ADVANCES IN IPV6 SECURITY

BRKSEC-3003

Eric VYNCKE

Cisco Networkers 2007

HOUSEKEEPING

- We value your feedback, don’t forget to complete your online session evaluations after each session and complete the Overall Conference Evaluation which will be available online from Friday.
- Visit the World of Solutions on Level -01!
- Please remember this is a ‘No Smoking’ venue!
- Please switch off your mobile phones!
- Please remember to wear your badge at all times including the Party!
- Do you have a question? Feel free to ask them during the Q&A section or write your question on the Question form given to you and hand it to the Room Monitor when you see them holding up the Q&A sign.

Session Objectives

- This session presents IPv6 security in comparison to IPv4 from a threat and mitigation perspective
- Advanced IPv6 security topics like transition options and dual stack environments
- Requirements: basic knowledge of the IPv6 and IPsec protocols as well as IPv4 security best practices

For your reference

For Reference Slides

- There are more slides in the hand-outs than presented during the class.
- Those slides are mainly for reference and are indicated by the book icon on the top right corner (as on this slide)

Agenda

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

Types of Threats

A quick taxonomy 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

Shared Issues

Security issues shared by IPv4 and IPv6

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

  10 Mpps= more than 50 000 years

- NMAP doesn’t even support ping sweeps on IPv6 networks

Reconnaissance in IPv6
Scanning Methods Are Likely to Change

- Public servers will still need to be DNS reachable
- Increased deployment/reliance on dynamic DNS

  => More information will be in DNS
- Administrators may adopt easy to remember addresses (::10,::20,::F00D, ::C5C0 or simply IPv4 last octet for dual stack)
- By compromising hosts in a network, an attacker can learn new addresses to scan

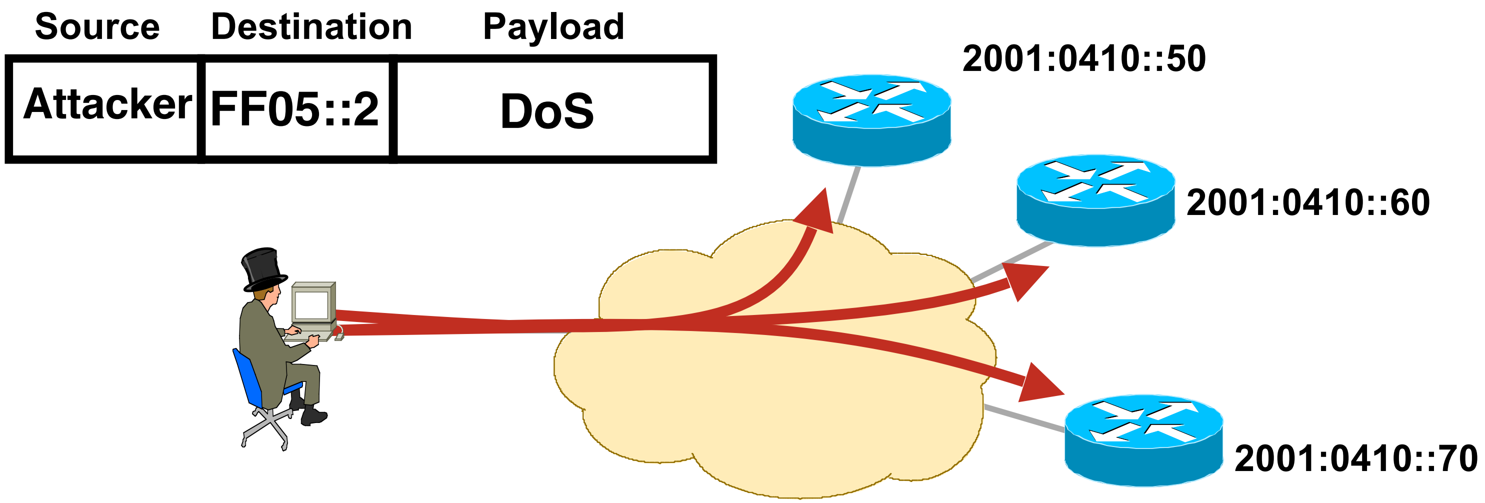
Reconnaissance in IPv6

New Multicast Addresses

- For example, all routers (FF05::2) and all DHCP servers (FF05::1:3)

  No need for reconnaissance anymore

- These addresses must be filtered at the border in order to make them unreachable from the outside

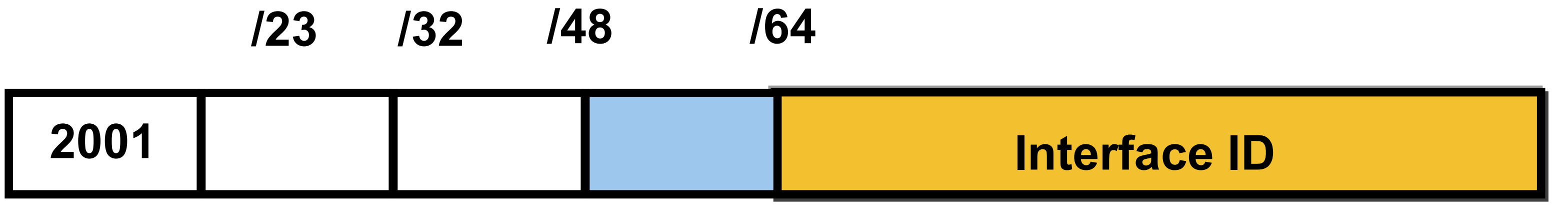


Source	Destination	Payload
Attacker	FF05::2	DoS

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

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

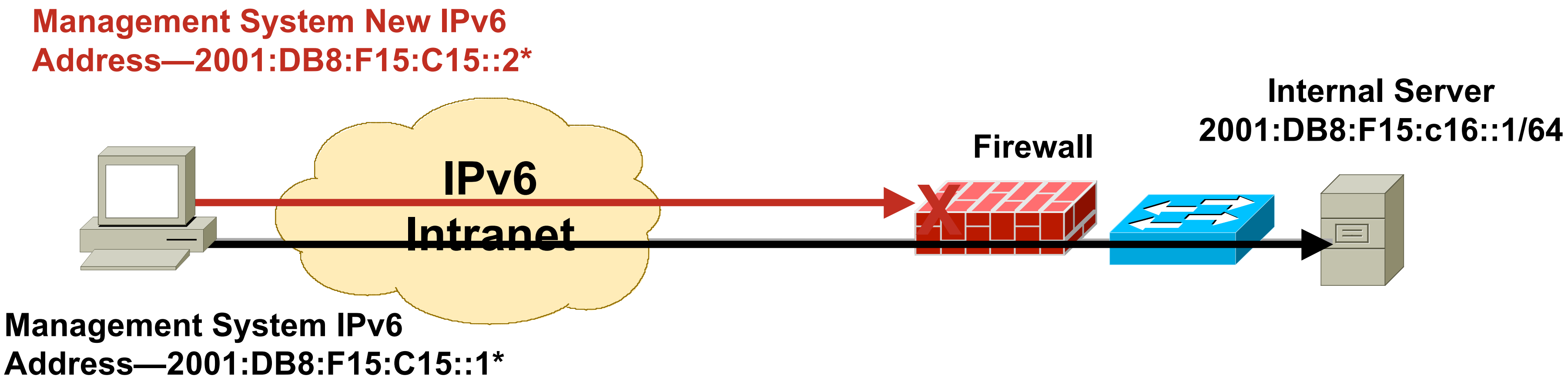
  Random 64 bit interface ID, run *Duplicate Address Detection* before using it

  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 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 :-)


Management System New IPv6 Address—2001:DB8:F15:C15::2*
Internal Server 2001:DB8:F15:c16::1/64
Firewall
IPv6 Intranet
X
Management System IPv6 Address—2001:DB8:F15:C15::1*

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

*—Not Real RFC3041 Derived Addresses

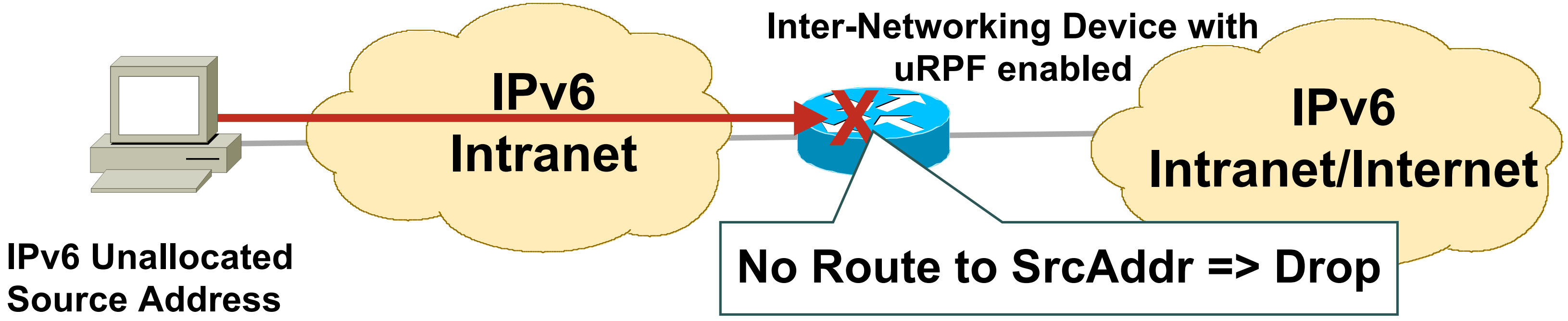
IPv6 Bogon Filtering

- In IPv4, easier to block bogons than to permit non-bogons
- In IPv6, in the beginning when a small amount of top-level aggregation identifiers (TLAs) have been allocated

  Easier to permit non-bogons

- Now IPv6 is in a similar situation as IPv4.

  => Same technique = uRPF


Inter-Networking Device with uRPF enabled
IPv6 Intranet
IPv6 Intranet/Internet
IPv6 Unallocated Source Address
No Route to SrcAddr => Drop

ICMPv4 vs. ICMPv6

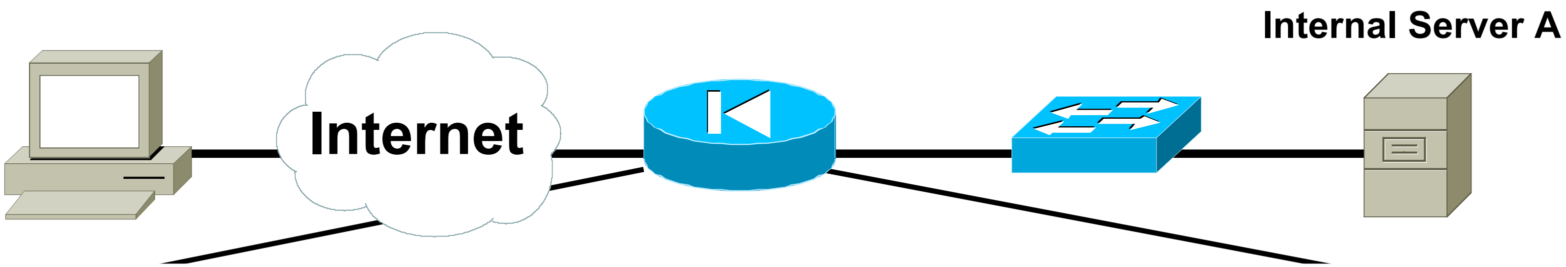
- Significant changes
- More relied upon

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

For your reference

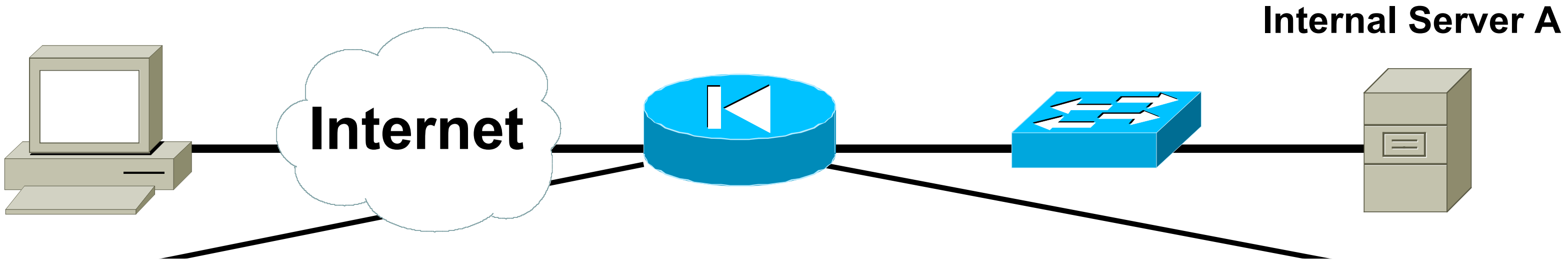
Generic ICMPv4 Border Firewall Policy



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

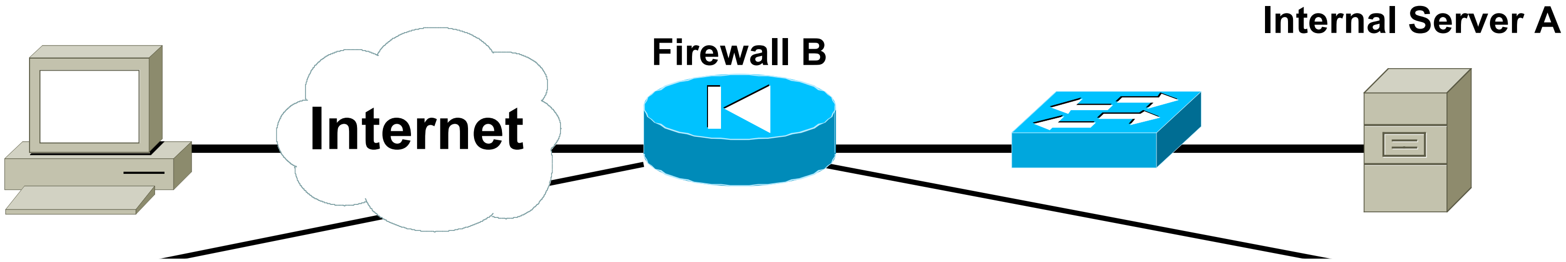
For your reference



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 Bord Firewall Policy*

For your reference

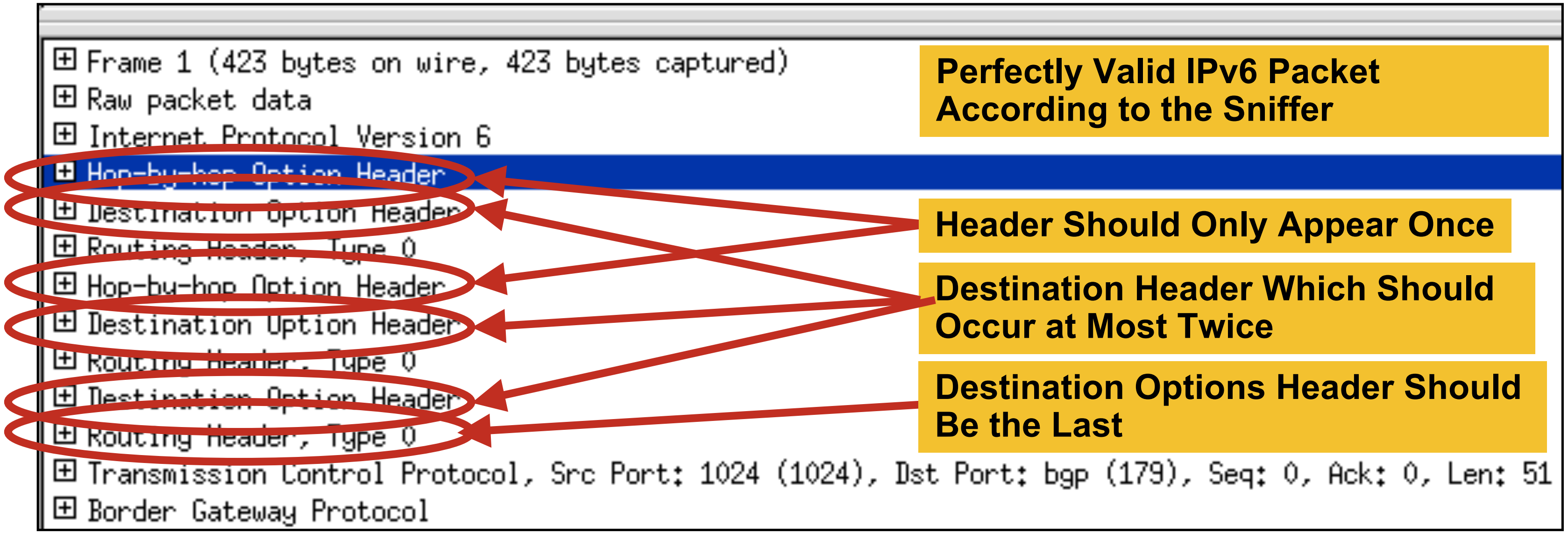


Action	Src	Dst	ICMPv6 Type	ICMPv6 Code	Name
Permit	Any	A	4	0	Parameter Problem
Permit	Any	B	2	0	Packet too Big
Permit	Any	B	130–132	0	Multicast Listener
Permit	Any	B	133/134	0	Neighbor Solicitation and Advertisement
Permit	Any	B	4	0	Parameter Problem

*draft-ietf-v6ops-icmpv6-filtering-recs-02.txt

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?



```
⊞ Frame 1 (423 bytes on wire, 423 bytes captured)
⊞ Raw packet data
⊞ Internet Protocol Version 6
⊞ Hop-by-hop Option Header
⊞ Destination Option Header
⊞ Routing Header, Type 0
⊞ Hop-by-hop Option Header
⊞ Destination Option Header
⊞ Routing Header, Type 0
⊞ Destination Option Header
⊞ Routing Header, Type 0
⊞ Transmission Control Protocol, Src Port: 1024 (1024), Dst Port: bgp (179), Seq: 0, Ack: 0, Len: 51
⊞ Border Gateway Protocol
```

Perfectly Valid IPv6 Packet According to the Sniffer

Header Should Only Appear Once

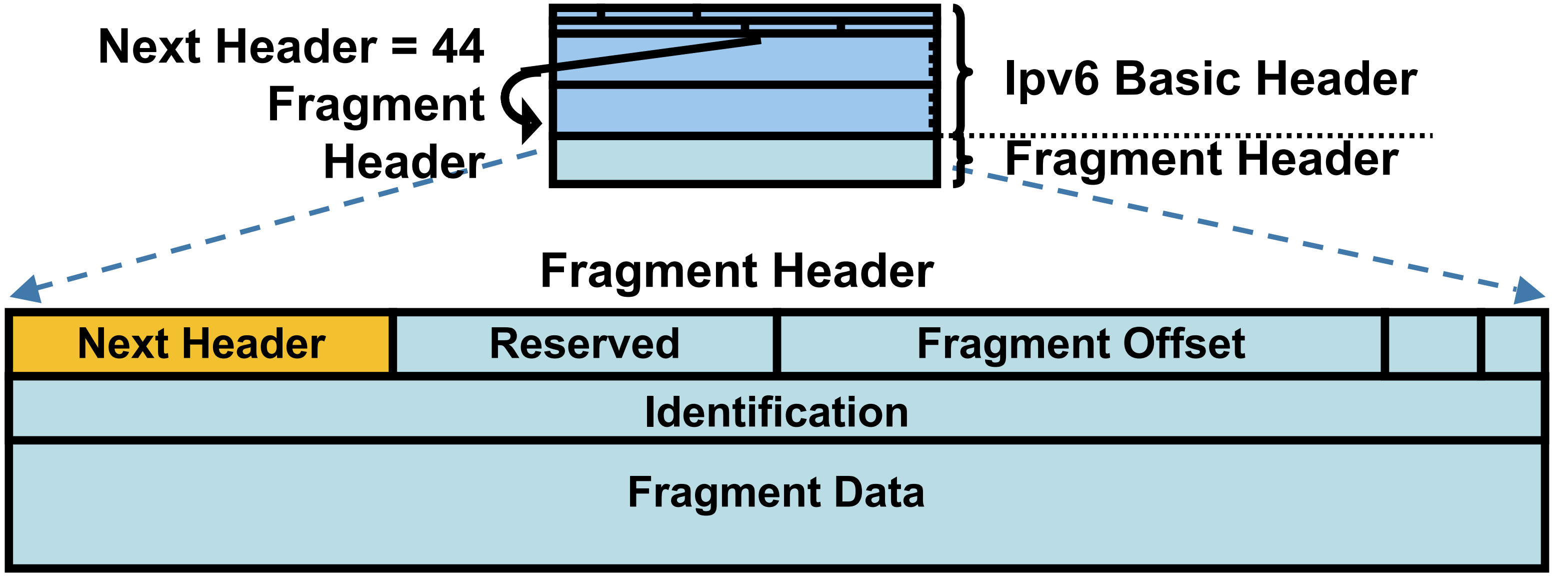
Destination Header Which Should Occur at Most Twice

Destination Options Header Should Be the Last

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

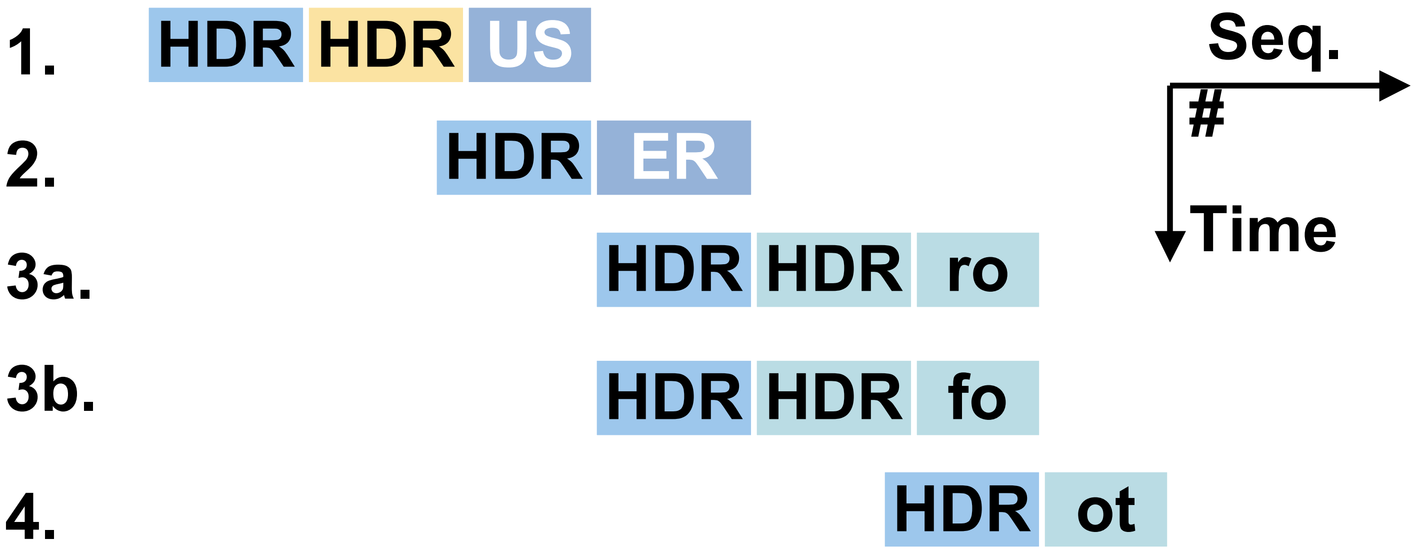
Fragment Header: IPv6



- 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:



1. HDR HDR US

2. HDR ER

3a. HDR HDR ro

3b. HDR HDR fo

4. HDR ot

Seq. #

Time

- 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

- Procedure
  1. Parse the next headers until the fragment header
     - extract the flags and offset
  2. Parse further NHs until the upper layer protocol
  3. 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

  But in a later fragment

  => Need for stateful inspection

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

Header Manipulation and Fragmentation Best Practices

- Deny IPv6 fragments destined to an internetworking device (DOS vector)

    Infrastructure ACL

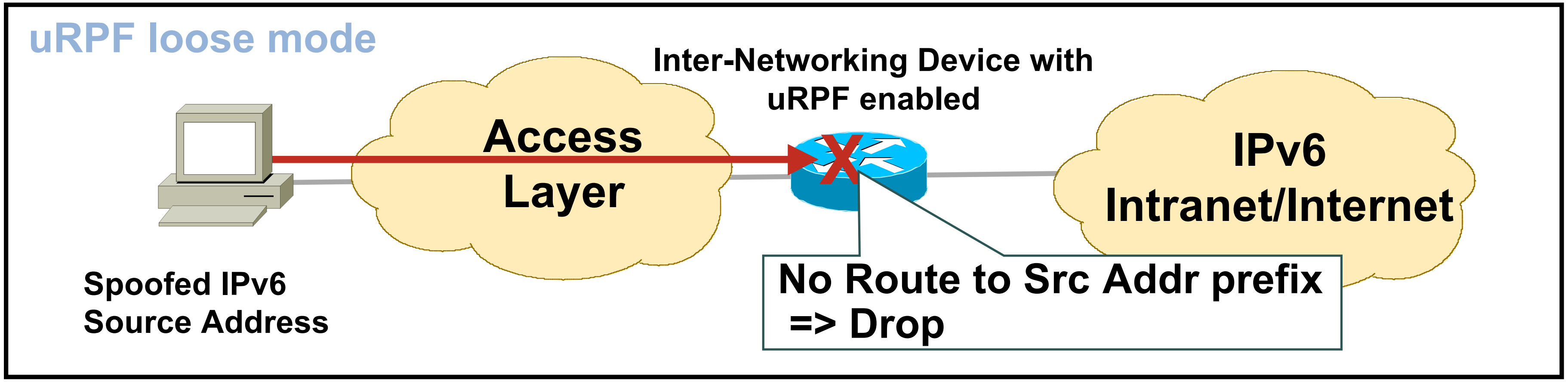
- Ensure adequate IPv6 fragmentation filtering capabilities; for example, drop all packets with the routing header 2 if you don’t have MIPv6

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

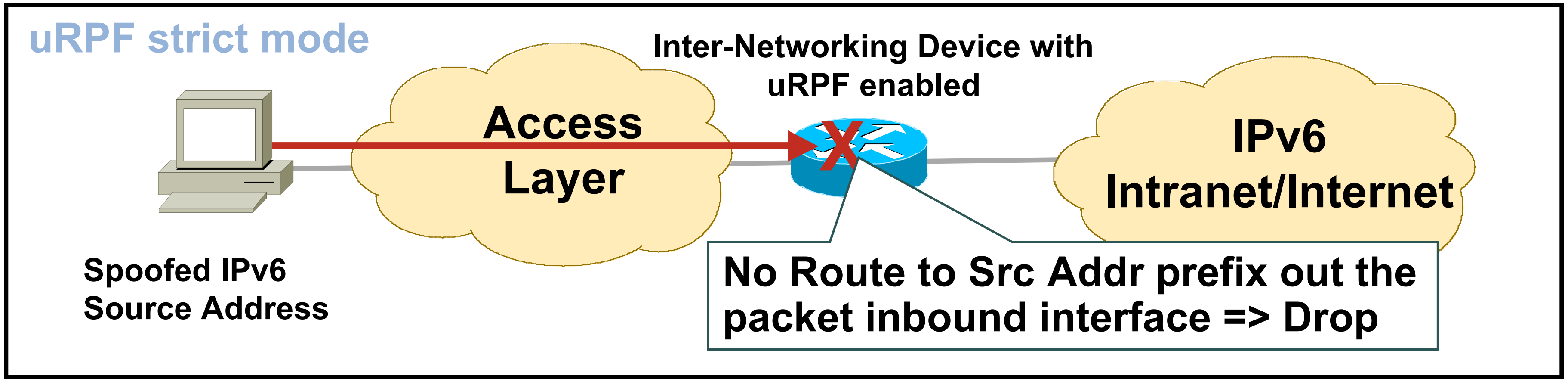
L3 Spoofing in IPv6

uRPF remains the primary tool for protecting against L3 spoofing



uRPF loose mode

No Route to Src Addr prefix => Drop



uRPF strict mode

No Route to Src Addr prefix out the packet inbound interface => Drop

IPv6 Routing Header

Routing Header Is:

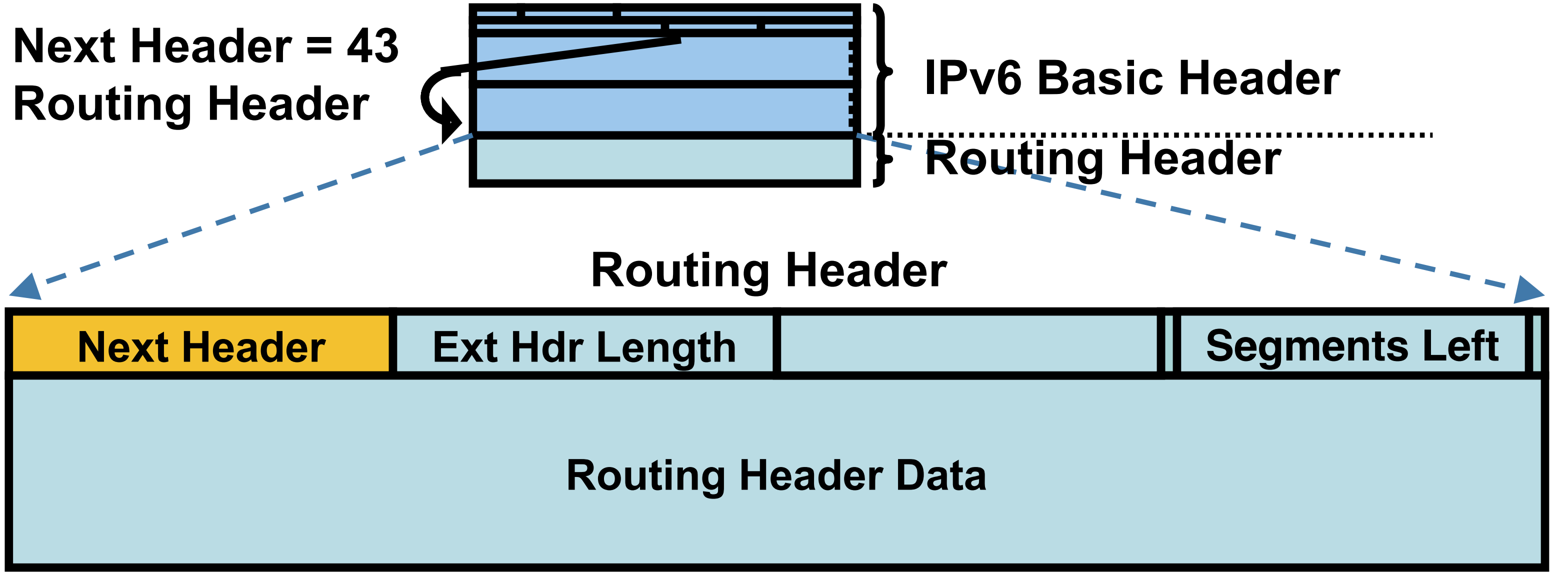
- An extension header
- Processed by the listed intermediate routers

Routing Header IPv6 ⇔ Source Routing in IPv4

Can Be Turned Off:

’no ipv6 source-route’

IPv6 ACL Could Also Be Used

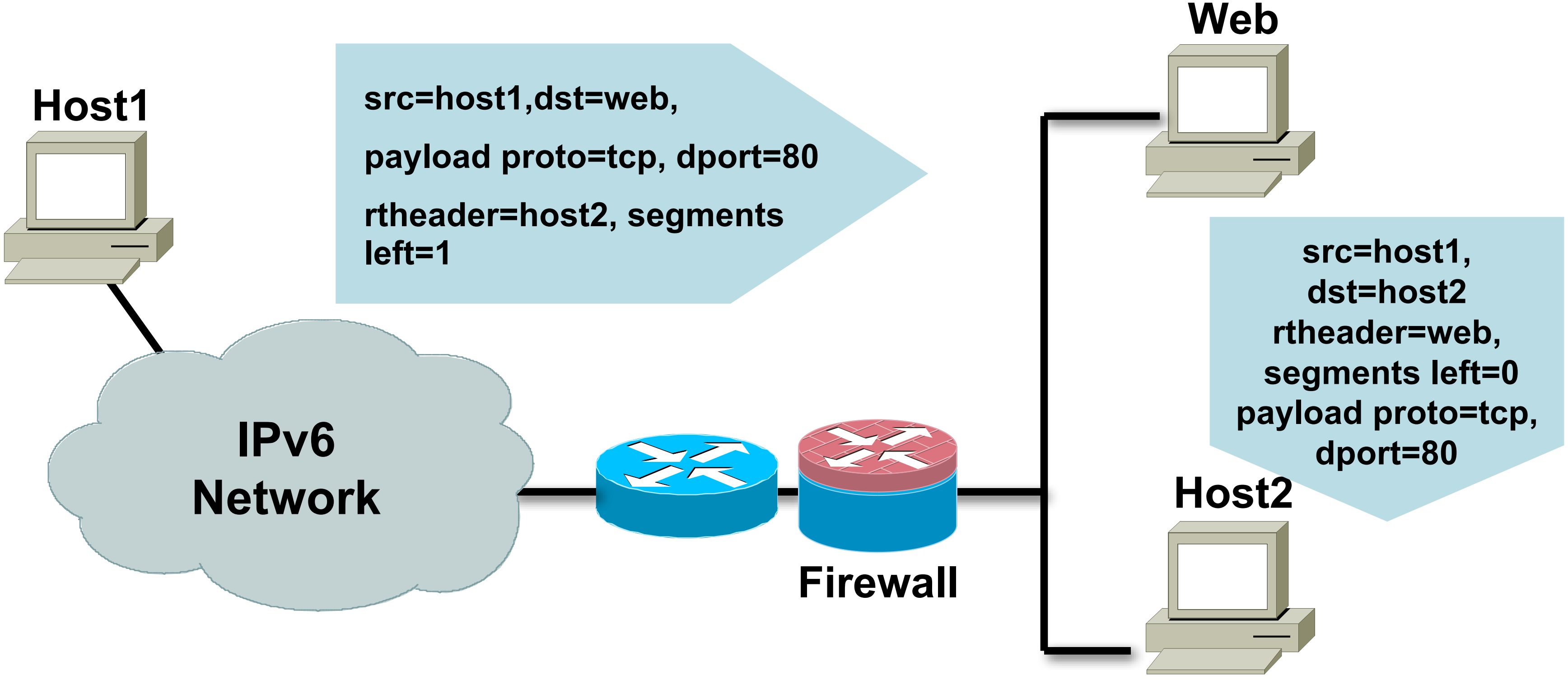


Issues with Routing Header

- 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



src=host1,dst=web,

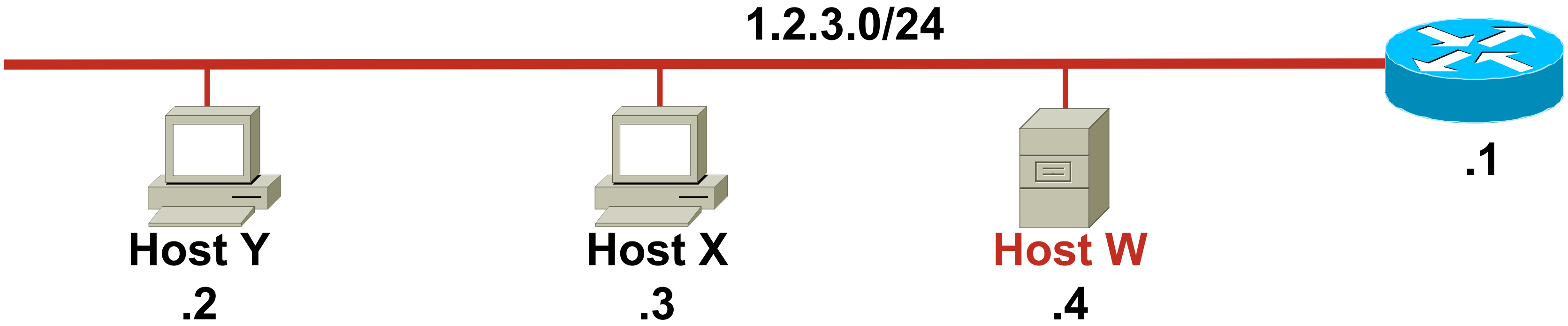
payload proto=tcp, dport=80

rtheader=host2, segments left=1

src=host1,
dst=host2
rtheader=web,
segments left=0
payload proto=tcp,
dport=80

Quick Refresh 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

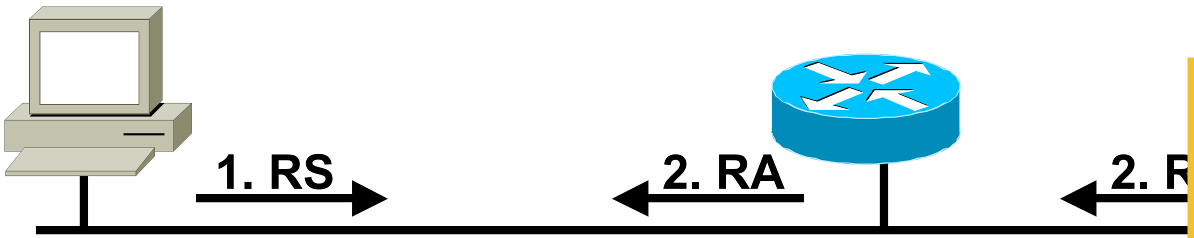


- With DHCP it is similar except the attacker just needs to put a DHCP server on the wire delivering false information (gateways, DNS servers, etc.)

Stateless Autoconfiguration

Router Solicitations 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



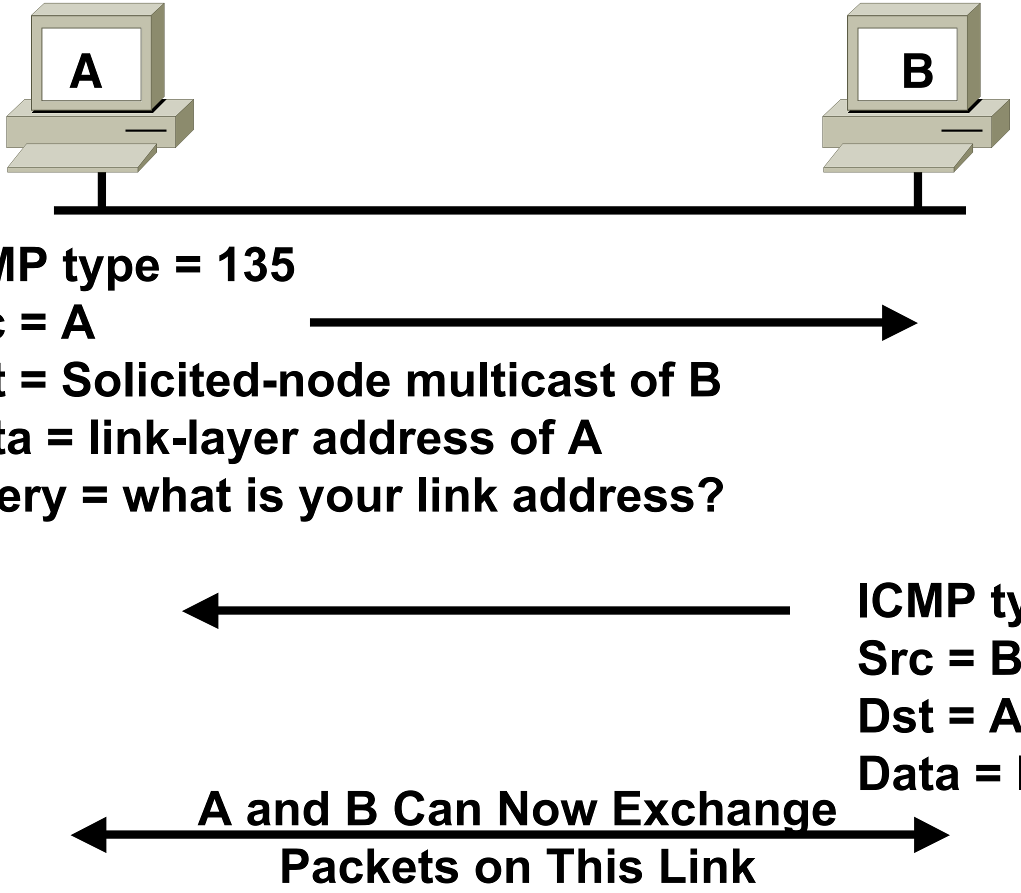
Attack tool:
fake_router6

Can make any IPv6 address the default router

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 Solicitation



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

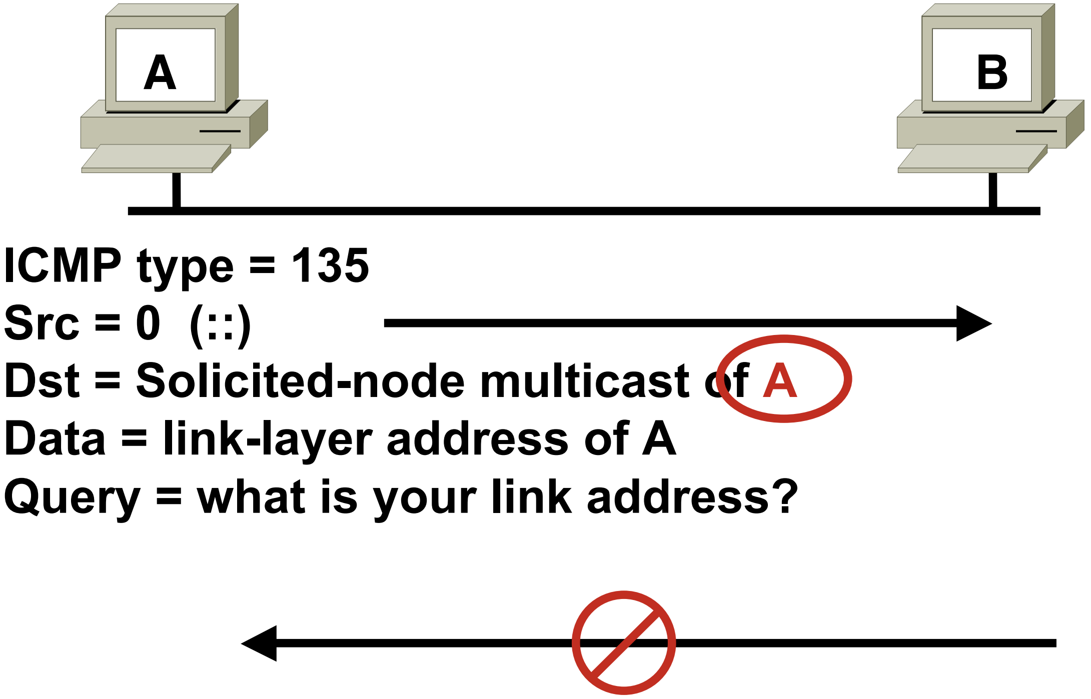
Security mechanisms built into Discovery Protocol = none

=> Another bootstrap security problem

Attack tool:
Parasite6
Answer to all NS, claiming to be all systems in the LAN...

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 @

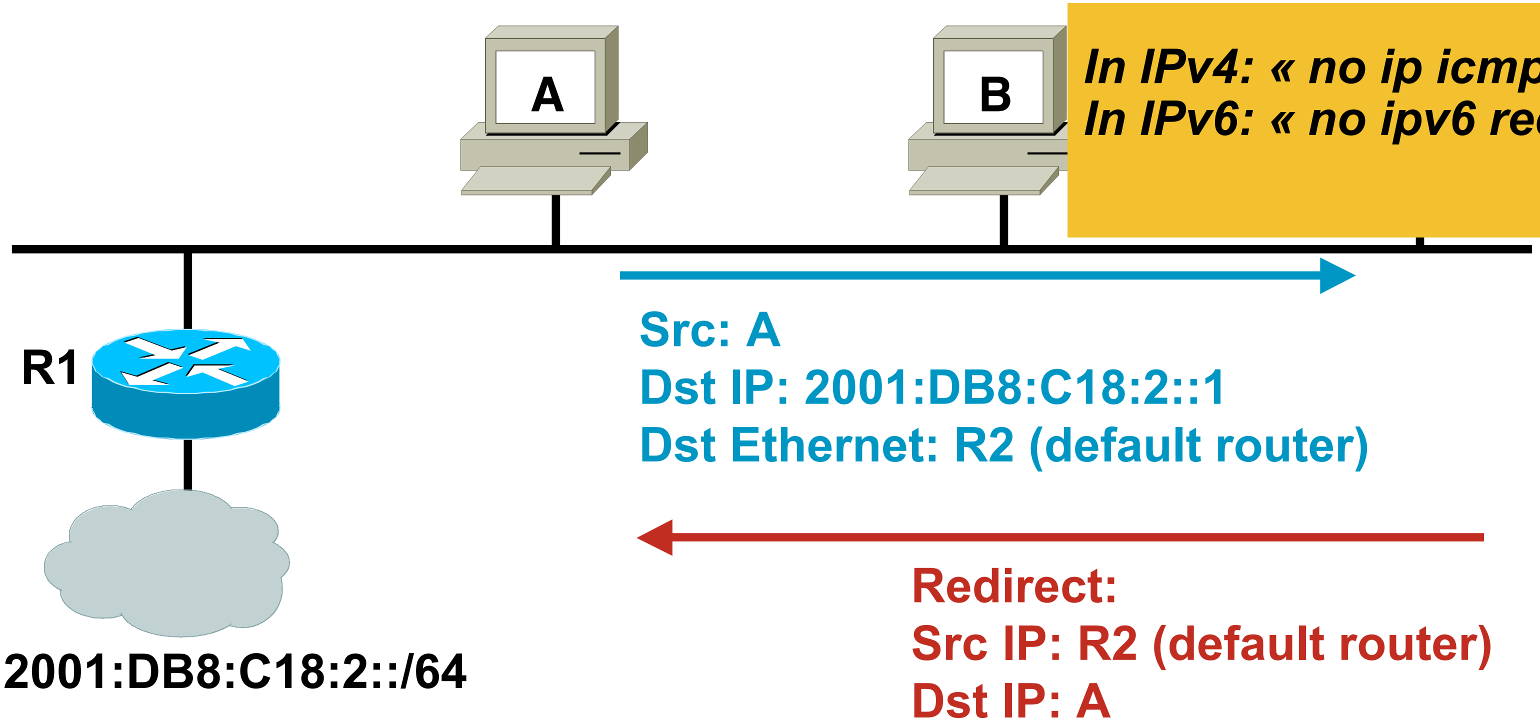
Attack tool:
Dos-new-ipv6

Spoofed Redirect

Redirect is used by a router to signal the re-route of a packet to a better router
Original packet has to be included...

Original packet has to be included to prevent spoofed redirect…
BUT
What if attacker first sent ICMP echo request? The reply packet is predictable…

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



Src: A
Dst IP: 2001:DB8:C18:2::1
Dst Ethernet: R2 (default router)

Redirect:
Src IP: R2 (default router)
Dst IP: A
Data: good router = R1

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

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 the interface identifier is cryptographically generated

- RSA signature option

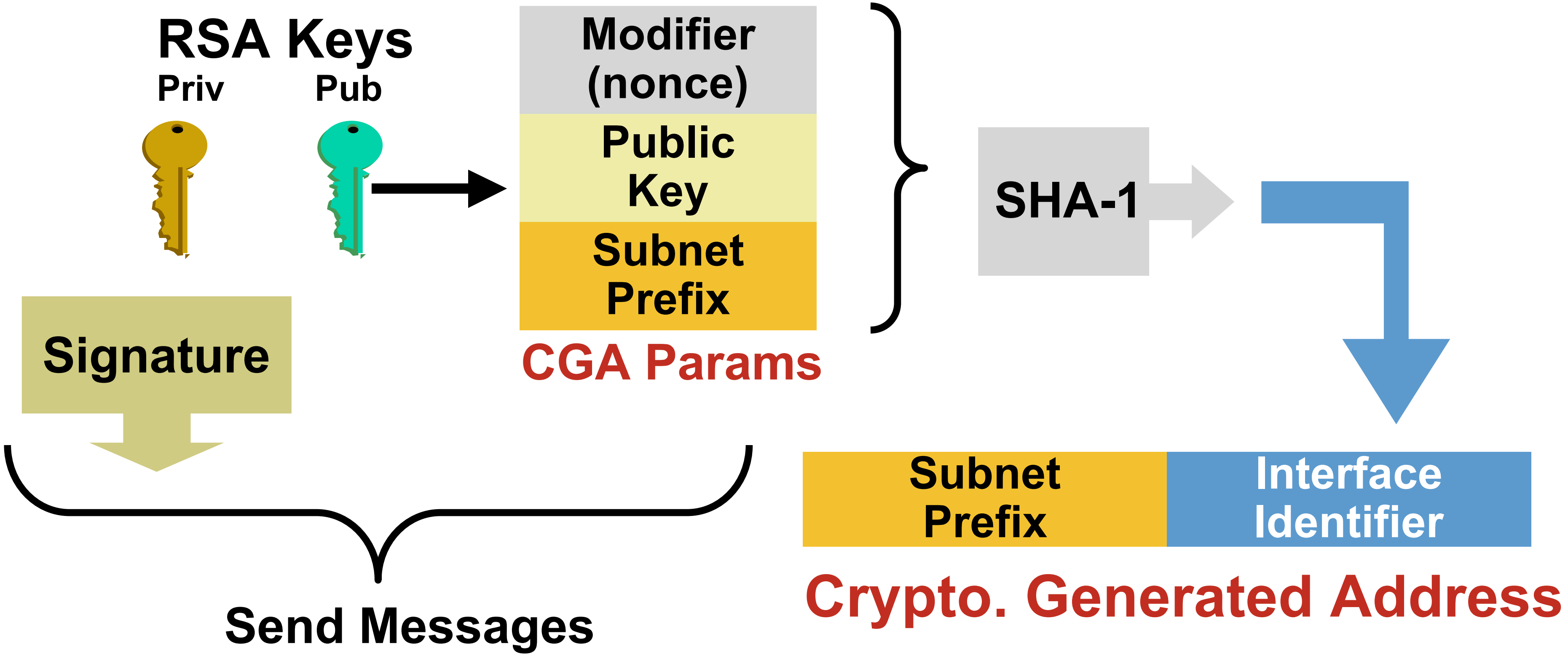
  Protect all all messages relating to neighbor and router discovery

- Timestamp and nonce 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: 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

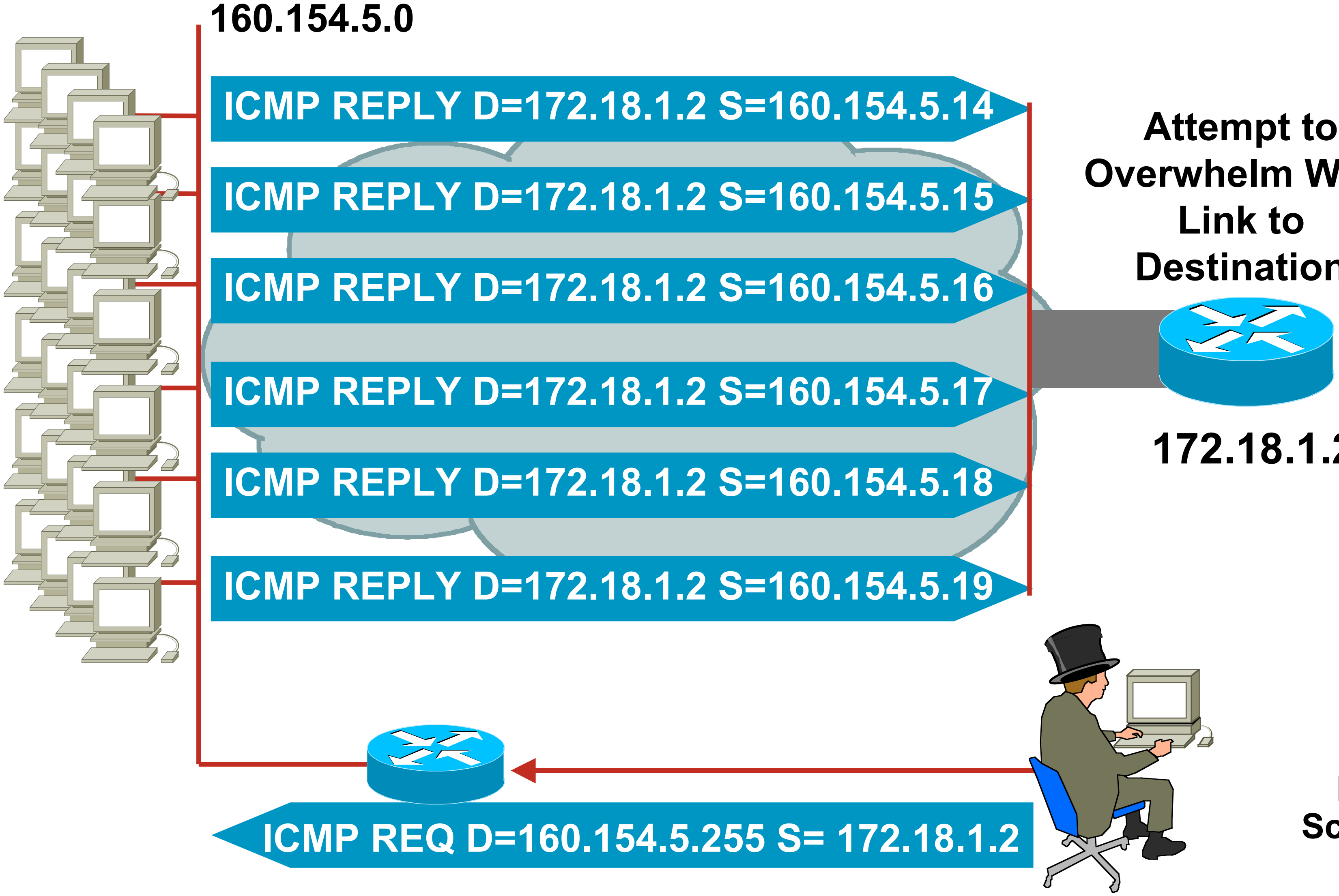
DHCPv6 Threat Mitigation

- 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)

Quick Reminder
IPv4 Broadcast Amplification: Smurf



160.154.5.0
ICMP REPLY D=172.18.1.2 S=160.154.5.14
ICMP REPLY D=172.18.1.2 S=160.154.5.15
ICMP REPLY D=172.18.1.2 S=160.154.5.16
ICMP REPLY D=172.18.1.2 S=160.154.5.17
ICMP REPLY D=172.18.1.2 S=160.154.5.18
ICMP REPLY D=172.18.1.2 S=160.154.5.19
172.18.1.2
ICMP REQ D=160.154.5.255 S= 172.18.1.2

Attempt to Overwhelm WAN Link to Destination

Belgian Schtroumpf

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
Rate limit ICMP packet

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

- Viruses and email 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

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

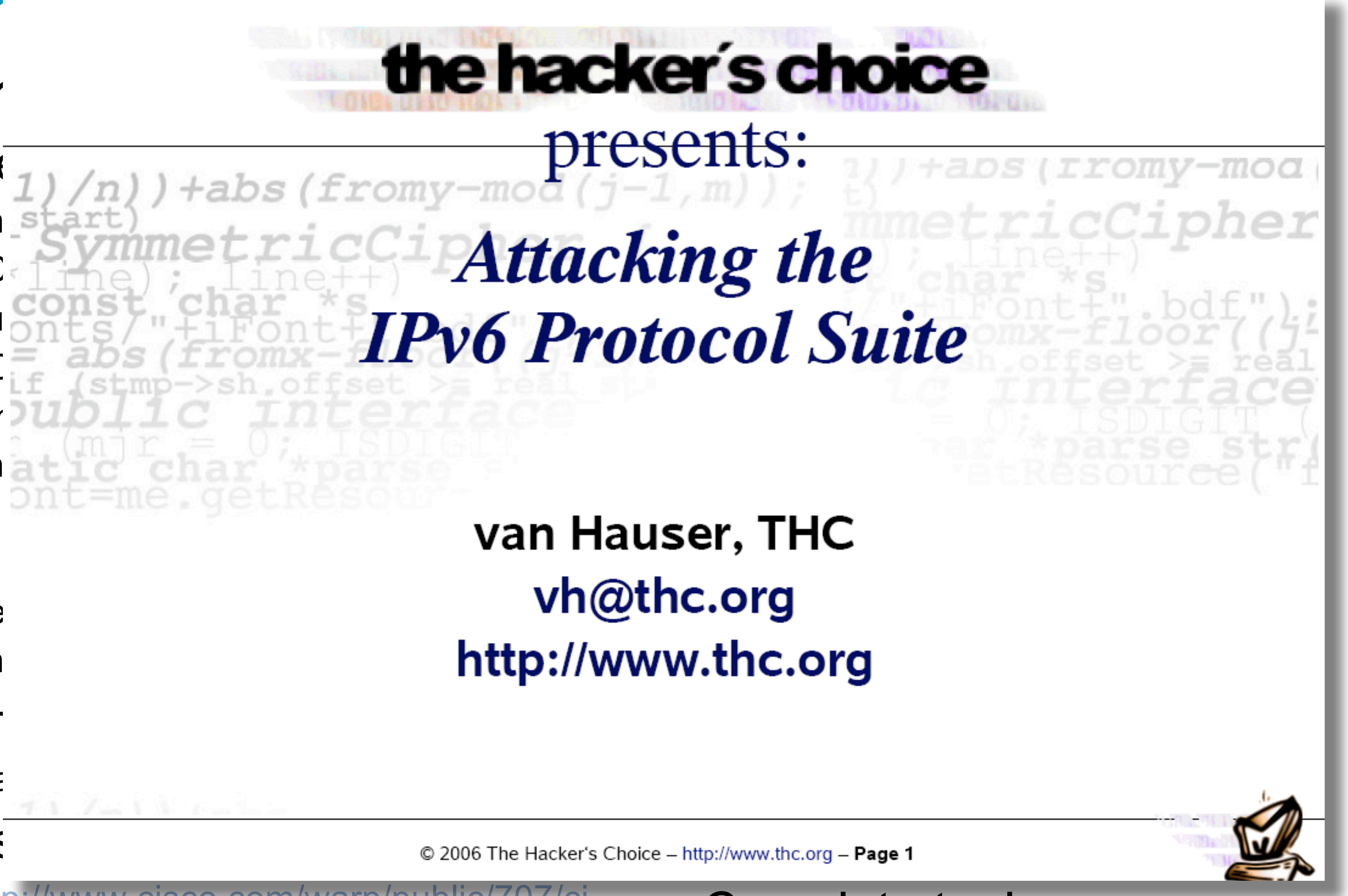
IPv6 Stacks Vulnerabilities

- IPv6 stack are new and could be buggy
- IPv6 enabled application can have bugs
- Some examples
  - Python getaddreinfo() remote IPv6 buffer overflow
  - Apache remote IPv6 buffer overflow
  - Postfix IPv6 unauthorized mail relay vulnerability
  - Linux kernel IPv6 DoS

By the Way: It Is Real ☹
IPv6 Hacking Tools

Let th

- Sniffe
  - Sn
  - TC
  - Su
  - CC
  - Eth
  - An
  - Wi
  - Wi
  - Ne
  - Sn
- Worr
  - Sla
- Advis
  - http://www.cisco.com/warp/public/707/cisco-sa-20050126-ipv6.shtml
  - http://www.kb.cert.org/vuls/id/658859



the hacker´s choice

presents:

Attacking the IPv6 Protocol Suite

van Hauser, THC

vh@thc.org

http://www.thc.org

© 2006 The Hacker's Choice – http://www.thc.org – **Page 1**

- Complete tool
  - http://www.thc.org/thc-ipv6/

Specific IPv6 Issues

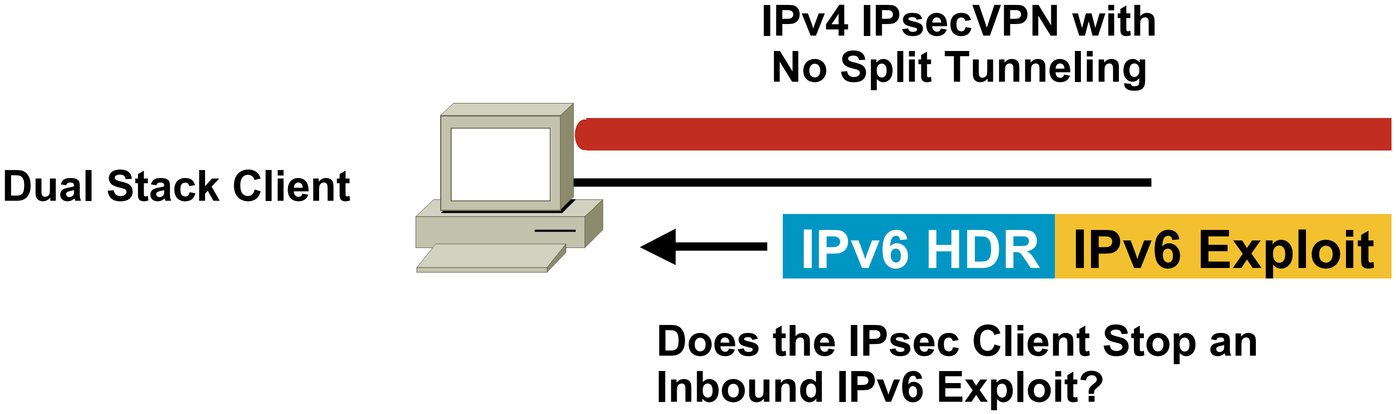
Issues applicable only to IPv6

IPv4 to IPv6 Transition 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)

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.


IPv4 IPsecVPN with No Split Tunneling
Dual Stack Client
IPv6 HDR
IPv6 Exploit
Does the IPsec Client Stop an Inbound IPv6 Exploit?

Dual Stack with enabled IPv6 by default

- Your host:

  IPv4 is protected by your favorite personal firewall...

  IPv6 is enabled by default (Vista, Linux, MacOS, ...)

- 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 configure IPv6 on your network

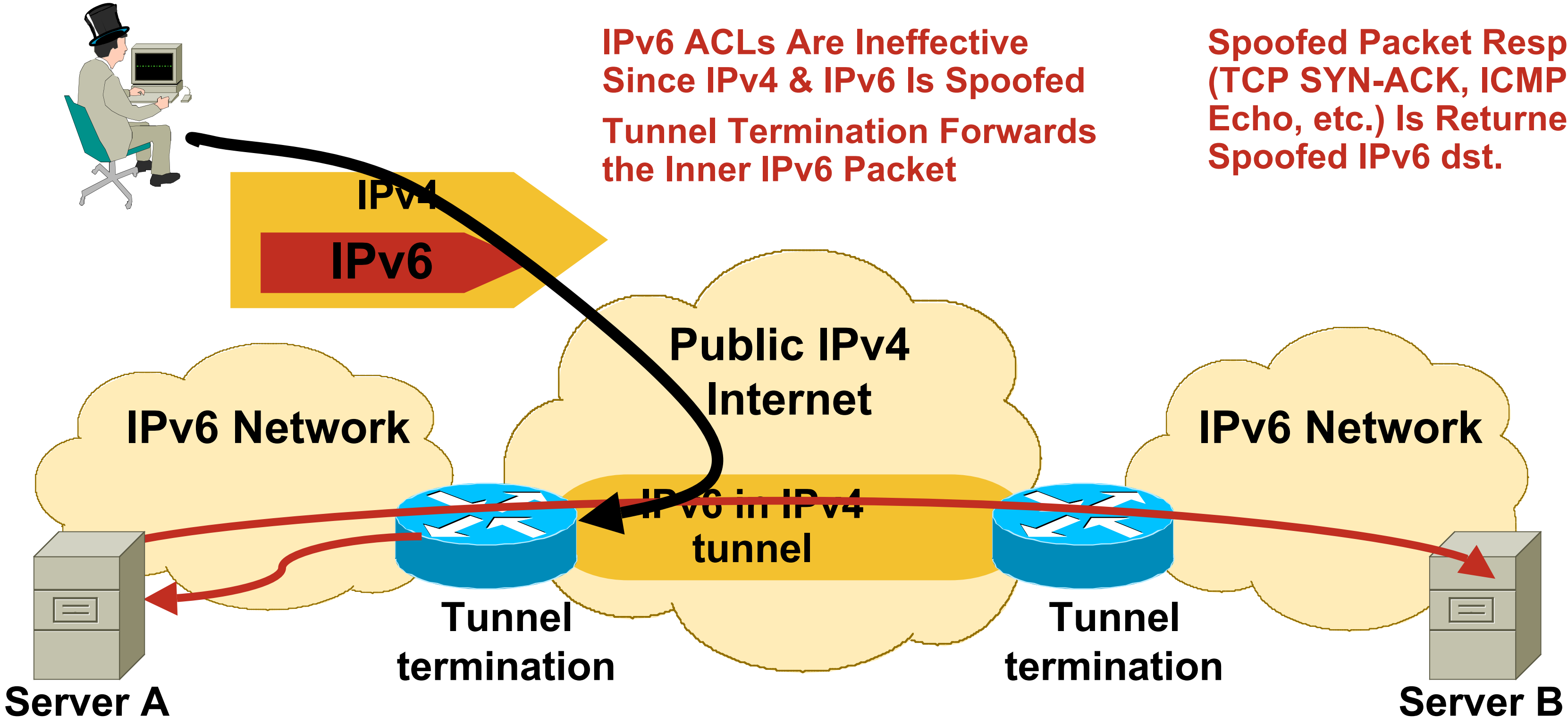
IPv6 Tunneling Summary

- 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
- 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



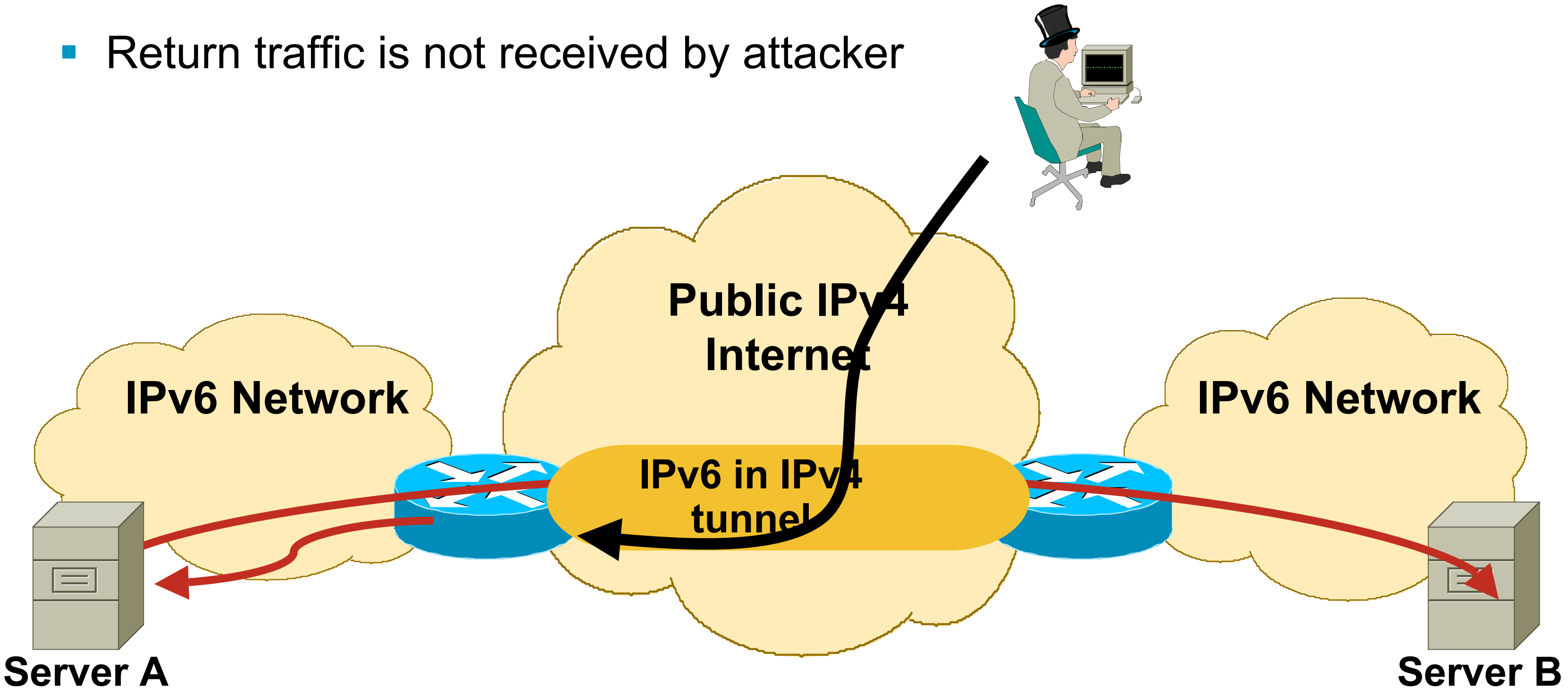
IPv6 ACLs Are Ineffective Since IPv4 & IPv6 Is Spoofed

Tunnel Termination Forwards the Inner IPv6 Packet

Spoofed Packet Response (TCP SYN-ACK, ICMPv6 Echo, etc.) Is Returned to Spoofed IPv6 dst.

L3-L4 Spoofing in IPv6
Dos Via Tunnels

- Harm is limited
- 1:1 ratio of packets—no amplification attack
  - Even bandwidth decrease after decapsulation ;-)
- There is a chokepoint against DoS
- Return traffic is not received by attacker



Transition Threats – ISATAP

- ISATAP threats

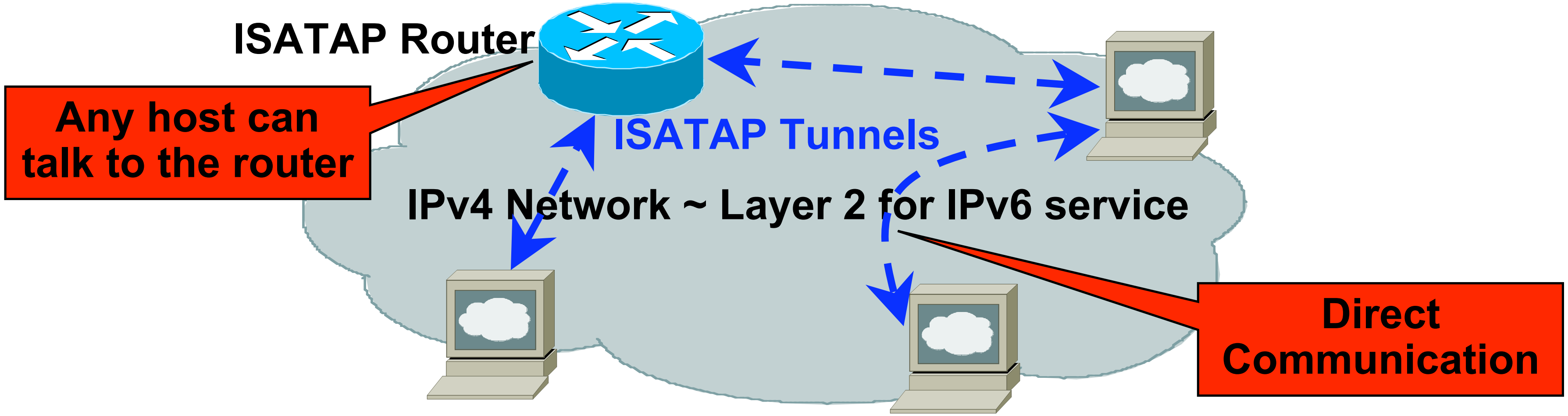
  Unauthorized tunnels—firewall bypass (protocol 41)

  IPv4 infrastructure 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



Any host can talk to the router

Direct Communication

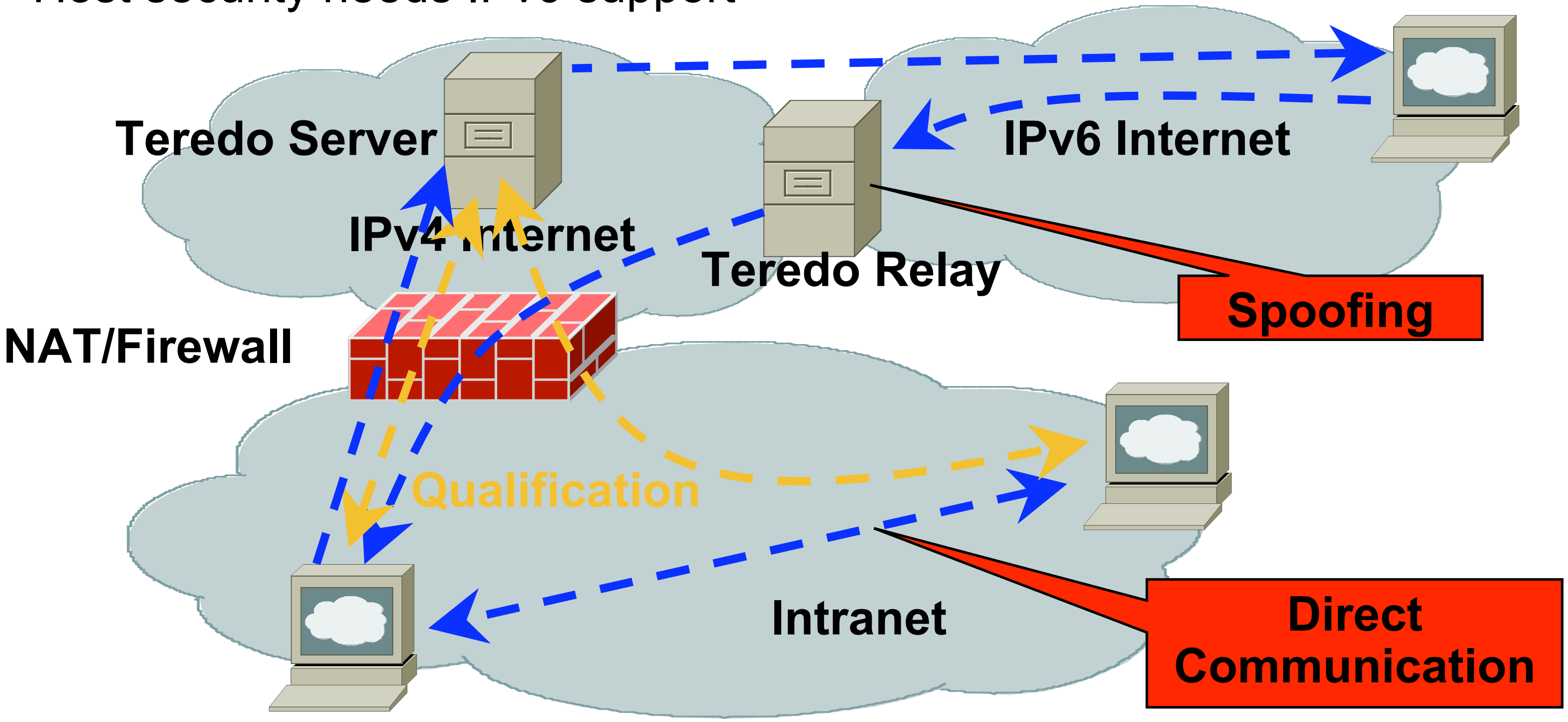
Transition Threats – Teredo

- Teredo threats—IPv6 over UDP (port 3544)

    Unauthorized tunnels—firewall bypass

    Rogue relays/servers can be used for DoS; possible for client to server communications

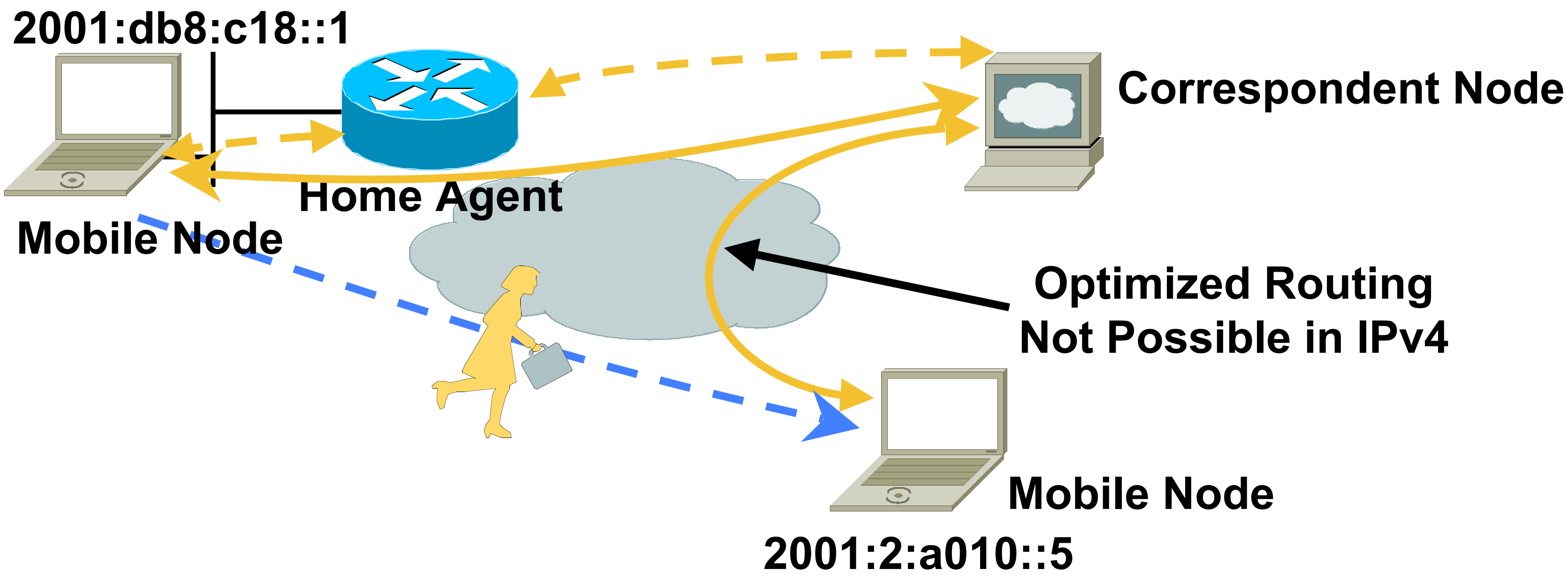
    Host security needs IPv6 support



Understand The Behavior Of Vista

- IPv6 is preferred over IPv4
  - Vista sends IPv6 NA/NS/RS upon link-up
    - Attempts DHCP for IPv6
    - Else wait for local RA received with Global or ULA
    - Else try ISATAP
    - Else try Teredo
    - Else use IPv4 – **LAST RESORT**
- ANY application built on the Peer-to-Peer Framework REQUIRES IPv6 and will NOT function over IPv4 - http://www.microsoft.com/technet/network/p2p/default.mspx

IP Mobility



Mobility Means:

- Mobile devices are fully supported while moving
- Built-in on IPv6

  Any node can use it
- Optimized 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 (specially for HA),

  Or binding authorization data option through the return routability procedure

- Protection of mobile prefix discovery

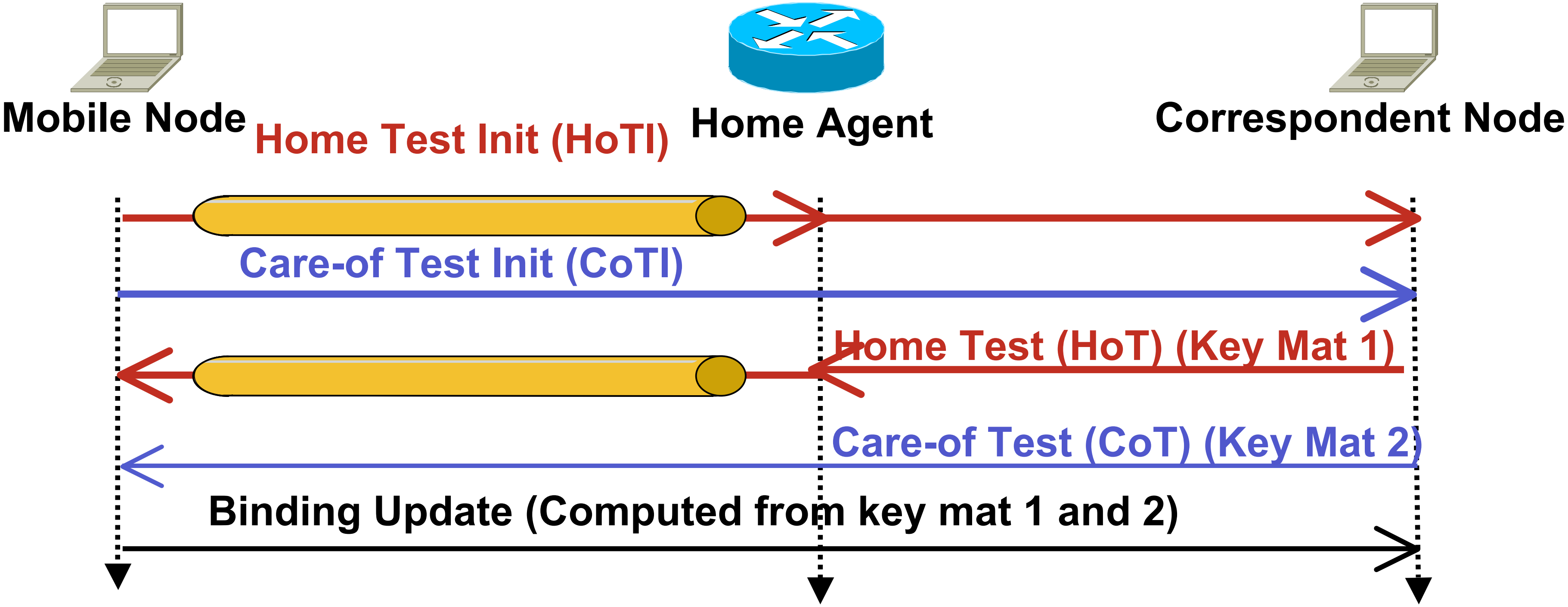
  Through the use of IPsec extension headers

- Protection of data packets transport

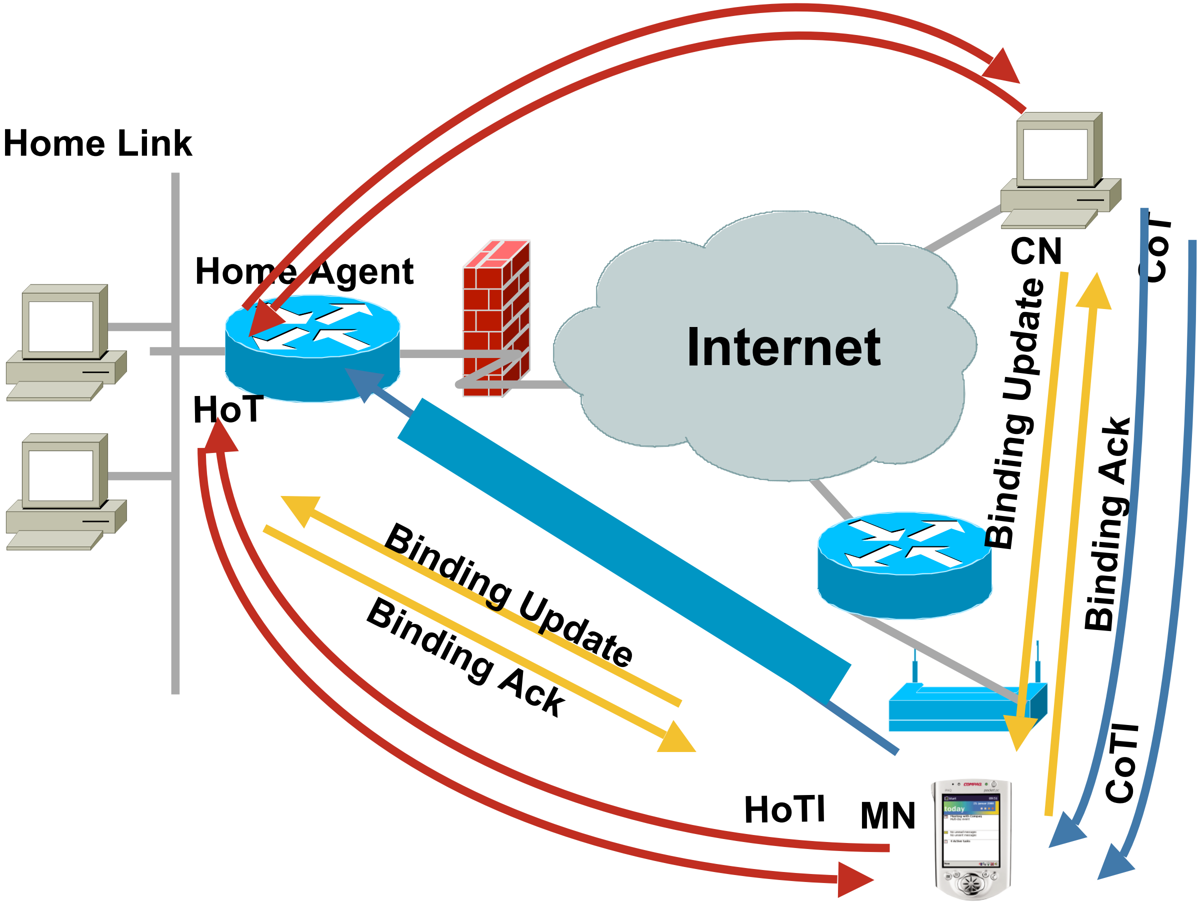
  Home address destination option and type two routing header specified in a manner which restricts their use
  in attacks

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 Node
Home Test Init (HoTI)
Home Agent
Correspondent Node
Care-of Test Init (CoTI)
Home Test (HoT) (Key Mat 1)
Care-of Test (CoT) (Key Mat 2)
Binding Update (Computed from key mat 1 and 2)

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

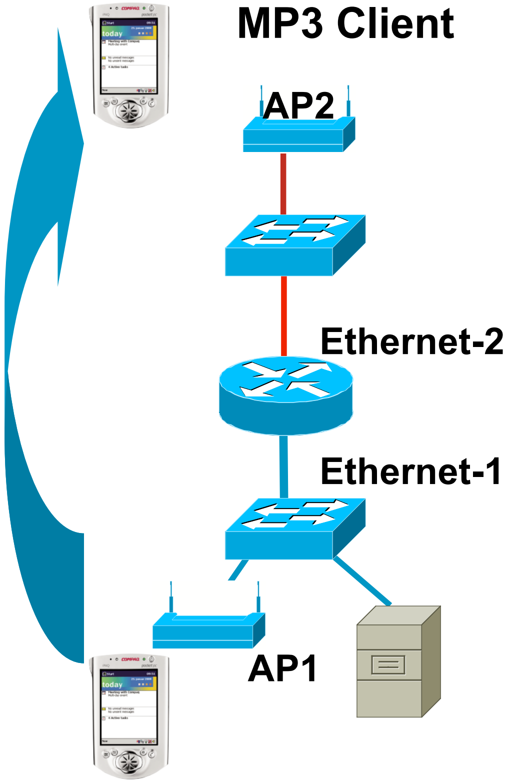
- BU/BA to HA must be secured through IPsec
- MN and HA should use an IPsec SA to protect the integrity and authenticity of the mobile prefix solicitations and advertisements
- Payload packets exchanged with MN can follow the same protection policy as other IPv6 hosts
- Specific security measures are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

MIPv6 Security Challenges

- Unlike IPv4 Mobility, IPv6 enables the MN and the CN to communicate directly through Route Optimization
- Security tools such as IDS/Firewall and Regulation implementation such as LI **can be bypassed** by design in the case of MIPv6

For your reference

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"

IPv6 Security
Best Common Practice

For your reference

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

Wrap Up: Candidate Best Practices (Cont.)

For your reference

- 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 static tunneling rather than dynamic tunneling
- Implement outbound filtering on firewall devices to allow only authorized tunneling endpoints

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
A Trivial Example

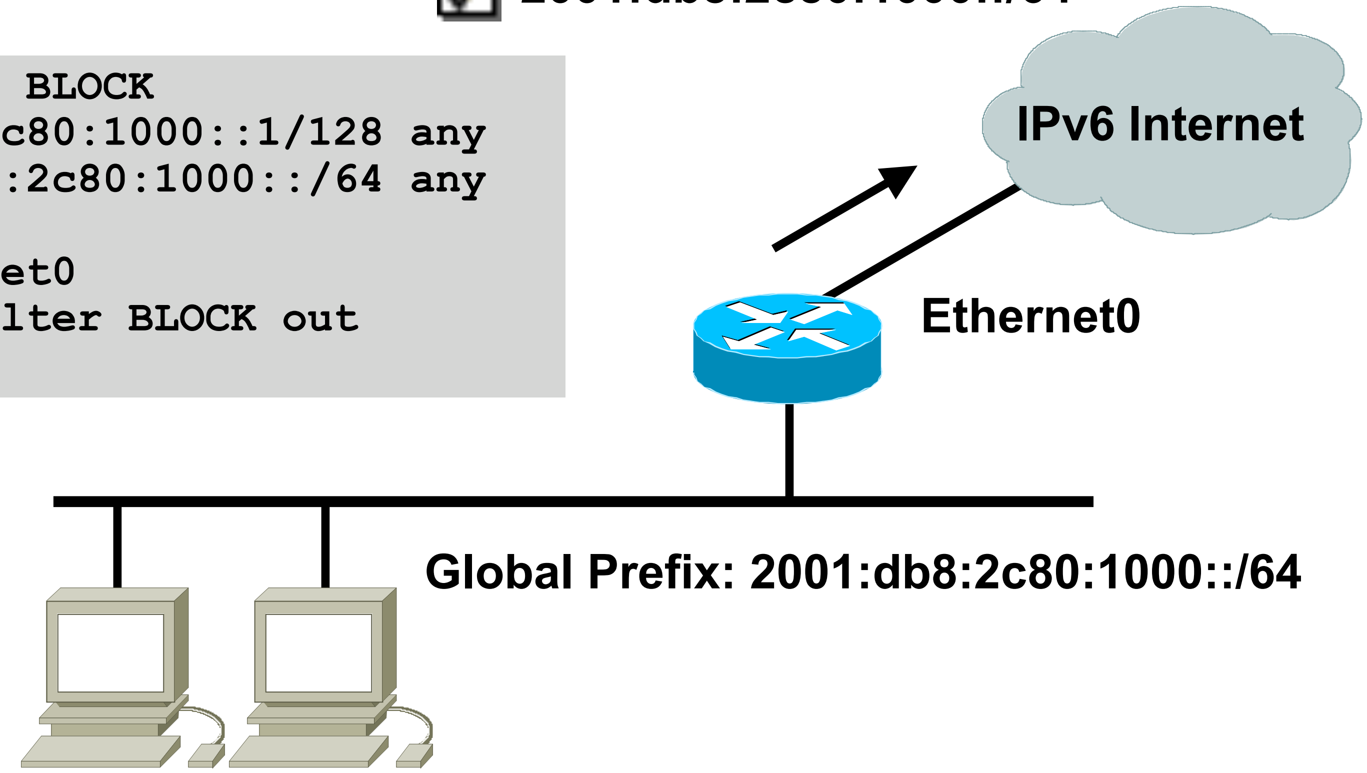
Filtering Outgoing Traffic from One Specific Source Address

⊘ 2001:db8:2c80:1000::1

☑ 2001:db8:2c80:1000::/64

```
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
```



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

For your reference

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
  ```

Control Plane Policing for IPv6 Protecting the Router CPU

For your reference

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

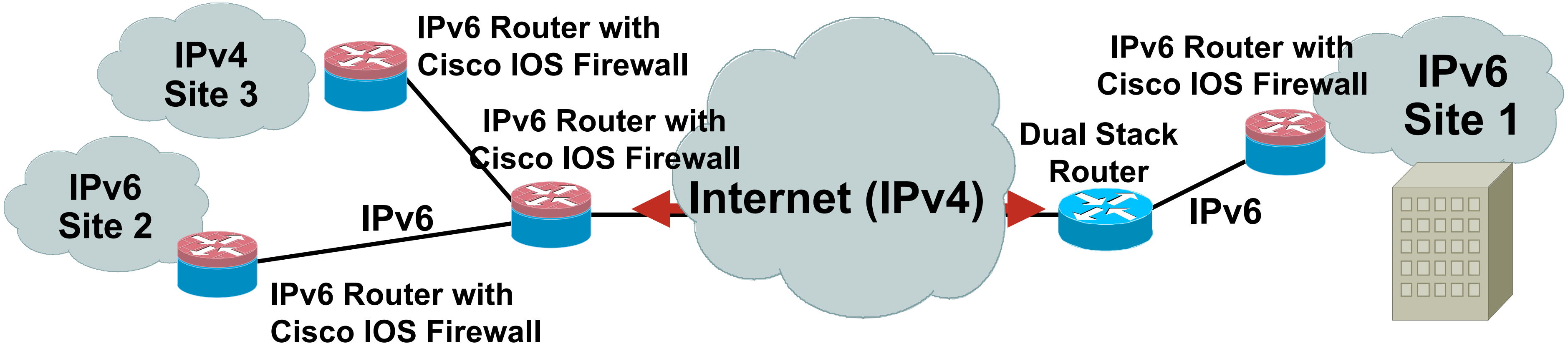
```
class-map match-all ipv6
 match protocol ipv6

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

control-plane
  service-policy input CoPP
```

Cisco IOS Firewall IPv6 Support

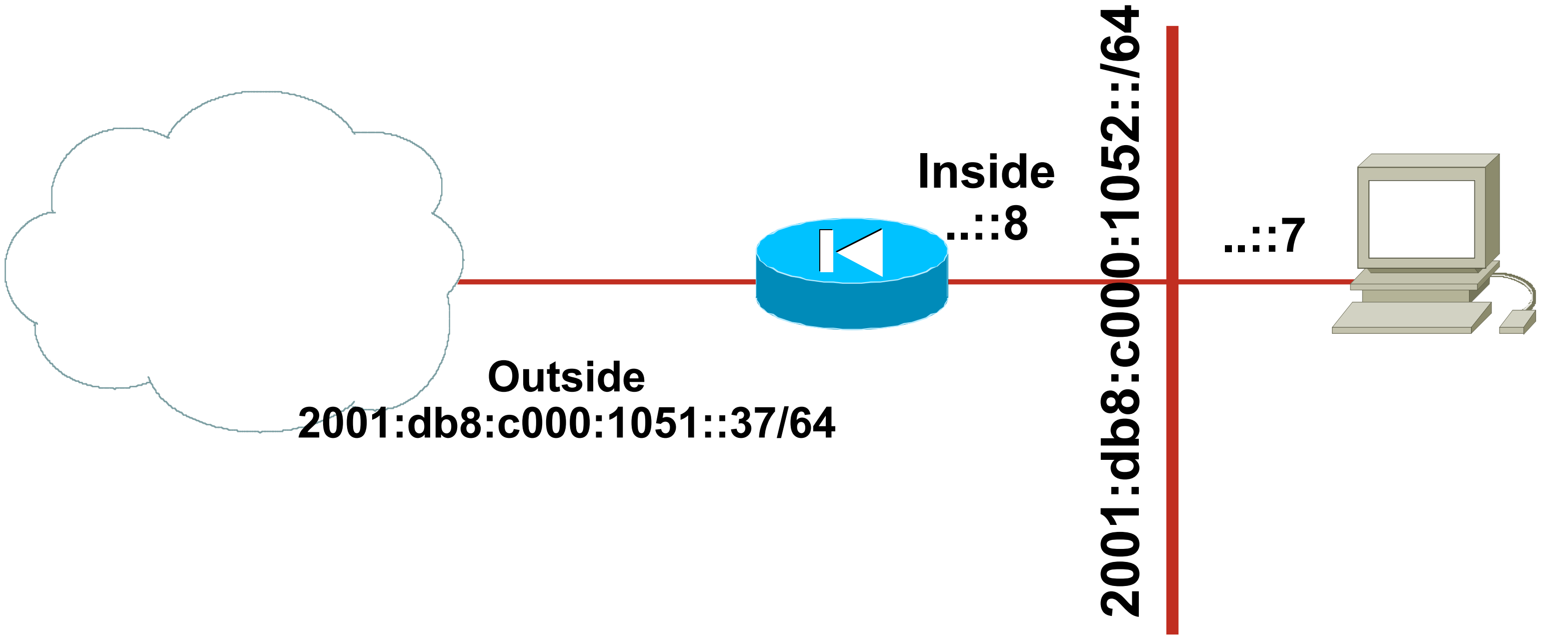
- Stateful protocol inspection (anomaly detection) of IPv6 fragmented packets, TCP, UDP, ICMP and FTP traffic
- Stateful inspection and translation services of IPv4/IPv6 packets
- IPv6 DoS attack mitigation
- IPv4/v6 coexistence, no need for new hardware, just software
- Recognizes IPv6 extension header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



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.x: ACL Very Similar to Cisco IOS

For your reference

```
interface Ethernet0
 nameif outside
 ipv6 address 2001:db8:c000:1051::37/64
 ipv6 enable
interface Ethernet1
 nameif inside
 ipv6 address 2001:db8:c000:1052::1/64
 ipv6 enable

ipv6 route outside ::/0 2001:db8:c000:1051::1

ipv6 access-list SECURE permit tcp any host
2001:db8:c000:1052::7 eq telnet
ipv6 access-list SECURE permit icmp6 any
2001:db8:c000:1052::/64

access-group SECURE in interface outside
```

For your reference

ASA and PIX 7.x: 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 2001:db8:c000:1051::138:53 in
2001:db8:c000:1052::7:50118 idle 0:00:02 flags -
TCP out 2001:200:0:8002:203:47ff:fea5:3085:80 in
2001:db8:c000:1052::7:11009 idle 0:00:14 bytes 8975 flags
UfFRIO
TCP out 2001:db8:c000:1051::1:11008 in
2001:db8: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

Enterprise Deployment: Secure IPv6 Connectivity

How to secure IPv6 over the WAN

Secure IPv6 Traffic over IPv6 Public Network

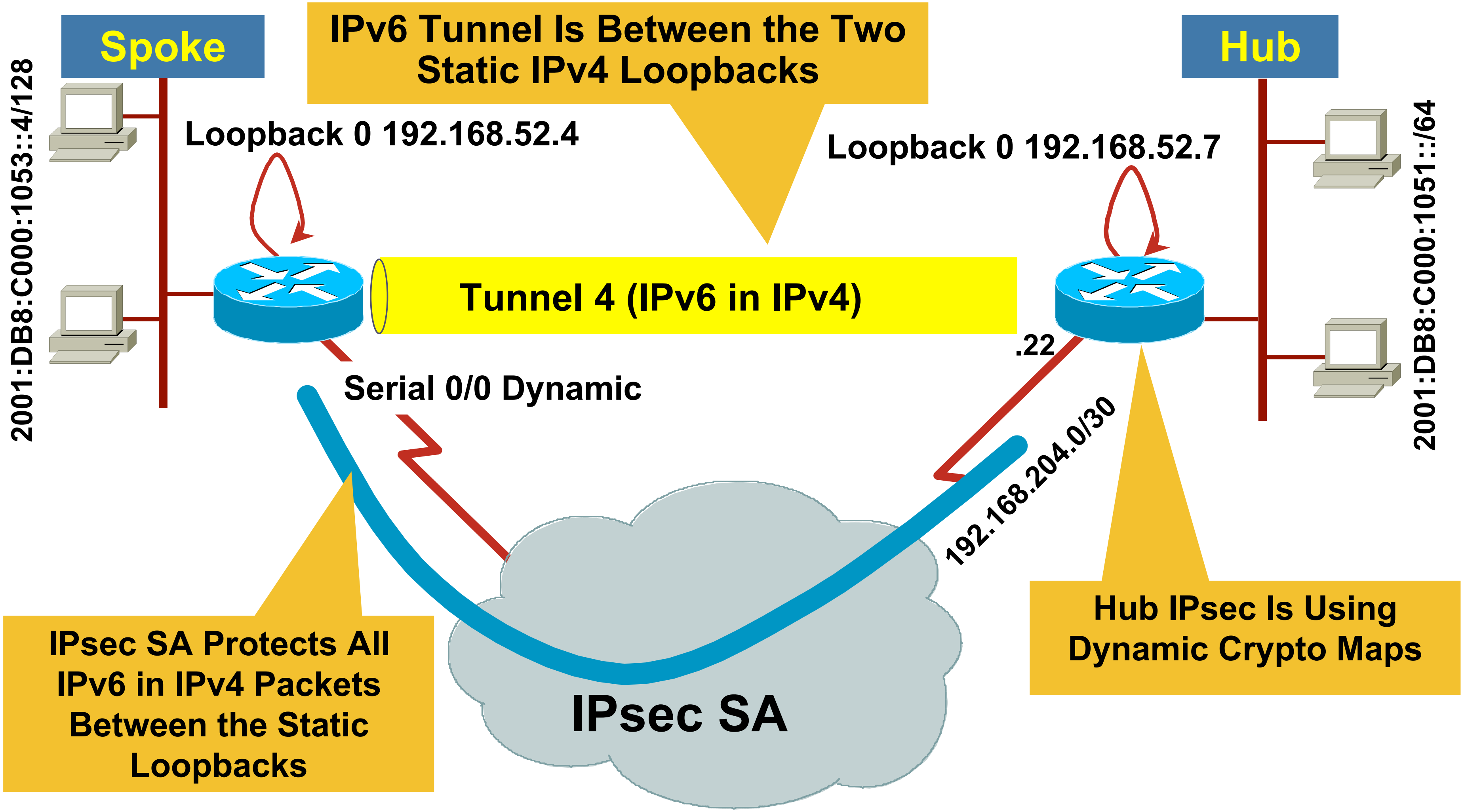
- Since 12.4(6)T, IPsec also works for IPv6
- Using the Virtual Interface

```
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
- Answer is IPsec
  - Site to site: encrypting IPv6 tunnels
  - Remote access: encrypting ISATAP or IPv6 tunnels

Secure Site to Site IPv6 Connectivity Topology



IPv6 Tunnel Is Between the Two Static IPv4 Loopbacks

IPsec SA Protects All IPv6 in IPv4 Packets Between the Static Loopbacks

Hub IPsec Is Using Dynamic Crypto Maps

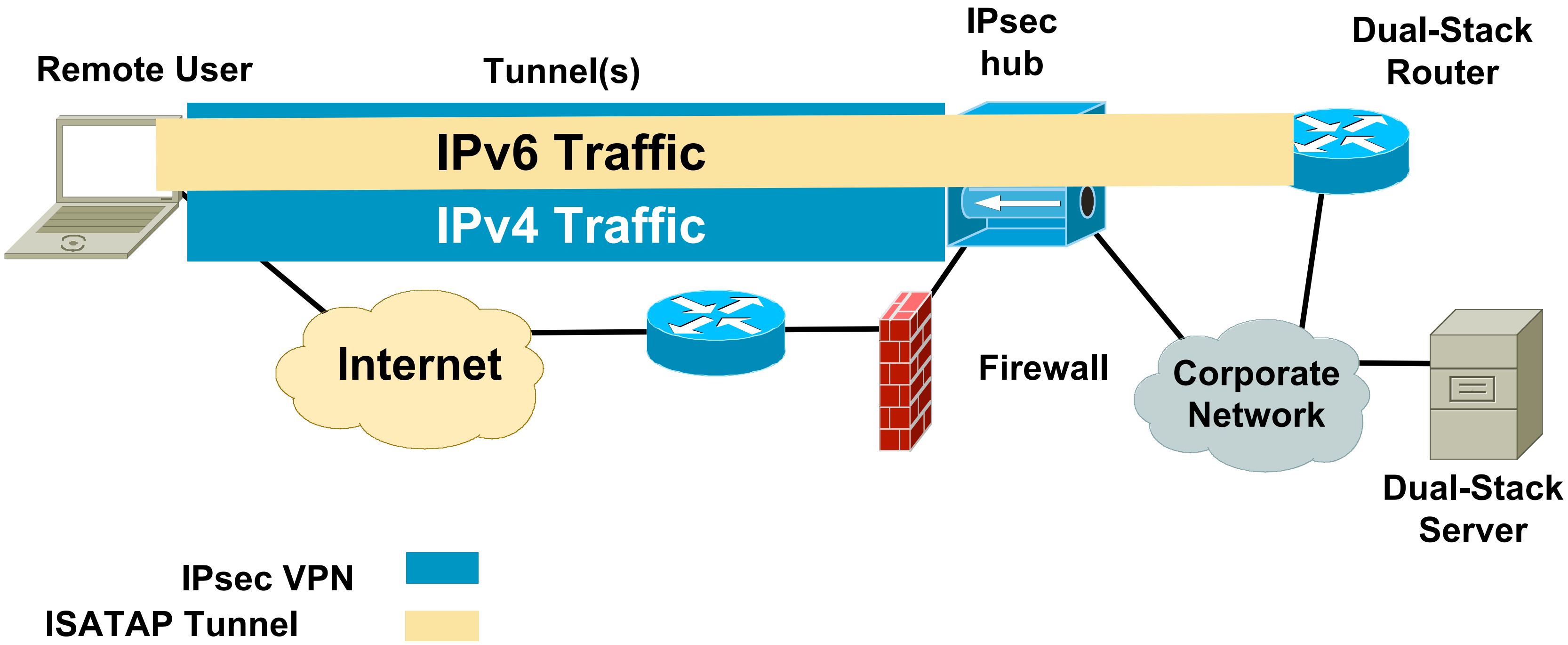
Secure Site to Site IPv6 Connectivity Key Design Points

- 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

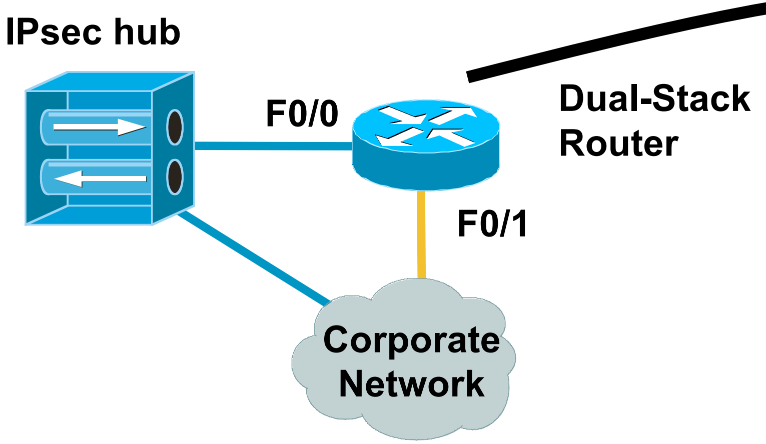
IPv6 for Remote Devices Tunnel Example



Note: The IPsec hub could be a VPN-enabled Cisco IOS Router or ASA/PIX™

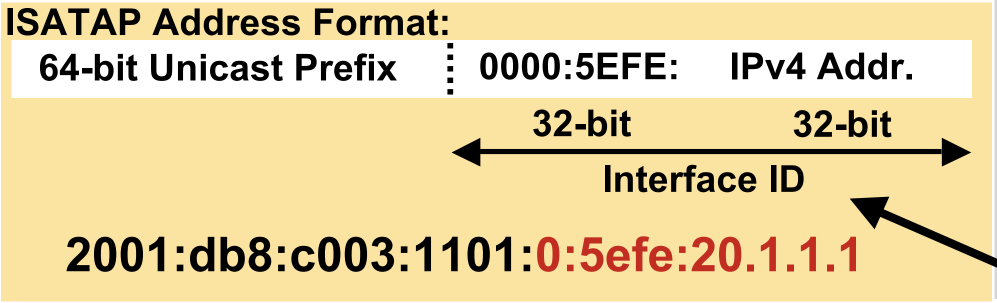
IPv6 for Remote Devices Router Configuration: ISATAP

For your reference



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 2001:db8:C003:111C::2/64
!
interface Tunnel0
no ip address
 ipv6 address 2001:db8:C003:1101::/64
   eui-64
 no ipv6 nd suppress-ra
 tunnel source FastEthernet0/0
 tunnel mode ipv6ip isatap
```



ISATAP Address Format:

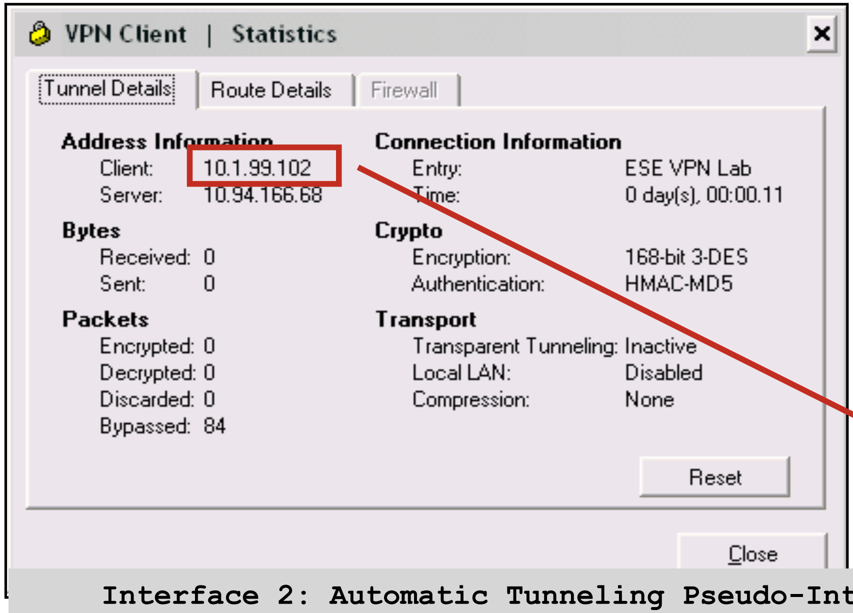
64-bit Unicast Prefix | 0000:5EFE: IPv4 Addr.

32-bit 32-bit

Interface ID

2001:db8:c003:1101:0:5efe:20.1.1.1

IPv6 for Remote Devices
Does It Work?



Address Information
Client: 10.1.99.102
Server: 10.94.166.68

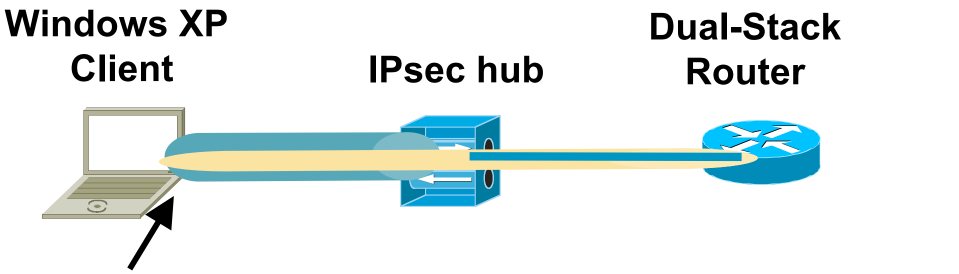
Bytes
Received: 0
Sent: 0

Packets
Encrypted: 0
Decrypted: 0
Discarded: 0
Bypassed: 84

Connection Information
Entry: ESE VPN Lab
Time: 0 day(s), 00:00.11

Crypto
Encryption: 168-bit 3-DES
Authentication: HMAC-MD5

Transport
Transparent Tunneling: Inactive
Local LAN: Disabled
Compression: None



10.1.99.102 - VPN address

2001:db8: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 2001:db8: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  2001:db8: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
- Deploy IPv6, don't wait for a rogue IPv6 network on your infrastructure

Meet the Experts
Security

- Andres Gasson
  Consulting Systems Engineer

- Christophe Paggen
  Technical Marketing Engineer

- Eric Vyncke
  Distinguished Consulting Engineer

- Erik Lenten
  Technical Marketing Engineer

- Fredéric Detienne
  CA Technical Leader

- Luc Billot
  Consulting Engineer

Meet the Experts
Security

- Michael Behringer
  Distinguished System Engineer

- Olivier Dupont
  Corporate Dev Consulting Engineer

- Peter Matthews
  Technical Marketing Engineer

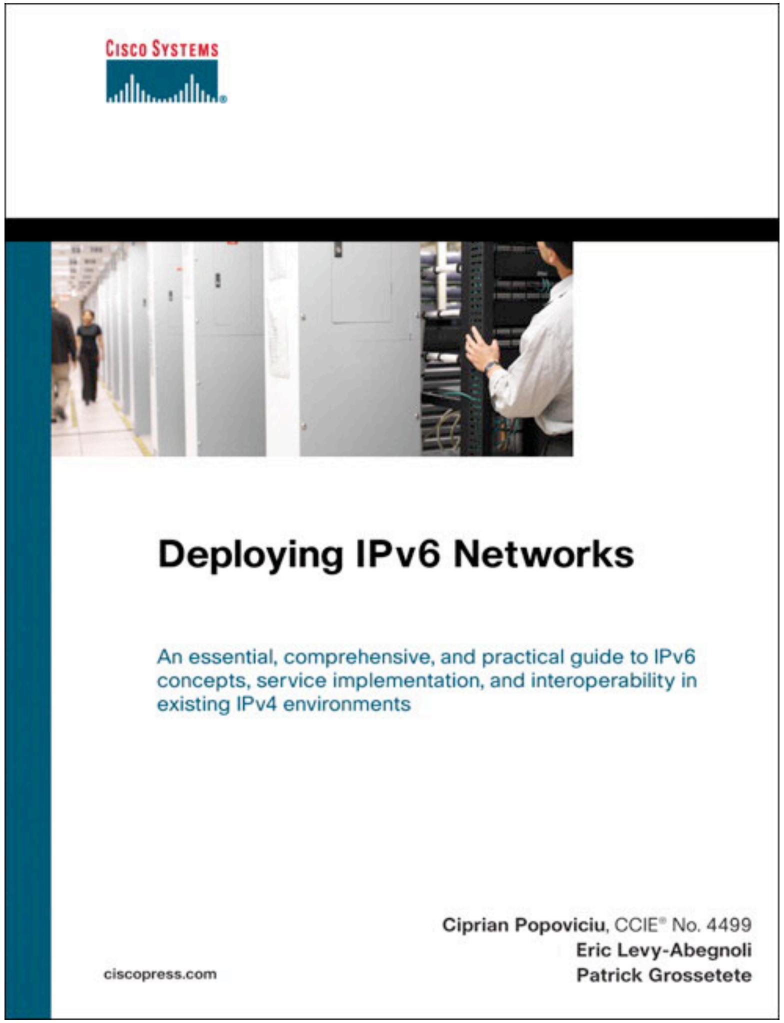
- Scott Wainner
  Distinguished System Engineer

- Steinthor Bjarnason
  Consulting Engineer

Recommended Reading

BRKSEC - 3003

- Deploying IPv6 Networks



Cisco Systems

Deploying IPv6 Networks

An essential, comprehensive, and practical guide to IPv6 concepts, service implementation, and interoperability in existing IPv4 environments

ciscopress.com

Ciprian Popoviciu, CCIE® No. 4499
Eric Levy-Abegnoli
Patrick Grossetete

Available in the Cisco Company Store

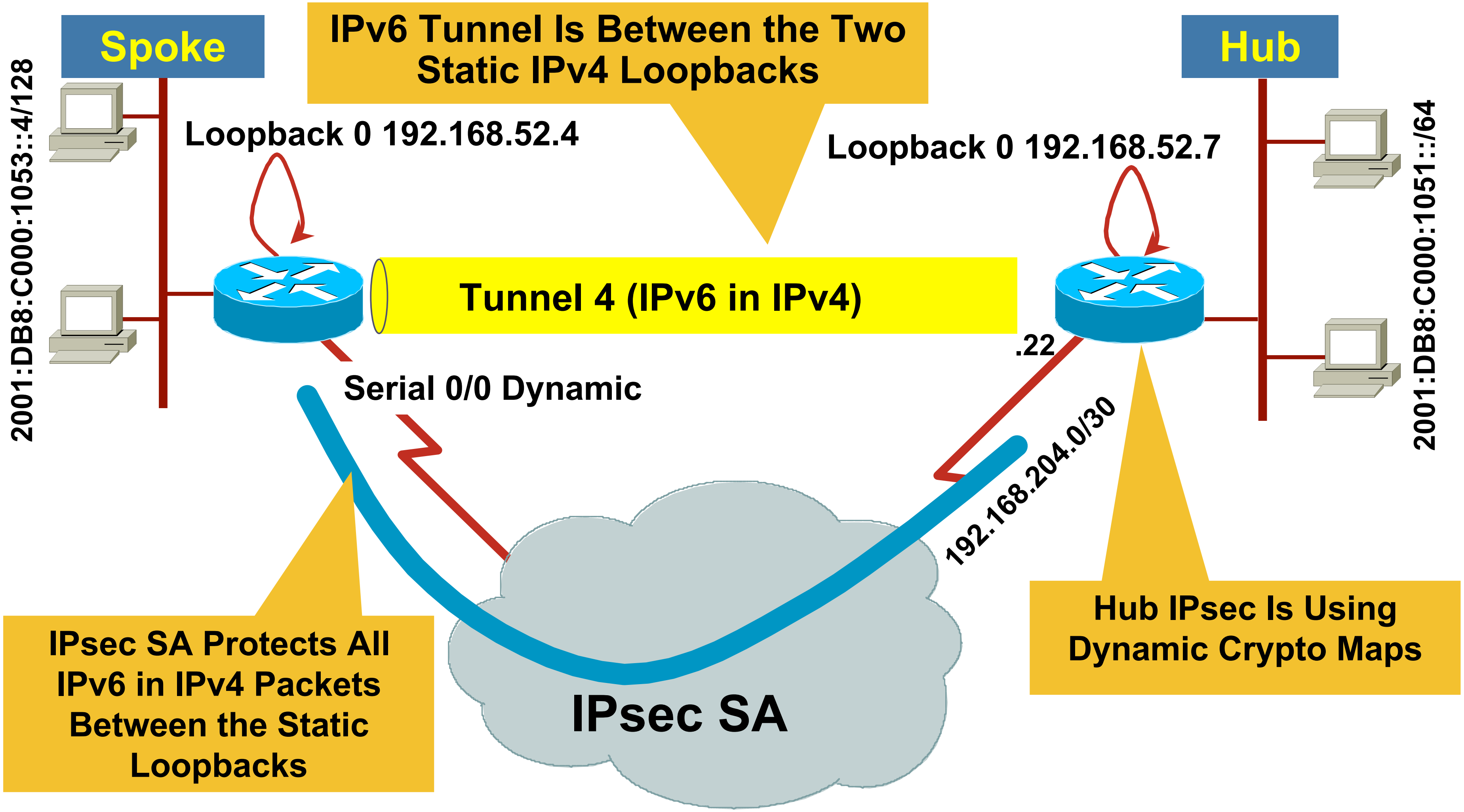
Q and A

Reference Slides

For reference only

For your reference

Secure Site to Site IPv6 Connectivity



IPv6 Tunnel Is Between the Two Static IPv4 Loopbacks

IPsec SA Protects All IPv6 in IPv4 Packets Between the Static Loopbacks

Hub IPsec Is Using Dynamic Crypto Maps

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-3des
!
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.
 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