IPv6 Security Threats and Mitigations

BRKSEC-2003
Session Objectives

- IPv6 vs. to IPv4 from a threat and mitigation perspective
- Advanced IPv6 security topics like transition options and dual stack environments
- The focus is Enterprises
  BRKOPT-1200 has a SP focus
- Requirements: basic knowledge of the IPv6 and IPSec protocols as well as IPv4 security best practices
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

- Shared Issues by IPv4 and IPv6
- Specific Issues for IPv6
  - IPsec everywhere, dual-stack, tunnels and 6VPE
- IPv6 Security Best Common Practice
- Enforcing a Security Policy in IPv6
  - ACL, Firewalls and Host IPS
- Enterprise Secure Deployment
  - Secure IPv6 transport over public network
Shared Issues

Security Issues Shared by IPv4 and IPv6
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

\[
\frac{2^{128}}{6.5 \text{ Billion}} = 52 \text{ Trillion Trillion IPv6 addresses per person}
\]

World’s population is approximately 6.5 billion
Reconnaissance In IPv6
Scanning Methods Are Likely to Change

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

- Potential router CPU attacks if aggressive scanning
  
  Router will do Neighbor Discovery... And waste CPU and memory
  
  Built-in rate limiter but no option to tune it

- Using a /64 on point-to-point links => a lot of addresses to scan!

- Using infrastructure ACL prevents this scanning
  
  iACL: edge ACL denying packets addressed to your routers
  
  Easy with IPv6 because new addressing scheme can be done 😊
Reconnaissance In IPv6? Easy With Multicast!

- No need for reconnaissance anymore
- 3 site-local multicast addresses
  - FF05::2 all-routers, FF05::FB mDNSv6, FF05::1:3 all DHCP servers
- Several link-local multicast addresses
  - FF02::1 all nodes, FF02::2 all routers, FF02::F all UPnP, ...
- Some deprecated (RFC 3879) site-local addresses but still used
  - FEC0:0:0:FFFF::1 DNS server

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Payload</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attacker</td>
<td>FF05::1:3</td>
<td>DHCP Attack</td>
</tr>
</tbody>
</table>

http://www.iana.org/assignments/ipv6-multicast-addresses/
Preventing Reconnaissance With IPv6 Multicast

- The site-local/anycast addresses must be filtered at the border in order to make them unreachable from the outside

- ACL block ingress/egress traffic to
  - Block FEC0::/10 (deprecated site-local addresses)
  - Permit mcast to FF02::/16 (link-local scope)
  - Permit mcast to FF0E::/16 (global scope)
  - Block all mcast

```plaintext
ipv6 access-list NO_RECONNAISSANCE
  deny any fec0::/10
  permit any ff02::/16
  permit any ff0e::/16
  deny any ff00::/8
  permit any any
```
Viruses and Worms In IPv6

- Viruses and email, IM worms: IPv6 brings no change

- Other worms:
  - IPv4: reliance on network scanning
  - IPv6: not so easy (see reconnaissance) => will use alternative techniques

- Worm developers will adapt to IPv6
- IPv4 best practices around worm detection and mitigation remain valid
- Potential router CPU attacks if aggressive scanning
  - Router will do Neighbor Discovery...
IPv6 Privacy Extensions (RFC 3041)

- Temporary addresses for IPv6 host client application, e.g. web browser
  - Inhibit device/user tracking
  - Random 64 bit interface ID, then run Duplicate Address Detection before using it
  - Rate of change based on local policy

**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/user
- Hard to define authorization policy when the Layer 3 information is always changing :-)

**IPv6 Intranet**

**Management System IPv6 Address**—2001:DB8:F15:C15::1*

**Firewall**

**Internal Server**

2001:DB8:F15:c16::1/64

<table>
<thead>
<tr>
<th>Action</th>
<th>Src</th>
<th>Dest</th>
<th>Src Port</th>
<th>Dst Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permit</td>
<td>2001:DB8:F15:C15::1</td>
<td>2001:DB8:F15:c16::1</td>
<td>Any</td>
<td>80</td>
</tr>
<tr>
<td>Deny</td>
<td>Any</td>
<td>Any</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Not real RFC3041 derived addresses
Disabling Privacy Extension

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

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

- **Alternatively**
  
  Use DHCP (see later) to a specific pool
  
  Ingress filtering allowing only this pool
L3 Spoofing In IPv6
uRPF Remains the Primary Tool for Protecting Against L3 Spoofing

**uRPF Loose Mode**

- Spoofed IPv6 Source Address
- Access Layer
- Inter-Networking Device with uRPF Enabled
- No Route to Src Addr prefix => Drop

**uRPF Strict Mode**

- Spoofed IPv6 Source Address
- Access Layer
- Inter-Networking Device with uRPF Enabled
- No Route to Src Addr prefix out the packet inbound interface => Drop

*IP Source Guard does not exist yet (see further slides)*
ICMPv4 vs. ICMPv6

- Significant changes
- More relied upon

<table>
<thead>
<tr>
<th>ICMP Message Type</th>
<th>ICMPv4</th>
<th>ICMPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connectivity Checks</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Informational/Error Messaging</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Fragmentation Needed Notification</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Address Assignment</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Address Resolution</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router Discovery</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multicast Group Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mobile IPv6 Support</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- => ICMP policy on firewalls needs to change
## Generic ICMPv4 Border Firewall Policy

### Table: Generic ICMPv4 Border Firewall Policy

<table>
<thead>
<tr>
<th>Action</th>
<th>Src</th>
<th>Dst</th>
<th>ICMPv4 Type</th>
<th>ICMPv4 Code</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permit</td>
<td>Any</td>
<td>A</td>
<td>0</td>
<td>0</td>
<td>Echo Reply</td>
</tr>
<tr>
<td>Permit</td>
<td>Any</td>
<td>A</td>
<td>8</td>
<td>0</td>
<td>Echo Request</td>
</tr>
<tr>
<td>Permit</td>
<td>Any</td>
<td>A</td>
<td>3</td>
<td>0</td>
<td>Dst. Unreachable—Net Unreachable</td>
</tr>
<tr>
<td>Permit</td>
<td>Any</td>
<td>A</td>
<td>3</td>
<td>4</td>
<td>Dst. Unreachable—Frag. Needed</td>
</tr>
<tr>
<td>Permit</td>
<td>Any</td>
<td>A</td>
<td>11</td>
<td>0</td>
<td>Time Exceeded—TTL Exceeded</td>
</tr>
</tbody>
</table>
## Equivalent ICMPv6 Border Firewall Transit Policy*

<table>
<thead>
<tr>
<th>Action</th>
<th>Src</th>
<th>Dst</th>
<th>ICMPv6 Type</th>
<th>ICMPv6 Code</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permit</td>
<td>Any</td>
<td>A</td>
<td>128</td>
<td>0</td>
<td>Echo Reply</td>
</tr>
<tr>
<td>Permit</td>
<td>Any</td>
<td>A</td>
<td>129</td>
<td>0</td>
<td>Echo Request</td>
</tr>
<tr>
<td>Permit</td>
<td>Any</td>
<td>A</td>
<td>1</td>
<td>0</td>
<td>No Route to Dst.</td>
</tr>
<tr>
<td>Permit</td>
<td>Any</td>
<td>A</td>
<td>2</td>
<td>0</td>
<td>Packet Too Big</td>
</tr>
<tr>
<td>Permit</td>
<td>Any</td>
<td>A</td>
<td>3</td>
<td>0</td>
<td>Time Exceeded—TTL Exceeded</td>
</tr>
<tr>
<td>Permit</td>
<td>Any</td>
<td>A</td>
<td>4</td>
<td>0</td>
<td>Parameter Problem</td>
</tr>
</tbody>
</table>

*RFC 4890*
### Potential Additional ICMPv6 Border Firewall Receive Policy*

<table>
<thead>
<tr>
<th>Action</th>
<th>Src</th>
<th>Dst</th>
<th>ICMPv6 Type</th>
<th>ICMPv6 Code</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permit</td>
<td>Any</td>
<td>B</td>
<td>2</td>
<td>0</td>
<td>Packet too Big</td>
</tr>
<tr>
<td>Permit</td>
<td>Any</td>
<td>B</td>
<td>130–132</td>
<td>0</td>
<td>Multicast Listener</td>
</tr>
<tr>
<td>Permit</td>
<td>Any</td>
<td>B</td>
<td>133/134</td>
<td>0</td>
<td>Neighbor Solicitation and Advertisement</td>
</tr>
<tr>
<td>Permit</td>
<td>Any</td>
<td>B</td>
<td>4</td>
<td>0</td>
<td>Parameter Problem</td>
</tr>
</tbody>
</table>

*RFC 4890*
Parsing the Extension Header Chain

- Finding the layer 4 information is not trivial in IPv6
  - Skip all known extension header
  - Until either known layer 4 header found => **SUCCESS**
  - Or unknown extension header/layer 4 header found... => **FAILURE**

<table>
<thead>
<tr>
<th>IPv6 hdr</th>
<th>HopByHop</th>
<th>Routing</th>
<th>AH</th>
<th>TCP</th>
<th>data</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 hdr</td>
<td>HopByHop</td>
<td>Routing</td>
<td>AH</td>
<td><strong>Unknown L4</strong></td>
<td>???</td>
</tr>
<tr>
<td>IPv6 hdr</td>
<td>HopByHop</td>
<td><strong>Unk. ExtHdr</strong></td>
<td>AH</td>
<td>TCP</td>
<td>data</td>
</tr>
</tbody>
</table>

Note: if chain is too long on HW routers, packet is process switched...
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
In IPv6 fragmentation is done only by the end system

Tunnel end-points are end systems => re-assembly can happen inside the network

Reassembly done by end system like in IPv4

Attackers can still fragment in intermediate system on purpose

==> a great obfuscation tool
Parsing the Extension Header Chain
Fragmentation Matters!

- Extension headers chain can be so large that it is fragmented!
- Finding the layer 4 information is not trivial in IPv6
  
  Skip all known extension header
  
  Until either known layer 4 header found => SUCCESS
  
  Or unknown extension header/layer 4 header found... => FAILURE
  
  Or end of extension header => FAILURE

IPv6 hdr | HopByHop | Routing | Destination | Destination | Fragment1
---|---|---|---|---|---
IPv6 hdr | HopByHop | Fragment2 | TCP | Data

Layer 4 header is in 2nd fragment
IPv6 Fragmentation and Cisco IOS ACL Fragment Keyword

- This makes matching against the first fragment non-deterministic:
  - Layer 4 header might not be there but in a later fragment
  - Need for stateful inspection

- `fragment` keyword matches
  - Non-initial fragments (same as IPv4)
  - And the first fragment if the L4 protocol cannot be determined
IPv6 Routing Header

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

- What if attacker sends a packet with RH containing
  A -> B -> A -> B -> A -> B -> A ...
- Packet will loop multiple time on the link R1-R2
- An amplification attack!
IPv6 Type 2 Routing Header

- Required by mobile IPv6 (see later)
- Rebound/amplification attacks impossible
  
  Only one intermediate router: the mobile node home address
Preventing Routing Header Attacks

- Apply same policy for IPv6 as for IPv4:
  - Block Routing Header type 0
- Prevent processing at the intermediate nodes
  - `no ipv6 source-route`
  - Windows, Linux, MacOS: default setting
- At the edge
  - With an ACL blocking routing header
- RFC 5095 (Dec 2007) RH0 is deprecated
  - Default IOS will change in 12.5T
Neighbor Discovery Issue#1
Stateless Autoconfiguration

Router Solicitations Are Sent by Booting Nodes to Request Router Advertisements for Stateless Address Auto-Configuring

- **RS:**
  - Src = ::
  - Dst = All-Routers multicast Address
  - ICMP Type = 133
  - Data = Query: please send RA

- **RA:**
  - Src = Router Link-local Address
  - Dst = All-nodes multicast address
  - ICMP Type = 134
  - Data = options, prefix, lifetime, autoconfig flag

Attack Tool: `fake_router6`
Can Make Any IPv6 Address the Default Router

RA/RS w/o Any Authentication Gives Exactly Same Level of Security as ARP for IPv4 (None)
ARP Spoofing is Now NDP Spoofing: Threats

- ARP is replaced by Neighbor Discovery Protocol
  - Nothing authenticated
  - Static entries overwritten by dynamic ones

- Stateless Address Autoconfiguration
  - rogue RA (malicious or not)
  - All nodes badly configured
  - DoS
  - Traffic interception (Man In the Middle Attack)

- Attack tools exist (from THC – The Hacker Choice)
  - Parasit6
  - Fakerouter6
  - ...
ARP Spoofing is Now NDP Spoofing: Mitigation

- **BAD NEWS:** nothing like dynamic ARP inspection for IPv6
  - Will require new hardware on some platforms
  - Not before mid-2010...

- **GOOD NEWS:** Secure Neighbor Discovery
  - SEND = NDP + crypto
  - IOS 12.4(24)T (advanced enterprise)
  - But not in Windows Vista, wait for next Windows version...
  - Crypto means slower...

- **Other GOOD NEWS:**
  - Private VLAN works with IPv6
  - Port security works with IPv6
  - 801.x works with IPv6
  - For FTTH & other broadband, DHCP-PD means not need to NDP-proxy
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 interface identifiers are cryptographically generated

- RSA signature option
  Protect all messages relating to neighbor and router discovery

- Timestamp and nonce options
  Prevent replay attacks

- Requires IOS 12.4(24)T advanced enterprise
Cryptographically Generated Addresses
CGA RFC 3972 (Simplified)

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

<table>
<thead>
<tr>
<th>RSA Keys</th>
<th>Modifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priv</td>
<td>Public Key</td>
</tr>
<tr>
<td>Pub</td>
<td>Subnet Prefix</td>
</tr>
</tbody>
</table>

CGA Params

Signature

SEND Messages

Crypto. Generated Address

SHA-1

Interface Identifier

Subnet Prefix
SeND in Cisco IOS 12.4(24)T Configuration

crypto key generate rsa label SEND modulus 1024
The name for the keys will be: SEND
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

ipv6 cga modifier rsakeypair SEND sec-level 1

ipv6 nd secured sec-level minimum 1

ipv6 nd secured full-secure

interface fastethernet 0/0
  ipv6 cga rsakeypair SEND
  ipv6 address 2001:db8::/64 cga
# show ipv6 neighbors detail

<table>
<thead>
<tr>
<th>IPv6 Address</th>
<th>TRLV</th>
<th>Age</th>
<th>Link-layer Addr</th>
<th>State</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001:DB8::2C8D:918B:3538:6820</td>
<td>2</td>
<td>1</td>
<td>001e.be50.dd08</td>
<td>STALE</td>
<td>Fa0/0</td>
</tr>
<tr>
<td>2001:DB8::3</td>
<td>0</td>
<td>20</td>
<td>0014.3850.bfe6</td>
<td>STALE</td>
<td>Fa0/0</td>
</tr>
<tr>
<td>FE80::214:38FF:FE50:BFE6</td>
<td>0</td>
<td>20</td>
<td>0014.3850.bfe6</td>
<td>STALE</td>
<td>Fa0/0</td>
</tr>
</tbody>
</table>
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)
  => Potential DoS target
  Routers need to keep more state
- Available:
  Unix (DoCoMo)
  Cisco IOS 12.4(24)T
- Microsoft:
  no support in Vista, in Windows 2008 (and probably not Windows7)
Securing Link Operations: on Nodes?

**Advantages**
- No central administration, no central operation
- No bottleneck, no single-point of failure
- Intrinsic part of the link-operations
- Efficient for threats coming from the link

**Disadvantages**
- Heavy provisioning of end-nodes
- Poor for threats coming from outside the link
- Bootstrapping issue
- Complexity spread all over the domain
- Transitioning quite painful
Securing Link Operations: First Hop Trusted Device

**Advantages**
- Central administration, central operation
- Complexity limited to first hop
- Transitioning lot easier
- Efficient for threats coming from the link
- Efficient for threats coming from outside

**Disadvantages**
- Applicable only to certain topologies
- Requires first-hop to learn about end-nodes
- First-hop is a bottleneck and single-point of failure
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 link-local multicast address (FF02::1:2): same threat as IPv4
  
  Rogue DHCPv6 servers on the site-local multicast address (FF05::1:3): new threat in IPv6

- Scanning possible if leased addresses are consecutive
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

- Port ACL can block DHCPv6 traffic from client ports
  - `deny udp any eq 547 any eq 546`

- Cisco Network Registrar
  - DHCPv6 Server
  - Leased addresses are random => scanning difficult
  - Can also lease temporary addresses (like privacy extension)
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

ICMP REQ D=160.154.5.255 S= 172.18.1.2

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 appropriate link local multicast addresses
  - Link Local All Nodes Multicast—FF02::1
  - Link Local All Routers Multicast—FF02::2
  - Link Local All mDNS Multicast—FF02::FB

Note: anti-spoofing also blocks amplification attacks because a remote attacker cannot masquerade as his victim

http://iana.org/assignments/ipv6-multicast-addresses/
IPv6 and Other Amplification Vectors

- IOS implements correctly RFC 4443 ICMPv6
  
  No ping-pong on a physical point-to-point link Section 3.1
  
  No ICMP error message should be generated in response to a packet with a multicast destination address Section 2.4 (e.3)
  
  Exceptions for Section 2.4 (e.3)
  
  – packet too big message
  
  – the parameter problem message
  
  • Rate Limit egress ICMP Packets
  
  • Rate limit ICMP messages generation
  
  • Secure the multicast network (source specific multicast)
  
  • Note: Implement Ingress Filtering of Packets with IPv6 Multicast Source Addresses
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, PIM also rely 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
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 Stack Vulnerabilities

- IPv6 stacks are new and could be buggy

### Some examples

<table>
<thead>
<tr>
<th>CVE-2008-2476</th>
<th>Oct 2008</th>
<th>FreeBSD, OpenBSD, NetBSD and others</th>
<th>Lack of validation of NDP messages</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2008-2136</td>
<td>May 2008</td>
<td>Linux</td>
<td>DoS caused by memory leak in IPv6 tunnels</td>
</tr>
<tr>
<td>CVE-2008-1153</td>
<td>Mar 2008</td>
<td>IOS</td>
<td>Cisco IOS dual-stack router IPv6 DoS</td>
</tr>
<tr>
<td>CVE-2007-4689</td>
<td>Nov 2007</td>
<td>Apple Mac OS X</td>
<td>Packet processing double-free memory corruption</td>
</tr>
</tbody>
</table>
By the Way: It Is Real 😞 IPv6 Hacking Tools
Let the Games Begin

- Sniffers/packet capture
  - Snort
  - TCPdump
  - Sun Solaris snoop
  - COLD
  - Wireshark
  - Analyzer
  - Windump
  - WinPcap

- Scanners
  - IPv6 security scanner
  - Halfscan6
  - Nmap
  - Strobe
  - Netcat

- DoS Tools
  - 6tunneldos
  - 4to6ddos
  - Imps6-tools

- Packet forgers
  - Scapy6
  - SendIP
  - Packit
  - Spak6

- Complete tool
Specific IPv6 Issues

Issues Applicable Only to IPv6
IPv6 Header Manipulation

- Unlimited size of header chain (spec-wise) can make filtering difficult
- Potential DoS with poor IPv6 stack implementations

More boundary conditions to exploit

Can I overrun buffers with a lot of extension headers?

---

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

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

- IPv6 mandates the implementation of IPsec
- IPv6 does not require the use of IPsec
- Some organizations believe that IPsec should be used to secure all flows...
  
  Interesting scalability issue (n^2 issue with IPsec)
  
  Need to trust endpoints and end-users because the network cannot secure the traffic: no IPS, no ACL, no firewall
  
  IOS 12.4(20)T can parse the AH
  
  Network telemetry is blinded: NetFlow of little use
  
  Network services hindered: what about QoS?

**Recommendation:** do not use IPsec end to end within an administrative domain.

**Suggestion:** Reserve IPsec for residential or hostile environment or high profile targets.
IPv4 to IPv6 Transition Challenges

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

- Host security on a dual-stack device
  Applications can be subject to attack on both IPv6 and IPv4
  Fate sharing: as secure as the least secure stack...

- Host security controls should block and inspect traffic from both IP versions
  Host intrusion prevention, personal firewalls, VPN clients, etc.

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, Mac OS/X, ...)

- Your network:
  - Does not run IPv6

- Your assumption:
  - I’m safe

- Reality
  - You are not safe
  - Attacker sends Router Advertisements
  - Your host configures silently to IPv6
  - You are now under IPv6 attack

- => Probably time to think about IPv6 in your network
TBD: Dual-Stack MacOS: any IPv6 Router?

2) Hacker: I’m the Router

3) Newly Enabled IPv6 MacOS does DAD

4) The Full IPv6 Address of the MacOS
IPv6 Tunneling Summary

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

- 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
Transition Threats—ISATAP

- 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
  - Windows default to isatap.example.com
- Ipv6 addresses can be guessed based on IPv4 prefix
6to4 Tunnels Bypass ACL

IPv4

6to4 relay

IPv6 Internet

ACL

IPv4
tunnel

6to4 router

Direct tunneled traffic ignores hub ACL

6to4 router

6to4 relays

6to4 router
6to4 Relay Security Issues

- Traffic injection & IPv6 spoofing
  Prevent spoofing by applying uRPF check
  Drops 6to4 packets whose addresses are built on IPv4 bogons
  Loopback
  RFC 1918

- Redirection and DoS
  Block most of the ICMPv6 traffic:
  No Neighbor Discovery
  No link-local traffic
  No redirect

- Traffic is asymmetric
  6to4 client/router -> 6to4 relay -> IPv6 server:
    client IPv4 routing selects the relay
  IPv6 server -> 6to4 relay -> 6to4 client/router:
    server IPv6 routing selects the relay
  Cannot insert a stateful device (firewall, ...) on any path
TEREDO?

- **Teredo navalis**
  A shipworm drilling holes in boat hulls

- **Teredo Microsoftis**
  IPv6 in IPv4 punching holes in NAT devices

Source: United States Geological Survey
Teredo Tunnels (1/3)
Without Teredo: Controls Are In Place

- All outbound traffic inspected: e.g., P2P is blocked
- All inbound traffic blocked by firewall
Teredo Tunnels (2/3)
No More Outbound Control

Teredo threats—IPv6 Over UDP (port 3544)

- Internal users wants to get P2P over IPv6
- Configure the Teredo tunnel (already enabled by default!)
- FW just sees IPv4 UDP traffic (may be on port 53)
- **No more outbound control by FW**
Teredo Tunnels (3/3)
No More Outbound Control

Once Teredo Configured

- **Inbound** connections are allowed
- IPv4 firewall unable to control
- IPv6 hackers can penetrate
- Host security needs IPv6 support now
Is It Real?
May Be uTorrent 1.8 (Released Aug. ‘08)
Can We Block Rogue Tunnels?

- Rogue tunnels by naïve users:
  
  Sure, block IP protocol 41 and UDP/3544

  In Windows:

  ```
  netsh interface 6to4 set state state=disabled undoonstop=disabled
  netsh interface isatap set state state=disabled
  netsh interface teredo set state type=disabled
  ```

- Really rogue tunnels (covert channels)
  
  No easy way...

  Teredo will run over a different UDP port of course

  Network devices can be your friend (more to come)

- Deploying native IPv6 (including IPv6 firewalls and IPS) is probably a better alternative

- Or disable IPv6 on Windows through GPO or CSA 6.0
Can the Network Block Rogue Tunnels?

- Use Flexible Packet Matching (FPM)
  Blocking all Teredo addresses 2001::/32 in the UDP payload

- FPM
  Available in software since 12.4(4)T
  Hardware implementation in PISA (requires Sup32 and Cat6K)
  Classify on multiple attributes within a packet
  String match and regex
  Expressed in XML

Cisco.com/go/fpm
FPM Configuration to Block Teredo

The trick is to block all packets containing a Teredo source or destination address in the UDP payload.

Teredo addresses are in the 2001::/32 (note 32) prefix.

```plaintext
load protocol bootdisk:ip.phdf
load protocol bootdisk:udp.phdf

class-map type stack match-all cm-ip-udp
  match field IP protocol eq 17 next UDP

class-map type access-control match-all cm-teredo1
  match start udp payload-start offset 0 size 1 eq 0x60 mask 15
  match start udp payload-start offset 8 size 4 eq 0x20010000

class-map type access-control match-all cm-teredo2
  match start udp payload-start offset 0 size 1 eq 0x60 mask 15
  match start udp payload-start offset 24 size 4 eq 0x20010000

class cm-teredo1
drop
class cm-teredo2
drop

policy-map type access-control pm-teredo
  class cm-teredo1
  drop
  class cm-teredo2
  drop

policy-map type access-control pm-udp-teredo
  class cm-ip-udp
  service-policy pm-teredo

interface GigabitEthernet1/36
  service-policy type access-control in pm-udp-teredo
```

For Your Reference

For Your Reference

The trick is to block all packets containing a Teredo source or destination address in the UDP payload.

Teredo addresses are in the 2001::/32 (note 32) prefix.

IP version = 6

Teredo prefix as embedded address
SP Transition Mechanism: 6VPE

- 6VPE: the MPLS-VPN extension to also transport IPv6 traffic over a MPLS cloud and IPv4 BGP sessions
6VPE Security

- 6PE (dual stack without VPN) is a simple case
- Security is identical to IPv4 MPLS-VPN, see RFC 4381
- Security depends on correct operation and implementation
  - QoS prevent flooding attack from one VPN to another one
  - PE routers must be secured: AAA, iACL, CoPP …
- **MPLS backbones can be more secure than “normal” IP backbones**
  - Core not accessible from outside
  - Separate control and data planes

- **PE security**
  - Advantage: Only PE-CE interfaces accessible from outside
  - Makes security easier than in “normal” networks
  - **IPv6 advantage:** PE-CE interfaces can use link-local for routing
    - => completely unreachable from remote (better than IPv4)
IPv6 Security Best Common Practice
Candidate Best Practices

- Train your network operators and security managers on IPv6
- **Selectively filter ICMP** (RFC 4890)
- Implement RFC 2827-like filtering
- Block Type 0 Routing Header at the edge
- Determine what extension headers will be allowed through the access control device
- Use traditional authentication mechanisms on BGP and IS-IS
- Use IPsec to secure protocols such as OSPFv3 and RIPng
- Document procedures for last-hop traceback
Candidate Best Practices (Cont.)

- Implement privacy extensions carefully
- Filter internal-use IPv6 addresses & ULA at the border routers
- Filter unneeded services at the firewall
- Maintain host and application security
- Use cryptographic protections where critical
- Implement ingress filtering of packets with IPv6 multicast source addresses
- Use static tunneling rather than dynamic tunneling
- Implement outbound filtering on firewall devices to allow only authorized tunneling endpoints
Enforcing a Security Policy
PCI DSS Compliance and IPv6

- Payment Card Industry Data Security Standard requires the use of NAT for security
  Yes, weird isn’t it?
  There is no NAT IPv6 <-> IPv6 in most of the firewalls
  IETF has just started to work on NAT66
- ➔ PCI DSS compliance cannot be achieved for IPv6?
Cisco IOS IPv6 Extended Access Control Lists

- Very much like in IPv4
  - Filter traffic based on
    - Source and destination addresses
    - Next header presence
    - Layer 4 information
  - Implicit deny all at the end of ACL
  - Empty ACL means traffic allowed
  - Reflexive and time based ACL

- Known extension headers (HbH, AH, RH, MH, destination, fragment) are scanned until:
  - Layer 4 header found
  - Unknown extension header is found

- Side note for 7600 & other switches:
  - No VLAN ACL
  - Port ACL on Nexus-7000, Cat 3750 (12.2(46)SE), Cat 4K (end 2009), Cat 6K (mid 2010)
  - Long extension headers chain force a software switching
Cisco IOS IPv6 Extended ACL

- Can match on
  - Upper layers: TCP, UDP, SCTP port numbers
  - TCP flags SYN, ACK, FIN, PUSH, URG, RST
  - ICMPv6 code and type
  - Traffic class (only six bits/8) = DSCP
  - Flow label (0-0xFFFFF)

- IPv6 extension header
  - `routing` matches any RH, `routing-type` matches specific RH
  - `mobility` matches any MH, `mobility-type` matches specific MH
  - `dest-option` matches any, `dest-option-type` matches specific destination options
  - `auth` matches AH
  - Can skip AH (but not ESP) since IOS 12.4(20)T

- `fragments` keyword matches
  - Non-initial fragments (same as IPv4)
  - `And` the first fragment if the L4 protocol cannot be determined

- `undetermined-transport` keyword matches (only for deny)
  - Any packet whose L4 protocol cannot be determined: fragmented or unknown extension header
Cisco IOS IPv6 ACL
A Trivial Example
Filtering inbound traffic to one specific destination address

Prefix: 2001:db8:2c80:1000::/64

ipv6 access-list MY_ACL
remark basic anti-spoofing
deny 2001:db8:2c80:1000::/64 any
permit any 2001:db8:2c80:1000::1/128

interface Serial 0
ipv6 traffic-filter MY_ACL in
IPv6 ACL Implicit Rules

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

```plaintext
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

```plaintext
permit icmp any any nd-na
permit icmp any any nd-ns
deny ipv6 any any log
```
Example: RFC 4890 ICMP ACL

```
ipv6 access-list RFC4890
  permit icmp any any echo-reply
  permit icmp any any echo-request
  permit icmp any any 1 3
  permit icmp any any 1 4
  permit icmp any any packet-too-big
  permit icmp any any time-exceeded
  permit icmp any any parameter-problem
  permit icmp any any mld-query
  permit icmp any any mld-reduction
  permit icmp any any mld-report
  permit icmp any any nd-na
  permit icmp any any nd-ns
  permit icmp any any router-solicitation
```
Example: Rogue RA & DHCP Port ACL

```
ipv6 access-list ACCESS_PORT
    remark Block all traffic DHCP server -> client
deny udp any eq 547 any eq 546
    remark Block Router Advertisements
deny icmp any any router-advertisement
    permit any any

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

*Note: PACL replaces RACL for the interface
In May 2009, only on Nexus-7000 and Cat 3750 12.2(46)SE*
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

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

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

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

- Stateful protocol inspection (anomaly detection) of IPv6 fragmented packets, TCP, UDP, ICMP and FTP traffic
- IOS 12.3(7)T (released 2005)
- Stateful inspection of IPv4/IPv6 packets
- IPv6 DoS attack mitigation
- Recognizes IPv6 extension headers
ASA Firewall IPv6 Support

- Since version 7.0 (April 2005)
- Dual-stack, IPv6 only, IPv4 only
- Extended IP ACL with stateful inspection
- Application awareness
  - HTTP, FTP, telnet, SMTP, TCP, SSH, UDP
- uRPF and v6 Frag guard
- IPv6 header security checks
- Management access via IPv6
  - Telnet, SSH, HTTPS
- Caveat: no fail-over support
ASA: Sample IPv6 Topology

Inside
2001:db8:c000:1052::/64

Outside
2001:db8:c000:1051::37/64
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
ASA 7.x: Stateful Inspection

ASA# 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
Cisco Security Agent and IPv6

- IPv6 support for Windows in CSA 6.0.1 (June 2008)
  - IPv6 ACL (only on Vista)
  - Disable IPv6 (XP and Vista)

  to any IPv6 addresses
CSA 6.0.1 In Action
IPv6 Traffic is Denied by CSA...

The process 'C:\Users\tmay' 22 to 2001:db8:1::1 using Details Rule 1160 Wizard
The process 'C:\Users\tmyer\Desktop\putty.exe' (as user Tobywv\tmyer) attempted to initiate a connection as a client on TCP port 22 to 2001:db8:1::1 using interface Wifi\infra The operation was denied.
Details Rule 1160 Wizard

The process 'C:\Windows\system32\svchost.exe -k NetworkService' (as user NT-AUTORITÄT\NETZWERKDIENST) attempted to initiate a connection as a client on UDP port 5355 to ff02::1:3 using int Details Rule 1160 Wizard
Cisco IPS 6.2 New IPv6 Engine

Drop Malware traffic

ASA 8.2 transfer IPv6 traffic To Sensor Engine

Rules to block traffic

- Deny Attacker Inline (Inline only)
- Deny Attacker Service Pair Inline (In...
- Deny Attacker Victim Pair Inline (Inli...
- Deny Connection Inline (Inline only)
- Log Attacker Packets
- Log Pair Packets
- Log Victim Packets
- Produce Alert
- Produce Verbose Alert
- Request Block Connection
- Request Block Host
- Request Rate Limit
- Request SNMP Trap
- Reset Tcp Connection

IPv6 malware traffic
Safe Traffic
Unselected Traffic

Internet

ASA

ASA 8.2 transfer IPv6 traffic To Sensor Engine

Drop Malware traffic
Summary of Cisco IPv6 Security Products

- **ASA Firewall**
  - Since version 7.0
  - Flexibility: Dual stack, IPv6 only, IPv4 only
  - SSL VPN for IPv6 (ASA 8.0)
  - No header extension parsing, no stateful-failover (coming)

- **FWSM**
  - IPv6 in software...

- **Cisco Security Agent**
  - Since version 6.0.1 for IPv6 network protection

- **IPS**
  - Since 6.2 (November 2008)
Enterprise Deployment: Secure IPv6 Connectivity

How to Secure IPv6 Over the WAN
Secure IPv6 Over IPv4/6 Public Internet

- No traffic sniffing
- No traffic injection
- No service theft

<table>
<thead>
<tr>
<th>Public Network</th>
<th>Site 2 Site</th>
<th>Remote Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4</td>
<td>▪ 6in4/GRE Tunnels Protected by IPsec</td>
<td>▪ ISATAP Protected by RA IPsec</td>
</tr>
<tr>
<td></td>
<td>▪ DMVPN 12.4(20)T</td>
<td>▪ SSL VPN Client AnyConnect</td>
</tr>
<tr>
<td>IPv6</td>
<td>IPsec VTI 12.4(6)T</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Secure Site to Site IPv6 Traffic Over IPv4 Public Network With GRE IPsec

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

See reference slides for more details

IPsec protects IPv4 unicast traffic... The encapsulated IPv6 packets

IPv4 in IPv4
Secure Site to Site IPv6 Traffic Over IPv4 Public Network With DMVPN

- IPv6 packets over DMVPN IPv4 tunnels
  - In IOS release 12.4(20)T (July 2008)
  - IPv6 and/or IPv4 data packets over same GRE tunnel
- Complete set of NHRP commands
  - network-id, holdtime, authentication, map, etc.
- NHRP registers two addresses
  - Link-local for routing protocol (Automatic or Manual)
  - Global for packet forwarding (Mandatory)
DMVPN for IPv6
Phase 1 Configuration

Hub

interface Tunnel0
!... IPv4 DMVPN configuration may be required...
  ipv6 address 2001:db8:100::1/64
  ipv6 eigrp 1
  no ipv6 split-horizon eigrp 1
  no ipv6 next-hop-self eigrp 1
  ipv6 nhrp map multicast dynamic
  ipv6 nhrp network-id 100006
  ipv6 nhrp holdtime 300
  tunnel source Serial2/0
  tunnel mode gre multipoint
  tunnel protection ipsec profile vpnprof

! interface Ethernet0/0
  ipv6 address 2001:db8:0::1/64
  ipv6 eigrp 1

! interface Serial2/0
  ip address 172.17.0.1 255.255.255.252

! ipv6 router eigrp 1
  no shutdown

Spoke

interface Tunnel0
!... IPv4 DMVPN configuration may be required...
  ipv6 address 2001:db8:100::11/64
  ipv6 eigrp 1
  ipv6 nhrp map multicast 172.17.0.1
  ipv6 nhrp map 2001:db8:100::1/128 172.17.0.1
  ipv6 nhrp network-id 100006
  ipv6 nhrp holdtime 300
  ipv6 nhrp nhs 2001:db8:100::1
  tunnel source Serial1/0
  tunnel mode gre multipoint
  tunnel protection ipsec profile vpnprof

! interface Ethernet0/0
  ipv6 address 2001:db8:1::1/64
  ipv6 eigrp 1

! interface Serial1/0
  ip address 172.16.1.1 255.255.255.252

! ipv6 router eigrp 1
  no shutdown
Secure Site to Site 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
```
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
      - Fixed IPv6 address enables server’s side of any application to be configured on an IPv6 host that could roam over the world
- Use of ASA 8.0 and SSL VPN Client AnyConnect
  - Can transfer IPv6 traffic over public IPv4
Secure RA IPv6 Traffic Over IPv4 Public Network: ISATAP In IPSec

IPsec protects IPv4 unicast traffic... The encapsulated IPv6 packets

IPsec with NAT-T can traverse NAT
ISATAP encapsulates IPv6 into IPv4

See reference slides for more details
Secure RA IPv6 Traffic Over IPv4 Public Network: AnyConnect SSL VPN Client

IPv4 and IPv6 Transport in SSL

IPv4 PC
AnyConnect

IPv4

ASA 8.0
SSL VPN Concentrator
Dual Stack

IPv6 Network
ASA 8.0 and AnyConnect 2.0 for IPv6 transport

- Since 8.0 ASA SSL VPN and AnyConnect can transport IPv6

```plaintext
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface

ipv6 local pool POOL_V6 2001:db8:5fff:81::1:1/64 8

tunnel-group DefaultWEBVPNGroup general-attributes
...
ipv6-address-pool POOL_V6
```

Ethernet adapter Cisco AnyConnect VPN Client Connection:

- Connection-specific DNS Suffix : cisco.com
- IP Address : 192.168.0.200
- Subnet Mask : 255.255.255.0
- IP Address : 2001:db8:5fff:81::1:1
- IP Address : fe80::205:9aff:fe3c:7a00%13
- Default Gateway : 192.168.0.1
  2001:db8:5fff:81::
Conclusion
Key Take Away

- So, nothing really new in IPv6
- Lack of operation experience may hinder security for a while: **training is required**
- Security enforcement is possible
  - Control your IPv6 traffic as you do for IPv4
- Leverage IPsec to secure IPv6 when suitable
Is IPv6 In My Network?

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

- Security
  - SEC1 – Data Loss Prevention Solutions and Services
  - SEC2 – Global Correlation Stops Threats
  - SEC3 – Cisco Identity-Based Security Solutions
  - SEC4 – Cisco Virtual Office Securing Remote Workers
Recommended Reading

Complete Your Online Session Evaluation

- Give us your feedback and you could win fabulous prizes. Winners announced daily.
- Receive 20 Passport points for each session evaluation you complete.
- Complete your session evaluation online now (open a browser through our wireless network to access our portal) or visit one of the Internet stations throughout the Convention Center.

Don’t forget to activate your Cisco Live Virtual account for access to all session material, communities, and on-demand and live activities throughout the year. Activate your account at the Cisco booth in the World of Solutions or visit www.ciscolive.com.
References Slides

Further Information Not Presented but Useful
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
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.
IPv6 for Remote Devices
Router Configuration: ISATAP

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:

<table>
<thead>
<tr>
<th>64-bit Unicast Prefix</th>
<th>0000:5EFE: IPv4 Addr.</th>
</tr>
</thead>
<tbody>
<tr>
<td>32-bit</td>
<td>32-bit</td>
</tr>
<tr>
<td>Interface ID</td>
<td></td>
</tr>
</tbody>
</table>

2001:db8:c003:1101:0:5efe:20.1.1.1
IPv6 for Remote Devices
Does It Work?

<table>
<thead>
<tr>
<th>Addr Type</th>
<th>DAD State</th>
<th>Valid Life</th>
<th>Pref. Life</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public</td>
<td>Preferred</td>
<td>29d23h56m5s</td>
<td>6d23h56m5s</td>
<td>2001:db8:c003:1101::/64</td>
</tr>
<tr>
<td>Link</td>
<td>Preferred</td>
<td>infinite</td>
<td>infinite</td>
<td>fe80::5efe:10.1.99.102</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Publish</th>
<th>Type</th>
<th>Met</th>
<th>Prefix</th>
<th>Idx</th>
<th>Gateway/Interface Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Autoconf</td>
<td>9</td>
<td>2001:db8:c003:1101::/64</td>
<td>2</td>
<td>Automatic Tunneling Pseudo-Interface</td>
</tr>
<tr>
<td>no</td>
<td>Manual</td>
<td>1</td>
<td>::/0</td>
<td>2</td>
<td>fe80::5efe:20.1.1.1</td>
</tr>
</tbody>
</table>
```
Secure Site-to-Site IPv6 Connectivity

IPv6 Tunnel Is Between the Two Static IPv4 Loopbacks

Tunnel 4 (IPv6 in IPv4)

Serial 0/0 Dynamic

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

Hub IPSec Is Using Dynamic Crypto Maps

Spoke

Hub

Loopback 0 192.168.52.4

Loopback 0 192.168.52.7

2001:DB8:C000:1051::/64

2001:DB8:C000:1053::4/128

IPv6 Connectivity For Your Reference
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 require 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)
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
Spoke Configuration (2/2): 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
Hub Configuration (1/2): 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
Hub Configuration (2/2): 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 192.168.204.26 255.255.255.252
  crypto map IPV6_SEC
!
  ip access-list extended SELECTOR
    permit 41 host 192.168.52.7 192.168.52.0 0.0.0.255
IPv6 Integration On MPLS VPN Infrastructure – 6VPE

- MPLS/IPv4 Core Infrastructure is IPv6-unaware
- PEs are updated to support Dual Stack/6VPE
- IPv6 VPN can co-exist with IPv4 VPN – same scope and policies
- 6VPE – RFC 4659 – Cisco authored for IPv6 VPN over MPLS/IPv4 infrastructure
- Shipping in:
  1. 12.2(33)SRB (Barracuda – C7600), Q1CY07
  2. 12.4(pi7)T (C7200, C7301, C2800, C3800), Q3CY07
  3. 12.2(x)SB (Exodus Rel5 – C10000), Q3CY07
  4. 12.2(33)SXI (Whitney 2.0 – C6500), Q4CY07
OSPF or EIGRP Authentication

interface Ethernet0/0
ipv6 ospf 1 area 0
ipv6 ospf authentication ipsec spi 500 md5
1234567890ABCDEF1234567890ABCDEF

interface Ethernet0/0
ipv6 authentication mode eigrp 100 md5
ipv6 authentication key-chain eigrp 100 MYCHAIN

key chain MYCHAIN
key 1
key-string 1234567890ABCDEF1234567890ABCDEF
accept-lifetime local 12:00:00 Dec 31 2006
12:00:00 Jan 1 2008
send-lifetime local 00:00:00 Jan 1 2007 23:59:59
Dec 31 2007