IPv6 Security

SEC-2003

Session Objectives

- This session presents IPv6 security as contrasted with IPv4 from a threat and mitigation perspectives
- Advanced IPv6 security topics like transition options and dual stack IPv6/IPv4 environments
- This session requires a basic knowledge of the IPv6 and IPsec protocols as well as IPv4 security best practices

Agenda

- Types of Threats
- IPv6 and IPv4 Threat Comparisons
- IPv6 Security Best Common Practice
- Specific Issues for IPv6
    - Tunnels and Mobile IPv6
- Enforcing a Security Policy in IPv6
    - ACL and Firewalls
- Enterprise Secure Deployment

Types of Threats

Types of Threats

- **Reconnaissance—Provide the adversary with information**
- **Unauthorized access—Exploit**
- **Header manipulation and fragmentation—Evade or overwhelm**
- **Layer 3–Layer 4 spoofing— Mask the intent or origin of the traffic**
- **ARP and DHCP attacks—Subvert the host initialization process**
- **Broadcast amplification attacks (smurf)—Amplify the effect of a flood**
- **Routing attacks—Disrupt or redirect traffic flows**

Types of Threats (Cont.)

- **Viruses and worms**— Propagation of the malicious payload
- **Sniffing**—Capturing data
- **Application layer attacks**— Attacks executed at Layer 7
- **Rogue devices**—Unauthorized devices connected to a network
- **Man-in-the-middle attacks**— Attacks which involve interposing an adversary between two communicating parties
- **Flooding**—Consume enough resources to delay processing of valid traffic

Threat Comparison

Reconnaissance in IPv4

In IPv4, Reconnaissance Is Relatively Easy

1. DNS/IANA crawling (whois) to determine ranges
2. Ping sweeps and port scans
3. Application vulnerability scans

```
[tick:/var] scott# nmap -sP 10.1.1.0/24
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Host (10.1.1.0) seems to be a subnet broadcast …
Host (10.1.1.1) appears to be up.
Host (10.1.1.12) appears to be up.
Host (10.1.1.22) appears to be up.
Host (10.1.1.23) appears to be up.
Host (10.1.1.101) appears to be up.
Host (10.1.1.255) seems to be a subnet broadcast …
Nmap run completed -- 256 IP addresses (7 hosts up)
scanned in 4 seconds
```

Reconnaissance in IPv6
Subnet Size Difference

- **Default subnets in IPv6 have 2^64 addresses**

  => scanning every address: centuries vs. seconds

- **NMAP doesn’t even support for ping sweeps on IPv6 networks (you’ll have retired by the time it finishes, even at one million packets per second)**

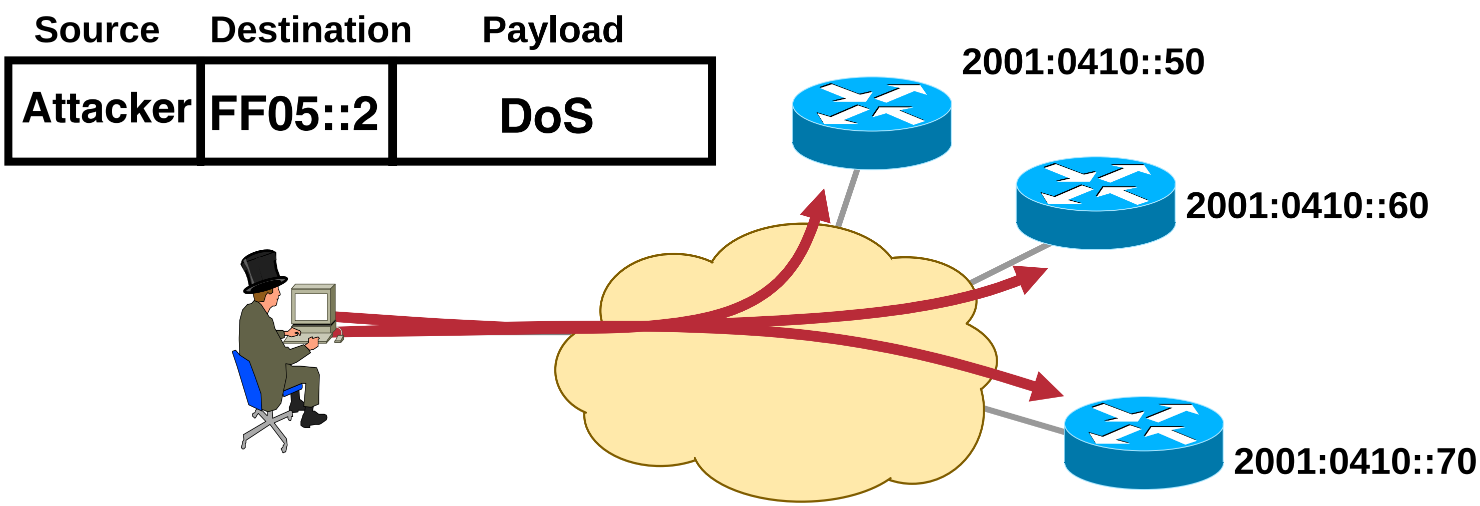
Reconnaissance in IPv6
IP6 Scanning Methods Are Likely to Change

- Public servers will still need to be DNS reachable
- Dynamic DNS adoption causing DNS servers to be rich sources of addresses to scan
- Administrators may adopt easy to remember addresses (::10,::20,::F00D, or simply IPv4 last octet)
- By compromising hosts in a network, an attacker can learn new addresses to scan

Reconnaissance in IPv6

New Multicast Addresses

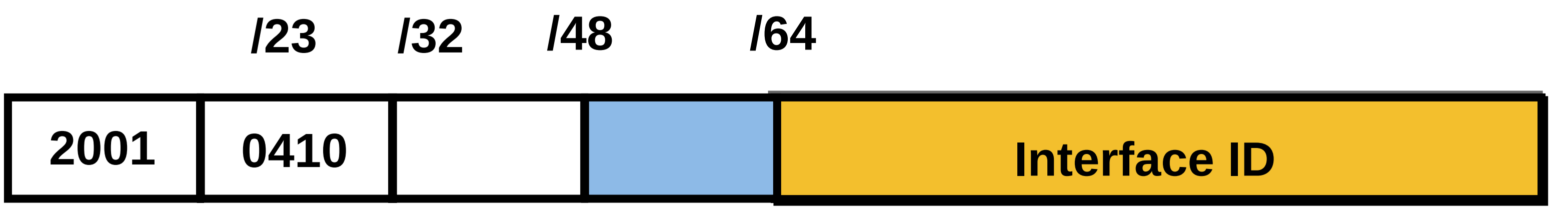
- **For example, all routers (FF05::2) and all DHCP servers (FF05::1:3)**
- **These addresses must be filtered at the border in order to make them unreachable from the outside**



Reconnaissance IPv6 Best Practices

- **Implement privacy extensions carefully—(next slide)**
- **Filter internal-use IPv6 addresses at organization border routers—prevent addresses like the all nodes multicast address from becoming conduits for attack**
- **Filter unneeded services at the firewall—just like in IPv4**
- **Selectively filter ICMP—more on this later**
- **Maintain host and application security—just like in IPv4**

IPv6 Privacy Extensions (RFC 3041)

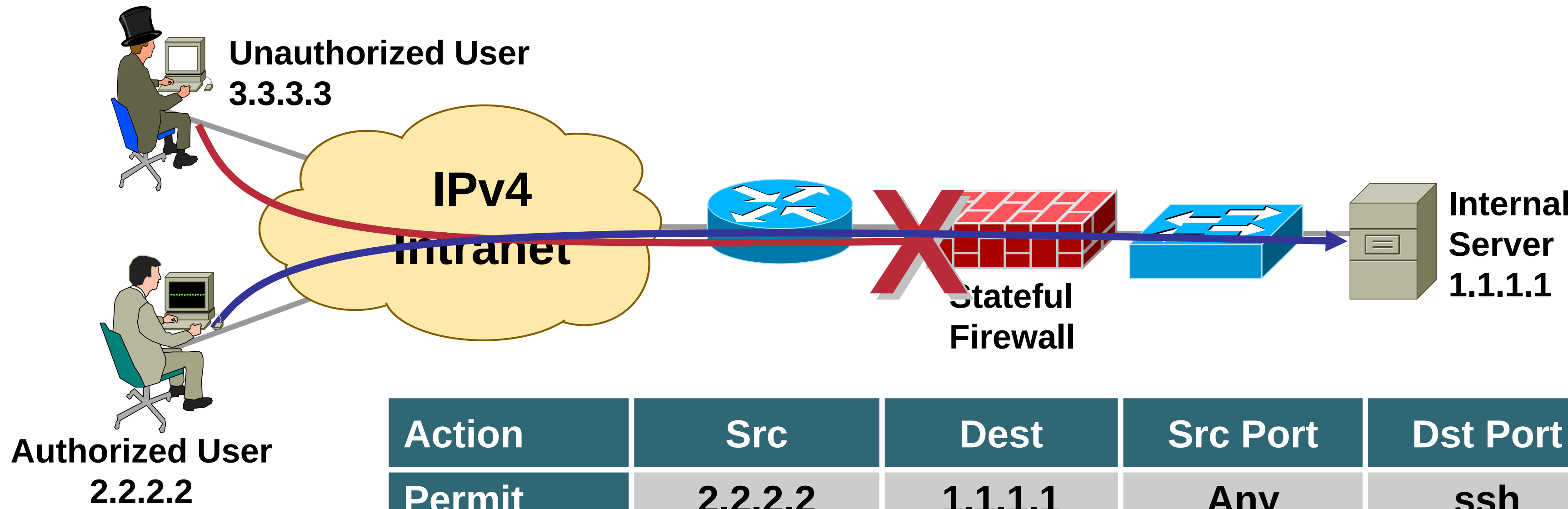


- **Temporary addresses for IPv6 host client application, e.g. web browser**
  - **Inhibit device/user tracking but many organizations want to do the tracking**
  - **Random 64 bit interface ID, run DAD before using it**
  - **Rate of change based on local policy**

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

Access Control in IPv4

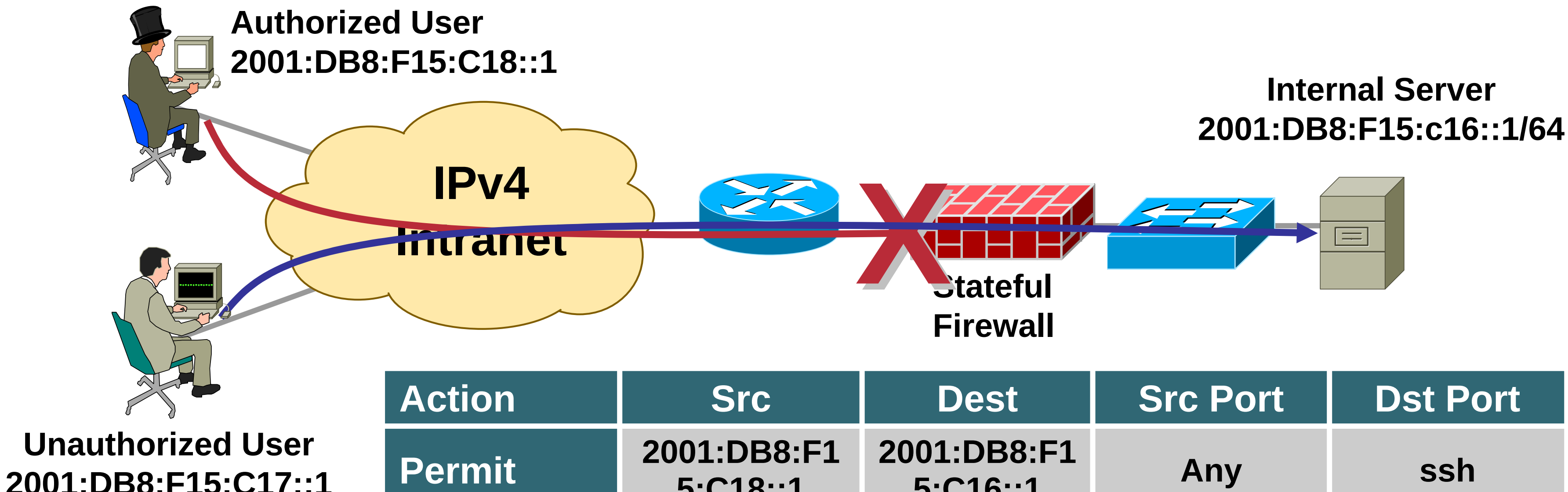
- **Access authorization mainly based on Layer 3 and Layer 4**



Action	Src	Dest	Src Port	Dst Port
Permit	2.2.2.2	1.1.1.1	Any	ssh
Deny	Any	Any		

Access Control in IPv6

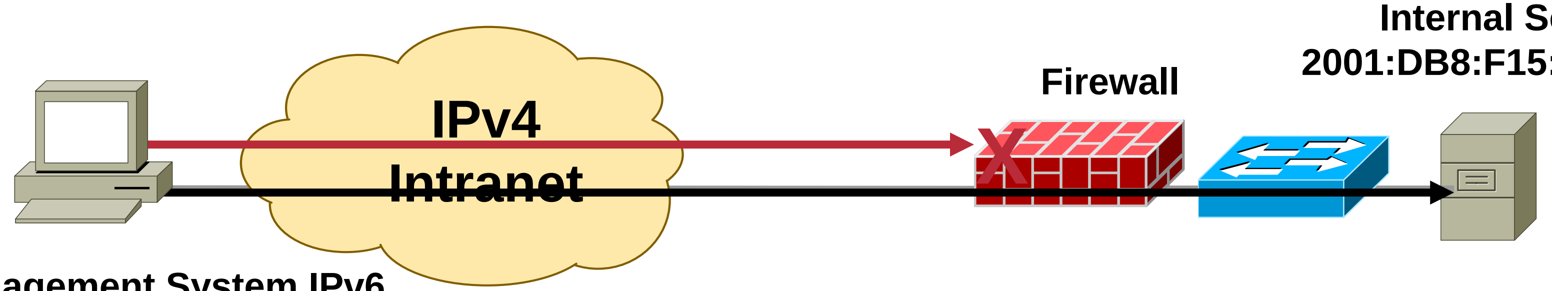
- **Access control in IPv6: Also based on Layer 3 and Layer 4 information**
- **In addition IPv6 has some unique considerations**



Action	Src	Dest	Src Port	Dst Port
Permit	2001:DB8:F15:C18::1	2001:DB8:F15:C16::1	Any	ssh
Deny	Any	Any		

Access Control in IPv6 Privacy Extension

- Good to protect the privacy of a host
- But hard to define authorization policy when the Layer 3 information is always changing :-)

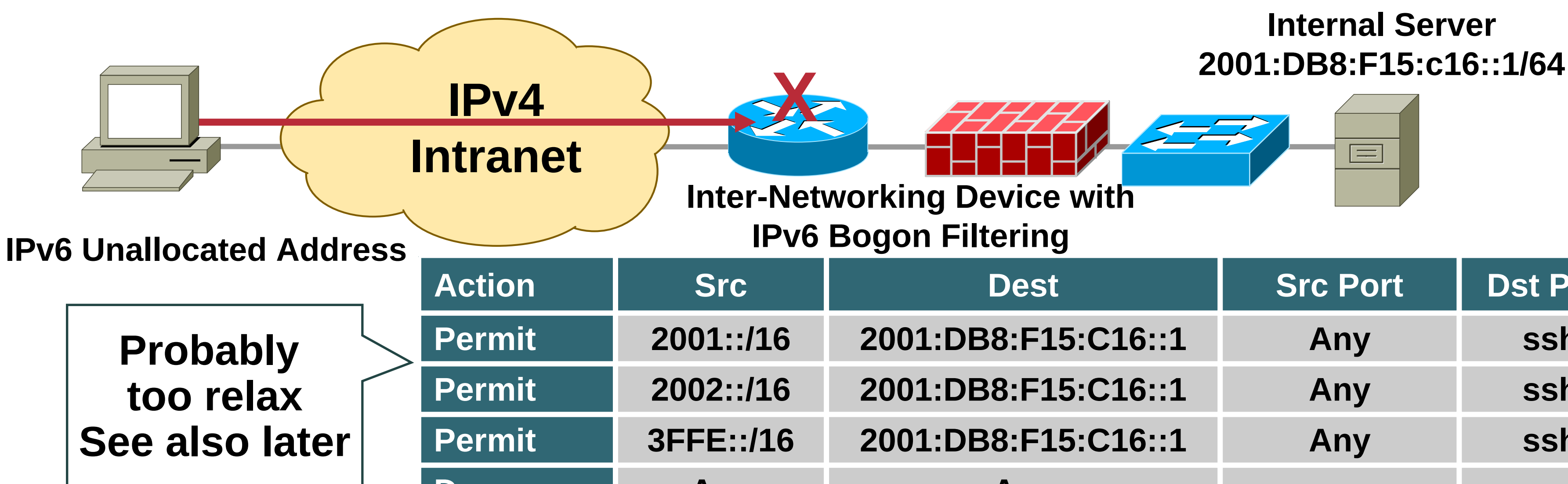


*—Not Real RFC3041 Derived Addresses

Action	Src	Dest	Src Port	Dst Port
Permit	2001:DB8:F15:C15::1	2001:DB8:F15:c16::1	Any	80
Deny	Any	Any		

Access Control in IPv6
Bogon Filtering

- **In IPv4, it is generally easier to block bogons than it is to permit non-bogons**
- **In IPv6, a small amount top-level aggregation identifiers (TLAs) have been allocated thus far**



Action	Src	Dest	Src Port	Dst Port
Permit	2001::/16	2001:DB8:F15:C16::1	Any	ssh
Permit	2002::/16	2001:DB8:F15:C16::1	Any	ssh
Permit	3FFE::/16	2001:DB8:F15:C16::1	Any	ssh
Deny	Any	Any		

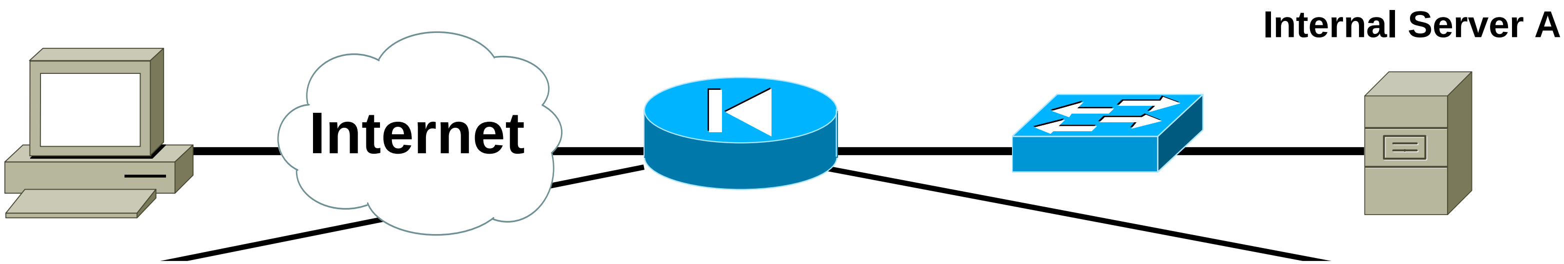
ICMPv4 vs. ICMPv6

- **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
Multicast Group Management		X
Mobile IPv6 Support		X

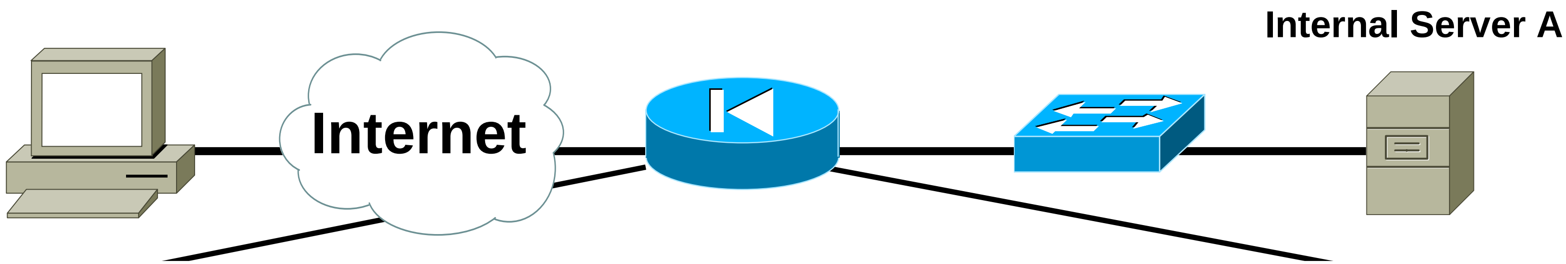
- **=> ICMP policy on firewalls needs to change**

Generic ICMPv4 Border Firewall Policy



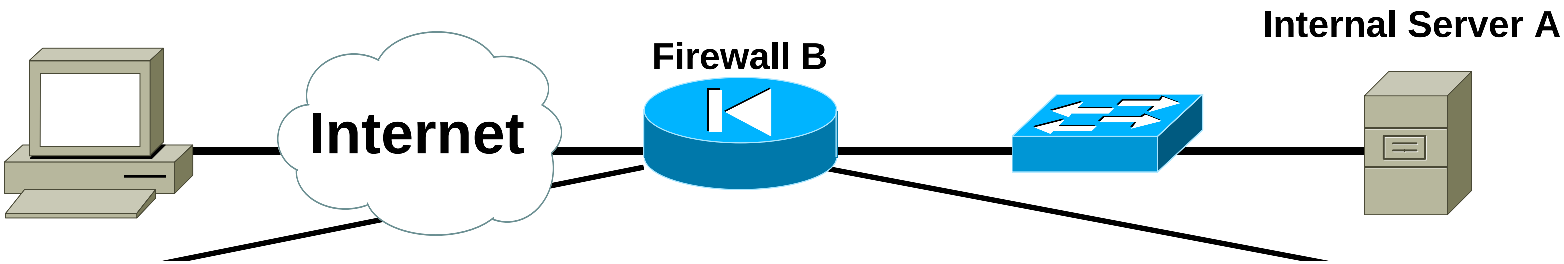
Action	Src	Dst	ICMPv4 Type	ICMPv4 Code	Name
Permit	Any	A	0	0	Echo Reply
Permit	Any	A	8	0	Echo Request
Permit	Any	A	3	0	Dst. Unreachable—Net Unreachable
Permit	Any	A	3	4	Dst. Unreachable—Frag. Needed
Permit	Any	A	11	0	Time Exceeded—TTL Exceeded

Equivalent Comparison ICMPv6 Border Firewall Policy



Action	Src	Dst	ICMPv6 Type	ICMPv6 Code	Name
Permit	Any	A	128	0	Echo Reply
Permit	Any	A	129	0	Echo Request
Permit	Any	A	1	0	No Route to Dst.
Permit	Any	A	2	0	Packet too Big
Permit	Any	A	3	0	Time Exceeded—TTL Exceeded

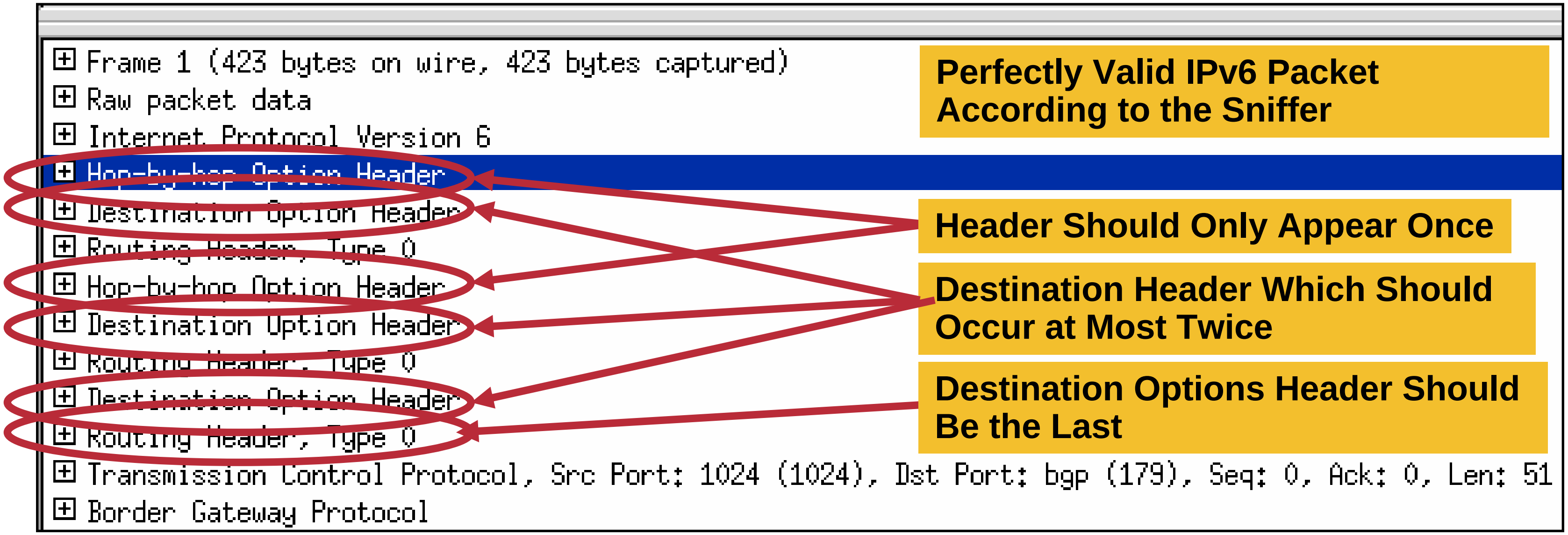
Potential Additional ICMPv6 Border Firewall Policy



Action	Src	Dst	ICMPv6 Type	ICMPv6 Code	Name
Permit	Any	A	4	0	Parameter Problem
Permit	Any	B	2	0	Packet too Big
Permit	Any	B	130–132	0	Multicast Listener
Permit	Any	B	133/134	0	Neighbor Solicitation and Advertisement
Permit	Any	B	4	0	Parameter Problem

IPv6 Header Manipulation

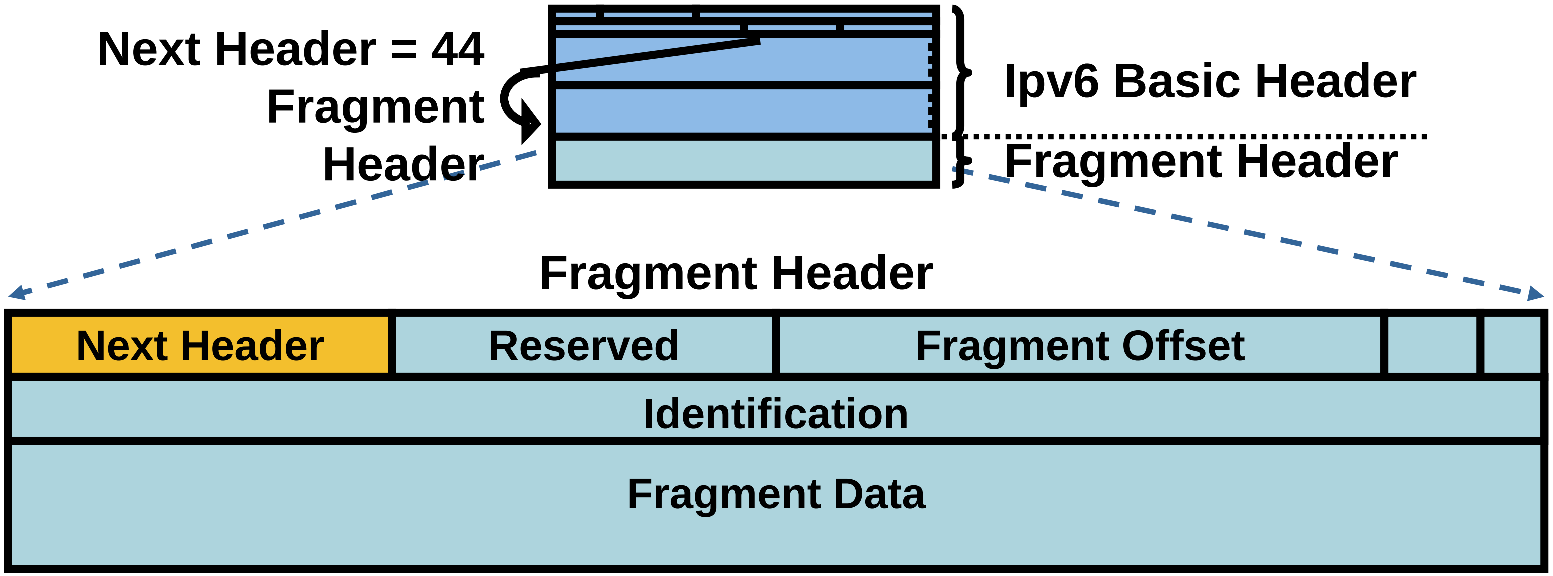
- **Unlimited size of header chain (spec wise) can make filtering difficult**
- **DoS a possibility with poor IPv6 stack implementations**
  - **More boundary conditions to exploit**
  - **Can I overrun buffers with a lot of extension headers?**



Fragmentation Used in IPv4 by Attackers

- **Great evasion techniques**
- **Tools like whisker, fragrout, etc.**
- **Makes firewall and network intrusion detection harder**
- **Used mostly in DoSing hosts, but can be used for attacks that compromise the host**

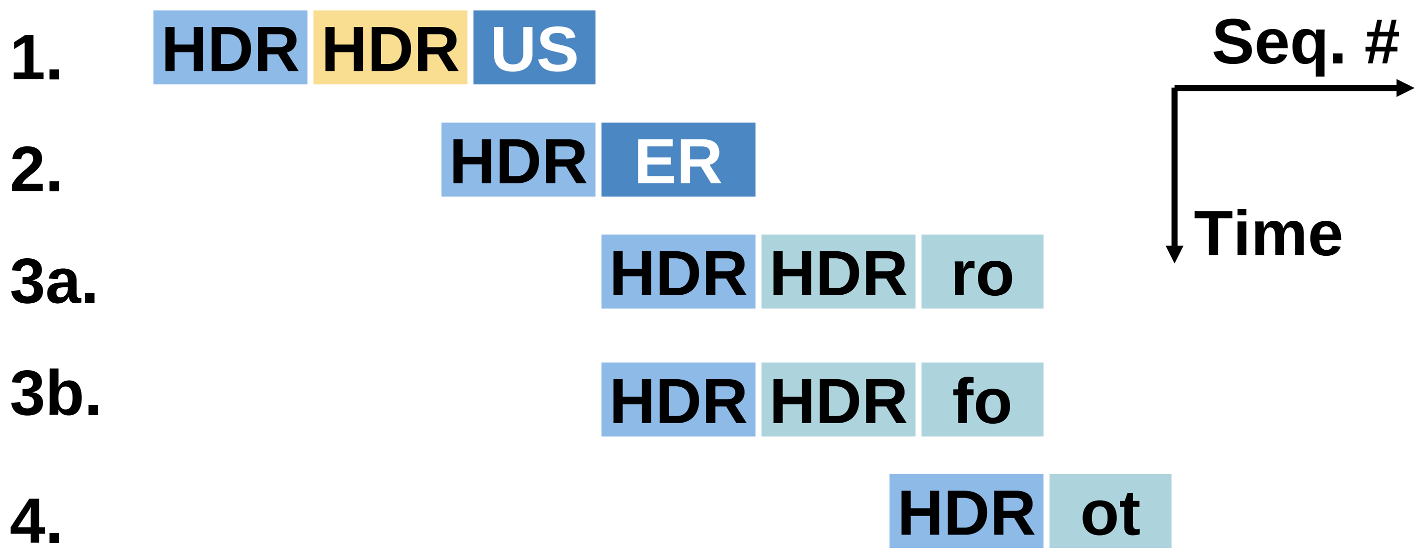
Fragment Header: IPv6



- **In IPv6 fragmentation is done only by the end system**
- **Reassembly done by end system like in IPv4**
- **Attackers can still fragment in intermediate system on purpose**
- **==> a great obfuscation tool**

IPv6 Fragmentation: Still Need Reassembly in the Firewall and NIDS

Imagine an Attacker Sends:



- **Should we consider 3a part of the data stream "USER root"?**
- **Or is 3b part of the data stream? "USER foot"**

  If the OS makes a different decision than the monitor: bad

  Even worse: different OSs have different protocol interpretations,

  If they are overlapping fragments BSD IPv6 drops packet; Linux IPv6 reassembly mimics IPv4 behavior

IPv6 Fragmentation
Issues for Non-Stateful Filtering Devices

- Traverse the next headers before reaching the fragment header to extract the flags and offset
- Then, further NHs before reaching the ULP
- Then check if enough of the upper Layer protocol header is within the first fragment
- This makes matching against the first fragment non-deterministic: tcp/udp/icmp might not be there

IPv6 Fragmentation: Fragment Keyword in IPv6 ACL

- `fragment` keyword matches
  - Non-initial fragments (same as IPv4)
  - And the first fragment if the protocol cannot be determined
- Note: Cisco IOS® also supports a new keyword "undetermined-transport"
  - matches any IPv6 packet where the Layer 4 cannot be determined

Header Manipulation and Fragmentation Best Practices

- **Deny IPv6 fragments destined to an internetworking device (DOS vector)**
- **Ensure adequate IPv6 fragmentation filtering capabilities; for example, drop all packets with the routing header if you don't have MIPv6**
- **If really paranoid: drop all fragments with less than 1280 octets (except the last fragment)**

L3-L4 Spoofing in IPv4

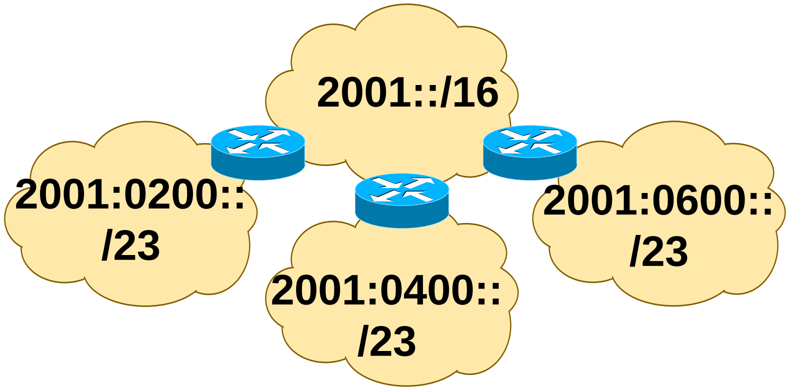
- **L4 spoofing can be done in concert with L3 spoofing to attack systems (most commonly running UDP, i.e. SNMP, Syslog, etc.)**
- **Nearly 50% of the current IPv4 space has not been allocated or is reserved for special use (RFC3330) making it easy to block at network ingress through bogons filtering**

L3-L4 Spoofing in IPv6

IPv6 Address Are Globally Aggregated

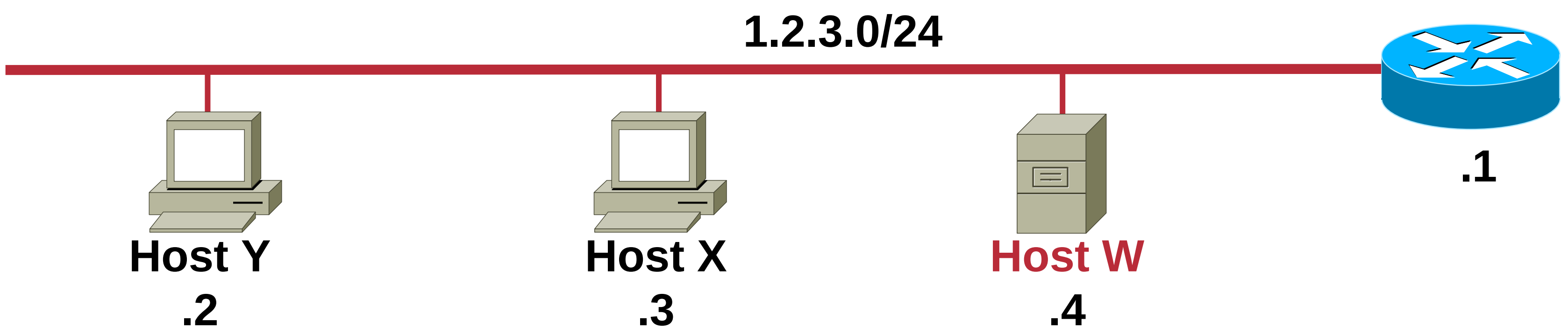
- ==> spoof mitigation at aggregation points easy to deploy
- 2001::/16—IPv6 Production
- 2002::/16—6to4 Tunneling
- 2003::/16—RIPE
- 3FFE::/16—6Bone Testing
- Unfortunately each subnet (even at the local level) still has a huge range of addresses to spoof

And now in 2006
2600::/12—ARIN (US DoD)
2A00::/16—RIPE
2400::/16—APNIC



ARP and DHCP Attacks in IPv4

- **With ARP misuse host W can claim to be the default gateway and hosts X and Y will route traffic through him; => man in the middle attack**



- **With DHCP it is similar except the attacker just needs to put a DHCP server on the wire delivering false information (gateways, DNS servers, etc.)**

Neighbor Discovery Attacks in IPv6 RFC 3756

- **Redirect attacks**

  A malicious node redirects packets away from a legitimate receiver to another node on the link

- **Denial-of-service attacks**

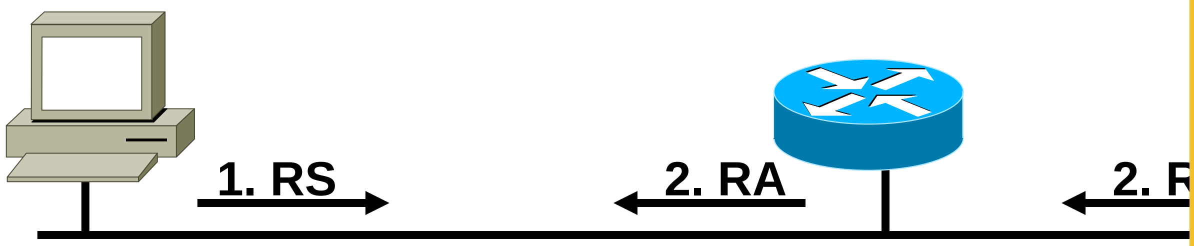
  A malicious node prevents communication between the node under attack and other nodes

- **Flooding denial-of-service attacks**

  A malicious node redirects other hosts' traffic to a victim node creating a flood of bogus traffic at the victim host

Stateless Autoconfiguration

Router Solicitation Are Sent By Booting Nodes to Request Router Advertisements for Configuring the Interfaces



ICMP w/o any authentication Gives Exactly Same Level of Security as ARP For IPv4 (None) Bootstrap Security Problem Just Like IPv4

1. **RS:**

   ICMP Type = 133

   Src = ::

   Dst = All-Routers multicast Address

   query= please send RA

2. **RA:**

   ICMP Type = 134

   Src = Router Link-local Address

   Dst = All-nodes multicast address

   Data= options, prefix, lifetime, autoconfig flag

Neighbor Discovery: Neighbor Solicitation

Security Mechanisms Built into Discovery Protocol = None
Another Bootstrap Security Problem

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

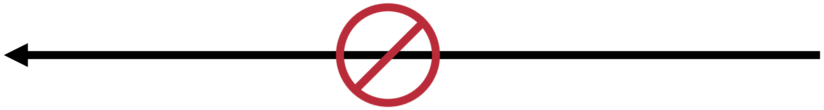
ICMP type = 136
Src = B
Dst = A
Data = link-layer address of B

A and B Can Now Exchange Packets on This Link

DAD (Duplicate Address Detection)

Duplicate Address Detection (DAD) Uses Neighbor Solicitation to Verify the Existence of an Address to be Configured

ICMP type = 135
Src = 0 (::)
Dst = Solicited-node multicast of A
Data = link-layer address of A
Query = what is your link address?

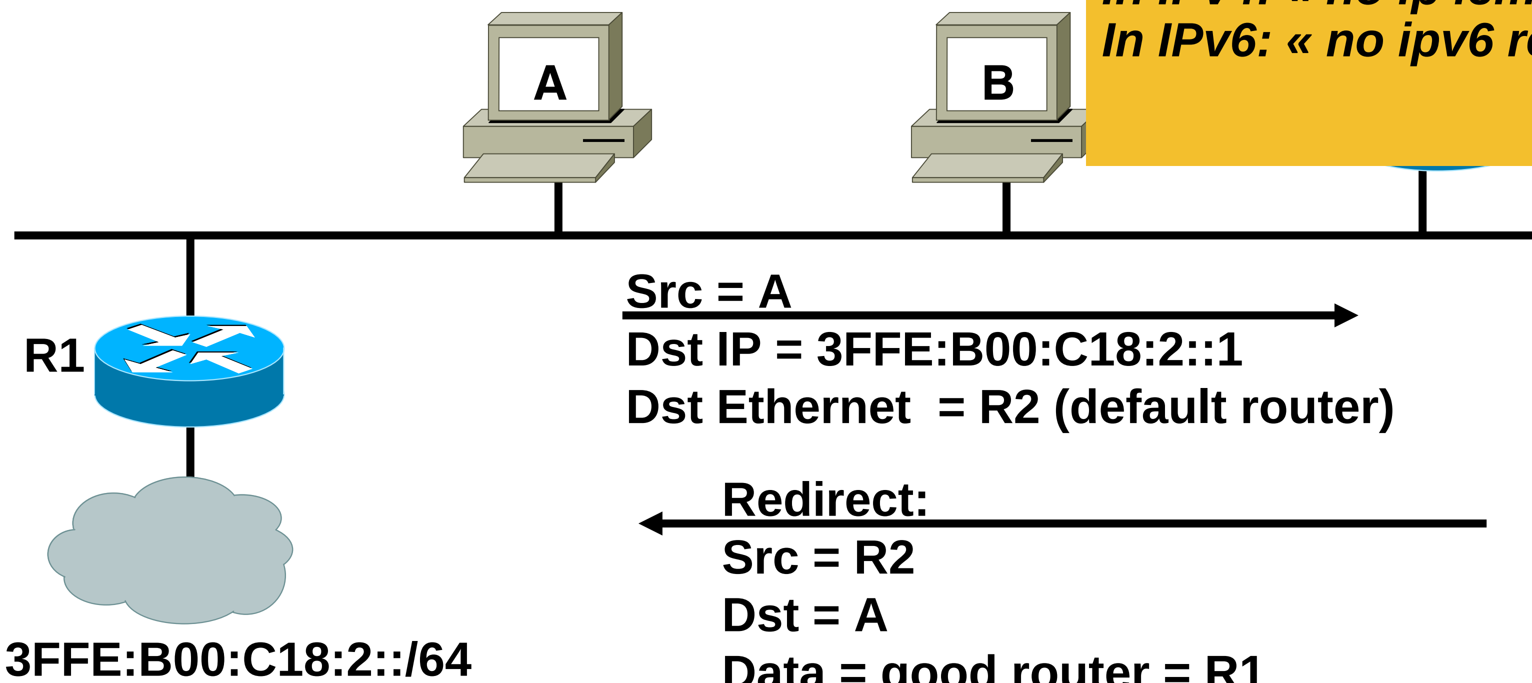


From RFC 2462:
« If a Duplicate @ Is Discovered… the Address Cannot Be Assigned to the Interface»
⇔ What If: Use MAC@ of the Node You Want to Dos and Fabricate Its IPv6 @

Neighbor Discovery: Spoofed Redirect

Redirect is Used by a Router to Signal the Re-Route of a Packet to a Better Router

In IPv4: « no ip icmp redirect »
In IPv6: « no ipv6 redirect »



Secure Neighbor Discovery (SEND) RFC 3971

- **Certification paths**

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

- **Cryptographically Generated Addresses (CGA)**

  IPv6 addresses whose the interface identifier is cryptographically generated

- **RSA signature option**

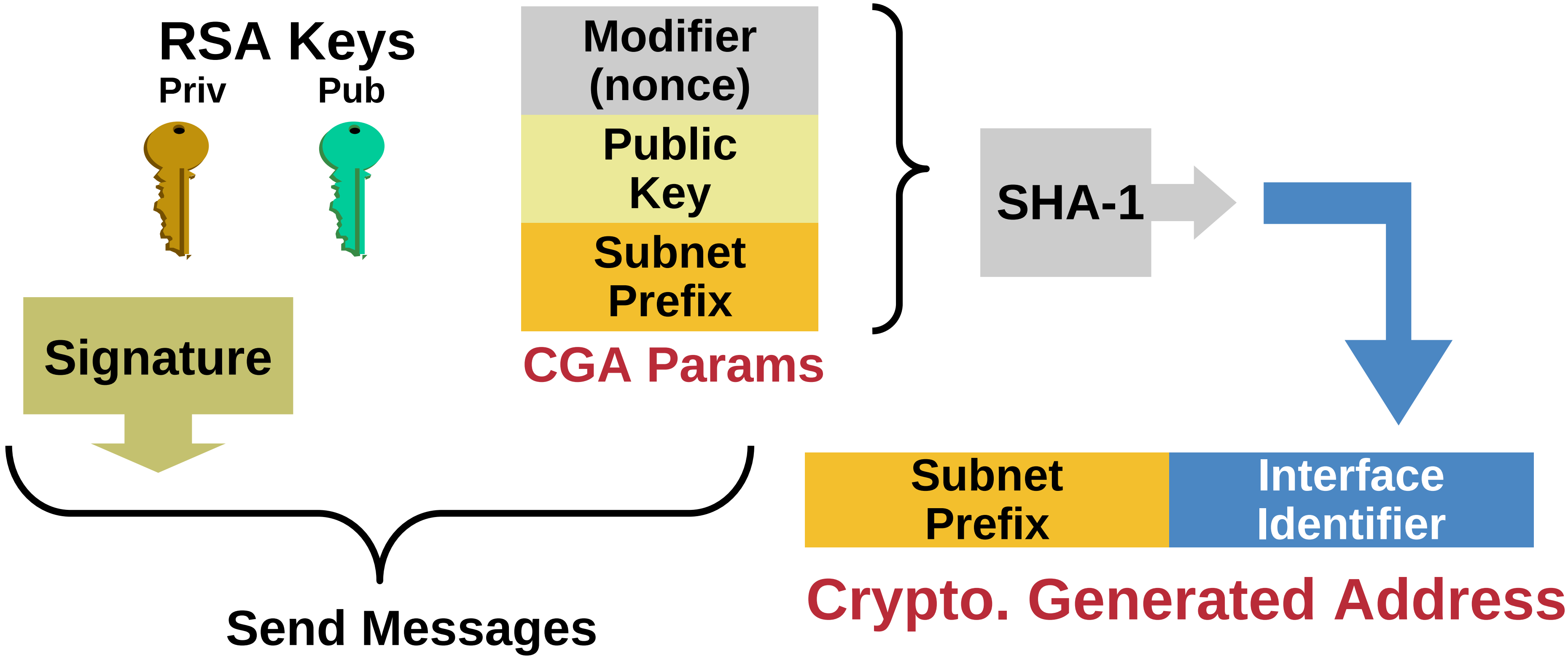
  Protect all all messages relating to neighbor and router discovery

- **Timestamp and nonce ND options**

  Prevent replay attacks

Cryptographically Generated Addresses CGA RFC 3972 (Simplified)

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



Secure Neighbor Discovery and CGA Caveats

- **Private/public key pair on all devices for CGA**
- **Overhead introduced**

  Routers have to do many public/private key calculation (some may be done in advance of use)
- **Available: Linux**
- **Coming in Microsoft Vista SP1**
- **Future implementation: Cisco IOS**

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 network (same threat as IPv4)**
  - **Rogue DHCPv6 servers on the site local multicast address (FF05::1:3) (new threat in IPv6)**
- **Tampering of communication between DHCPv6 relays and servers**

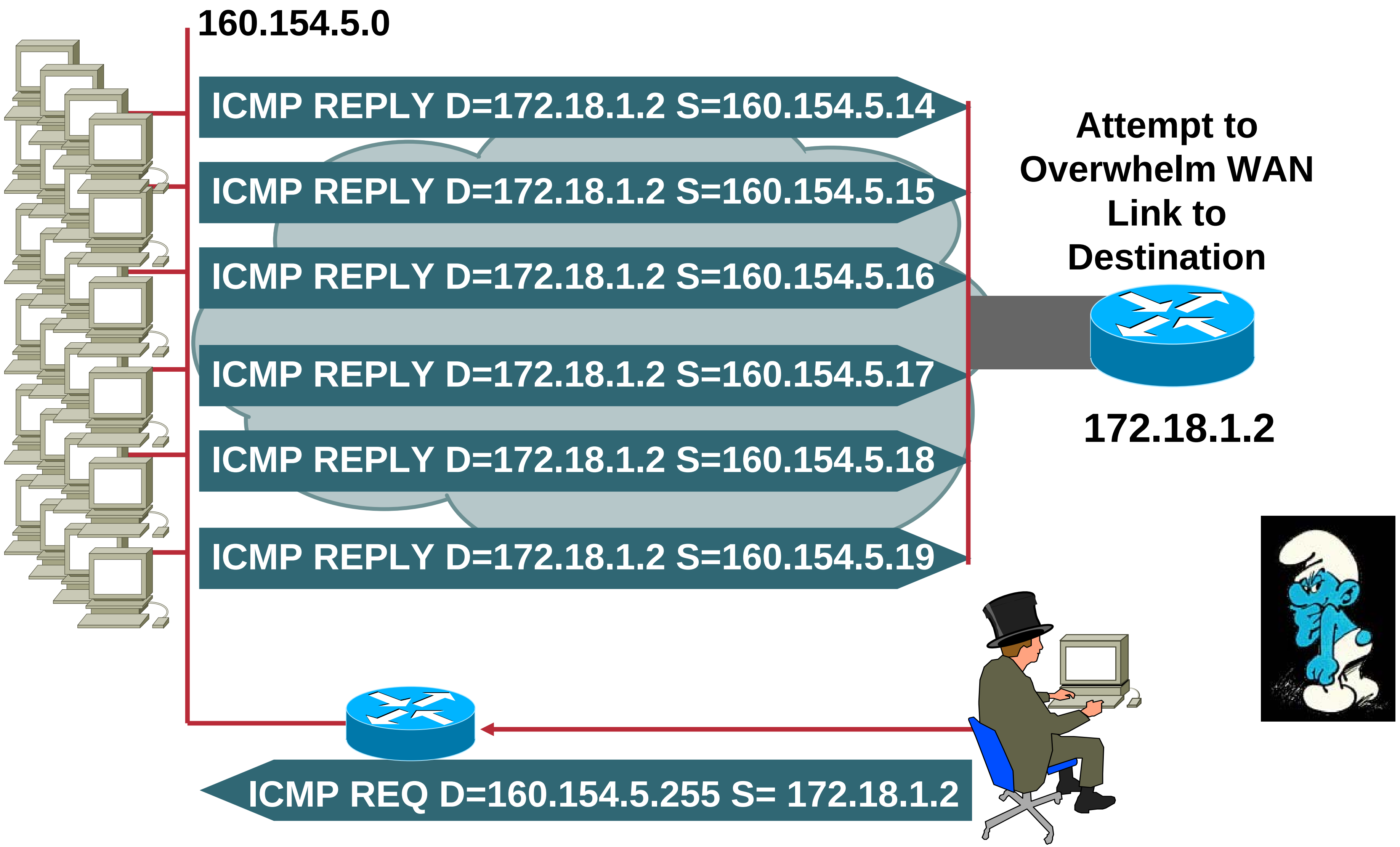
DHCPv6 Threat Mitigation

- **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.

- **For paranoid: protect the relay to server communications with IPsec (similar to IPv4)**

IPv4 Broadcast Amplification: Smurf



IPv6 and Broadcasts

- **There are no broadcast addresses in IPv6**
- **Broadcast address functionality is replaced with the appropriate link local multicast address**

    Link Local All Nodes Multicast—FF02::1

    Link Local All Routers Multicast—FF02::2

IPv6 and Other Amplification Vectors

- **Specific mention is made in ICMPv6 RFC that no ICMP error message should be generated in response to a packet with a multicast destination address**
- **The exceptions are the packet too big message and the parameter problem ICMP messages**
- **RFC 2463 Section 2.4 (e.2)**

Implement Ingress Filtering of Packets With
IPv6 Multicast Source Addresses
IPv6 Mcast Dest Address and Above ICMP Packet Types

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**
- **RIPng also relies on IPsec**
- **IPv6 routing attack best practices**
  - **Use traditional authentication mechanisms on BGP and IS-IS**
  - **Use IPsec to secure protocols such as OSPFv3 and RIPng**

Viruses and Worms in IPv6

- Pure viruses don't change in IPv6 but hybrid and pure worms do
  - Hybrids and pure worms today rely in Internet scanning to infect other hosts, this isn't feasible as shown earlier in this presentation
  - At one million packets per second on a IPv6 subnet with 10,000 hosts it would take over 28 years to find the first host to infect
- Worm developers will adapt to IPv6 but pure random scanning worms will be much more problematic for the attacker; best practices around worm detection and mitigation from IPv4 remain

IPv6 Attacks with Strong IPv4 Similarities

- **Sniffing**

  Without IPsec, IPv6 is no more or less likely to fall victim to a sniffing attack than IPv4

- **Application layer attacks**

  Even with IPsec, 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 IPsec, any attacks utilizing MITM will have the same likelihood in IPv6 as in IPv4

- **Flooding**

  Flooding attacks are identical between IPv4 and IPv6

By the Way: It Is Real ☹ IPv6 Hacking Tools

Let the Games Begin

- **Sniffers/packet capture**
  - Snort
  - TCPdump
  - Sun Solaris snoop
  - COLD
  - Ethereal
  - Analyzer
  - Windump
  - WinPcap
  - NetPeek
  - Sniffer Pro
- **Worms**
  - Slapper
- **Advisories/field notices**
  - http://www.cisco.com/warp/public/707/cisco-sa-20050126-ipv6.shtml
  - http://www.kb.cert.org/vuls/id/658859
- **Scanners**
  - IPv6 security scanner
  - Halfscan6
  - Nmap
  - Strobe
  - Netcat
- **DoS Tools**
  - 6tunneldos
  - 4to6ddos
  - Imps6-tools
- **Packet forgers**
  - SendIP
  - Packit
  - Spak6
- **Complete tool**
  - http://www.thc.org/thc-ipv6/

IPv6 Security Best Practice

Wrap Up: Candidate Best Practices

- Implement privacy extensions carefully
- Filter internal-use IPv6 addresses at the enterprise border routers
- Filter unneeded services at the firewall
- Selectively filter ICMP
- Maintain host and application security
- Determine what extension headers will be allowed through the access control device
- Determine which ICMPv6 messages are required
- Deny IPv6 fragments destined to an internetworking device when possible
- Ensure adequate IPv6 fragmentation filtering capabilities
- Drop all fragments with less than 1280 octets (except the last one)

Wrap Up: Candidate Best Practices (Cont.)

- Implement RFC 2827-like filtering and encourage your ISP to do the same
- Document procedures for last-hop traceback
- Use cryptographic protections where critical
- Use static neighbor entries for critical systems
- Implement ingress filtering of packets with IPv6 multicast source addresses
- Use traditional authentication mechanisms on BGP and IS-IS
- Use IPsec to secure protocols such as OSPFv3 and RIPng
- Use IPv6 hop limits to protect network devices
- Use static tunneling rather than dynamic tunneling
- Implement outbound filtering on firewall devices to allow only authorized tunneling endpoints

Specific IPv6 Issues

IPv6 Transition Mechanism Challenges

- **16+ methods, possibly in combination**
  - IP spoofing
- **Dual stack**
  - Consider security for both protocols
  - Cross v4/v6 abuse
  - Resiliency (shared resources)
- **Tunnels**
  - Bypass firewalls (protocol 41)

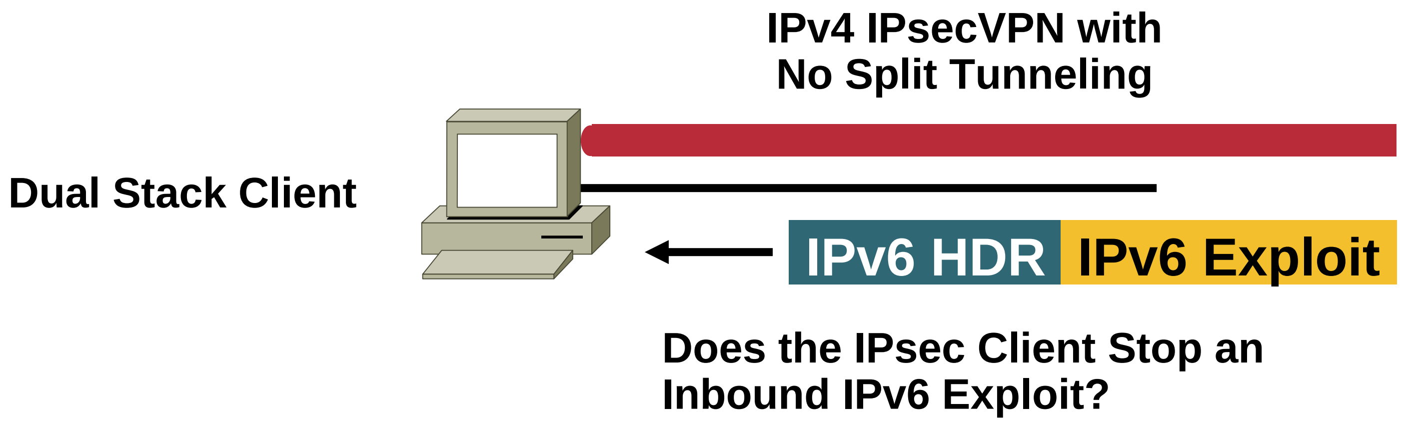
IPv6 Dual Stack Host Considerations

- **Host security on a dual-stack device**

  Applications can be subject to attack on both IPv6 and IPv4

- **Host security controls should block and inspect traffic from both IP versions**

  Host intrusion prevention, personal firewalls, VPN clients, etc.



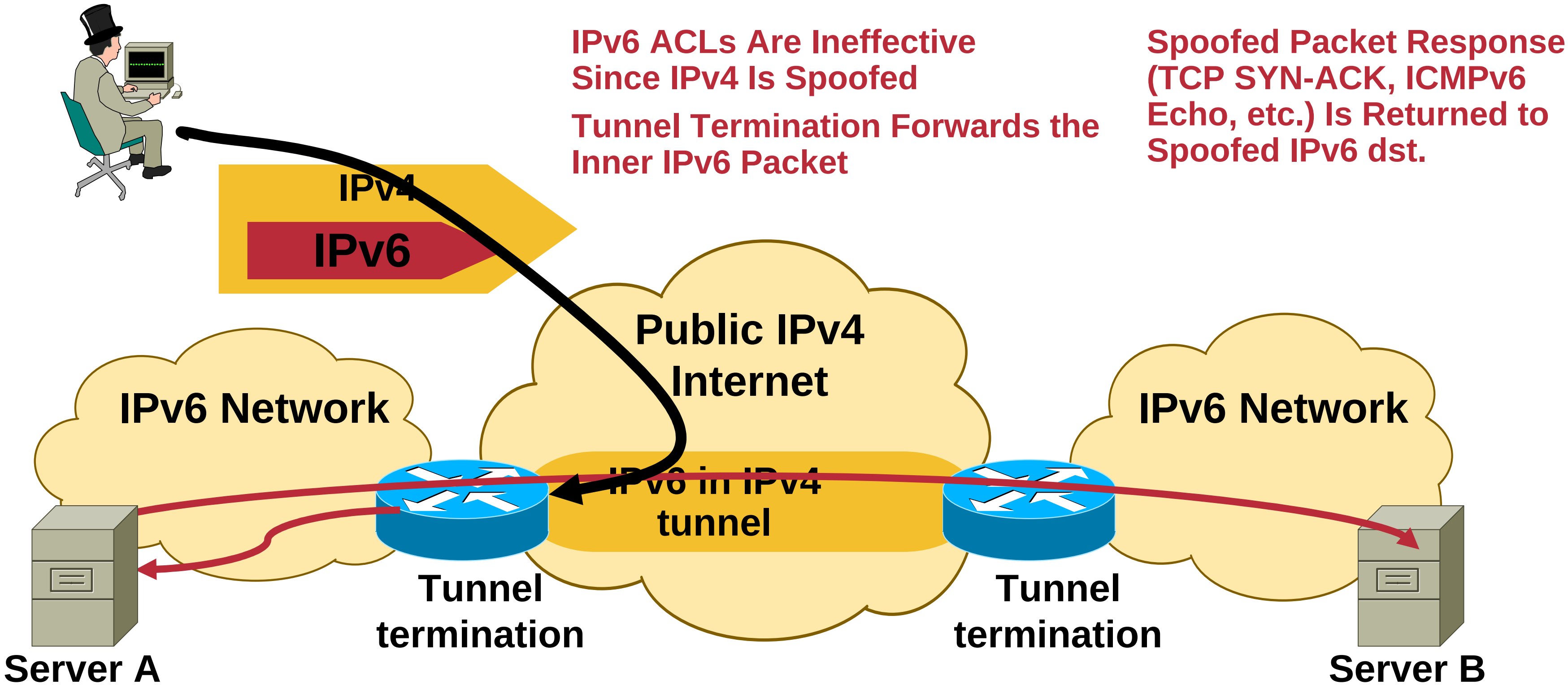
IPv6 Tunneling Summary

- 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
- ISATAP tunnel
- MobileIPv6 (uses RFC2473)
- Teredo tunnels

- 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
- 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

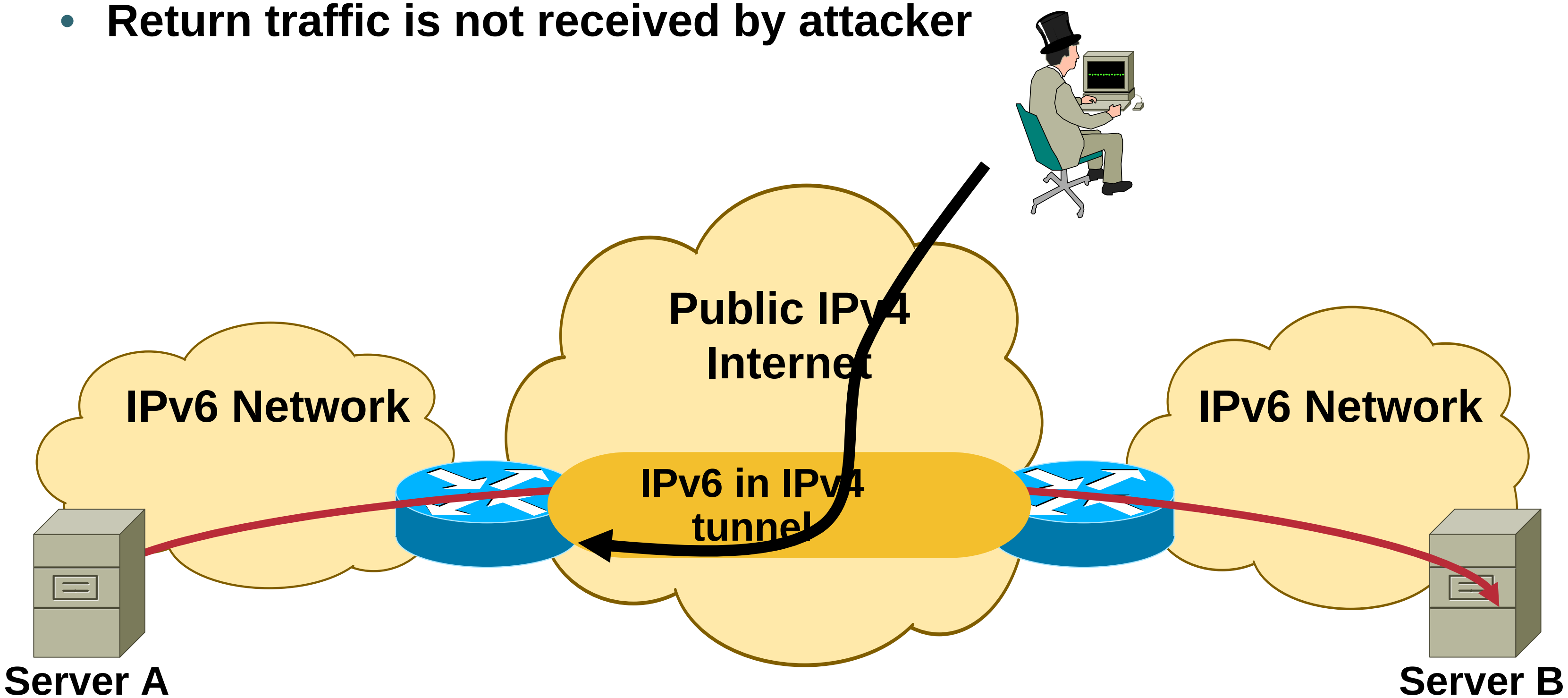
L3-L4 Spoofing in IPv6 When Using IPv6 over IPv4 Tunnels

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



L3-L4 Spoofing in IPv6 Via Tunnels

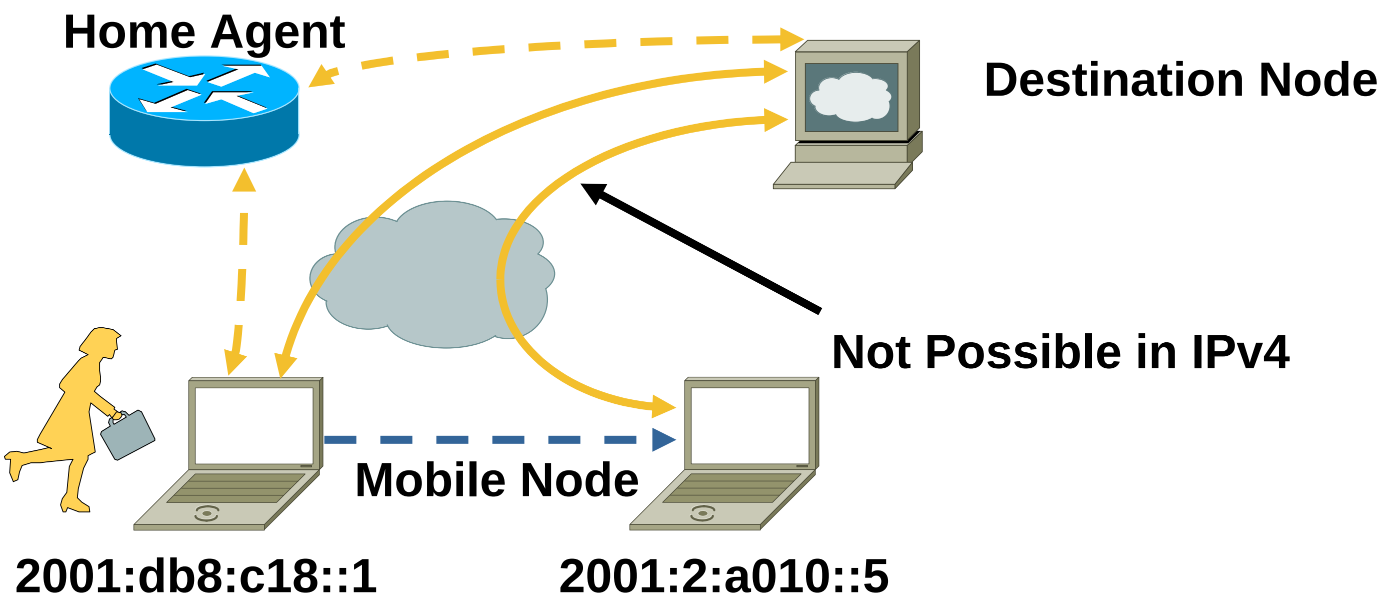
- Harm is limited
- 1:1 ratio of packets—no amplification attack
- There is a chokepoint against DoS
- Return traffic is not received by attacker



Transition Threats

- **ISATAP threats**
  - Unauthorized tunnels—firewall bypass (protocol 41)
  - ISATAP looks like a Layer 2 network to ALL ISATAP hosts in the enterprise
  - This has implications on network segmentation and network discovery
  - No authentication in ISATAP—rogue routers are possible
  - Host security needs IPv6 support
- **Teredo threats—IPv6 over UDP (port 3544)**
  - Unauthorized tunnels—firewall bypass
  - Rogue relays/servers can be used for DoS; a possible for client to server communications
  - Host security needs IPv6 support

IP Mobility



Mobility Means:

- Mobile devices are fully supported while moving
- Built-in on IPv6
    - Any node can use it
- Efficient routing means performance for end-users
- Filtering challenges

Mobile IPv6 Security Features Overview

- **Protection of binding updates both to home agents and correspondent nodes**

  IPsec,

  Or binding authorization data option through the return routability procedure

- **Protection of mobile prefix discovery**

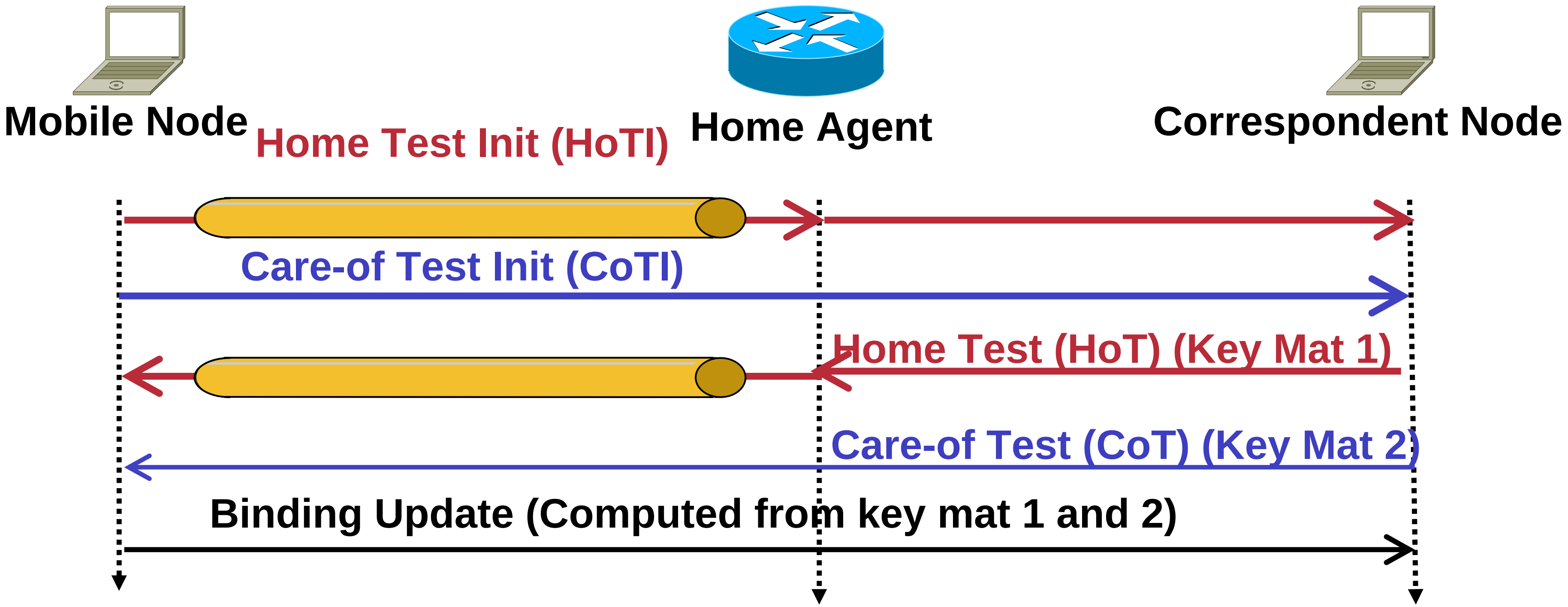
  Through the use of IPsec extension headers

- **Protection of data packets transport**

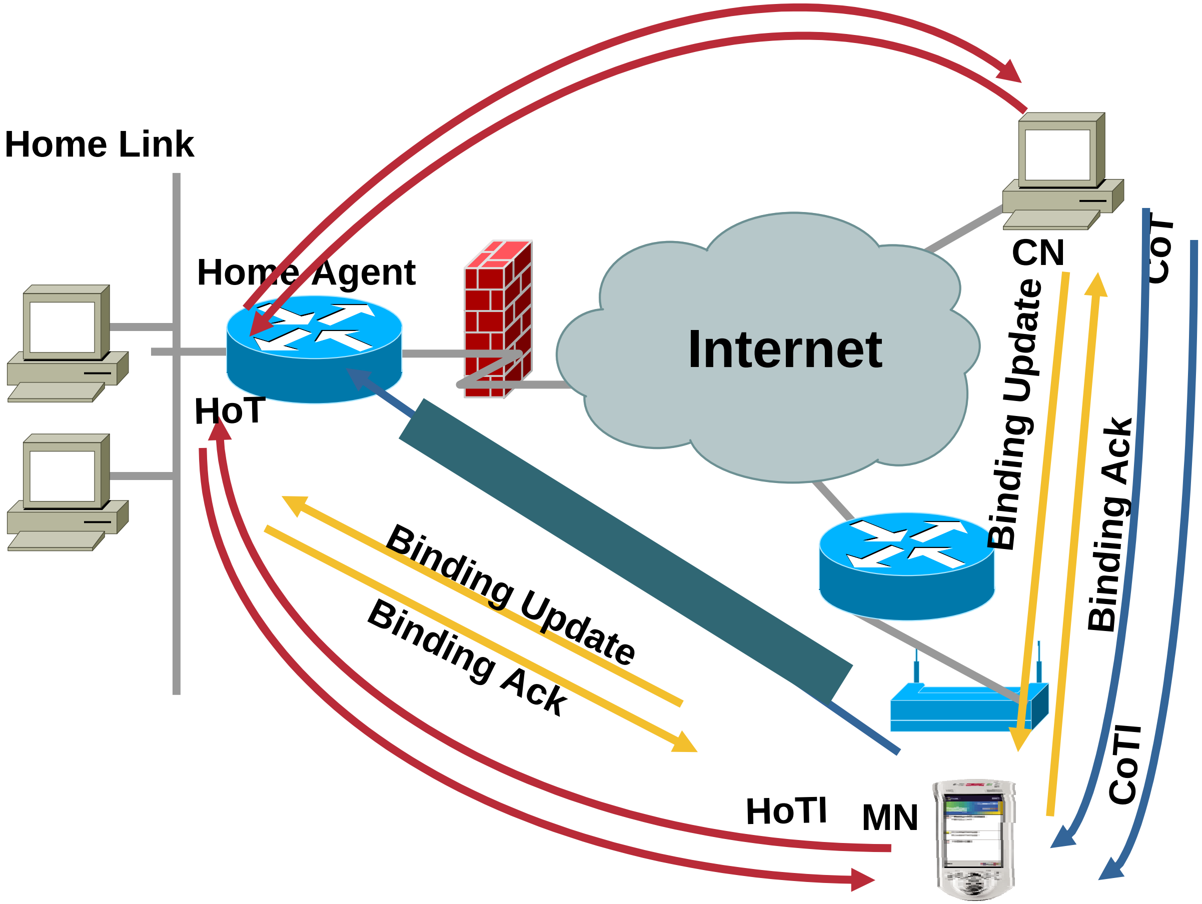
  Home address destination option and type two routing header specified in a manner which restricts their use in attacks

Mobile IPv6 Security
Return Routability Test

- Provides reasonable assurance that the MN is addressable at its claimed CoA and at its HoA
- Test whether packets addressed to the two claimed addresses are routed back to the MN



Mobile IPv6 Global Picture

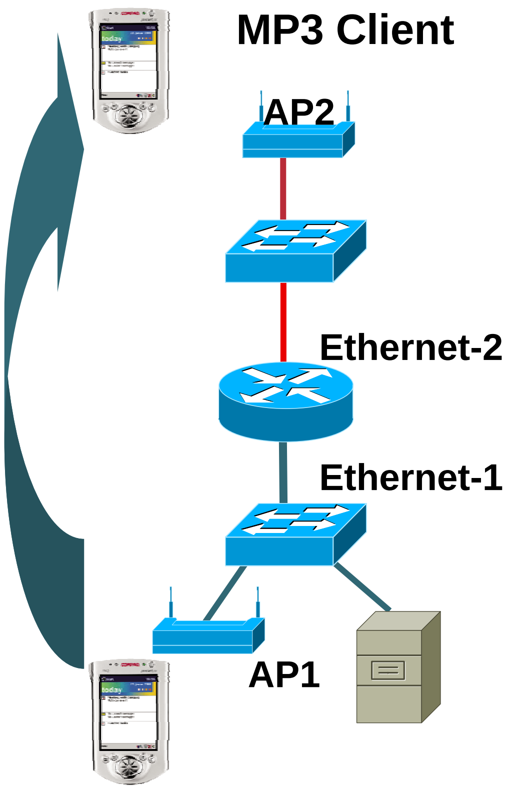


- **Correspondent Node**
  - Arbitrary: No Preexisting Security Association
- **Return Routability Test**
  - Verifies the collocation of the CoA and the home address
  - Assumes better security association between HA and MN
  - Scalable and stateless
- **Reverse Tunnel**
  - Secured by IPsec
  - Requires a preexisting Security Association

MIPv6 Security Protections

- BU/BA to HA must be secured through IPsec
- MN and HA should use an IPsec SA to protect the integrity and authenticity of the mobile prefix solicitations and advertisements
- Payload packets exchanged with MN can be follow the same protection policy as other IPv6 hosts
- Specific security measures are defined to protect the specificity of MIPv6
  - Home address destination option
  - Type 2 Routing header
  - Tunnelling headers

Mobile IPv6 ACL



Router# (config-if) ipv6 mobile home-agent access <acl>

- Binding update filter: all received binding updates are filtered
- This feature may be used to deny home agent services to mobile nodes that have roamed to particular sub-networks

  When the filter blocks a binding update, a binding acknowledgement is returned with error status “administratively prohibited"

Enforcing a Security Policy

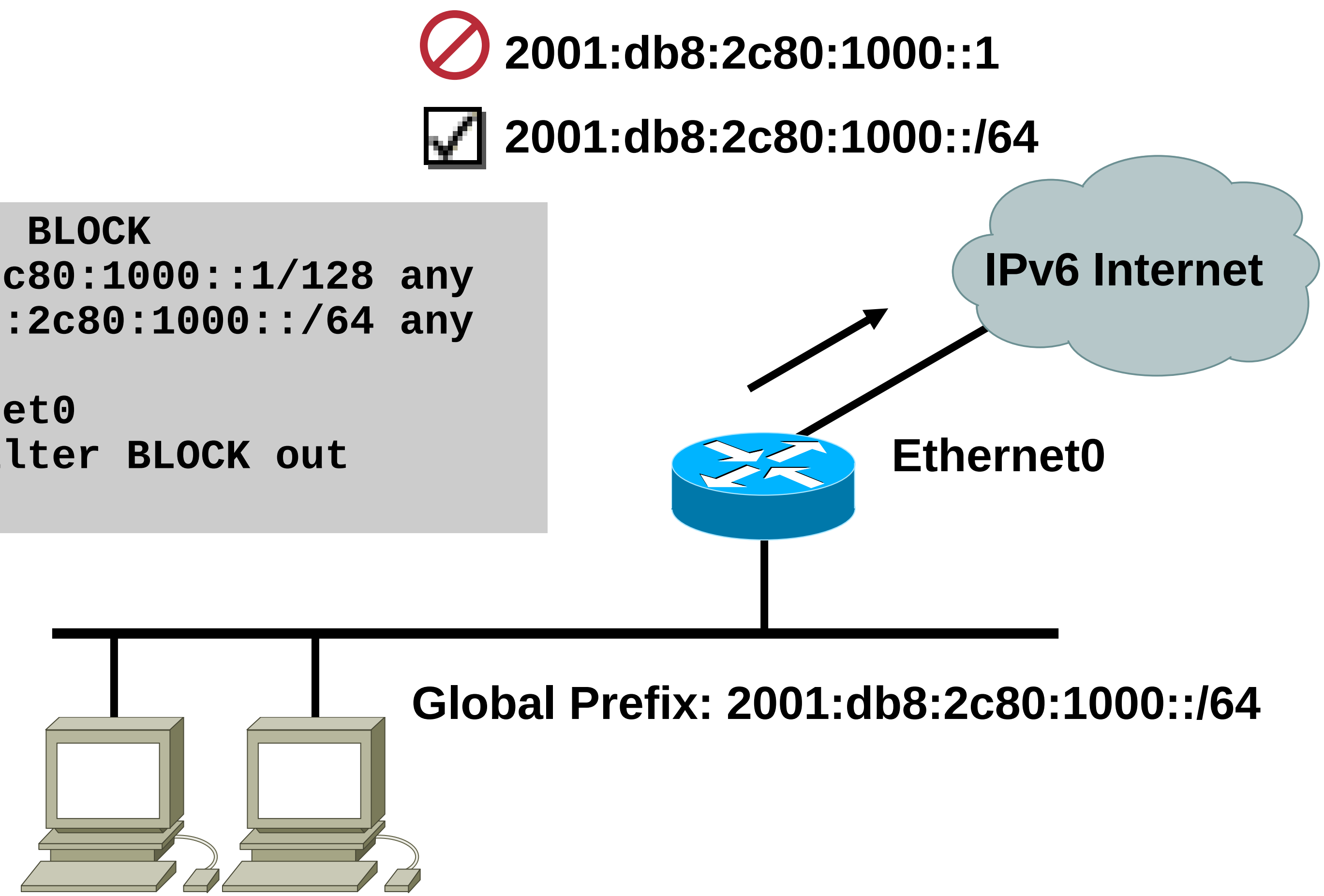
Cisco IOS IPv6 Access Control Lists

- Can filter traffic based on source and destination address
- Can filter traffic inbound or outbound to a specific interface
- Implicit "deny all" at the end of access list
- Very much like in IPv4

Cisco IOS IPv6 Access Control Lists

Filtering Outgoing Traffic from One Specific Source Address

```
ipv6 access-list BLOCK
 deny 2001:db8:2c80:1000::1/128 any
 permit 2001:db8:2c80:1000::/64 any

interface Ethernet0
 ipv6 traffic-filter BLOCK out
```



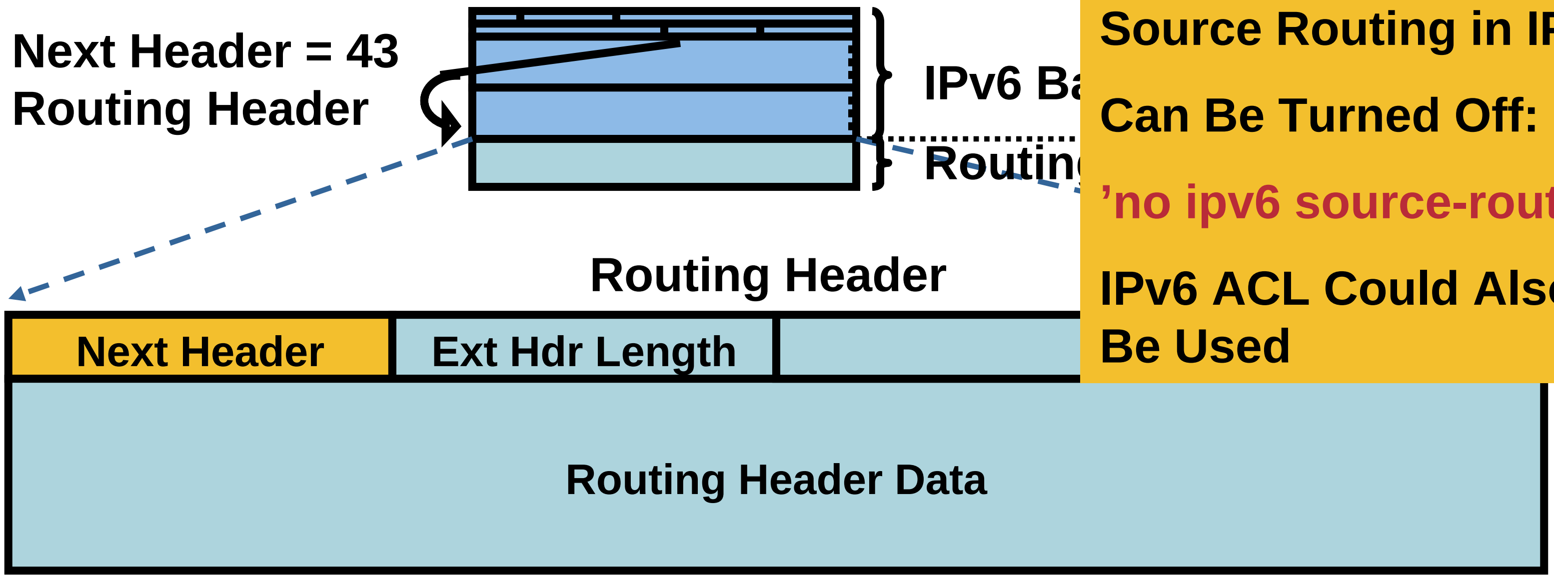
Filtering Extension Headers

- **IPv6 headers and optional extensions need to be scanned to access the upper layer protocols (UPL)**
- **May require searching through several extensions headers**
- **Important: a router must be able to filter both option header and L4 at the same time**

IPv6 Routing Header

Routing Header Is:

- **An extension header**
- **Processed by the listed intermediate routers**



Routing Header IPv6 ⇔ Source Routing in IPv4

Can Be Turned Off:

'no ipv6 source-route'

IPv6 ACL Could Also Be Used

Issues with Routing Header

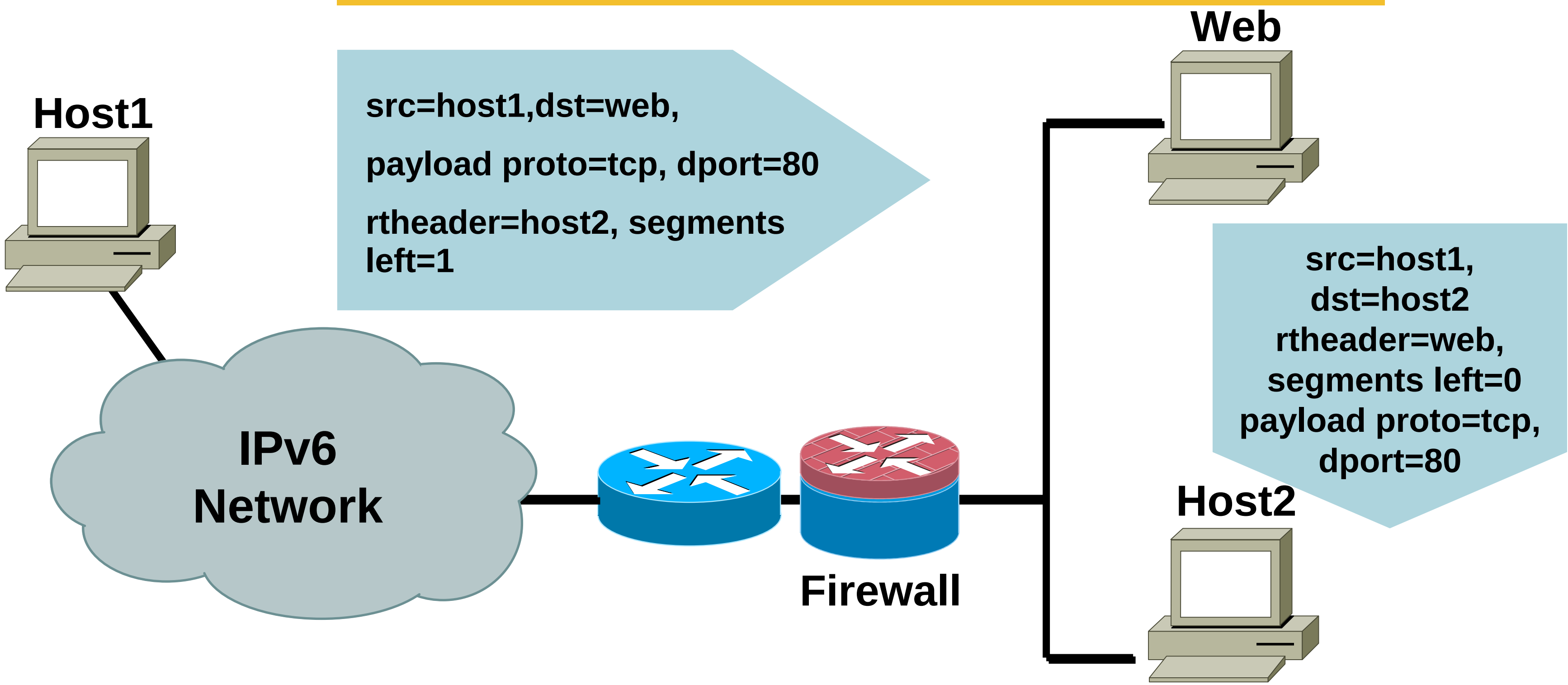
- **Could be used as a rebound/relay to the victim**
- **Because destination address is replaced at every routing header processing point, it's difficult to perform traffic filtering based on destination addresses**
- **http://www.ietf.org/internet-drafts/draft-savola-ipv6-rh-ha-security-03.txt**

Routing Header: Traffic Reflector

Rule on the Firewall

Allow proto tcp from any to webserver port 80

Deny proto tcp from any to any



IPv6 Extended Access Control Lists

- Upper layers : ICMP, TCP, UDP, SCTP, any value
- ICMPv6 code and type
- TCP SYN, ACK, FIN, PUSH, URG, RST
- L4 port numbers
- Traffic class (only six bits/8) = DSCP
- Flow label (0-0xFFFFF)
- IPv6 header options
    - Fragments
    - Routing header type
    - Destination header type

IPv6 ACL Implicit Rules

Implicit Permit for Enable Neighbor Discovery

- The following implicit rules exist at the end of each IPv6 ACL to allow ICMPv6 neighbor discovery:

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

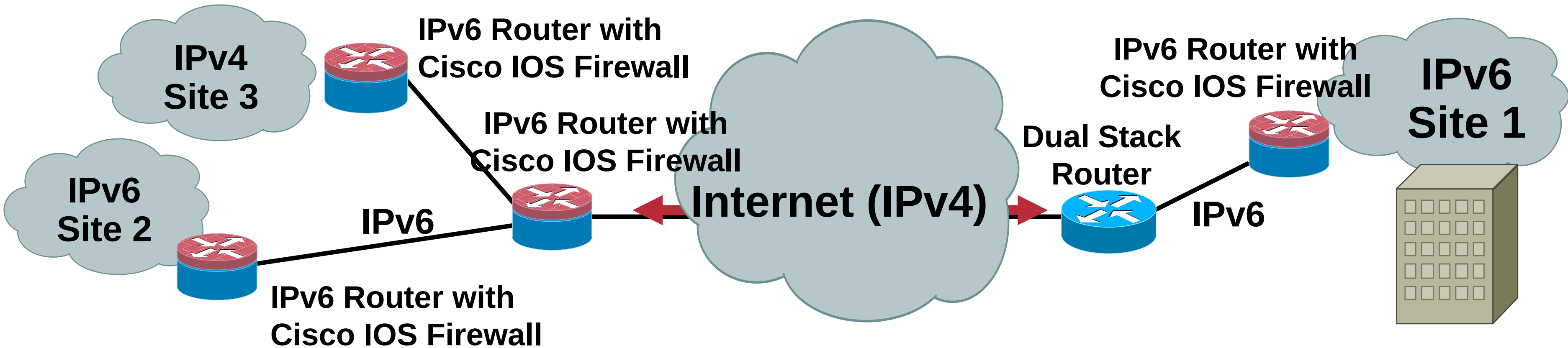
- Be careful when adding « `deny ipv6 any any log` » at the end

IPv6 ACL to Protect VTY

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


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

Cisco IOS Firewall IPv6 Support

- Stateful protocol inspection (anomaly detection) of IPv6 fragmented packets, TCP, UDP, ICMP and FTP traffic
- Stateful inspection and translation services of IPv4/IPv6 packets
- IPv6 DoS attack mitigation
- IPv4/v6 coexistence, no need for new hardware, just software
- Recognizes IPv6 extension header information such as routing header, hop-by-hop options header, fragment header, etc



Control Plane Policing for IPv6 Protecting the Router CPU

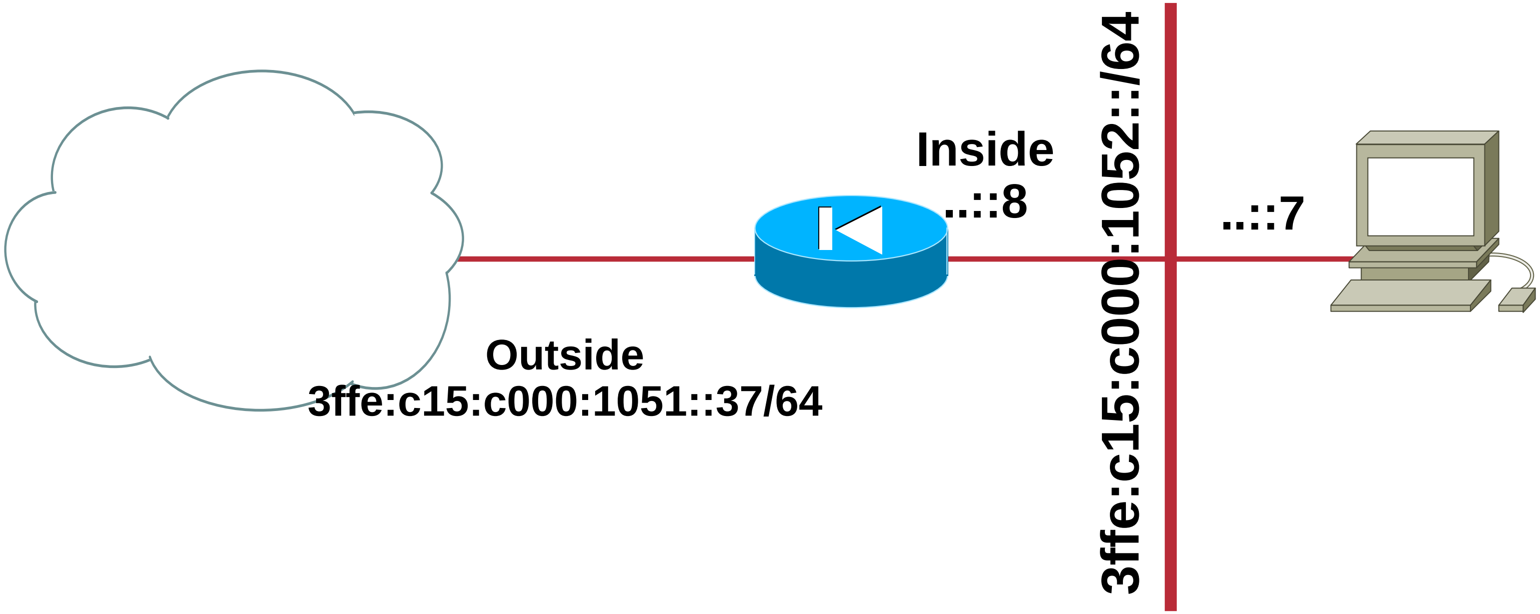
- **Against DoS with Neighbor Discovery,**
- **Can also throttle IPv6 traffic when processed in SW while IPv4 is in HW (legacy platform)**
- **In doubts:** `show proc cpu | include IPv6`

```
class-map match-all ipv6
 match protocol ipv6

policy-map CoPP
 class ipv6
  police rate 100 pps
    conform-action transmit
    exceed-action drop

control-plane
  service-policy input CoPP
```

ASA and PIX Firewall IPv6 Support

- **Recognition of IPv6 traffic**
  - Dual-stack, IPv6 only, IPv4 only
- **Extended IP ACL with stateful inspection**
- **Application awareness**
  - HTTP, FTP, telnet, SMTP, TCP, SSH, UDP
- **uRPF**
- **v6 Frag guard**
- **IPv6 header security checks**
- **Management access via IPv6**
  - Telnet, SSH, HTTPS

ASA: Sample IPv6 Topology



ASA and PIX 7.0: ACL Very Similar to Cisco IOS

For Your Reference

```
interface Ethernet0
 nameif outside
 ipv6 address 3ffe:c15:c000:1051::37/64
 ipv6 enable
interface Ethernet1
 nameif inside
 ipv6 address 3ffe:c15:c000:1052::1/64
 ipv6 enable

ipv6 unicast-routing

ipv6 route outside ::/0 3ffe:c15:c000:1051::1

ipv6 access-list SECURE permit tcp any host
3ffe:c15:c000:1052::7 eq telnet
ipv6 access-list SECURE permit icmp6 any
3ffe:c15:c000:1052::/64

access-group SECURE in interface outside
```

For Your Reference

ASA and PIX 7.0: Stateful Inspection

```
pixA# show conn
4 in use, 7 most used
ICMP out fe80::206:d7ff:fe80:2340:0 in
fe80::209:43ff:fea4:dd07:0 idle 0:00:00 bytes 16
UDP out 3ffe:c15:c000:1051::138:53 in
3ffe:c15:c000:1052::7:50118 idle 0:00:02 flags -
TCP out 2001:200:0:8002:203:47ff:fea5:3085:80 in
3ffe:c15:c000:1052::7:11009 idle 0:00:14 bytes 8975 flags
UfFRIO
TCP out 3ffe:c15:c000:1051::1:11008 in
3ffe:c15:c000:1052::7:23 idle 0:00:04 bytes 411 flags UIOB
```

“There is no reason anymore to let your site wide open for IPv6”

An IPv6 Site Admin
Previously Fully Opened In IPv6
and Restricted in IPv4

Enterprise Deployment: Secure IPv6

Secure IPv6 Traffic over IPv6 Public Network

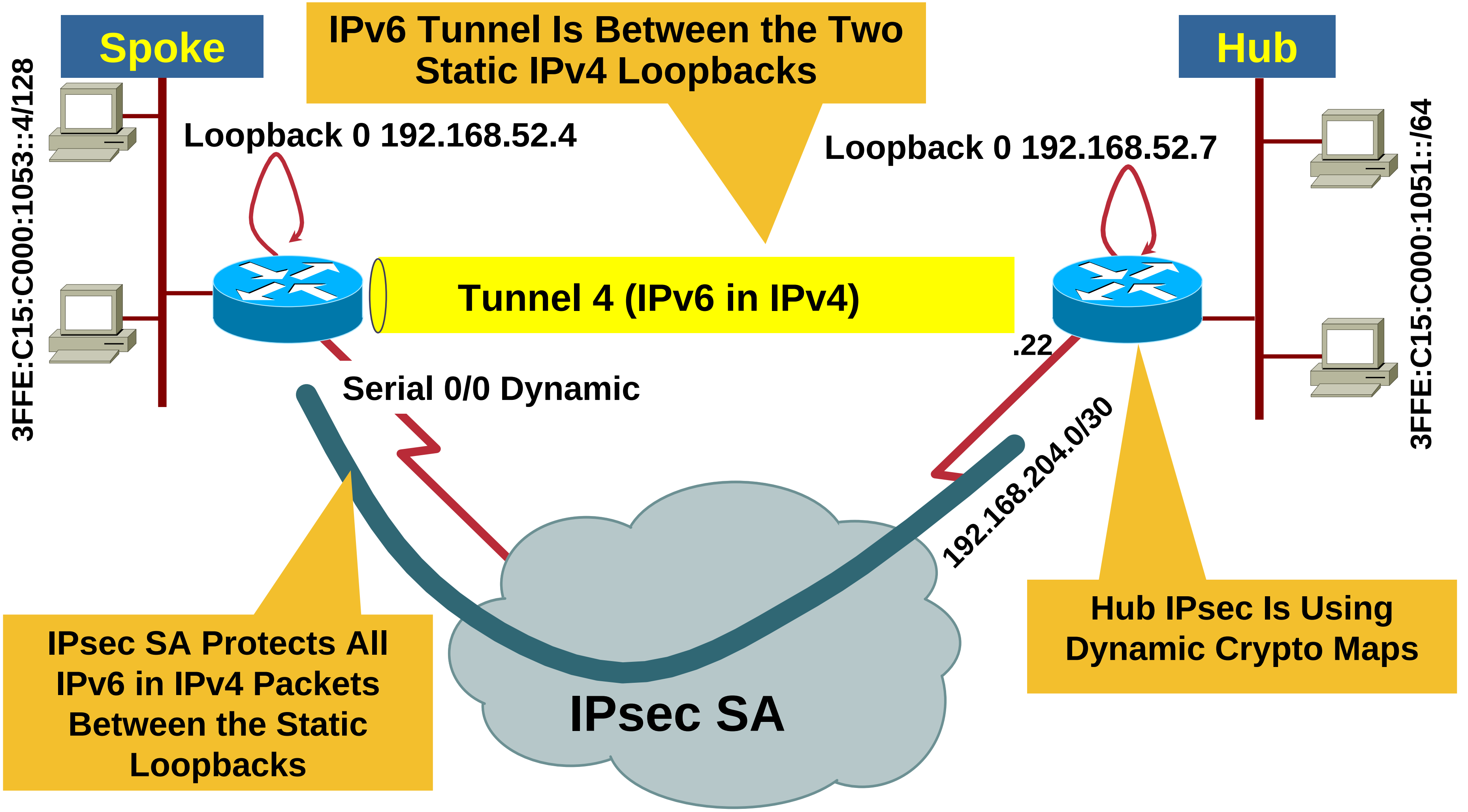
- **Since 12.4(6)T, IPsec also works for IPv6**
- **Using the Virtual Interface**

```
interface Tunnel0
 no ip address
 ipv6 address 2001:DB8::2811/64
 ipv6 enable
 tunnel source Serial0/0/1
 tunnel destination 2001:DB8:7::2
 tunnel mode ipsec ipv6
 tunnel protection ipsec profile ipv6
```

Secure IPv6 over IPv4 Public Internet

- **How can we transport IPv6 securely over IPv4 Internet?**
  - **No traffic sniffing**
  - **No traffic injection**
- **IPsec**
  - **Site to site: encrypting IPv6 tunnels**
  - **Remote access: encrypting ISATAP or IPv6 tunnels**

Secure Site to Site IPv6 Connectivity



Key Design Points

- Requires a fixed IPv4 address for hub
- IPv6-in-IPv4 tunnels are anchored on IPv4 loopbacks

    Tunnels requires static sources and destinations

- IPsec dynamic crypto maps are used

    Allows for dynamic spoke IPv4 addresses

    IPsec works on IPv4 packets (containing the IPv4 packets)

- Traffic initiated from spokes (hub is using dynamic crypto maps)

IPv6 for Remote Devices Solutions

- **Enabling IPv6 traffic inside the Cisco VPN Client tunnel**

  NAT and Firewall traversal support

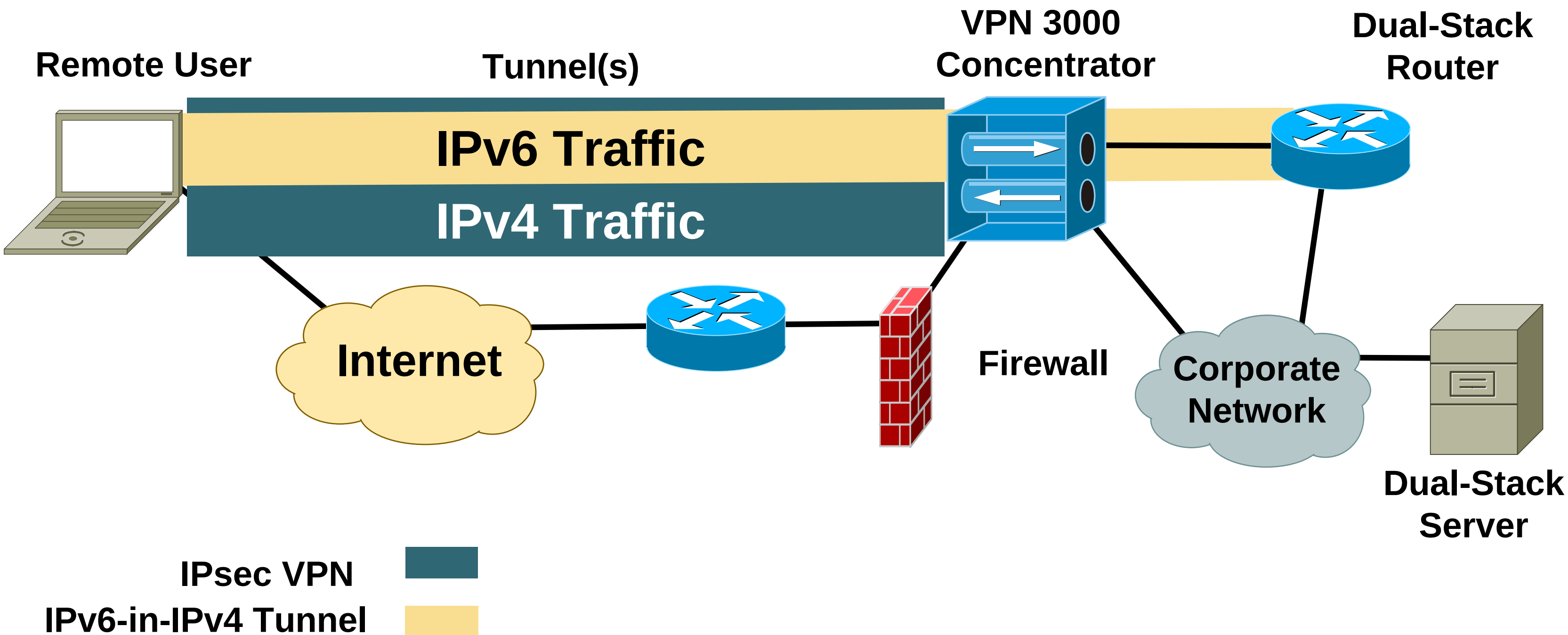
- **Allow remote host to establish a v6-in-v4 tunnel either automatically or manually**

  ISATAP—Intra Site Automatic Tunnel Addressing Protocol

  Configured—Static configuration for each side of tunnel

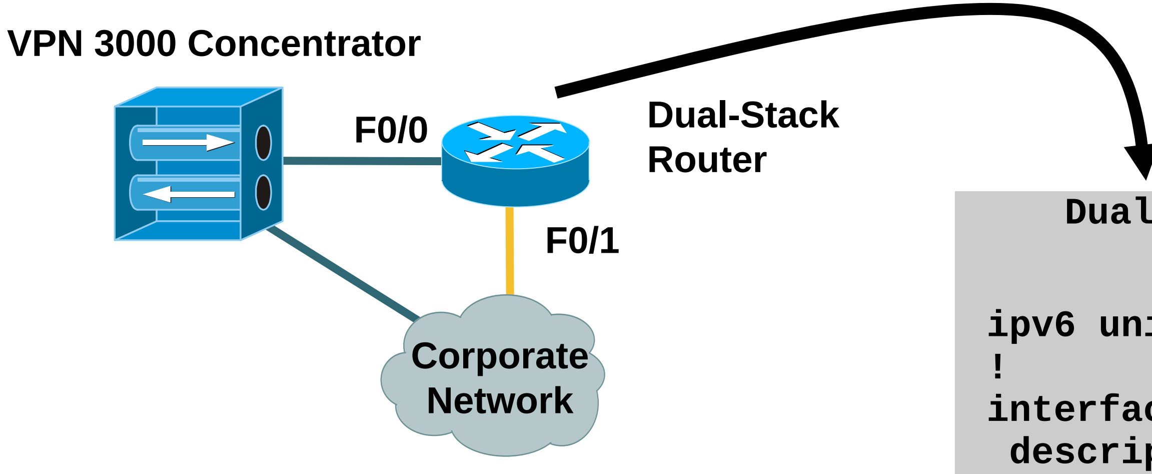
  Fixed IPv6 address enables server's side of any application to be configured on an IPv6 host that could roam over the world

IPv6-in-IPv6 Tunnel Example



Note: The VPN concentrator could be replaced with a VPN-enabled Cisco IOS Router or PIX™

Router Configuration: ISATAP



Dual-stack router configuration

```
ipv6 unicast-routing
!
interface FastEthernet0/0
 description TO VPN 3000
 ip address 20.1.1.1 255.255.255.0
!
interface FastEthernet0/1
 description TO Campus Network
 ipv6 address 3FFE:C15:C003:111C::2/64
!
interface Tunnel0
no ip address
 ipv6 address 3FFE:C15:C003:1101::/64
   eui-64
 no ipv6 nd suppress-ra
 tunnel source FastEthernet0/0
 tunnel mode ipv6ip isatap
```

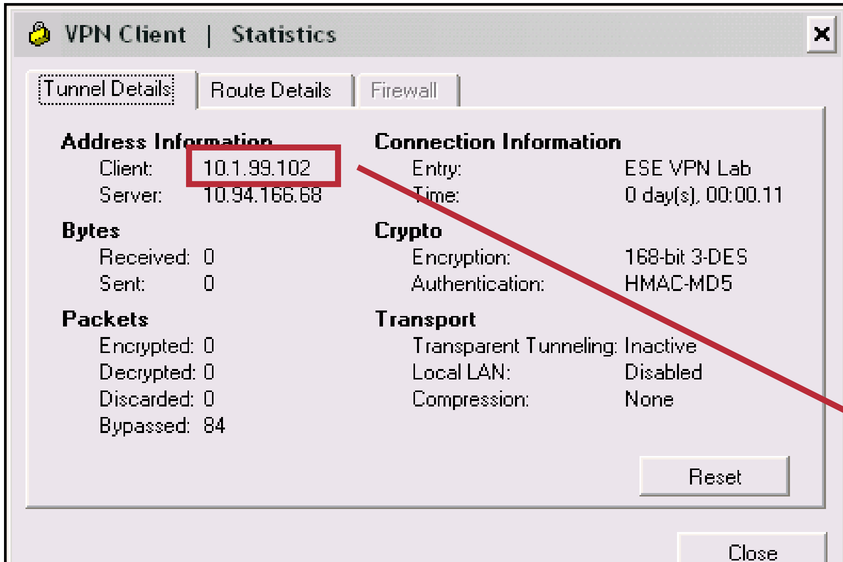
ISATAP Address Format:

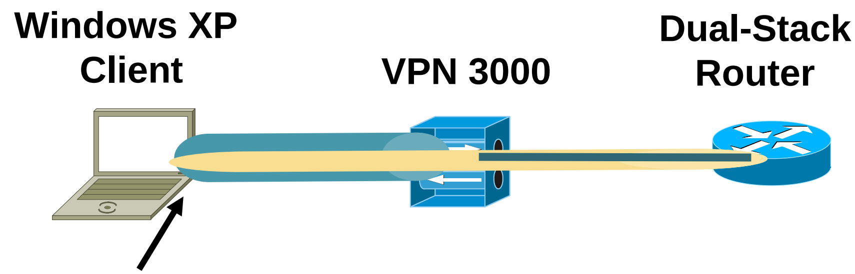
64-bit Unicast Prefix	0000:5EFE:	IPv4 Addr.
	32-bit	32-bit

Interface ID

3ffe:c15:c003:1101:0:5efe:20.1.1.1

Does It Work?





10.1.99.102 - VPN address

3ffe:c15:c003:1101:0:5efe:10.1.99.102 - IPv6 address

```
Interface 2: Automatic Tunneling Pseudo-Interface

Addr Type  DAD State  Valid Life   Pref. Life   Address
---------  ---------- ------------ ------------ -----------------------------
Public     Preferred   29d23h56m5s   6d23h56m5s 3ffe:c15:c003:1101:0:5efe:10.1.99.102
Link       Preferred      infinite     infinite fe80::5efe:10.1.99.102
```

```
netsh interface ipv6>show route
Querying active state...

Publish  Type       Met  Prefix                   Idx  Gateway/Interface Name
-------  --------  ----  ------------------------ ---  ---------------------
no       Autoconf     9  3ffe:c15:c003:1101::/64    2  Automatic Tunneling Pseudo-Interface
no       Manual       1  ::/0                       2  fe80::5efe:20.1.1.1
```

Conclusion

Summary Findings

- IPv6 makes some things better, other things worse, and most things are just different, but no more or less secure
  - Better
    - Automated scanning and worm propagation is harder due to huge subnets
  - Worse
    - Increased complexity in addressing and configuration
    - Lack of familiarity with IPv6 among operators
    - Vulnerabilities in transition techniques
- Most of the legacy issues with IPv4 security remain in IPv6
  - For example, ARP security issues in IPv4 are simply replaced with ND security issues in IPv6

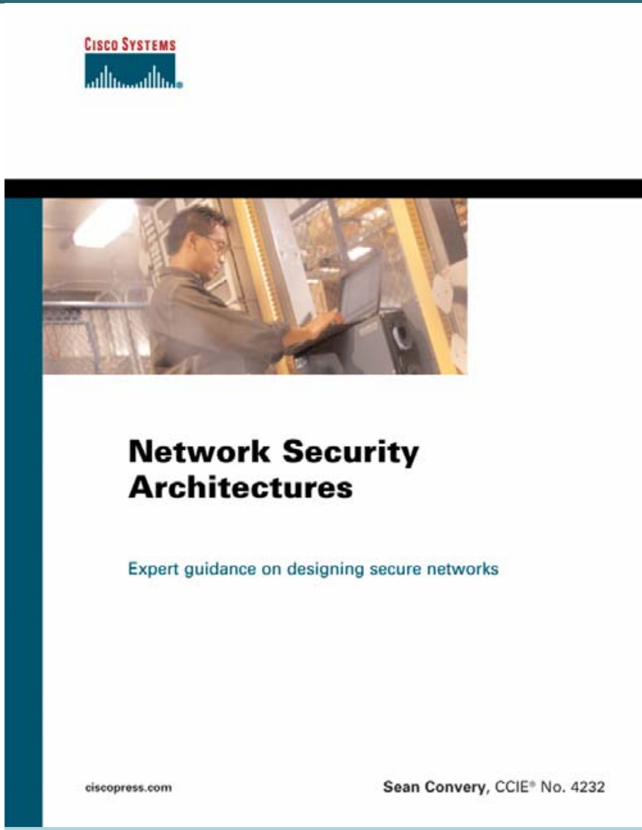
Key Take Away

- So, nothing really new in IPv6
- Security enforcement is possible
    - Control your IPv6 traffic as you do for IPv4
- Leverage IPsec to secure IPv6 when possible

Q and A

Recommended Reading

- **Continue your Networkers learning experience with further reading for this session from Cisco Press™**
- **Check the Recommended Reading flyer for suggested books**



Available Onsite at the Cisco Company Store

Complete Your Online Session Evaluation

- **Win fabulous prizes; Give us your feedback**
- **Receive ten Passport Points for each session evaluation you complete**
- **Go to the Internet stations located throughout the Convention Center to complete your session evaluation**
- **Drawings will be held in the World of Solutions**

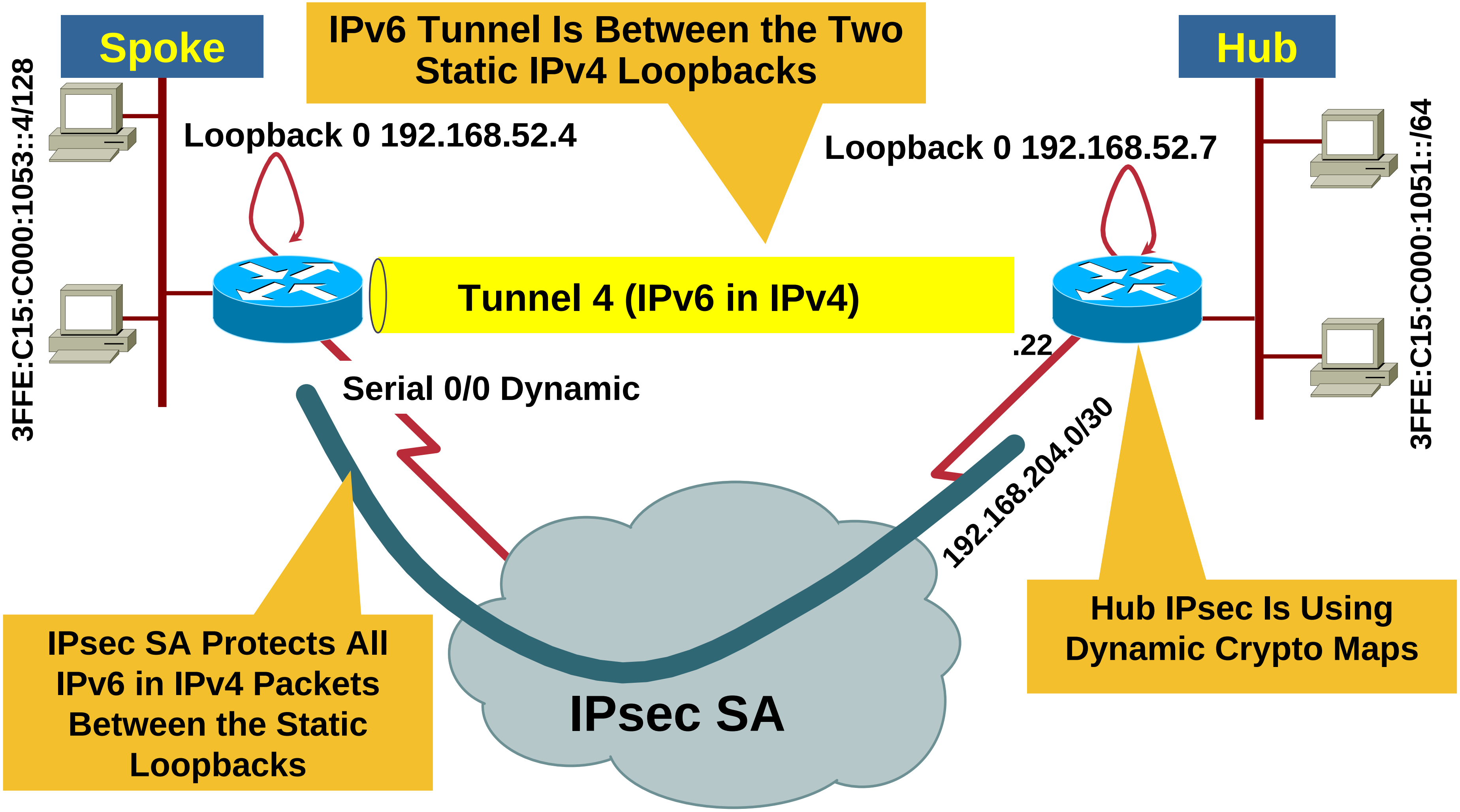
  Tuesday, June 20 at 12:15 p.m.

  Wednesday, June 21 at 12:15 p.m.

  Thursday, June 22 at 12:15 p.m. and 2:00 p.m.

Reference Slides

Secure Site to Site IPv6 Connectivity



For Your Reference

Spoke Configuration/1: IPv6 Tunnels

```
interface Loopback0
 ip address 192.168.52.4 255.255.255.255

interface Tunnel4
 no ip address
 ipv6 unnumbered FastEthernet0/0
 ipv6 enable
 tunnel source Loopback0
 tunnel destination 192.168.52.7
 tunnel mode ipv6ip
!
ip route 192.168.52.0 255.255.255.0 Serial0/0
```

Static IPv4 Addresses

For Your Reference

Spoke Configuration/2: IPv4 IPsec

```
crypto ipsec transform-set 3DES esp-3des
!
crypto map IPV6_SEC 10 ipsec-isakmp
 set peer 192.168.204.26
 set transform-set 3DES
 match address SELECTOR
!
interface Serial0/0
 crypto map IPV6_SEC
!
ip access-list extended SELECTOR
 permit 41 host 192.168.52.4 host 192.168.52.7
```

IPv4 Address of Hub

IPsec Traffic Selectors: Fixed IPv4 Loopback Addresses, i.e., Encapsulated IPv6 Traffic

For Your Reference

Hub Configuration/1: IPv6 Tunnels

```
interface Loopback0
 ip address 192.168.52.7 255.255.255.255
!
interface Tunnel4
 no ip address
 ipv6 unnumbered FastEthernet0/1
 ipv6 enable
 tunnel source Loopback0
 tunnel destination 192.168.52.4
 tunnel mode ipv6ip

… a lot more interfaces Tunnel…

ip route 192.168.52.0 255.255.255.0 Serial0/0
```

Static IPv4 addresses

For Your Reference

Hub Configuration/2: IPv4 IPsec

```
crypto ipsec transform-set 3DES esp-3d
!
crypto dynamic-map TEMPLATE 10
 set transform-set 3DES
 match address SELECTOR
!
crypto map IPV6_SEC 10 ipsec-isakmp dynamic TEMPLATE
!
interface Serial0/0
 ip address 192.168.204.26 255.255.25
 crypto map IPV6_SEC
!
ip access-list extended SELECTOR
 permit 41 host 192.168.52.7 192.168.52.0 0.0.0.255
```

Dynamic crypto map: Allow IPsec from every IP address with correct IKE authentication

IPsec traffic selectors: fixed IPv4 loopback addresses, i.e., encapsulated IPv6 traffic