NETWORKERS 2004

IPv6 SECURITY

SESSION SEC-2003

Introduction

- **Discussions around IPv6 security have centered on IPsec**
  - **Though IPsec is mandatory in IPv6, the same issues with IPsec deployment remain from IPv4:**
    - **Configuration complexity**
    - **Key management**
  - **Many IPv6 stacks do not today support IPsec**
  - **Therefore, IPv6 will be deployed largely without cryptographic protections of any kind**
- **Security in IPv6 is a much broader topic than just IPsec**
  - **Even with IPsec, there are many threats which still remain issues in IP networking**
- **This presentation will cover the rest of the things you should understand to consider the security implications of v6 on your network**

Considerations

Cisco.com

- IPv6 security is a fairly new area, many of the best practices in this presentation could change as new realities with IPv6 security are uncovered by the community
  - Best practices presented here should be viewed as candidates
- This presentation is focused on IPv6 as a technology, not Cisco's implementation of IPv6 security features (we're security geeks, not product managers)
- This presentation assumes that IPv4 security is very familiar to you
- MIPv6 security is not addressed specifically in this presentation

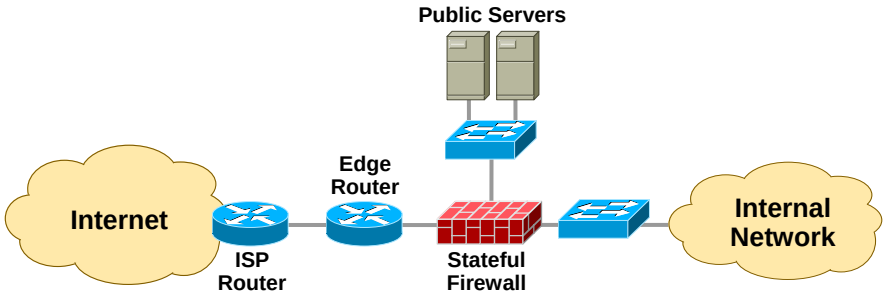
Agenda

Cisco.com

- IPv4 Best Practices Summary and Attack Example
- IPv6 Protocol Summary (Quick, Promise!)
- Types of Threats
- IPv6 and IPv4 Threat Comparisons (The Meat)
- IPv6 Topology and BP Summary
- v6/v4 Dual-Stack Attack Example

Traditional IPv4 Edge Security Design

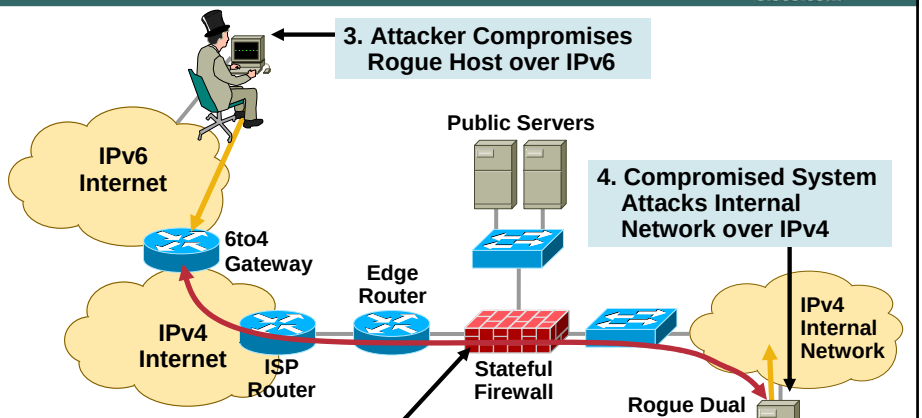
Cisco.com



- This design can be augmented with NIDS, application proxies, and a range of host security controls
- The 3-interface FW design as shown here is in use at thousands of locations worldwide
- Firewall policies are generally permissive outbound and restrictive inbound
- As organizations expand in size, the number of “edges” and the ability to clearly identify them becomes more difficult

IPv6 Attack Against IPv4

Cisco.com



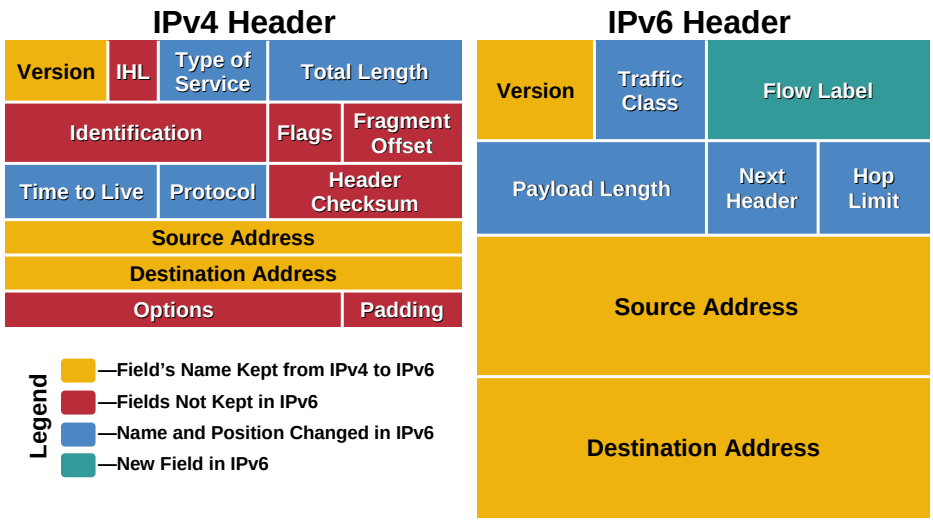
Agenda

Cisco.com

- IPv4 Best Practices Summary and Attack Example
- IPv6 Protocol Summary
  (Quick, Attend RST-1305 for More)
- Types of Threats
- IPv6 and IPv4 Threat Comparisons (The Meat)
- IPv6 Topology and BP Summary
- v6/v4 Dual-Stack Attack Example

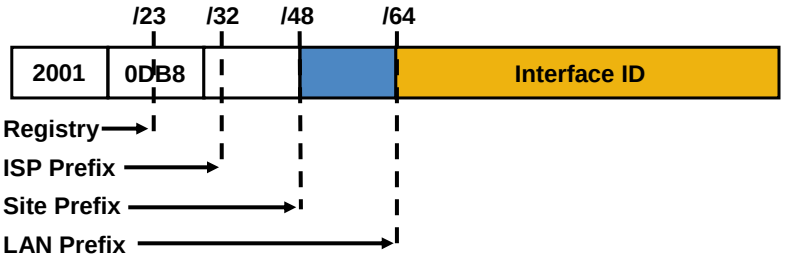
IPv4 and IPv6 Header Comparison

Cisco.com



Address Allocation Policy

Cisco.com



- The allocation process is under reviewed by the registries:
  - IANA allocates 2001::/16 to registries
  - Each registry gets a /23 prefix from IANA
  - Formerly, all ISP were getting a /35
  - With the new policy, Registry allocates a /32 prefix to an IPv6 ISP
  - Then the ISP allocates a /48 prefix to each customer (or potentially /64)
  - ftp://ftp.cs.duke.edu/pub/narten/ietf/global-ipv6-assign-2002-06-26.txt

Address Types

Cisco.com

- Unicast
  - Global
  - Link-local
  - Site-local (deprecated)/local unicast
  - Compatible (IPv4, IPX, NSAP)
- Multicast (one to many)
- Anycast (one to nearest)
- Reserved

IPv6 Addressing per Device

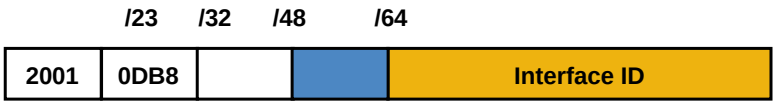
Cisco.com

- In IPv4, devices were restricted to one IPv4 address per interface
- In IPv6, devices have multiple addresses per interface

```
Ethernet0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::201:96FF:FE5B:E161
  Global unicast address(es):
        2001:0DB8:DEEE:19::1, subnet is 2001:0DB8:DEEE:19::/64
  Joined group address(es):
        FF02::1 "All nodes link local multicast"
        FF02::2 "All routers link local multicast"
        FF02::9 "All RIP routers link local multicast"
```


IPv6 Privacy Extensions (RFC 3041)

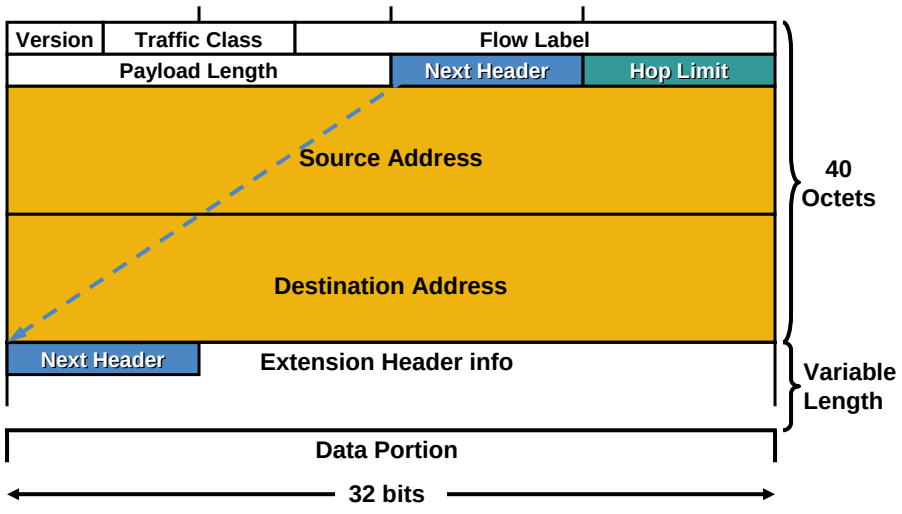
Cisco.com



- 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
  - Implemented on Microsoft Windows XP
  - Recommendation: use privacy extensions for external communication but not for internal networks

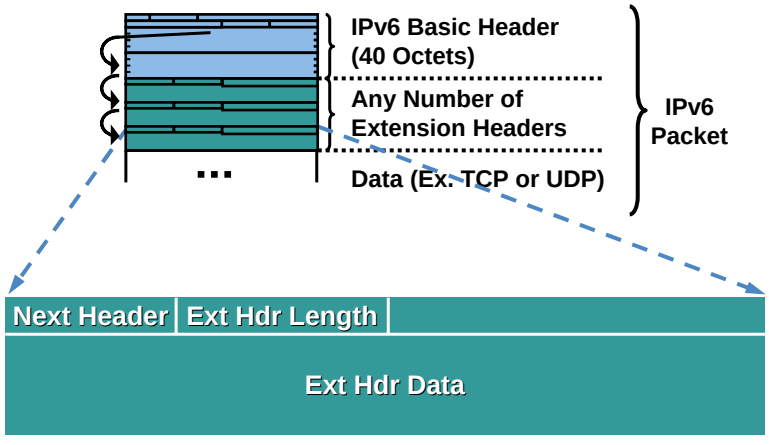
IPv6 Header Format: Next Header

Cisco.com



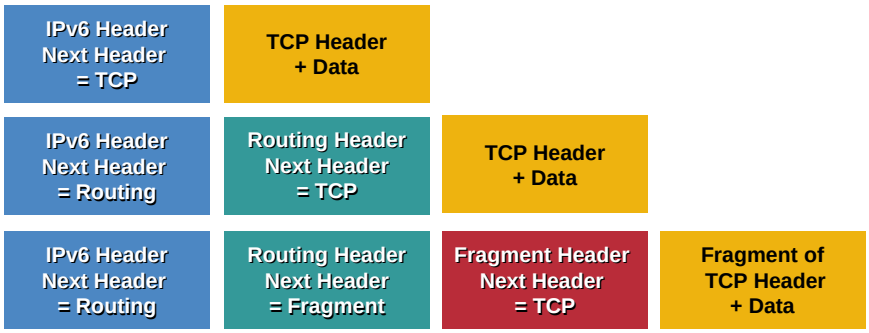
Extension Headers

Cisco.com



IPv6 Header Options (RFC 2460)

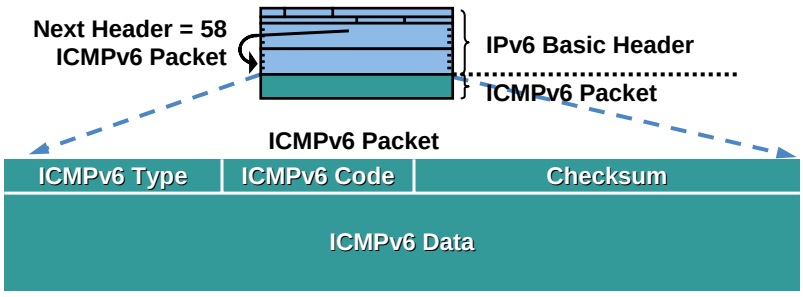
Cisco.com



- Processed only by node identified in IPv6 destination address field => much lower overhead than IPv4 options
  - Exception: hop-by-hop options header
- Eliminated IPv4's 40-octet limit on options
  - In IPv6, limit is total packet size, or path MTU in some cases

ICMPv6

Cisco.com



- ICMPv6 is similar to ICMPv4:
  - Provides diagnostic and error messages
  - Is used for path MTU discovery
  - Runs on top of IPv6
  - Limited security

Agenda

Cisco.com

- IPv4 Best Practices Summary and Attack Example
- IPv6 Protocol Summary
- Types of Threats
- IPv6 and IPv4 Threat Comparisons
- IPv6 Topology and BP Summary
- v6/v4 Dual-Stack Attack Example

Types of Threats (1/2)

Cisco.com

- Reconnaissance—provide the adversary with information enabling other attacks
- Unauthorized Access—exploit the open transport policy inherent in the IPv4 protocol
- Header Manipulation and Fragmentation—evade or overwhelm network devices with carefully-crafted packets
- Layer-3–Layer-4 Spoofing—modify the IP address and port information to mask the intent or origin of the traffic
- ARP and DHCP Attacks—subvert the host initialization process or a device the host accesses for transit
- Broadcast Amplification Attacks (Smurf)—amplify the effect of an ICMP flood by bouncing traffic off of a network which inappropriately processes directed ICMP echo traffic
- Routing Attacks—disrupt or redirect traffic flows in a network

Types of Threats (2/2)

Cisco.com

- **Viruses and Worms—attacks which infect hosts and optionally automate propagation of the malicious payload to other systems**
- **Sniffing—capturing data in transit over a network**
- **Application Layer Attacks—broad category of attacks executed at Layer 7**
- **Rogue Devices—unauthorized devices connected to a network**
- **Man-in-the-Middle Attacks—attacks (generally crypto-based) which involve interposing an adversary between two communicating parties**
- **Flooding—sending bogus traffic to a host or network designed to consume enough resources to delay processing of valid traffic**

Agenda

Cisco.com

- **IPv4 Best Practices Summary and Attack Example**
- **IPv6 Protocol Summary**
- **Types of Threats**
- **IPv6 and IPv4 Threat Comparisons (The Meat)**
- **IPv6 Topology and BP Summary**
- **v6/v4 Dual-Stack Attack Example**

IPv6 and IPv4 Threat Comparisons

Cisco.com

- **Attacks with New Considerations in IPv6**
  - **Reconnaissance**
  - **Unauthorized Access**
  - **Header Manipulation And Fragmentation**
  - **Layer 3–Layer 4 Spoofing**
  - **ARP and DHCP Attacks**
  - **Broadcast Amplification Attacks (Smurf)**
  - **Routing Attacks**
  - **Viruses and Worms**
  - **Translation, Transition, and Tunneling Mechanisms**
- **Attacks with Strong IPv4 and IPv6 Similarities**
  - **Sniffing**
  - **Application Layer Attacks**
  - **Rogue Devices**
  - **Man-in-the-middle Attacks**
  - **Flooding**

Reconnaissance in IPv4

Cisco.com

- **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

Cisco.com

- **Subnet size difference**
  - **Default subnets in IPv6 have 2^{64} addresses (approx. 18 quintillion); scanning every address on a subnet is no longer reasonable (centuries vs. seconds)**
  - **NMAP doesn't even support ping sweeps on IPv6 networks (you'll have retired by the time it finishes, even at one million packets per second)**
  - **There are likely to be ways an attacker seeks to get around this…**

Reconnaissance in IPv6

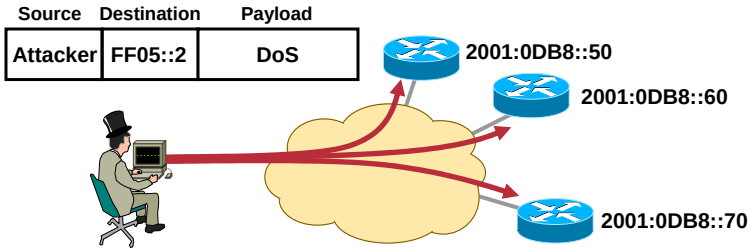
Cisco.com

- **IPv6 scanning methods are likely to change**
  - **Public servers will still need to be DNS reachable giving adversaries SOME hosts to attack**
  - **Decrease in NAT usage will increase dynamic DNS adoption making DNS a likely target**
  - **Administrators may adopt easy to remember addresses (::10, ::20, ::F00D, IPv4 last octet)**
  - **IPv6 addresses derived from IEEE Organizational Unit Identifier (OUI) designations, allow scanning focus on popular NIC vendor's ranges**
  - **Compromised routers at key transit points**

Reconnaissance in IPv6

Cisco.com

- New multicast addresses—IPv6 supports new multicast addresses that can enable an adversary to identify key resources on a network and attack them
  - 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

Cisco.com

- Implement privacy extensions carefully—using them everywhere will complicate attack traceback and troubleshooting within your own organization
- Filter internal-use IPv6 addresses at organization border routers—prevent addresses like the all-nodes multicast address from becoming conduits for attack
- Use standard, but nonobvious static addresses for critical systems—try something a bit more complicated than ::1 for your default gateways (perhaps ::DEF1)
- 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 (though less security technologies are able to deal with IPv6 security)

IPv6 and IPv4 Threat Comparisons

Cisco.com

- **Attacks with New Considerations in IPv6**
  - Reconnaissance
  - Unauthorized Access
  - Header Manipulation and Fragmentation
  - Layer 3–Layer 4 Spoofing
  - ARP and DHCP Attacks
  - Broadcast Amplification Attacks (Smurf)
  - Routing Attacks
  - Viruses and Worms
  - Translation, Transition, and Tunneling Mechanisms
- **Attacks with Strong IPv4 and IPv6 Similarities**
  - Sniffing
  - Application Layer Attacks
  - Rogue Devices
  - Man-in-the-Middle Attacks
  - Flooding

IPv6 and IPv4 Threat Comparisons

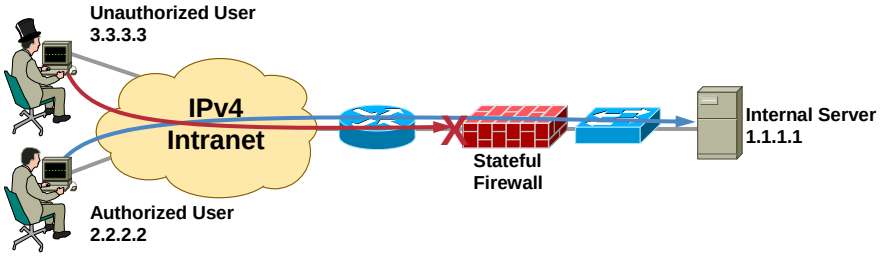
Cisco.com

- **Unauthorized Access**
  - General
  - ICMP
  - Multicast

Unauthorized Access in IPv4

Cisco.com

- Authorizing access to computer systems is a policy decision that is often implemented in IPv4 with Layer-3 and Layer-4 filtering (no kidding…)

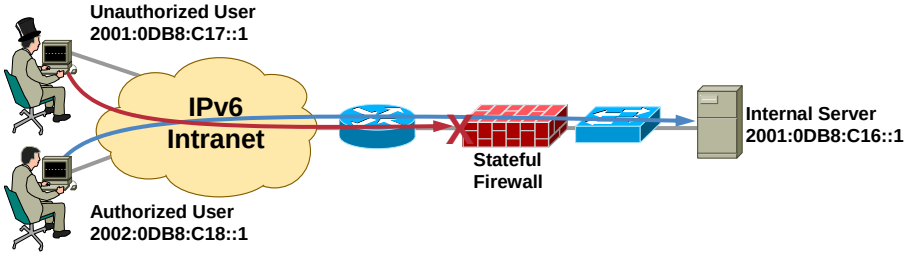


Action	Src	Dest	Src Port	Dst Port
Permit	2.2.2.2	1.1.1.1	Any	ssh
Deny	Any	Any		

Unauthorized Access in IPv6

Cisco.com

- Implementation of policy in IPv6 still relies on access control being implemented using Layer-3 and Layer-4 information
- IPv6 has some unique considerations that must be considered in order to implement their policy correctly

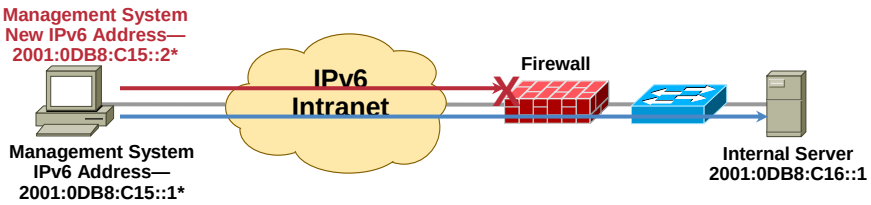


Action	Src	Dest	Src Port	Dst Port
Permit	2001:0DB8:C18::1	2001:0DB8:C16::1	Any	ssh
Deny	Any	Any		

Privacy Extensions Considerations

Cisco.com

- Privacy extensions limit the exposure to a security threat that targets a host IPv6 address directly
- This is great for making an end host harder to identify to an attacker, but it also makes an end host harder to identify to the network administrator



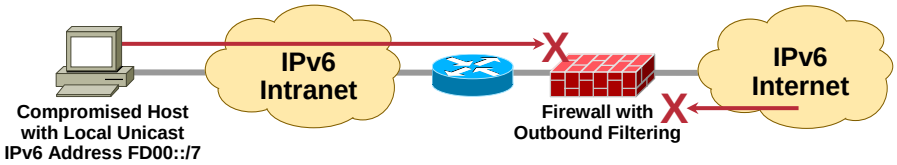
Action	Src	Dest	Src Port	Dst Port
Permit	2001:0DB8:C15::1	2001:0DB8:C16::1	Any	80
Deny	Any	Any		

* Not Real RFC3041 Derived Addresses

Local Unicast Filtering

Cisco.com

- IPv6 allows multiple addresses on one adapter: link local, local unicast* and global



Action	Src	Dest	Src Port	Dst Port
Deny	FD00::/7	Any		
Deny	Any	FD00::/7		

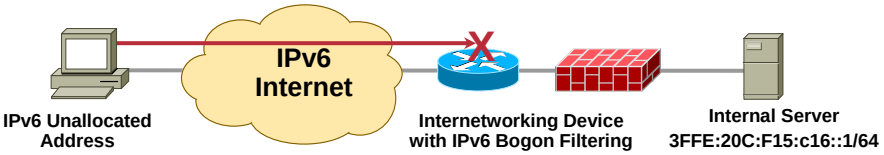
- With the use of the local unicast addressing an enterprise can automatically deny inbound and outbound access for the enterprise-only services
  - By filtering the route to FD00::/7, explicit ACLs may not even be necessary

*http://www.ietf.org/internet-drafts/draft-ietf-ipv6-unique-local-addr-03.txt

Bogon Filtering in IPv6

Cisco.com

- IPv6 bogon filtering is significantly different from IPv4 bogon filtering
- In IPv4, because so much of the IPv4 range has been allocated, it is generally easier to block bogons than it is to permit non-bogons
- In IPv6, only three top-level aggregation identifiers (TLAs) have been allocated thus far; therefore, ACLs can permit these ranges (and certain multicast ranges if used) and block all other IPv6 traffic

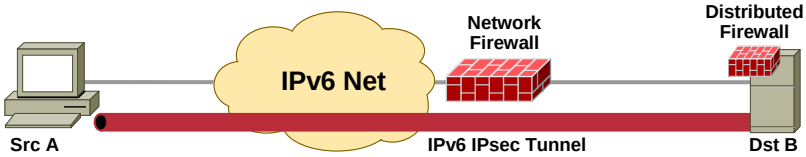


Action	Src	Dest	Src Port	Dst Port
Permit	2001::/16	3FFE:20C:F15:C16::/64	Any	Any
Permit	2002::/16	3FFE:20C:F15:C16::/64	Any	Any
Permit	3FFE::/16	3FFE:20C:F15:C16::/64	Any	Any
Deny	Any	Any		

IPsec Filtering Considerations

Cisco.com

- IPsec with encryption makes current network-based firewalls blind to the upper-layer information
- Distributed (personal) firewalls can see the packet after decryption
- IPsec with AH does not do encryption, but does provide integrity; AH is not widely used in IPv4 and in some instances not supported in the IPsec implementation

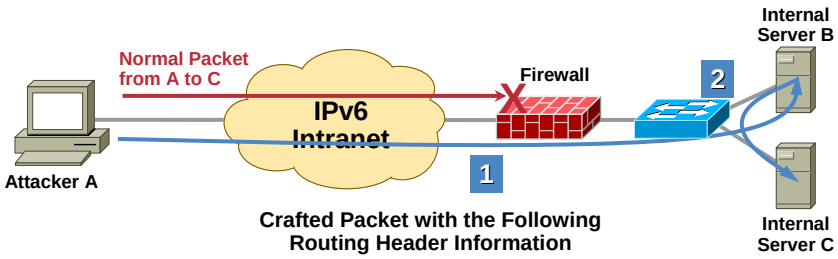


Src A Dst B	ESP HDR	&*^(UYGOUHG&^%HI		What the Network Firewall Sees
Src A Dst B	UDP HDR	Data		What the Distributed Firewall Sees
Src A Dst B	AH HDR	UDP HDR	Data	What the Network Firewall Sees with AH

Routing Header Considerations (1/2)

Cisco.com

- All IPv6 endpoints are required to accept IPv6 packets with a routing header
- It is theoretically possible that in addition to accepting IPv6 packets with routing headers, end hosts also process routing headers and forward the packet



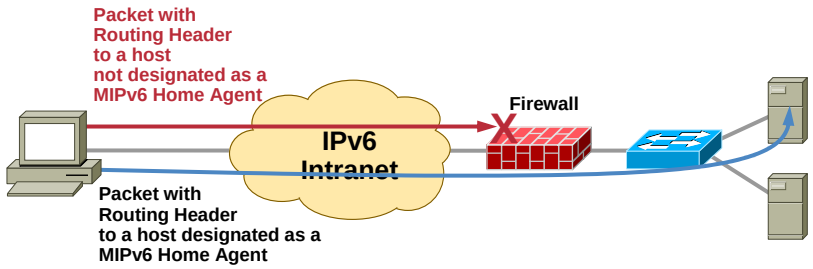
Crafted Packet with the Following Routing Header Information

Packet	Src	Dst	dport	Rt Header Segs Left	Rt Header Address
1	A	B	53	1	C
2	A	C	53	0	B

Routing Header Considerations (2/2)

Cisco.com

- The network designer should validate that the operating systems within their organization do not forward packets that include a routing header
- A specific set of nodes should be designated as MIPv6 home agents; if MIPv6 is not needed the network manager can filter IPv6 packets that contain the routing header at an access control device



IPv6 and IPv4 Threat Comparisons

Cisco.com

- **Unauthorized Access**
  - **General**
  - **ICMP**
  - **Multicast**

ICMPv4 vs. ICMPv6

Cisco.com

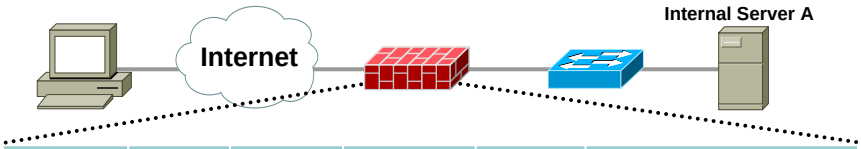
- **ICMPv6 has changed significantly from ICMPv4 and is more heavily relied upon within IPv6 that it was in IPv4**

ICMP Message Type	ICMPv4	ICMPv6
Reachability 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

- **With this in mind ICMP policy on firewalls needs to change to accommodate the changes in ICMPv6**

Generic ICMPv4 Border Firewall Policy

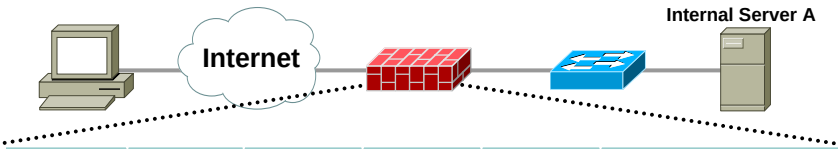
Cisco.com



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

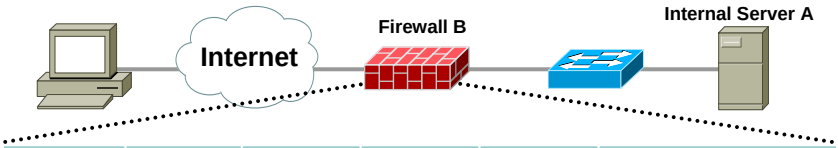
Cisco.com



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

Cisco.com



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

IPv6 and IPv4 Threat Comparisons

Cisco.com

- Unauthorized Access
  - General
  - ICMP
  - Multicast

Multicast and Transparent Firewalls

Cisco.com

- Firewalls must at a minimum allow link-local multicast traffic to the device (FF02::/10)
- In transparent mode a firewall must understand all the new uses of ICMPv6 and allow filters to be defined for each case
- For instance, a transparent firewall must allow the definition of FF02::1 since this is the link local all nodes multicast address
- Another example that the transparent firewall needs to forward is the all routers link-local multicast address (FF02::2)

Unauthorized Access Best Practices

Cisco.com

- Determine what extension headers will be allowed through the access control device—network designers should match their IPv6 extension header policy closely to their IPv4 IP options policy
- Determine which ICMPv6 messages are required through the access control device and apply filters appropriately—it is recommended that administrators map their ICMPv6 policy closely to the equivalent ICMPv4 policy with the following additions:
  - ICMPv6 Type 2—Packet too big
  - ICMPv6 Type 4—Parameter problem
  - ICMPv6 Type 130-132—Multicast listener
  - ICMPv6 Type 133/134—Router solicitation and router advertisement
  - ICMPv6 Type 135/126—Neighbor solicitation and neighbor advertisement

IPv6 and IPv4 Threat Comparisons

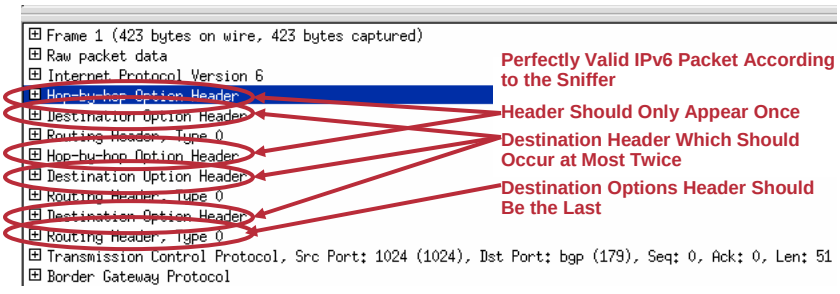
Cisco.com

- **Attacks with New Considerations in IPv6**
  - Reconnaissance
  - Unauthorized Access
  - Header Manipulation and Fragmentation
  - Layer 3–Layer 4 Spoofing
  - ARP and DHCP Attacks
  - Broadcast Amplification Attacks (Smurf)
  - Routing Attacks
  - Viruses and Worms
  - Translation, Transition, and Tunneling Mechanisms
- **Attacks with Strong IPv4 and IPv6 Similarities**
  - Sniffing
  - Application Layer Attacks
  - Rogue Devices
  - Man-in-the-Middle Attacks
  - Flooding

Header Manipulation

Cisco.com

- **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 on a host if I feed it an large set of extension headers



Fragmentation Attacks in IPv4

Cisco.com

- Great evasion techniques
- Tools like whisker, fragroute…
- Makes firewall and network intrusion detection harder
- Used mostly in DoSing hosts, but can be used for attacks that compromise the host
- Ptacek and Newsham—Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection

  http://www.insecure.org/stf/secnet_ids/secnet_ids.pdf

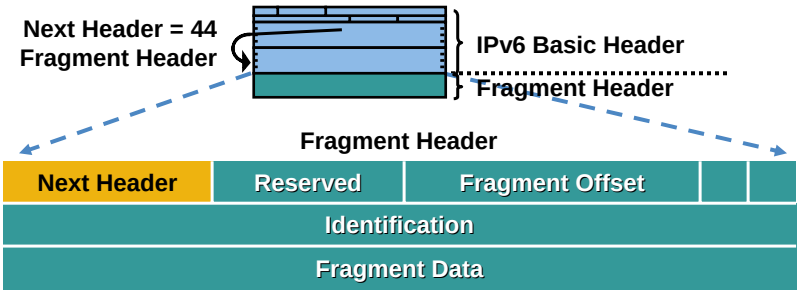
Fragmentation Filtering in IPv4

Cisco.com

- In IPv4, you can use the fragment keyword for an extended ACL
- The only packets that will match are those that have fragment offset != 0, that is, noninitial fragments
- For IPv4 we know the protocol and fragments flags and offset from the IP header, so we can easily calculate if enough of the Upper Layer Protocol (ULP) is within the first fragment (likely)
- First fragments and nonfragmented packets go through the normal “extract L4 info” process

Fragment Header: IPv6

Cisco.com

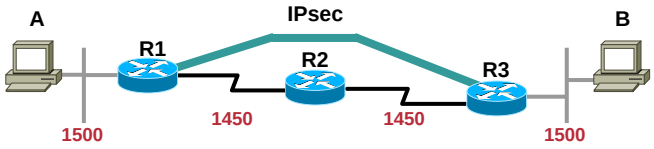


- In IPv6 fragmentation is done ONLY by the end system
- Reassembly done by end system like in IPv4

IPv6 Fragmentation: Path MTU Discovery

Cisco.com

- IPsec tunnel: esp-des/esp-md5-hmac = 56 bytes overhead



At R1 IPsec SA: Path MTU is 1450

A → B
Packet = 1480 Bytes

A ← R1
ICMPv6 Type 2,
Code 0 (MTU = 1394)
"Packet Too Big"

A → B
Packet = 1394 Bytes

But:
Available MTU Next Link = 1450 - 56 = 1394
Packet Size > 1394

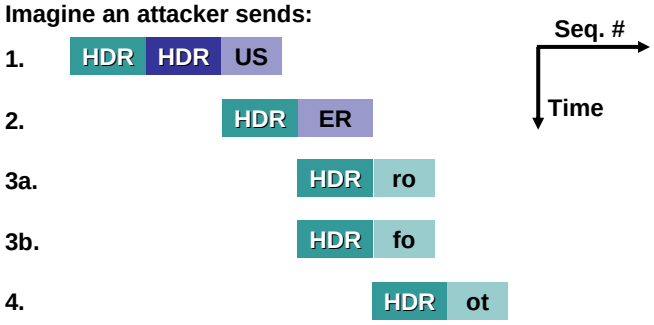
Only End Node Can Fragment in IPv6

IPv6 Fragmentation: Still Needs Reassembly in the Firewall and NIDS

Cisco.com

- Fragmentation is still a great obfuscation tool

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

IPv6 Fragmentation: Issues for Non-Stateful Filtering Devices IPv6

Cisco.com

- For IPv6, we must traverse the Next Headers (NHs) before reaching the fragment header to extract the flags and offset
- Then, we may need to traverse further NHs before reaching the Upper Layer Protocol (ULP) and then check if enough of the ULP header is within the first fragment
- This makes matching against the first fragment non-deterministic: tcp/udp/icmp might not be there
- For IPv6, the fragment keyword matches noninitial fragments (same as IPv4) AND the first fragment if the protocol cannot be determined

Note: Cisco IOS Also Supports a New Keyword “undetermined-transport” which Matches Any IPv6 Packet where the Layer 4 Cannot Be Determined

Header Manipulation and Fragmentation Best Practices

Cisco.com

- **Deny IPv6 fragments destined to an internetworking device—used as a DoS vector to attack the infrastructure**
- **Ensure adequate IPv6 header filtering capabilities—for example, drop all packets with the routing header if you don't have MIPv6**

IPv6 and IPv4 Threat Comparisons

Cisco.com

- **Attacks with New Considerations in IPv6**
  - **Reconnaissance**
  - **Unauthorized Access**
  - **Header Manipulation and Fragmentation**
  - **Layer 3—Layer 4 Spoofing**
  - **ARP and DHCP Attacks**
  - **Broadcast Amplification Attacks (Smurf)**
  - **Routing Attacks**
  - **Viruses and Worms**
  - **Translation, Transition, and Tunneling Mechanisms**
- **Attacks with Strong IPv4 and IPv6 Similarities**
  - **Sniffing**
  - **Application Layer Attacks**
  - **Rogue Devices**
  - **Man-in-the-Middle Attacks**
  - **Flooding**

L3–L4 Spoofing in IPv4

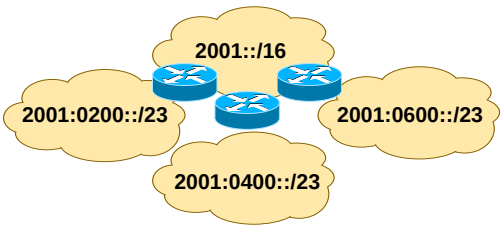
Cisco.com

- L3 spoofing is very common in IPv4, RFC 2827 defines mechanisms to largely eliminate L3 spoofing but this has not seen broad adoption
  - IPv4 addresses do not globally summarize (120,000 routes in the global BGP table); this makes RFC 2827 a network-by-network implementation effort
    - Note that RFC 2827 stops the spoofing of the network portion of an IP address, not the host portion
- 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 bogon filtering

L3–L4 Spoofing in IPv6

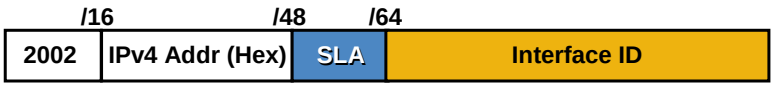
Cisco.com

- While L4 spoofing remains the same, IPv6 address are globally aggregated making spoof mitigation at aggregation points easy to deploy
  - 2001::/16—IPv6 production
  - 2002::/16—6to4 tunneling
  - 3FFE::/16—6 bone testing
  - Unfortunately each subnet (even at the local level) still has a huge range of addresses to spoof



L3–L4 Spoofing in IPv6 (via 6to4)

Cisco.com

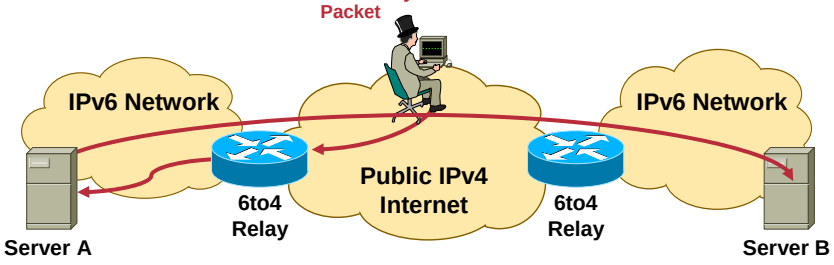


- Some of the IPv4—IPv6 tunneling mechanisms can be a conduit for spoofed traffic

IPv4 Src: Spoofed IPv4 Address
IPv4 Dst: 6to4 Relay
IPv6 Src: Spoofed Source Server B
IPv6 Dst: Server A

6to4 ACLs Are Ineffective Since IPv4 Is Spoofed
6to4 Relay Strips the IPv4 Header So Traceback Is Difficult
6to4 Relay Forwards the Inner Packet

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



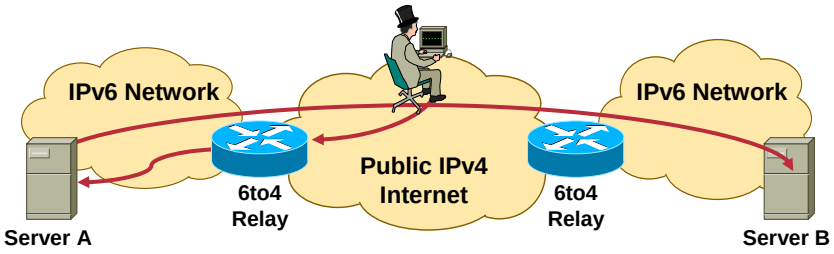
L3–L4 Spoofing in IPv6 (via 6to4)

Cisco.com

- Harm is limited
- 1:1 ratio of packets—no amplification attack
- There is a chokepoint

- Attacker chooses the relays; some relays use the 6to4 anycast address (192.88.99.1); tracing is more difficult
- Attacker might spoof the 6to4 relay's address making it seem to be the source of the attack

- Can be somewhat mitigated
- Checks within the 6to4 relay to not accept 6to4 addresses (ex. 192.88.99.1)



IPv6 and IPv4 Threat Comparisons

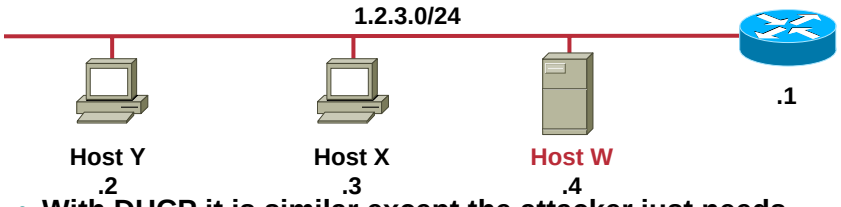
Cisco.com

- **Attacks with New Considerations in IPv6**
  - Reconnaissance
  - Unauthorized Access
  - Header Manipulation and Fragmentation
  - Layer 3–Layer 4 Spoofing
  - ARP and DHCP Attacks
  - Broadcast Amplification Attacks (Smurf)
  - Routing Attacks
  - Viruses and Worms
  - Translation, Transition, and Tunneling Mechanisms
- **Attacks with Strong IPv4 and IPv6 Similarities**
  - Sniffing
  - Application Layer Attacks
  - Rogue Devices
  - Man-in-the-Middle Attacks
  - Flooding

ARP and DHCP Attacks in IPv4

Cisco.com

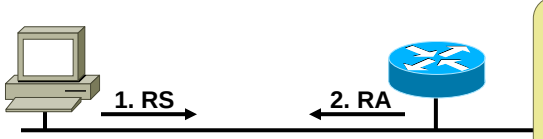
- **With ARP misuse host W can claim to be the default gateway and hosts X and Y will route traffic through him; ARP has no notion of ownership of IP or MAC addresses**



- **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

Cisco.com



ICMP w/o IPsec AH 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

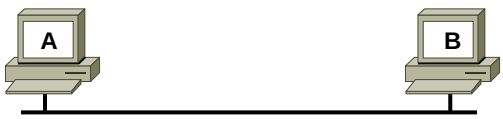
2. RA:

- ICMP Type = 134
- Src = Router Link
- Dst = All-Node
- Data = Options, Prefix, Lifetime, Autoconfig Flag

Router Solicitation Are Sent by Booting Nodes to Request RAs for Configuring the Interfaces

Neighbor Discovery: Neighbor Solicitation

Cisco.com



ICMP Type = 135
Src = A
Dst = Solicited-Node Multicast of B
Data = Link-Layer Address of A
Query = What Is Your Link Address?

Security Mechanisms Built into Discovery Protocol = None;

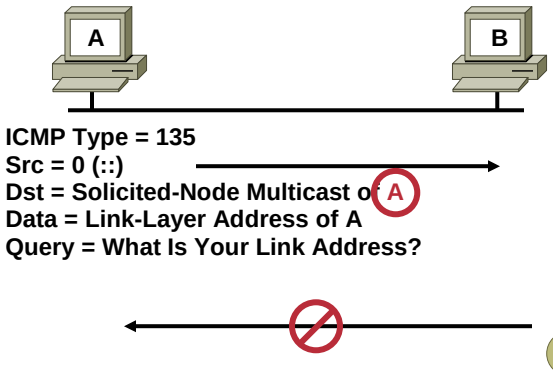
Another Bootstrap Security Problem!

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)

Cisco.com



From RFC 2462:

«If a Duplicate @ Is Discovered…the Address CANNOT Be Assigned to the Interface…»

What If: Use MAC Addr of the Node You Want to DoS and Fabricate its IPv6 Addr

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

ARP and DHCP Best Practices

Cisco.com

- Use static neighbor entries for critical systems—a static entry to its default router avoids many of the typical neighbor-discovery attacks
  - This is a very administratively burdensome practice and should not be undertaken lightly
- SEcure Neighbor Discovery (SEND)—IETF proposed standard to secure the neighbor discover process
  - Relies on private/public key cryptography with digital signatures
  - Crypogaphically binds public signature keys with IPv6 addresses through the use of hashes
  - http://www.potaroo.net/ietf/ids-wg-send.html

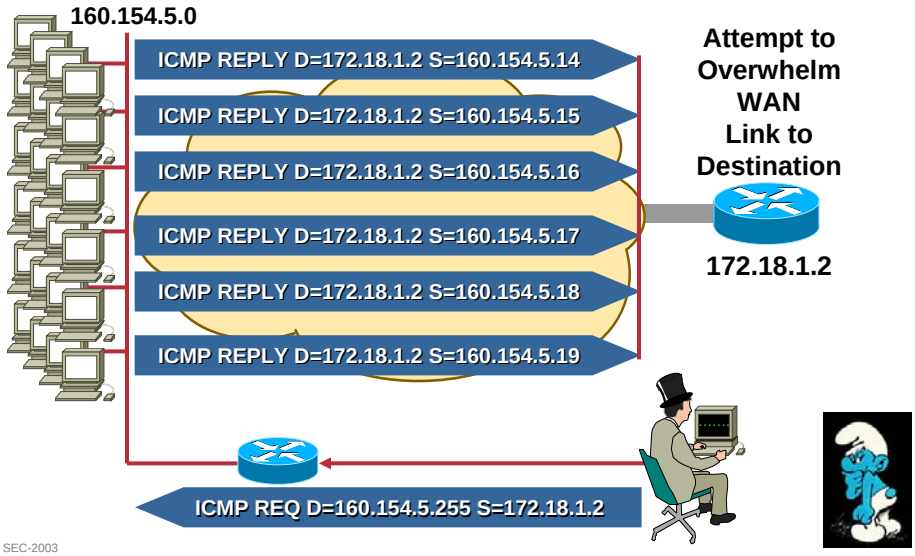
IPv6 and IPv4 Threat Comparisons

Cisco.com

- **Attacks with New Considerations in IPv6**
  - Reconnaissance
  - Unauthorized Access
  - Header Manipulation and Fragmentation
  - Layer 3–Layer 4 Spoofing
  - ARP and DHCP Attacks
  - Broadcast Amplification Attacks (Smurf)
  - Routing Attacks
  - Viruses and Worms
  - Translation, Transition, and Tunneling Mechanisms
- **Attacks with Strong IPv4 and IPv6 Similarities**
  - Sniffing
  - Application Layer Attacks
  - Rogue Devices
  - Man-in-the-Middle Attacks
  - Flooding

Smurf Attack

Cisco.com



IPv6 and Broadcasts

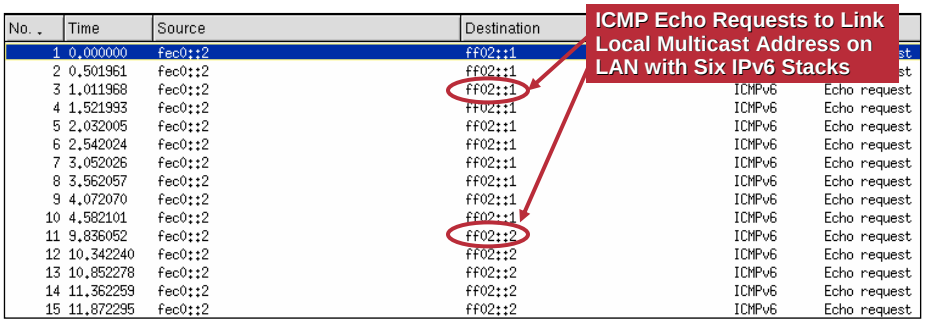
Cisco.com

- 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

Cisco.com

- Specific mention is made in ICMPv6 RFC that no ICMP 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 section 2.4 (e.2)
- Fraggle (UDP echo) attacks are still theoretically possible



No.	Time	Source	Destination		
1	0.000000	fec0::2	ff02::1		
2	0.501961	fec0::2	ff02::1		
3	1.011968	fec0::2	ff02::1	ICMPv6	Echo request
4	1.521993	fec0::2	ff02::1	ICMPv6	Echo request
5	2.032005	fec0::2	ff02::1	ICMPv6	Echo request
6	2.542024	fec0::2	ff02::1	ICMPv6	Echo request
7	3.052026	fec0::2	ff02::1	ICMPv6	Echo request
8	3.562057	fec0::2	ff02::1	ICMPv6	Echo request
9	4.072070	fec0::2	ff02::1	ICMPv6	Echo request
10	4.582101	fec0::2	ff02::1	ICMPv6	Echo request
11	9.836052	fec0::2	ff02::2	ICMPv6	Echo request
12	10.342240	fec0::2	ff02::2	ICMPv6	Echo request
13	10.852278	fec0::2	ff02::2	ICMPv6	Echo request
14	11.362259	fec0::2	ff02::2	ICMPv6	Echo request
15	11.872295	fec0::2	ff02::2	ICMPv6	Echo request

Best Practices for Amplification Attacks

Cisco.com

- There are no broadcasts in IPv6!
- Implement filtering of packet with IPv6 multicast src/dst addresses where possible
  - Lots of new multicast address that have site and global reachability
  - Limited valid reasons for a multicast source address, so the administrator should drop any packets with a multicast source address at the border of the network

IPv6 and IPv4 Threat Comparisons

Cisco.com

- Attacks with New Considerations in IPv6
  - Reconnaissance
  - Unauthorized Access
  - Header Manipulation and Fragmentation
  - Layer 3–Layer 4 Spoofing
  - ARP and DHCP Attacks
  - Broadcast Amplification Attacks (Smurf)
  - Routing Attacks
  - Viruses and Worms
  - Translation, Transition, and Tunneling Mechanisms
- Attacks with Strong IPv4 and IPv6 Similarities
  - Sniffing
  - Application Layer Attacks
  - Rogue Devices
  - Man-in-the-Middle Attacks
  - Flooding

IPv4 Routing Attacks

Cisco.com

- The primary purpose of IPv4 routing attacks are to disrupt/corrupt router peering or routing information
- An attacker may be able to:
  - Source packets which are delivered to the router under attack
  - Configure a router through console access or some other means
  - Attach to the network and act as a part of the routing domain
- You need to protect:
  - Routers from being compromised
  - Peering sessions between routers
  - The routing topology and reachability information from false information

IPv6 Routing Attacks

Cisco.com

- The exact same purpose, requirements, and protection are applicable in IPv6 routing
- BGP, ISIS, EIGRP session protections don't change for IPv6
- Typically this is an MD5 authentication of the routing update
- OSPFv3 has changed
  - MD5 authentication pulled from the protocol and instead relies on 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 as vendor implementations allow

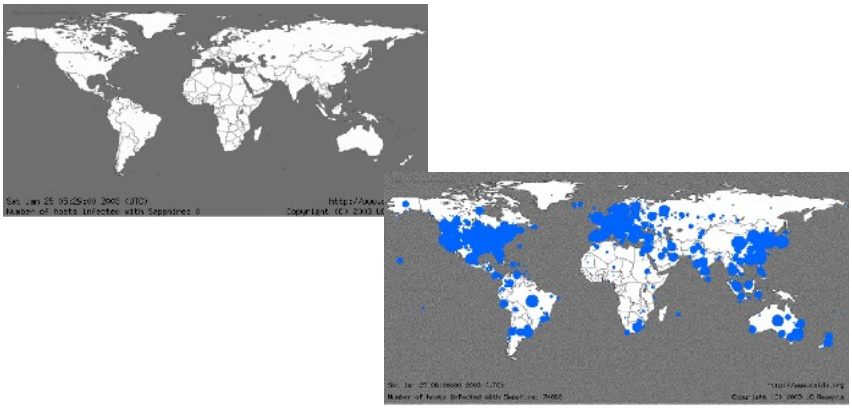
IPv6 and IPv4 Threat Comparisons

Cisco.com

- **Attacks with New Considerations in IPv6**
  - Reconnaissance
  - Unauthorized Access
  - Header Manipulation and Fragmentation
  - Layer 3–Layer 4 Spoofing
  - ARP and DHCP Attacks
  - Broadcast Amplification Attacks (Smurf)
  - Routing Attacks
  - Viruses and Worms
  - Translation, Transition, and Tunneling Mechanisms
- **Attacks with Strong IPv4 and IPv6 Similarities**
  - Sniffing
  - Application Layer Attacks
  - Rogue Devices
  - Man-in-the-Middle Attacks
  - Flooding

Viruses and Worms in IPv4

Cisco.com



- **Slammer infected most of the IPv4 Internet in 10 minutes (75,000 hosts infected in one-half hour)**

Source caida.org

Viruses and Worms in IPv6

Cisco.com

- 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 1 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
  - Let's take a look at the same animation this time simulating how slammer might fare in an all IPv6 Internet:

- 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 and IPv4 Threat Comparisons

Cisco.com

- Attacks with New Considerations in IPv6
  - Reconnaissance
  - Unauthorized Access
  - Header Manipulation and Fragmentation
  - Layer 3–Layer 4 Spoofing
  - ARP and DHCP Attacks
  - Broadcast Amplification Attacks (Smurf)
  - Routing Attacks
  - Viruses and Worms
  - Translation, Transition, and Tunneling Mechanisms
- Attacks with Strong IPv4 and IPv6 Similarities
  - Sniffing
  - Application Layer Attacks
  - Rogue Devices
  - Man-in-the-Middle Attacks
  - Flooding

IPv6 Transition Techniques

Cisco.com

- There are numerous ways proposed to transition from an IPv4 to IPv6
- The primary ways can be categorized in the following manner
  - Dual stack
  - Tunneling
  - Translation
- IPv6 tunneling and translation are the two techniques most commonly identified as having a security impact for an enterprise; while they deserve consideration…
  - http://www.6net.org/publications/standards/draft-savola-v6ops-6to4-security-02.txt

IPv6 Translation, Transition, and Tunneling

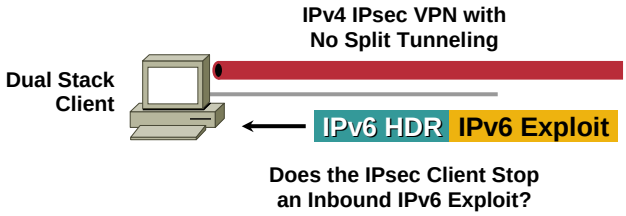
Cisco.com

- Tunneling and address translation are security issues regardless of protocol
- Tunneling—ICMP tunneling, IPv4 over HTTP, etc.
  - These have been covert channels for attackers for many years
  - IPv6 tunnels are only another avenue of attack for the adversary
- NAT has been a challenge to security as well
- NAT limits the ability to trace an attack to a source machine
  - IPv4 NAT has been known to break applications and security
  - For example, an internet draft was developed to make IPsec work nicely with NAT. :-)

IPv6 Translation, Transition, and Tunneling: Dual-Stack Host Considerations

Cisco.com

- **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 Translation, Transition, and Tunneling Summary Table

Cisco.com

Technology	Considerations	Mechanisms
Tunneling	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	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)
Translation	NAT-PT (Protocol Translation) Is Application Unaware; App Gateways Will Have to be Added; Didn't We Just Do This with IPv4? :-) NAT-PT Defeats Many Traceback Mechanisms	RFC 2766 NAT-PT
Dual Stack	Timeliness of Backbone IPv6 Deployment Native Security Technologies Must Support IPv6	Native Application Access and Native Security Mechanisms

IPv6 and IPv4 Threat Comparisons

Cisco.com

- **Attacks with New Considerations in IPv6**
  - Reconnaissance
  - Unauthorized Access
  - Header Manipulation and Fragmentation
  - Layer 3–Layer 4 Spoofing
  - ARP and DHCP Attacks
  - Broadcast Amplification Attacks (Smurf)
  - Routing Attacks
  - Viruses and Worms
  - Translation, Transition, and Tunneling Mechanisms
- **Attacks with Strong IPv4 and IPv6 Similarities**
  - Sniffing
  - Application Layer Attacks
  - Rogue Devices
  - Man-in-the-Middle Attacks
  - Flooding

IPv6 Attacks with Strong IPv4 Similarities

Cisco.com

- **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 liklihood in IPv6 as in IPv4
- **Flooding**
  - Flooding attacks are identical between IPv4 and IPv6

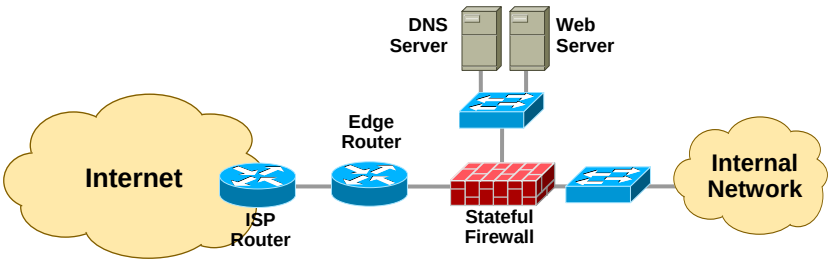
Agenda

Cisco.com

- IPv4 Best Practices Summary and Attack Example
- IPv6 Protocol Summary
- Types of Threats
- IPv6 and IPv4 Threat Comparisons (The Meat)
- IPv6 Topology and BP Summary
- v6/v4 Dual-Stack Attack Example

IPv6 Edge Security Design

Cisco.com



- This design can be augmented with NIDS, application proxies, and a range of host security controls IF they have IPv6 support
- The 3-interface FW design as shown here is widely used in IPv4 and should still be applicable to IPv6
- Firewall policies should match IPv4 policy, but take into account the unique characteristics of IPv6
  - ICMPv6 differences, bogon filtering, the use of IPv6 local unicast addresses, etc.

Candidate Best Practices (1/2)

Cisco.com

- Implement privacy extensions carefully
- Filter internal-use IPv6 addresses at the enterprise border routers
- Use standard, but nonobvious static addresses for critical systems
- 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

Candidate Best Practices (2/2)

Cisco.com

- 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 dual stack as your preferred IPv6 migration choice
- Use static tunneling rather than dynamic tunneling
- Implement outbound filtering on firewall devices to allow only authorized tunneling endpoints

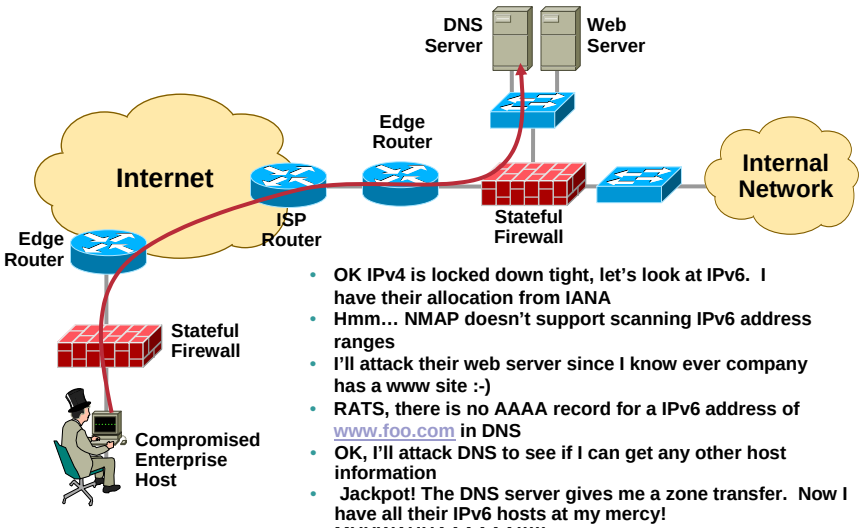
Agenda

Cisco.com

- IPv4 Best Practices Summary and Attack Example
- IPv6 Protocol Summary
- Types of Threats
- IPv6 and IPv4 Threat Comparisons (The Meat)
- IPv6 Topology and BP Summary
- v6/v4 Dual-Stack Attack Example

IPv6 Dual Stack Attack Example

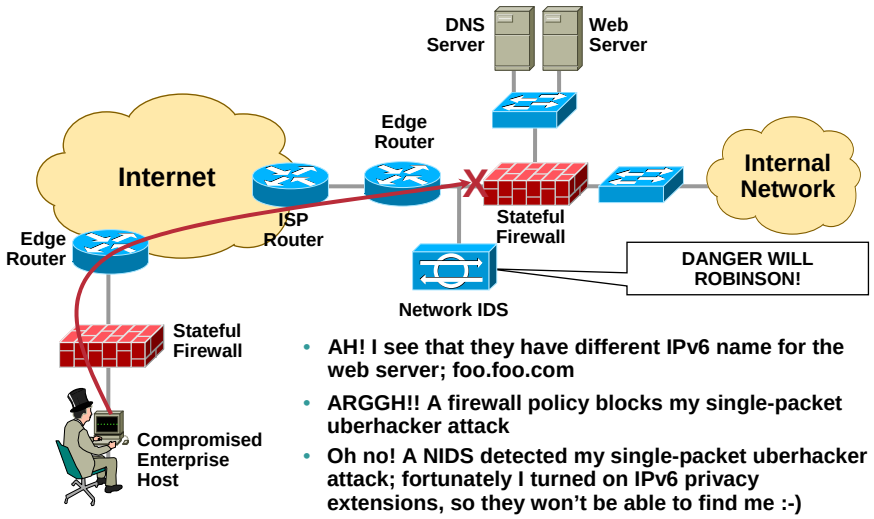
Cisco.com



- OK IPv4 is locked down tight, let's look at IPv6. I have their allocation from IANA
- Hmm… NMAP doesn't support scanning IPv6 address ranges
- I'll attack their web server since I know ever company has a www site :-)
- RATS, there is no AAAA record for a IPv6 address of www.foo.com in DNS
- OK, I'll attack DNS to see if I can get any other host information
- Jackpot! The DNS server gives me a zone transfer. Now I have all their IPv6 hosts at my mercy! MUHWAHHAAAAAA!!!!!

IPv6 Dual Stack Attack Example

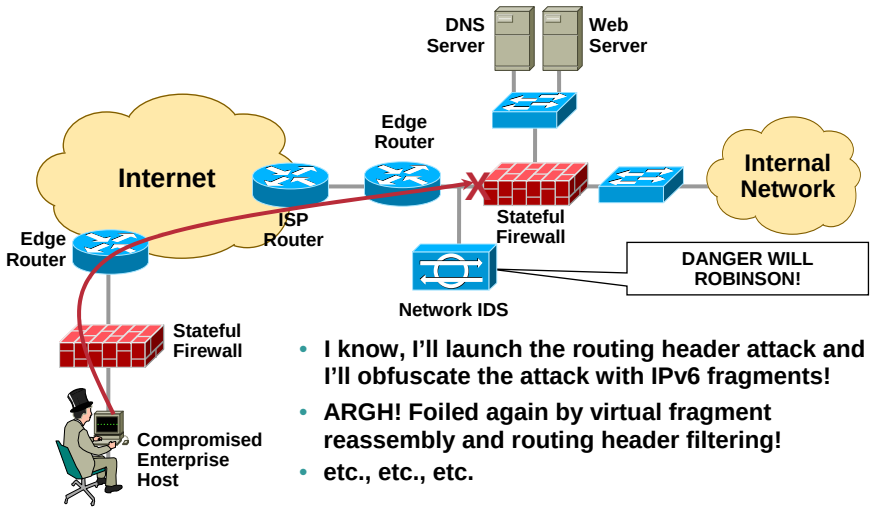
Cisco.com



- AH! I see that they have different IPv6 name for the web server; foo.foo.com
- ARGGH!! A firewall policy blocks my single-packet uberhacker attack
- Oh no! A NIDS detected my single-packet uberhacker attack; fortunately I turned on IPv6 privacy extensions, so they won't be able to find me :-)

IPv6 Dual Stack Attack Example

Cisco.com



- I know, I'll launch the routing header attack and I'll obfuscate the attack with IPv6 fragments!
- ARGH! Foiled again by virtual fragment reassembly and routing header filtering!
- etc., etc., etc.

Summary

Cisco.com

- IPv6 makes some things better/worse/different, but no more or less secure
- Better
  - Automated scanning and worm propagation is harder due to huge subnets
  - IPsec is a mandatory feature
- Worse
  - Increased complexity in addressing and configuration
  - Immaturity of software
  - Vulnerabilities in transition techniques
- Different
  - ICMPv6 expanded use
  - New addressing—multiple IPv6 addresses, local unicast, IPv6 TLAs, multicast address

Reference Materials

Cisco.com

- IPv6 IPv4 Threat Comparison and Best Practice Evaluation, Convery and Miller
  - http://www.cisco.com/security_services/ciag/documents/v6-v4-threats.pdf
- S Deering, R Hinden, "Internet Protocol, Version 6 (IPv6) Specification" (December 1998), RFC 2460 at http://www.ietf.org/rfc/rfc2460.txt
- R Hinden, S Deering, "IP Version 6 Addressing Architecture" (July 1998), RFC 2373 at http://www.ietf.org/rfc/rfc2373.txt
- Look at the above whitepaper for more references

Associated Sessions

Cisco.com

- RST-1305—IPv6 Concepts
- RST-2305—IPv6 Deployment
- SEC-2000—Secure Enterprise Design
- SEC-2T01—Infrastructure Security for Large Networks

Recommended Reading

Cisco.com

- Cisco Self-Study: Implementing Cisco IPv6 Networks (IPV6), Regis Desmeules, CiscoPress
- IPv6 Essentials, Silvia Hagen, O'Reilly
- IETF IPv6 mailing list for updates on IETF drafts and RFCs

  Really there's good comprehensible information here :-)

  http://playground.sun.com/pub/ipng/html/instructions.html

Complete Your Online Session Evaluation!

Cisco.com

WHAT: Complete an online session evaluation and your name will be entered into a daily drawing

WHY: Win fabulous prizes! Give us your feedback!

WHERE: Go to the Internet stations located throughout the Convention Center

HOW: Winners will be posted on the onsite Networkers Website; four winners per day