Cisco

Cisco live!
Jan 30 - Feb 3, 2012 · London, UK

IPv6 Security Threats and Mitigations

Agenda

- Debunking IPv6 Myths
- Shared Issues by IPv4 and IPv6
- Specific Issues for IPv6
  - Extension headers, IPsec everywhere, transition techniques
- Enforcing a Security Policy in IPv6

Learn. Connect.
Collaborate. together.

IPv6 Security Myths…

IPv6 Myths: Better, Faster, More Secure

1995: RFC 1883

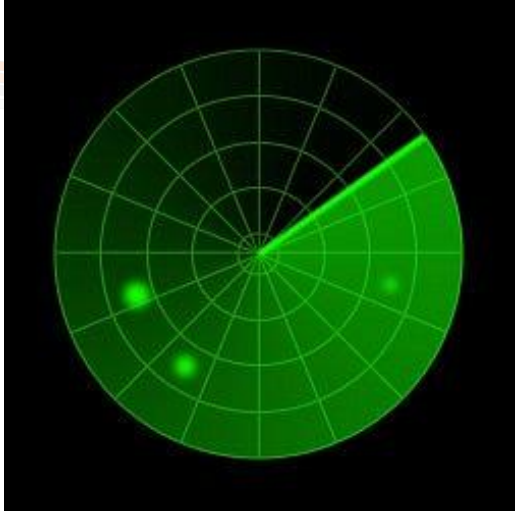
2012: IPv6

Is IPv6 (a teenager) really ‘better and more secure’?

The Absence of Reconnaissance Myth

- Default subnets in IPv6 have 2^{64} addresses
  - 10 Mpps = more than 50 000 years

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

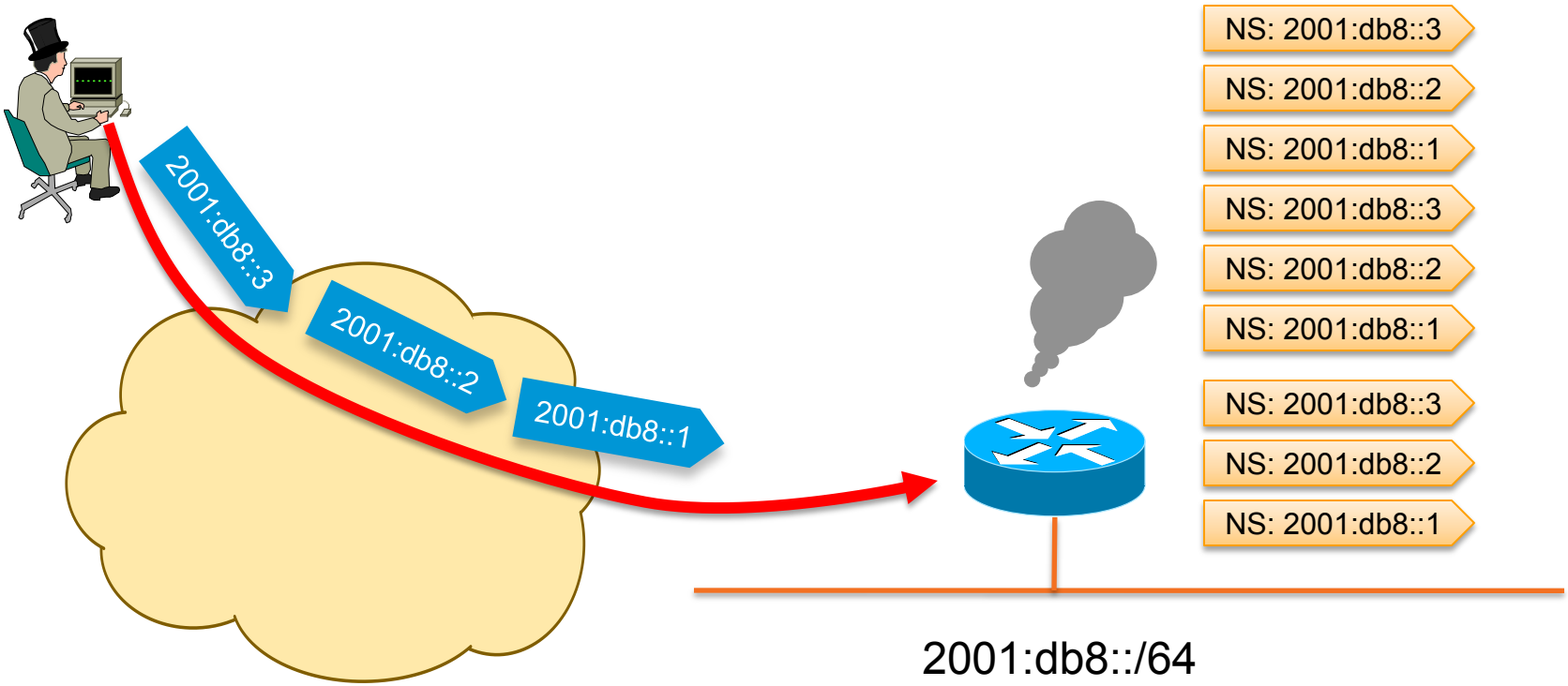
Viruses and Worms in IPv6

- Viruses and email, IM worms: IPv6 brings no change
- Other worms:
  - IPv4: reliance on network scanning
  - IPv6: not so easy (see reconnaissance) => will use alternative techniques

- Worm developers will adapt to IPv6
- IPv4 best practices around worm detection and mitigation remain valid

Scanning Made Bad for CPU
Remote Neighbor Cache Exhaustion

- Potential router CPU/memory attacks if aggressive scanning
  - Router will do Neighbor Discovery... And waste CPU and memory



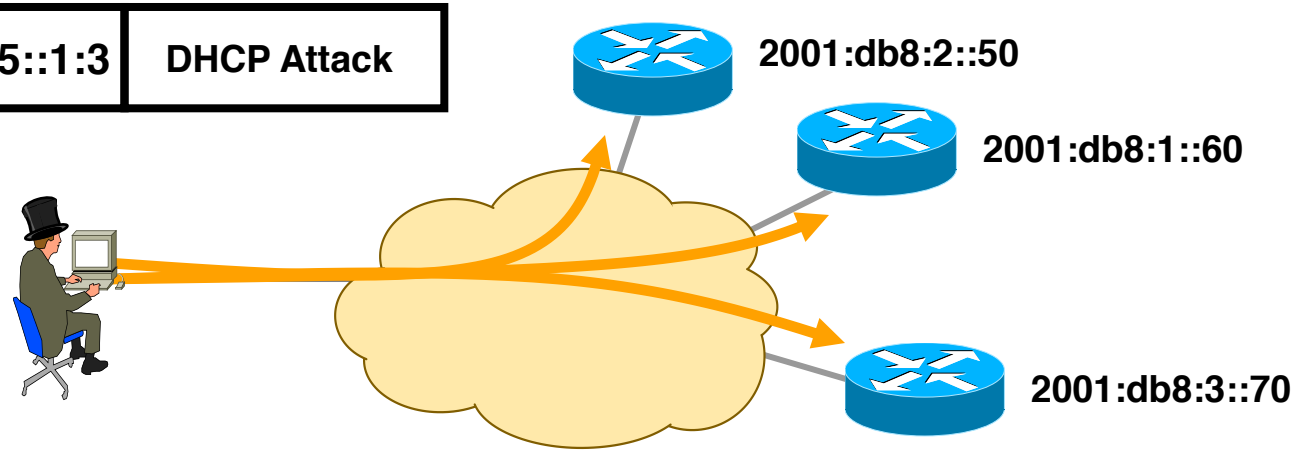
Mitigating Remote Neighbor Cache Exhaustion

- Built-in rate limiter but no option to tune it
  - Since 15.1(3)T: **`ipv6 nd cache interface-limit`**
  - Or IOS-XE 2.6: **`ipv6 nd resolution data limit`**
  - Destination-guard is coming with First Hop Security phase 3
- Using a /64 on **point-to-point links** => a lot of addresses to scan!
  - Using /127 could help (RFC 6164)
- **Internet edge/presence**: a target of choice
  - Ingress ACL permitting traffic to specific statically configured (virtual) IPv6 addresses only
- Using infrastructure ACL prevents this scanning
  - iACL: edge ACL denying packets addressed to your routers
  - Easy with IPv6 because new addressing scheme can be done ☺

Reconnaissance in IPv6? Easy with Multicast!

- No need for reconnaissance anymore
- 3 site-local multicast addresses (not enabled by default)
  - FF05::2 all-routers, FF05::FB mDNSv6, FF05::1:3 all DHCP servers
- Several link-local multicast addresses (enabled by default)
  - FF02::1 all nodes, FF02::2 all routers, FF02::F all UPnP, …

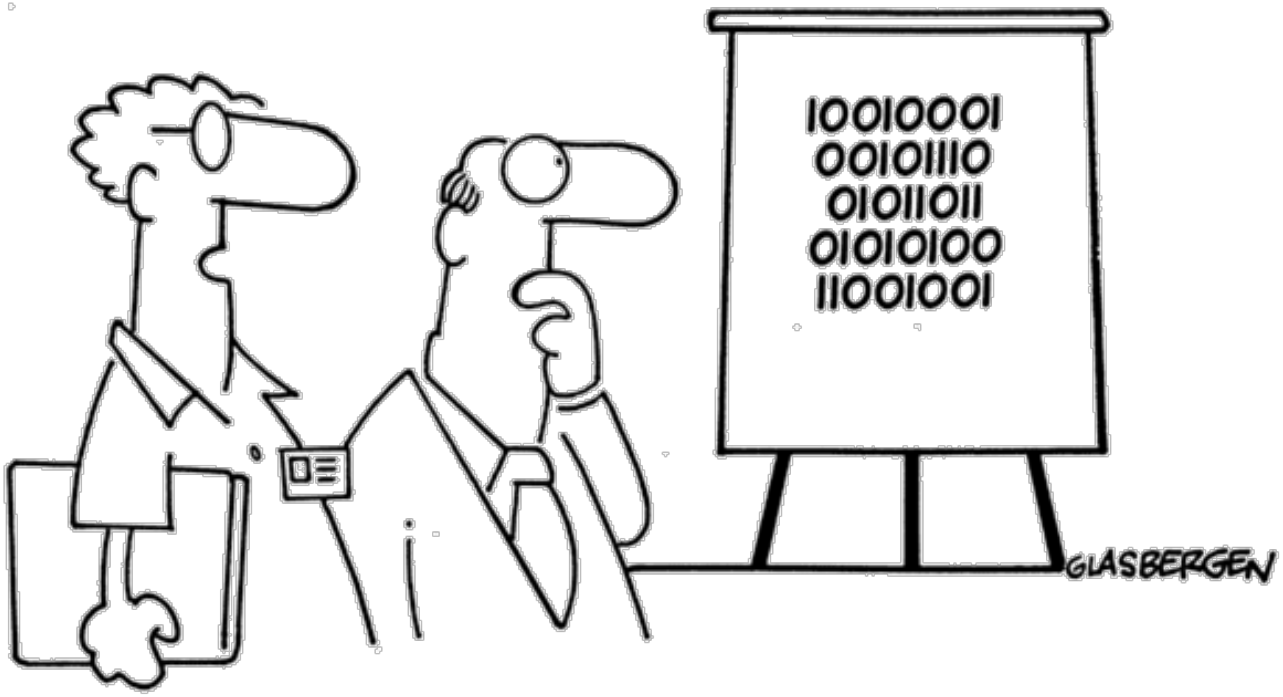
Source	Destination	Payload
Attacker	FF05::1:3	DHCP Attack



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

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…



"We've devised a new security encryption code. Each digit is printed upside down."

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

The No Amplification Attack Myth IPv6 and Broadcasts

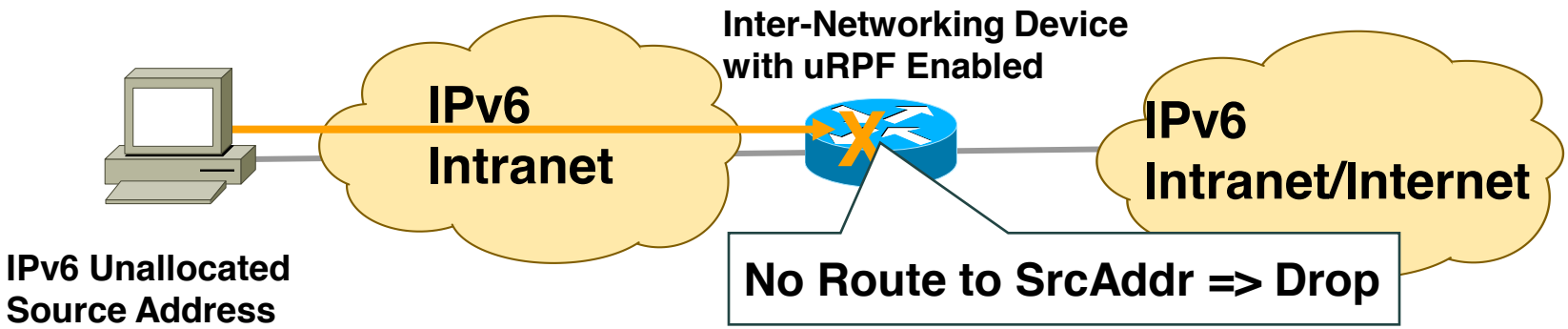
- There are no broadcast addresses in IPv6
- Broadcast address functionality is replaced with appropriate link local multicast addresses
  - Link Local All Nodes Multicast—FF02::1
  - Link Local All Routers Multicast—FF02::2
  - Link Local All mDNS Multicast—FF02::FB
  - **Note: anti-spoofing also blocks amplification attacks because a remote attacker cannot masquerade as his victim**

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

Shared Issues

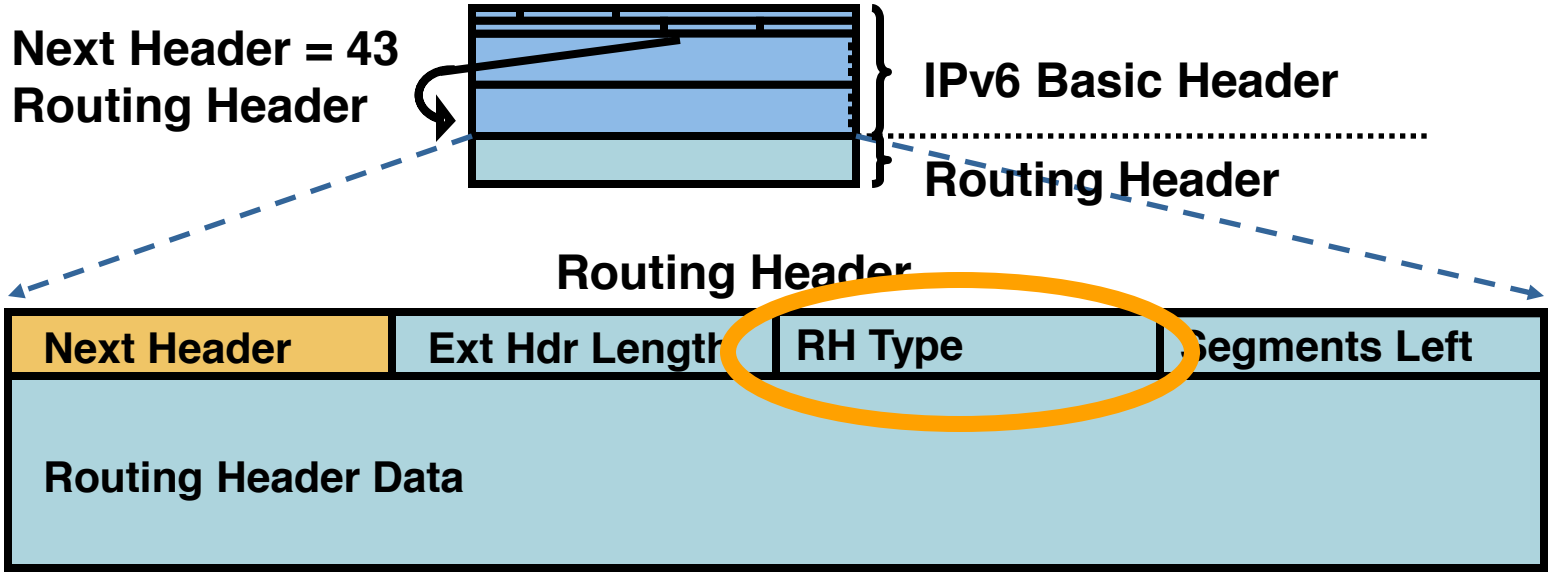
IPv6 Bogon and Anti-Spoofing Filtering

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



IPv6 Routing Header

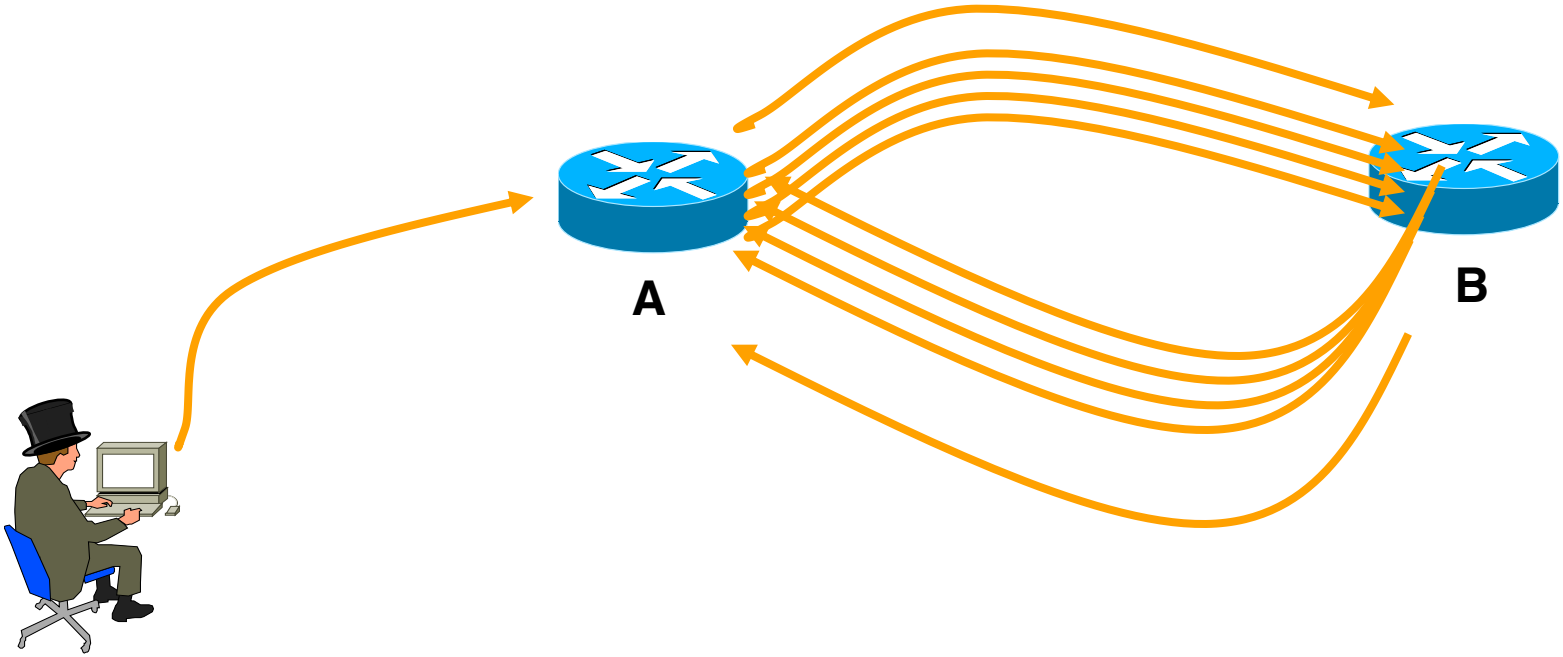
- An extension header
- Processed by the listed intermediate routers
- Two types (*)
  - Type 0: similar to IPv4 source routing (multiple intermediate routers)
  - Type 2: used for mobile IPv6



*: http://tools.ietf.org/html/draft-ietf-6man-rpl-routing-header (work in progress, should be OK for security)

Type 0 Routing Header
Issue #2: Amplification Attack

- What if attacker sends a packet with RH containing
  - A -> B -> A -> B -> A -> B -> A -> B -> A ....
- Packet will loop multiple time on the link A-B
- An amplification attack!



Preventing Routing Header Attacks

- Apply same policy for IPv6 as for Ipv4:
  - Block Routing Header type 0
- Prevent processing at the intermediate nodes
  - ***`no ipv6 source-route`***
  - Windows, Linux, Mac OS: default setting
  - IOS-XR before 4.0: a bug prevented the processing of RH0
  - IOS before 12.4(15)T: by default RH0 were processed
- At the edge
  - With an ACL blocking routing header
- RFC 5095 (Dec 2007) RH0 is deprecated
  - Default changed in IOS 12.4(15)T and IOS-XR 4.0 to ignore and drop RH0

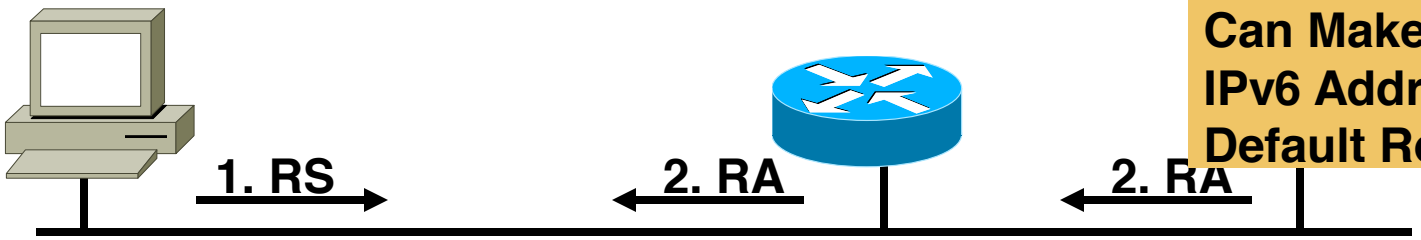
Neighbor Discovery Issue#1 Stateless Autoconfiguration

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

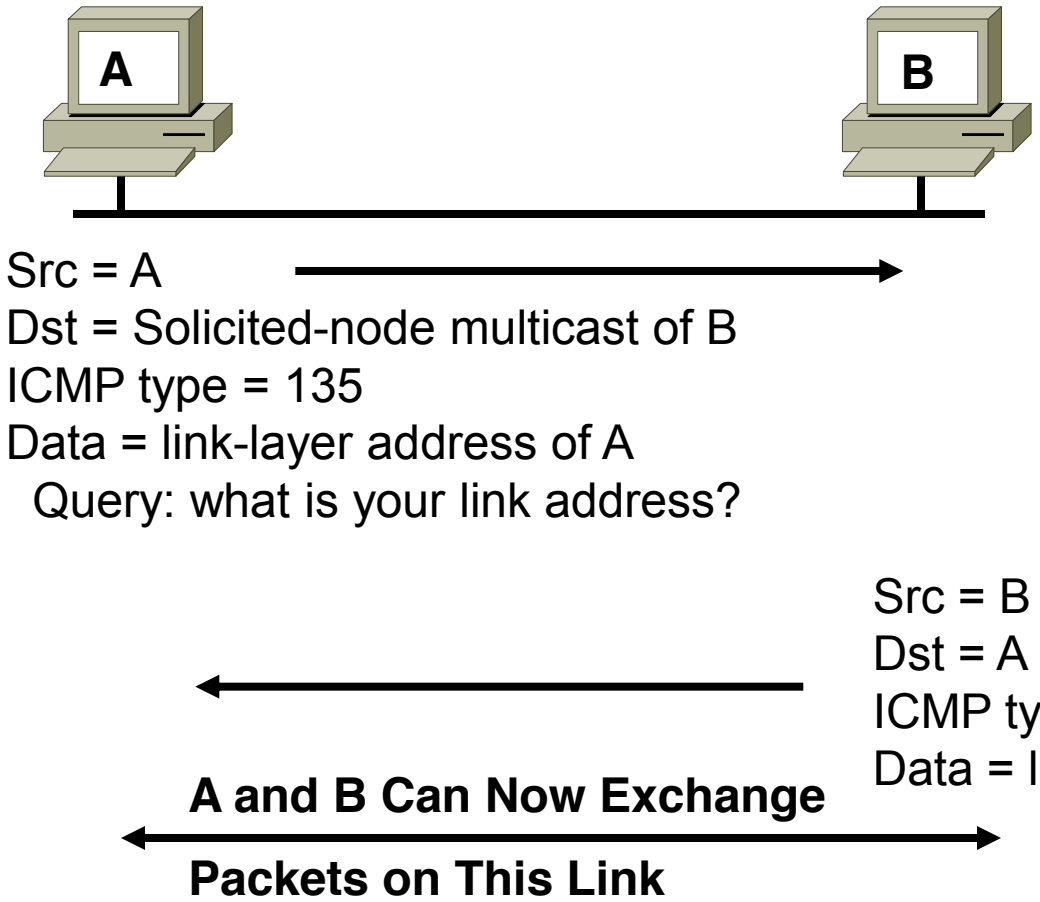
Can Make Any IPv6 Address the Default Router



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

Neighbor Discovery Issue#2
Neighbor Solicitation



Security Mechanisms Built into Discovery Protocol = None

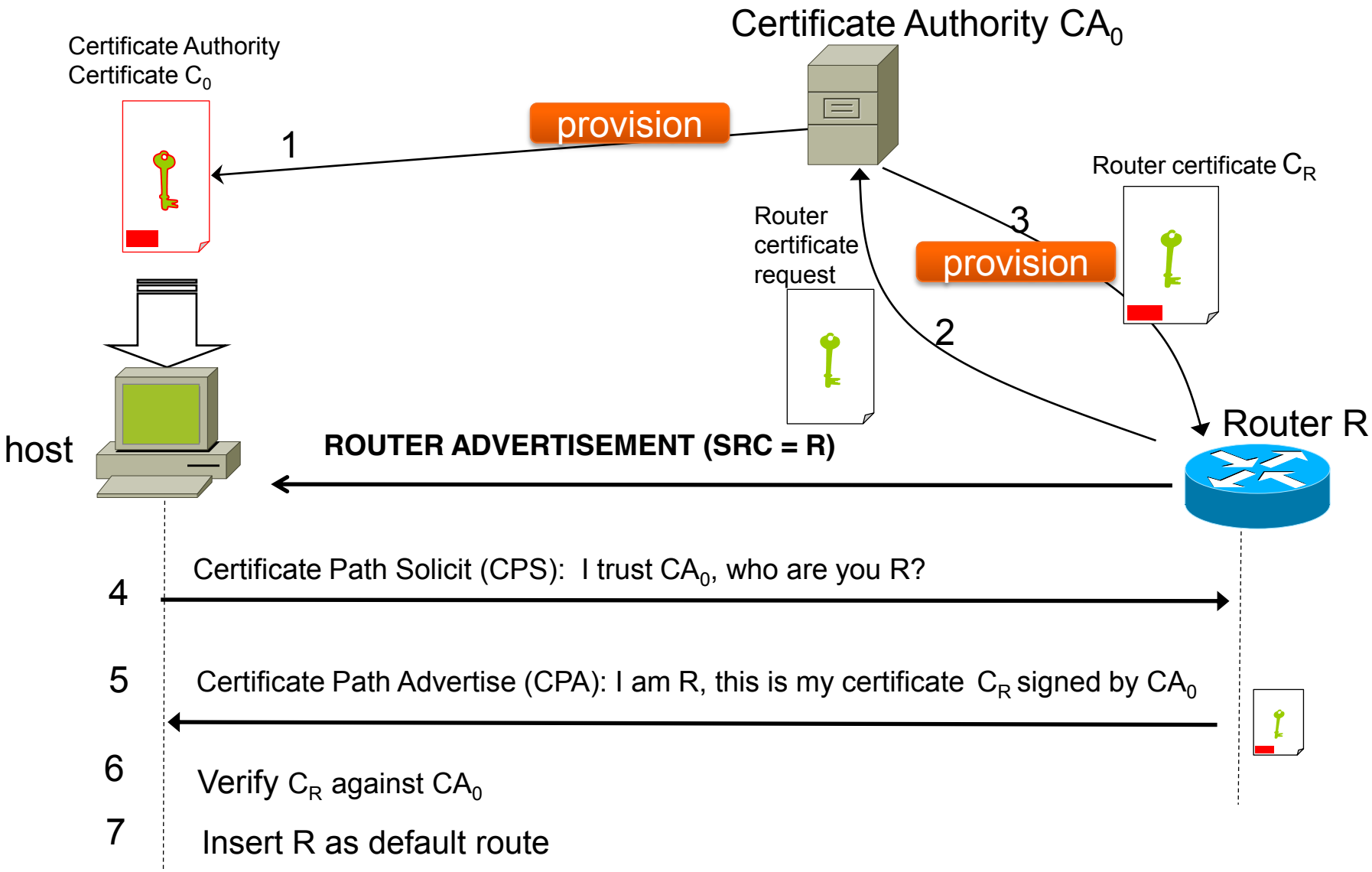
=> Very similar to ARP

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

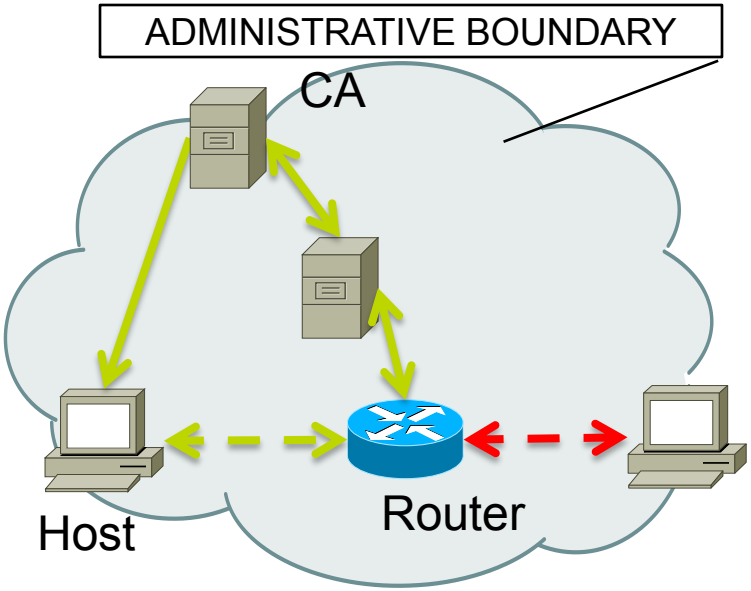
ARP Spoofing is now NDP Spoofing: Mitigation

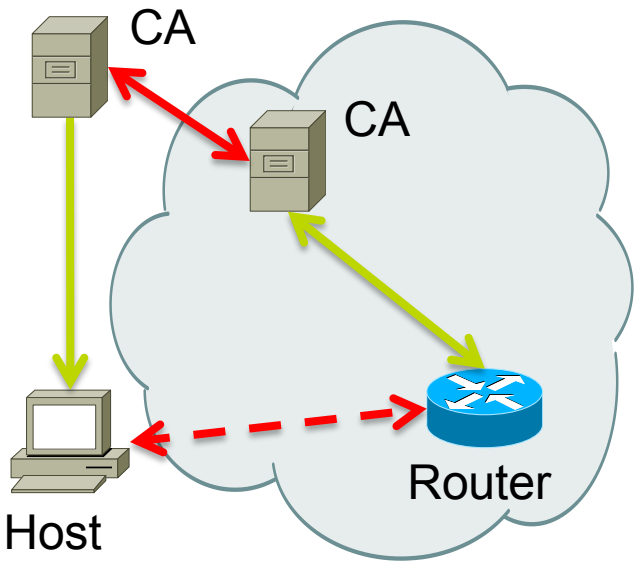
- **SEMI-BAD NEWS**: nothing yet like dynamic ARP inspection for IPv6
  - First phase (Port ACL & RA Guard) available since Summer 2010
  - Second phase (NDP & DHCP snooping) starting to be available since Summer 2011
  - http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-first_hop_security.html
- **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 802.1X works with IPv6 (except downloadable ACL)

Router Theft – Mitigation: Router Authorization overview cont'd



Router Theft – Mitigation: SeND Deployment Challenges





→ To benefit fully from SeND, nodes must be provisioned with CA certificate(s)

→ A chain of trust is "easy" to establish within the administrative boundaries, <u>but very hard outside</u>

→ It is a 2 player game! And very few IPv6 stacks can play the game today

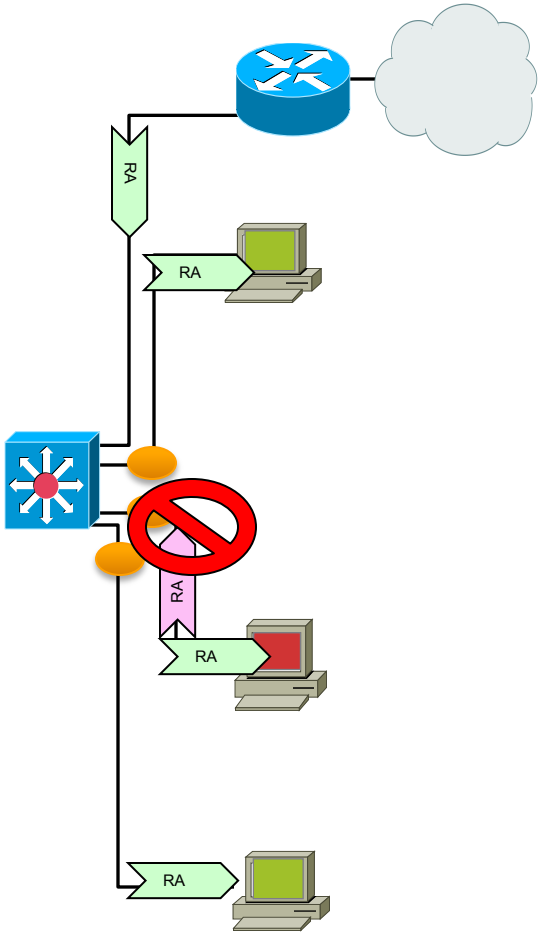
First Hop Security Phase I in 2010
Protecting against Rogue RA

- 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
```

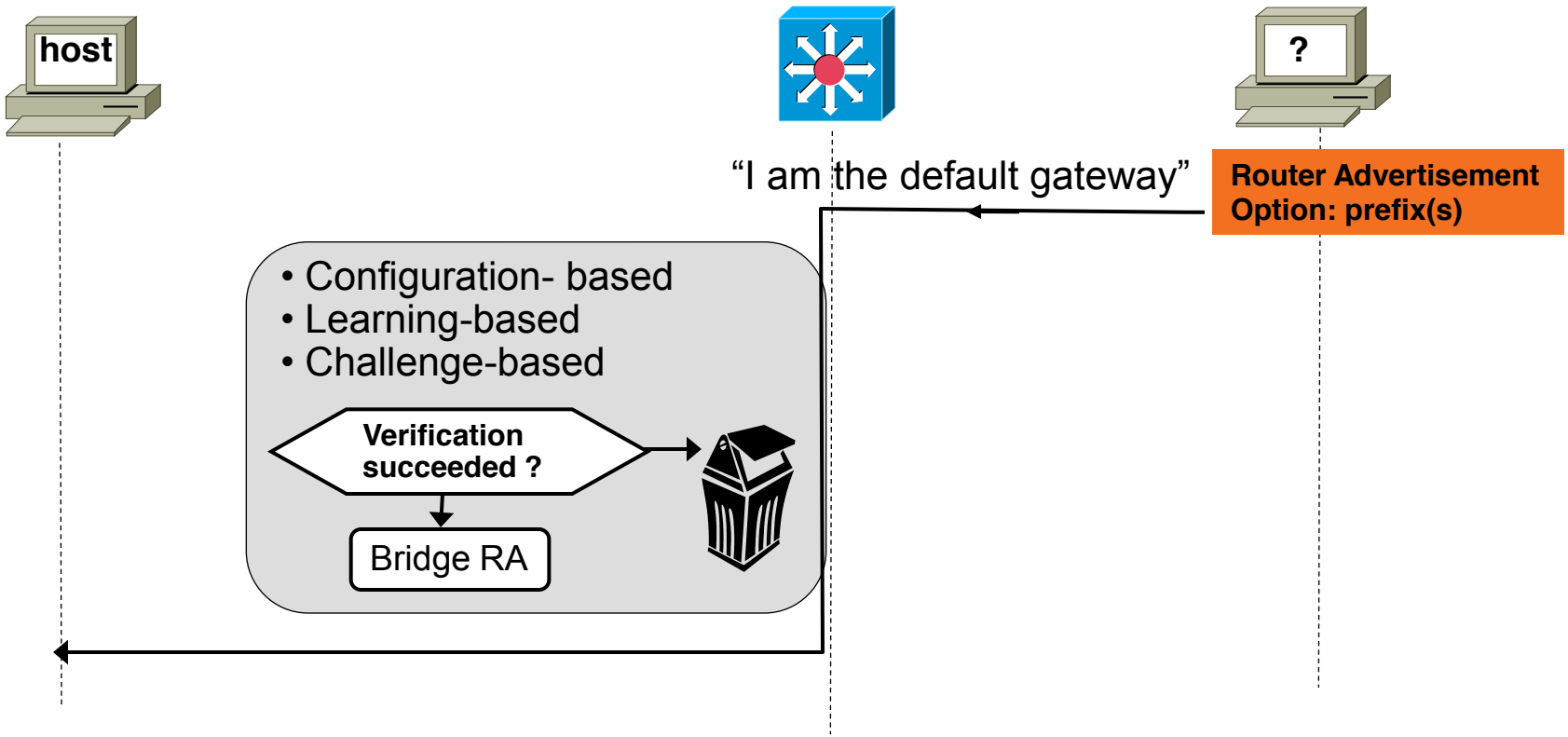
- RA-guard feature in host mode (12.2(33)SXI4 & 12.2(54)SG): also dropping all RA received on this port

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



RA-Guard

Goal: mitigate against rogue RA



- Switch selectively accepts or rejects RAs based on various criteria's
- Can be ACL based, learning based or challenge (SeND) based.
- Hosts see only allowed RAs, and RAs with allowed content

ICMPv4 vs. ICMPv6

- Significant changes
- More relied upon

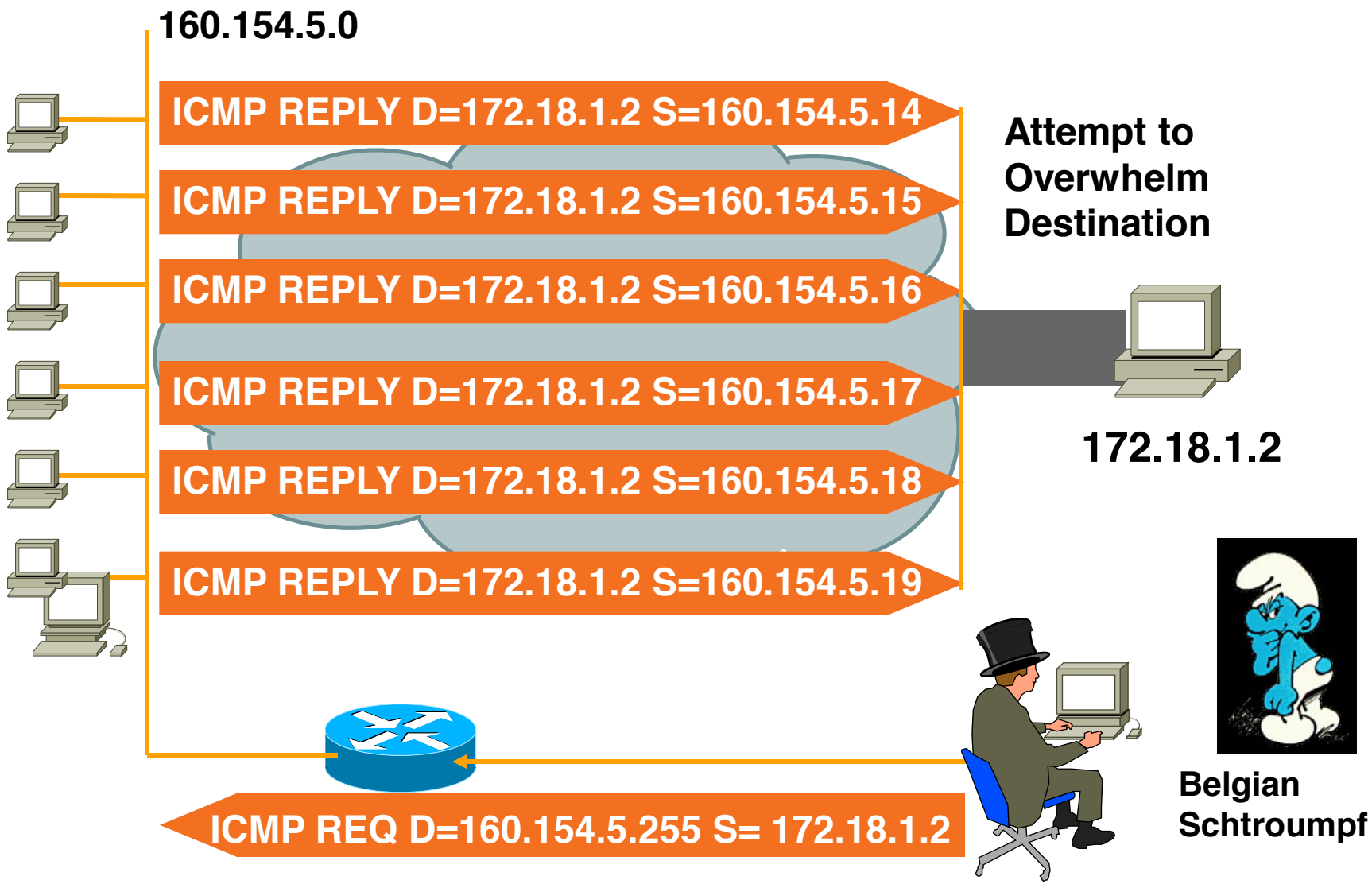
ICMP Message Type	ICMPv4	ICMPv6
Connectivity Checks	X	X
Informational/Error Messaging	X	X
Fragmentation Needed Notification	X	X
Address Assignment		X
Address Resolution		X
Router Discovery		X
Multicast Group Management		X
Mobile IPv6 Support		X

- => ICMP policy on firewalls needs to change

Information Leak with Hop-Limit

- IPv6 hop-limit has identical semantics as IPv4 time-to-live
- Can be leveraged by design
  - To ensure packet is local iff hop-limit = 255
  - Notably used by Neighbor Discovery
- Can be leveraged by malevolent people
  - Guess the remote OS: Mac OS/X always set it to 64
  - Evade inspection: hackers send some IPv6 packets analyzed by the IPS but further dropped by the network before reaching destination… Could evade some IPS
  - Threat: low and identical to IPv4

Quick Reminder
IPv4 Broadcast Amplification: Smurf

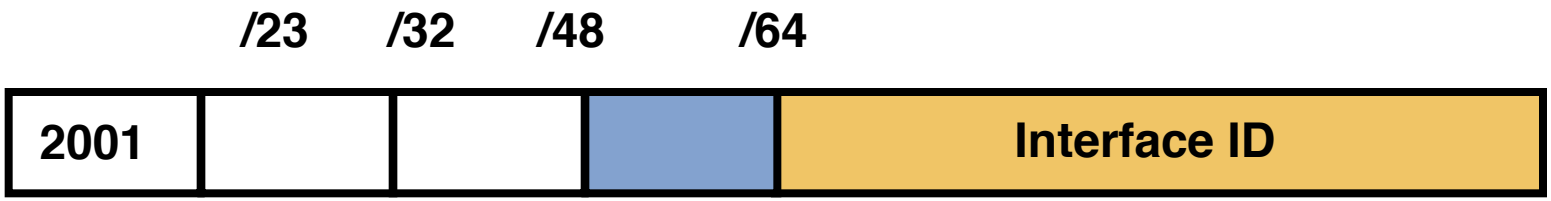


IPv6 Attacks with Strong IPv4 Similarities

- 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

Specific IPv6 Issues

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
- Enabled by default in Windows, Android, iOS

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

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 auto-configuration and force DHCPv6
  - 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
```

IPv4 to IPv6 Transition Challenges

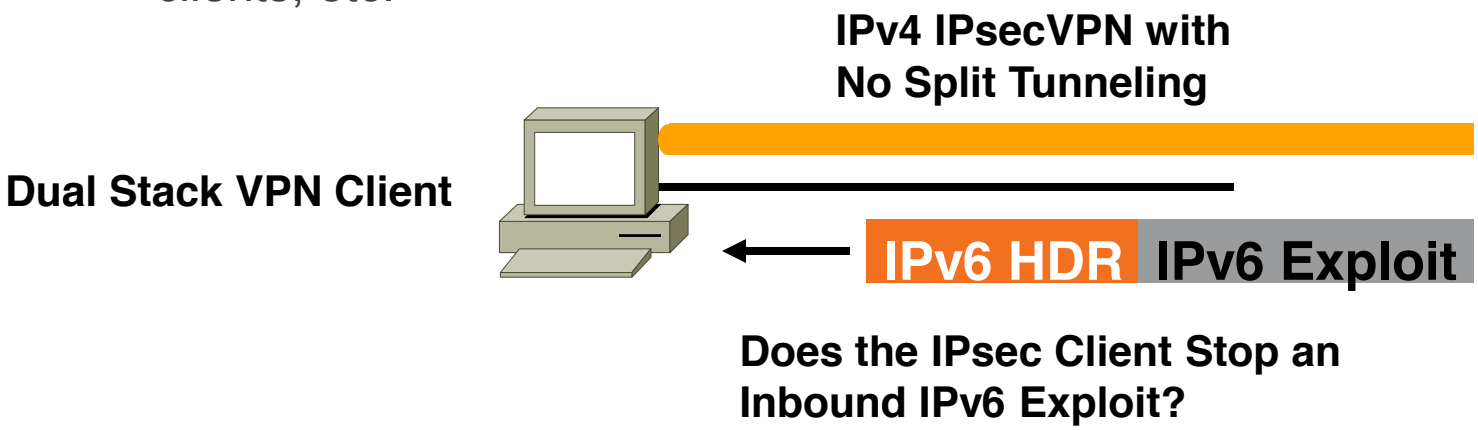
- 16+ methods, possibly in combination
- Dual stack
  - Consider security for both protocols
  - Cross v4/v6 abuse
  - Resiliency (shared resources)
- Tunnels
  - Bypass firewalls (protocol 41 or UDP)
  - Can cause asymmetric traffic (hence breaking stateful firewalls)

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

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.



Bored at BRU Airport on a Sunday at 22:00

```
$ ifconfig en1
en1: flags=8863<UP,BROADCAST,SM                                  tu 1500
          ether 00:26:bb:xx:
          inet6 fe80::226:bb                                     d 0x6
          inet 10.19.19.118                                      19.19.255
          media: autoselect
          status: active
```

Humm…
Is there an IPv6 Network?

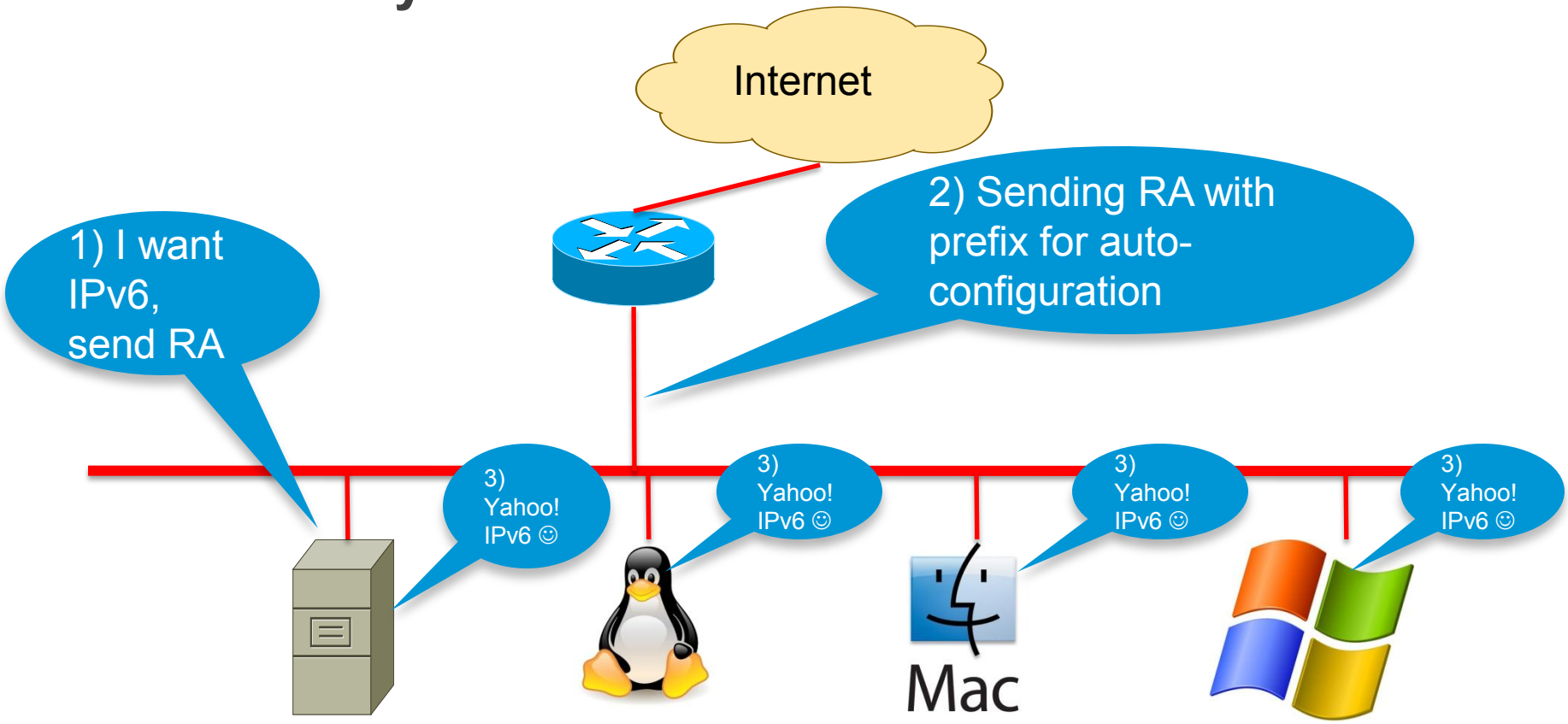
```
$ ping6 -I en1 ff02::1%en1
PING6(56=40+8+8 bytes) fe80::226:bbff:fe
16 bytes from fe80::226:bbff                                     .140 ms
. . .
16 bytes from fe80::cabc:                                        02.112 ms
^C
--- ff02::1%en1 ping6 statistics
4 packets transmitted, 4 packets recei d, +142 duplicates, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.140/316.721/2791.178/412.276 ms
```

Humm…
Are there any IPv6 peers?

```
$ ndp -an
Neighb
200
. . .
$ ndp
      64
```

Let's have some fun here… Configure a tunnel, enable forwarding and transmit RA

Enabling IPv6 in the IPv4 Data Center
The Fool's Way



IPv4 protection: iptables

IPv4 protection: ipfw

IPv4 Protection: Security center

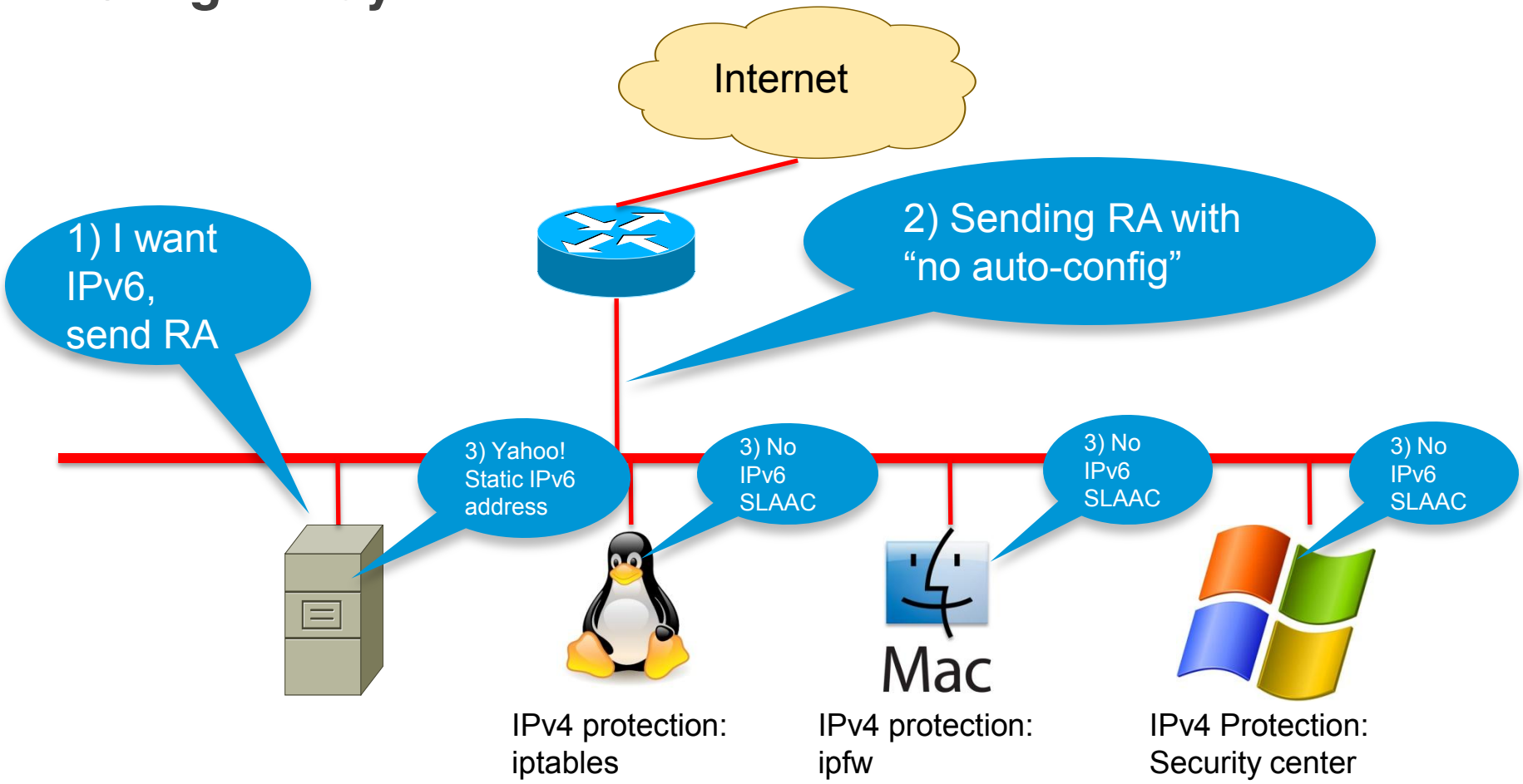
4) Default protection…

IPv6 Protection: No ip6tables ✗

IPv6 Protection: No ip6fw ✗

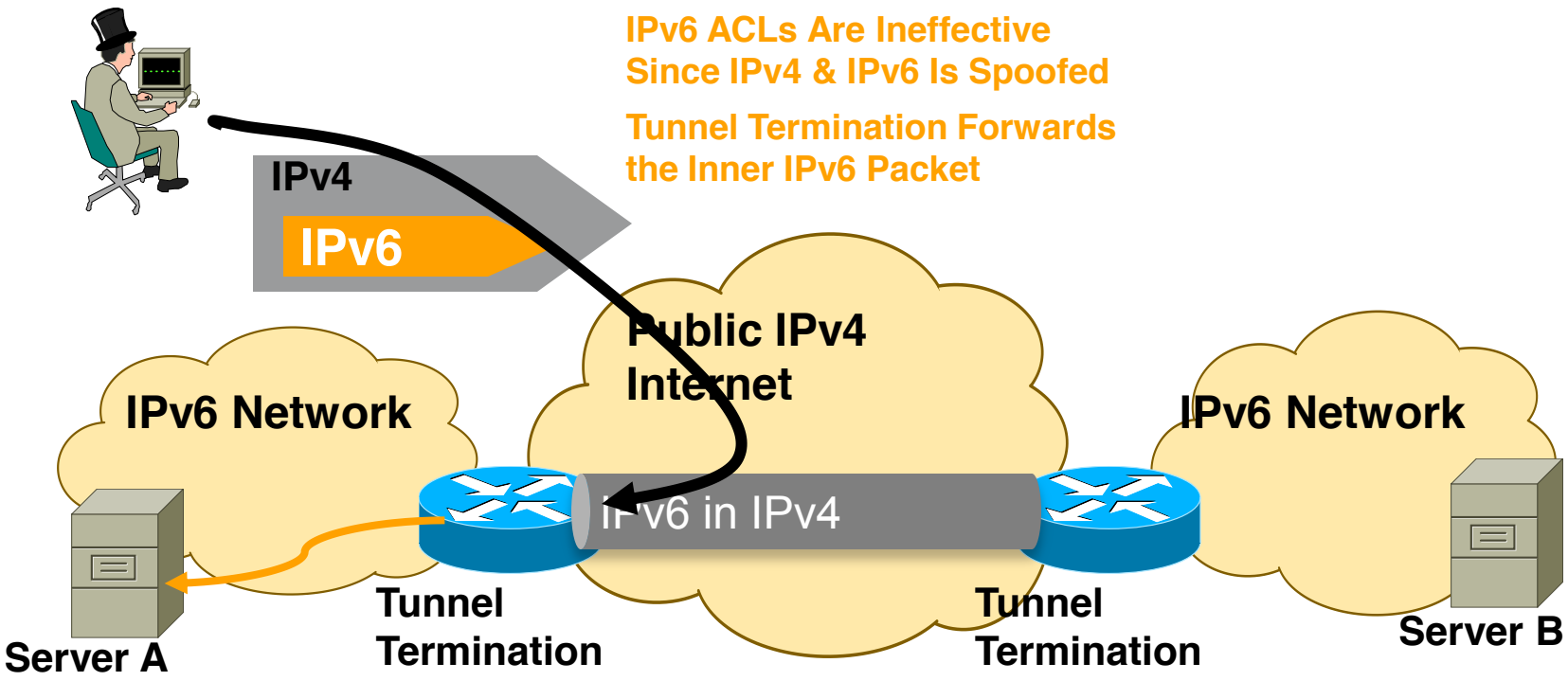
IPv6 Protection: Security center ✔

Enabling IPv6 in the IPv4 Data Center The Right Way



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



IPv6 Tunneling Summary

- RFC 1933/2893 configured and automatic tunnels
- RFC 2401 IPSec tunnel
- RFC 2473 IPv6 generic packet tunnel
- RFC 2529 6over4 tunnel
- RFC 3056 6to4 tunnel
- RFC 5214 ISATAP tunnel
- MobileIPv6 (uses RFC2473)
- RFC 4380 Teredo tunnels
- RFC 5569 6RD

- Only allow authorized endpoints to establish tunnels
- Static tunnels are deemed as “more secure,” but less scalable
- Automatic tunneling mechanisms are susceptible to packet forgery and DoS attacks
- These tools have the same risk as IPv4, just new avenues of exploitation
- Automatic IPv6 over IPv4 tunnels could be secured by IPv4 IPSec

Enforcing a Security Policy

Cisco IOS IPv6 Extended Access Control Lists

- Very much like in IPv4
  - Filter traffic based on
    - Source and destination addresses
    - Next header presence
    - Layer 4 information
  - Implicit deny all at the end of ACL
  - Empty ACL means traffic allowed
  - Reflexive and time based ACL
- Known extension headers (HbH, AH, RH, MH, destination, fragment) are scanned until:
  - Layer 4 header found
  - Unknown extension header is found
- Side note for 7600 & other switches:
  - No VLAN ACL on the roadmap
  - Port ACL on Nexus-7000, Cat 3750 (12.2(46)SE not in base image), Cat 4K (12.2(54)SG), Cat 6K (12.3(33)SXI4)

IPv6 ACL Implicit Rules RFC 4890

- Implicit entries exist at the end of each IPv6 ACL to allow neighbor discovery:

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

- Nexus 7000 also allows RS & RA

IPv6 ACL Implicit Rules – Cont. Adding a deny-log

- The beginner's mistake is to add a deny log at the end of IPv6 ACL

```
. . .
! Now log all denied packets
deny ipv6 any any log
! Heu . . . I forget about these implicit lines
permit icmp any any nd-na
permit icmp any any nd-ns
deny ipv6 any any
```

- Solution, explicitly add the implicit ACE

```
. . .
! Now log all denied packets
permit icmp any any nd-na
permit icmp any any nd-ns
deny ipv6 any any log
```

Example: Rogue RA & DHCP Port ACL

```
ipv6 access-list ACCESS_PORT
    remark for paranoid, block 1st fragment w/o L4 info
    deny ipv6 any any undetermined-transport
    remark Block all traffic DHCP server -> client
    deny udp any eq 547 any eq 546
    remark Block Router Advertisements
    deny icmp any any router-advertisement
    permit ipv6 any any

Interface gigabitethernet 1/0/1
    switchport
    ipv6 traffic-filter ACCESS_PORT in
```

Note: PACL replaces RACL for the interface (or is merged with RACL 'access-group mode prefer port')
In August 2010, Nexus-7000, Cat 3750 12.2(46)SE, Cat 4500 12.2(54)SG and Cat 6500 12.2(33)SXI4

IPv6 ACL to Protect VTY

For Your Reference

```
ipv6 access-list VTY
  permit ipv6 2001:db8:0:1::/64 any


line vty 0 4
  ipv6 access-class VTY in
```

MUST BE DONE before '***ipv6 enable***' on any interface!

Control Plane Policing for IPv6 Protecting the Router CPU

For Your Reference

- Against DoS with NDP, Hop-by-Hop, Hop Limit Expiration...
- Software routers (ISR, 7200): works with CoPPr (CEF exceptions)

```
policy-map COPPr
 class ICMP6_CLASS
   police 8000
 class OSPF_CLASS
   police 200000
 class class-default
   police 8000
!
control-plane cef-exception
 service-policy input COPPr
```

- Cat 6K & 7600
  - IPv6 shares mls rate-limit with IPv4 for NDP & HL expiration

```
mls rate-limit all ttl-failure 1000
mls rate-limit unicast cef glean 1000
```

ASA Firewall IPv6 Support

- Since version 7.0 (April 2005)
- Dual-stack, IPv6-only, IPv4-only
- Extended IP ACL with stateful inspection
- Application awareness: TTP, FTP, telnet, SMTP, TCP, SSH, UDP
- uRPF and v6 Frag guard
- IPv6 header security checks (length & order)
- Management access via IPv6: Telnet, SSH, HTTPS
- ASDM support (ASA 8.2)
- Routed & transparent mode (ASA 8.2)
- Fail-over support (ASA 8.2.2)
- Selective permit/deny of extension headers (ASA 8.4.2)
- *OSPFv3, DHCPv6 relay, stateful NAT64/46/66 (expected mid 2012)*

Summary

Key Take Away

- 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 feature coming
  - ICMPv6 firewalls need to change policy to allow NDP
  - Extension headers: firewall & ACL can process them
  - Amplification attacks by multicast mostly impossible
  - Potential loops between tunnel endpoints: ACL must be used
- 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

Is IPv6 in My Network?

- Easy to check!
- Look inside NetFlow records
  - Protocol 41: IPv6 over IPv4 or 6to4 tunnels
  - IPv4 address: 192.88.99.1 (6to4 anycast server)
  - UDP 3544, the public part of Teredo, yet another tunnel
- Look into DNS server log for resolution of ISATAP
- Beware of the IPv6 latent threat: ***your IPv4-only network may be vulnerable to IPv6 attacks NOW***

Questions and Answers?

Thank you.