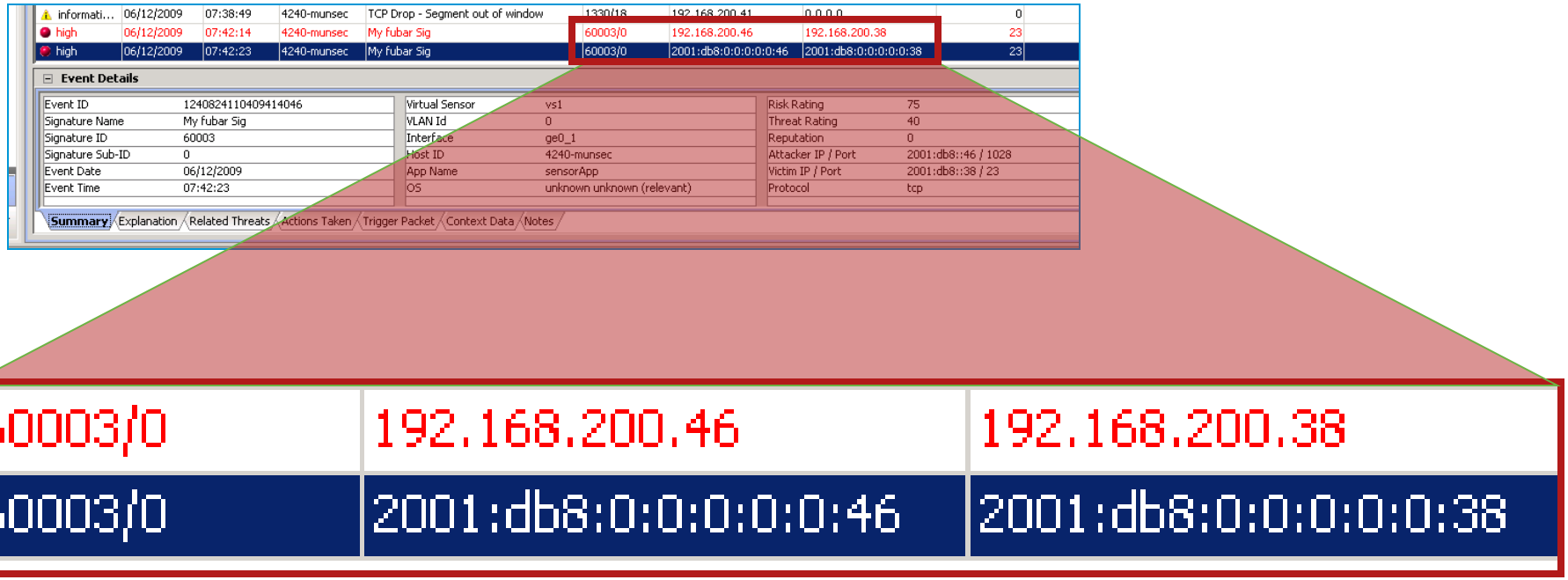
Dual-Stack IPS Engines
Service HTTP



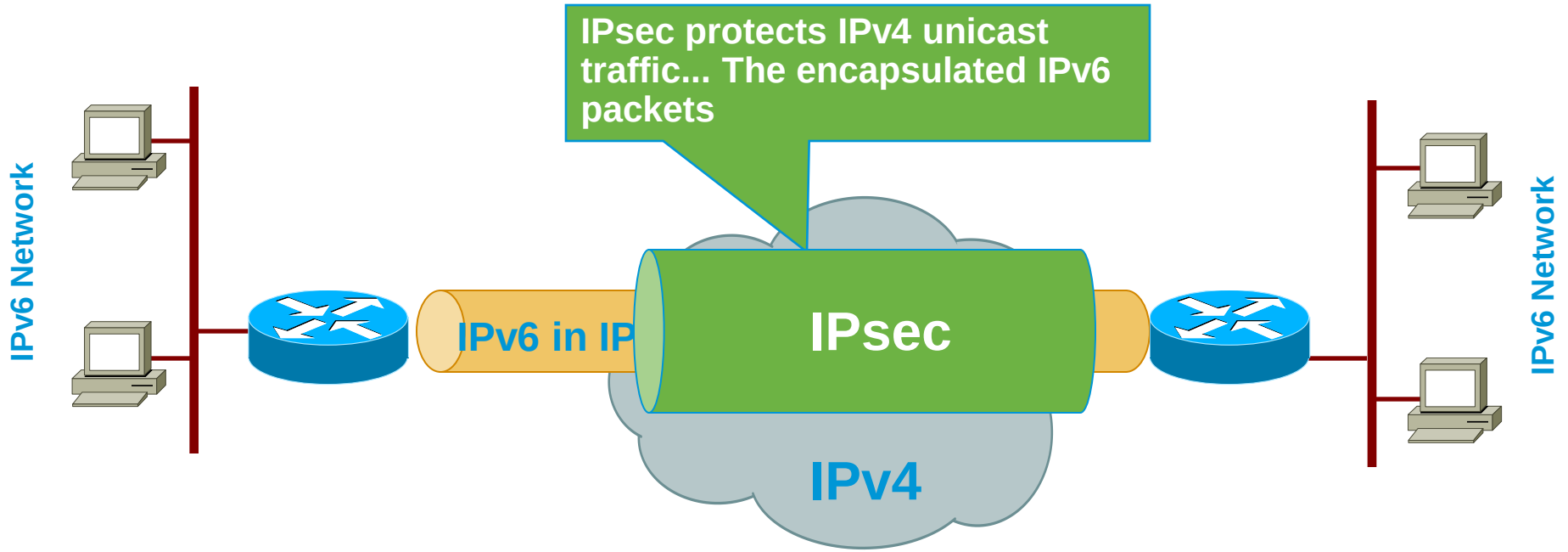
	Sig. Name	Sig. ID	Attacker IP	Victim IP	Vicitm Port	Th
c	Dot Dot Slash in URI	5256/0	192.168.200.46	192.168.200.38	80	
c	Dot Dot Slash in URI	5256/0	2001:db8:0:0:0:0:0:46	2001:db8:0:0:0:0:0:38	80	

Dual-Stack Engine
String TCP with Custom Signature

- Yet another example of an engine supporting both IPv4 and IPv6

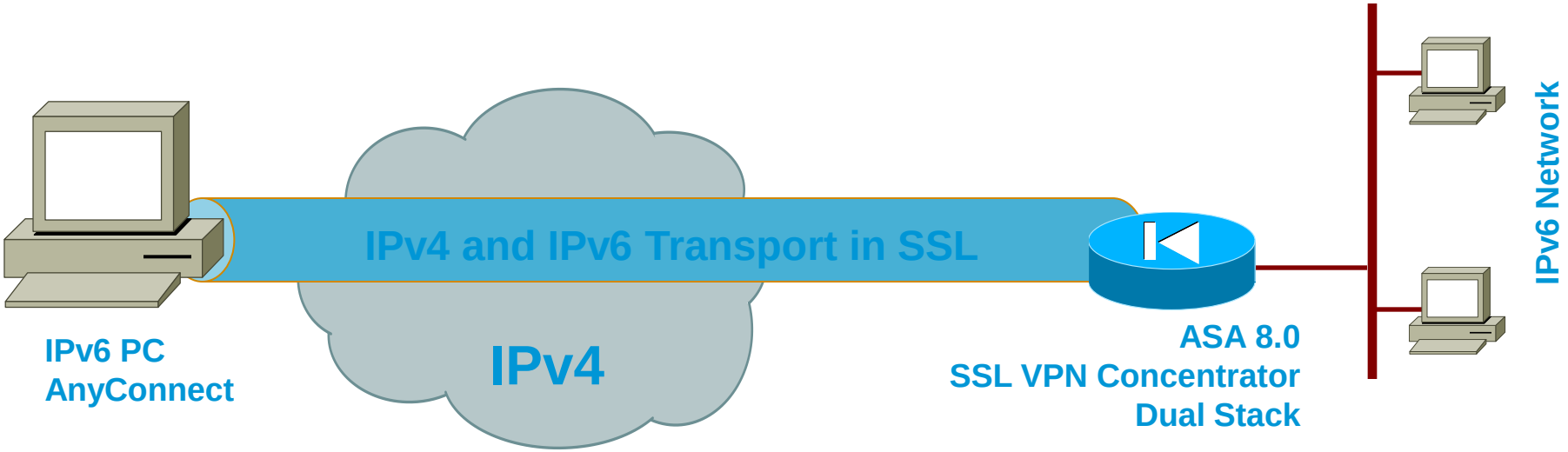


Secure Site to Site IPv6 Traffic over IPv4 Public Network with GRE IPsec



GRE tunnel can be used to transport both IPv4 and IPv6 in the same tunnel

Secure RA IPv6 Traffic over IPv4 Public Network: AnyConnect SSL VPN Client



IPv6 Security Controls EXIST! USE THEM ☺

- Using Cisco as an example
- ASA Firewall
  - Since version 7.0 (released 2005)
  - Flexibility: Dual stack, IPv6 only, IPv4 only
  - SSL VPN for IPv6 (ASA 8.0)
  - Stateful-Failover (ASA 8.2.2)
  - Extension header filtering and inspection (ASA 8.4.2)
- IOS Firewall
  - IOS 12.3(7)T (released 2005)
  - Zone-based firewall on IOS-XE 3.6 (2012)
- IPS
  - Since 6.2 (released 2008)
- Email Security Appliance (ESA) under beta testing since 2010, IPv6 support since 7.6.1 (May 2012)
- Web Security Appliance (WSA) with explicit proxy then transparent mode, work in progress
- ScanSafe expected to be available in 2012

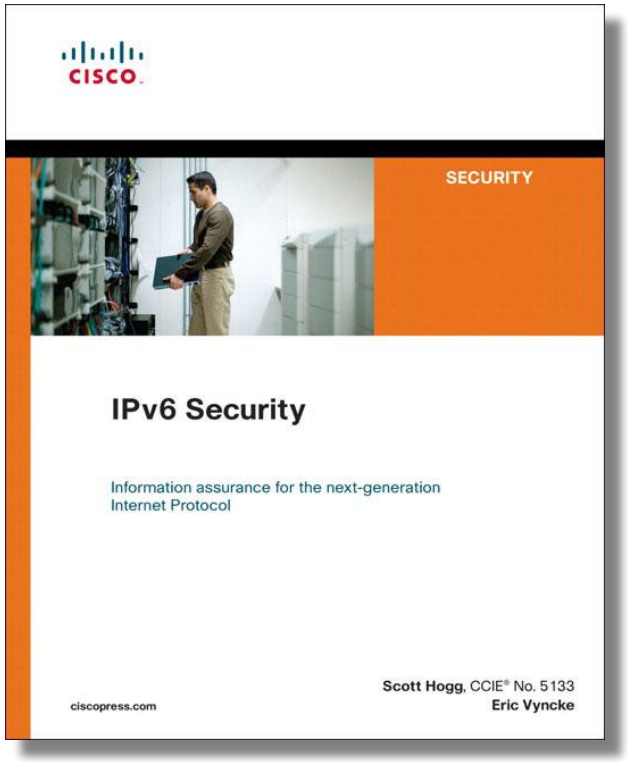
Summary

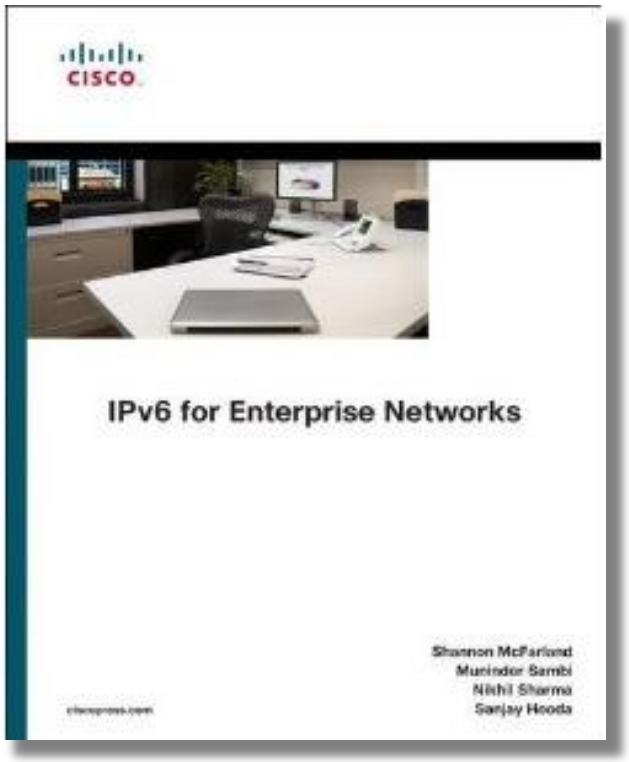
Key Take Away Security is not a reason to delay IPv6

- So, nothing really new in IPv6
  - Reconnaissance: address enumeration replaced by DNS enumeration
  - Spoofing & bogons: uRPF is our IP-agnostic friend
  - NDP spoofing: RA guard and more features coming
  - ICMPv6 firewalls need to change policy to allow NDP
  - Extension headers: firewall & ACL can process them
  - Fragmentation: undetermined-transport is your friend
- 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 when suitable

Questions and Answers?

Recommended Reading



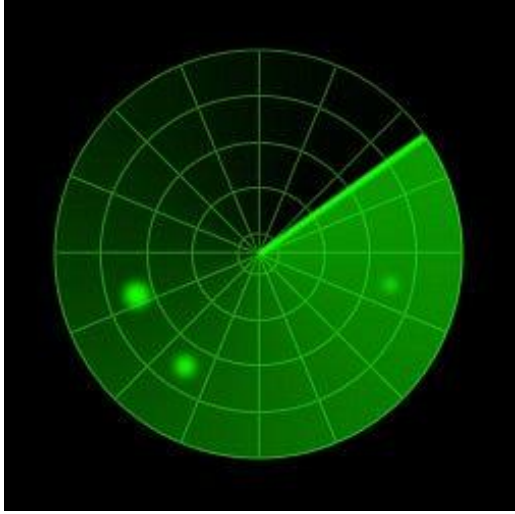


Source: Cisco Press

Thank you.

Back-up (for reference) slides

Reconnaissance in IPv6
Scanning Methods Are Likely to Change



- Public servers will still need to be DNS reachable
  - ⇒More information collected by Google...
- Increased deployment/reliance on dynamic DNS
  - ⇒More information will be in DNS
- Using peer-to-peer clients gives IPv6 addresses of peers
- Administrators may adopt easy-to-remember addresses (::10,::20,::F00D, ::C5C0, :ABBA:BABE or simply IPv4 last octet for dual stack)
- By compromising hosts in a network, an attacker can learn new addresses to scan

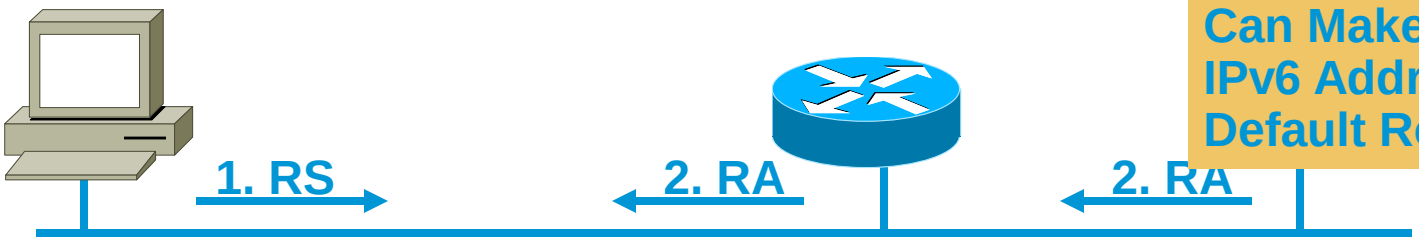
Neighbor Discovery Issue#1 Stateless Autoconfiguration

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, autoconfig flag

Preventing IPv6 Routing Attacks Protocol Authentication

- BGP, ISIS, EIGRP no change:
  - An MD5 authentication of the routing update
- OSPFv3 has changed and pulled MD5 authentication from the protocol and instead is supposed to rely on transport mode IPsec (for authentication and confidentiality)
  - IPsec means crypto image
  - But see draft-ietf-ospf-auth-trailer-ospfv3
- IPv6 routing attack best practices
  - Use traditional authentication mechanisms on BGP and IS-IS
  - Use IPsec to secure protocols such as OSPFv3

Disabling Privacy Extension

For Your Reference

- Microsoft Windows
  - Deploy a Group Policy Object (GPO)
  - Or

```
netsh interface ipv6 set global randomizeidentifiers=disabled
netsh interface ipv6 set global randomizeidentifiers=disabled store=persistent
netsh interface ipv6 set privacy state=disabled store=persistent
```

- Alternatively disabling stateless autoconfiguration for DHCP
  - Send Router Advertisements with
    - all prefixes with A-bit set to 0 (disable SLAAC)
    - M-bit set to 1 to force stateful DHCPv6
  - Use DHCP to a specific pool + ingress ACL allowing only this pool

```
interface fastEthernet 0/0
  ipv6 nd prefix default no-autoconfig
  ipv6 dhcp server . . . (or relay)
  ipv6 nd managed-config-flag
```