What You Make Possible
IPv6 Security Threats and Mitigations
BRKSEC-2003
Session Objectives

- Leverage existing IPv4 network security knowledge
- Advanced IPv6 security topics like transition options and dual stack environments
- Requirements: basic knowledge of the IPv6 and IPsec protocols as well as IPv4 network 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).
- Some reference URL have a QR for your convenience.
Agenda

- Debunking IPv6 Myths
- Shared Issues by IPv4 and IPv6
- Specific Issues for IPv6
  - Extension headers, IPsec everywhere, transition techniques
- Enforcing a Security Policy in IPv6
  - ACL, Firewalls and IPS
- Enterprise Secure Deployment
  - Secure IPv6 transport over public network
IPv6 Security Myths…
IPv6 Myths: Better, Faster, More Secure

Sometimes, newer means better and more secure

Sometimes, experience IS better and safer!
The Absence of Reconnaissance Myth

- Default subnets in IPv6 have $2^{64}$ addresses
  - 10 Mpps = more than 50 000 years
Reconnaissance in IPv6 Scanning Methods Will Change

- Public servers will still need to be DNS reachable
  - More information collected by Google...

- Increased deployment/reliance on dynamic DNS
  - More information will be in DNS

- Using peer-to-peer clients gives IPv6 addresses of peers

- Administrators may adopt easy-to-remember addresses (::10, ::20, ::F00D, ::C5C0, :ABBA:BABE or simply IPv4 last octet for dual stack)

- By compromising hosts in a network, an attacker can learn new addresses to scan
Viruses and Worms in IPv6

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

- Worm developers will adapt to IPv6
- IPv4 best practices around worm detection and mitigation remain valid
Scanning Made Bad for CPU Remote Neighbour Cache Exhaustion

- Potential router CPU/memory attacks if aggressive scanning
  - Router will do Neighbour Discovery... And waste CPU and memory
- Local router DoS with NS/RS/…
Mitigating Remote Neighbour Cache Exhaustion

- Built-in rate limiter but no option to tune it
  - Since 15.1(3)T: `ipv6 nd cache interface-limit`
  - Or IOS-XE 2.6: `ipv6 nd resolution data limit`
  - **Destination-guard** is part of First Hop Security phase 3

- Using a /64 on **point-to-point links** => a lot of addresses to scan!
  - Using /127 could help (RFC 6164)

- **Internet edge/presence**: a target of choice
  - Ingress ACL permitting traffic to specific statically configured (virtual) IPv6 addresses only

- Using infrastructure ACL prevents this scanning
  - iACL: edge ACL denying packets addressed to your routers
  - Easy with IPv6 because new addressing scheme can be done 😊
Simple Fix for Remote Neighbour Cache Exhaustion

- Ingress ACL allowing only valid destination and dropping the rest
- NDP cache & process are safe
- Requires DHCP or static configuration of hosts

2001:db8::/64

NS: 2001:db8::1
NA: 2001:db8::1
Reconnaissance in IPv6? Easy with Multicast!

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

<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/
The IPsec Myth:
IPsec End-to-End will Save the World

- “IPv6 mandates the implementation of IPsec”
- Some organisations believe that IPsec should be used to secure all flows…

“Security expert, W., a professor at the University of <foo> in the UK, told <newspaper> the new protocol system – IPv6 – comes with a security code known as IPSEC that would do away with anonymity on the web.

*If enacted globally, this would make it easier to catch cyber criminals, Prof W. said.*”
The IPsec Myth: IPsec End-to-End will Save the World

- IPv6 originally mandated the implementation of IPsec (but not its use)
- Now, RFC 6434 “IPsec SHOULD be supported by all IPv6 nodes”
- Some organisations still believe that IPsec should be used to secure all flows...
  - Interesting scalability issue (n^2 issue with IPsec)
  - Need to trust endpoints and end-users because the network cannot secure the traffic: no IPS, no ACL, no firewall

  IOS 12.4(20)T can parse the AH
  - Network telemetry is blinded: NetFlow of little use
  - Network services hindered: what about QoS?

Recommendation: do not use IPsec end to end within an administrative domain.
Suggestion: Reserve IPsec for residential or hostile environment or high profile targets EXACTLY as for IPv4
Quick Reminder
IPv4 Broadcast Amplification: Smurf

Attempt to Overwhelm Destination

ICMP REQ D=160.154.5.255 S=172.18.1.2

160.154.5.0

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

172.18.1.2

Belgian Schtroumpf
The No Amplification Attack Myth
IPv6 and Broadcasts

- There are no broadcast addresses in IPv6
- Broadcast address functionality is replaced with appropriate link local multicast addresses
  - Link Local All Nodes Multicast—FF02::1
  - Link Local All Routers Multicast—FF02::2
  - Link Local All mDNS Multicast—FF02::FB

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

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

- 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
  
  - ICMP information message (echo reply) should be generated even if destination is multicast

• 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
• Note: anti-spoofing also blocks amplification attacks because a remote attacker cannot masquerade as his victim
Shared Issues
IPv6 Bogon and Anti-Spoofing Filtering

- Bogon filtering (data plane & BGP route-map):
- Anti-spoofing = uRPF

![Diagram of IPv6 Intranet and Inter-Networking Device with uRPFEnabled]

IPv6 Unallocated Source Address

IPv6 Intranet

Inter-Networking Device with uRPF Enabled

IPv6 Intranet/Internet

No Route to SrcAddr => Drop
Remote Triggered Black Hole

- RFC 5635 RTBH is easy in IPv6 as in IPv4
- uRPF is also your friend for blackholing a source
- RFC 6666 has a specific discard prefix
  100::/64
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

Next Header = 43
Routing Header

IPv6 Basic Header

Routing Header Data

Type 0 Routing Header
Issue #2: Amplification Attack

- What if attacker sends a packet with RH containing
  - A -> B -> A -> B -> A -> B -> A -> B ...

- Packet will loop multiple time on the link A-B
- An amplification attack!
Preventing Routing Header Attacks

- Apply same policy for IPv6 as for IPv4:
  - Block Routing Header type 0
- Prevent processing at the intermediate nodes
  - `no ipv6 source-route`
  - Windows, Linux, Mac OS: default setting
  - IOS-XR before 4.0: a bug prevented the processing of RH0
  - IOS before 12.4(15)T: by default RH0 were processed
- At the edge
  - With an ACL blocking routing header
- RFC 5095 (Dec 2007) RH0 is deprecated
  - Default changed in IOS 12.4(15)T and IOS-XR 4.0 to ignore and drop RH0
Neighbour Discovery Issue#1
SLAAC Rogue Router Advertisement

Router Advertisements contains:
- Prefix to be used by hosts
- Data-link layer address of the router
- Miscellaneous options: MTU, DHCPv6 use, …

1. RS:
   - Data = Query: please send RA

2. RA:
   - Data = options, prefix, lifetime, A+M+O flags

RA w/o Any Authentication Gives Exactly Same Level of Security as DHCPv4 (None)
Neighbour Discovery Issue#2
Neighbour Solicitation

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

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

A and B Can Now Exchange
Packets on This Link

Security Mechanisms
Built into Discovery Protocol = None

=> Very similar to ARP

Attack Tool:
Parasite6
Answer to all NS, Claiming to Be All Systems in the LAN...
ARP Spoofing is now NDP Spoofing: Mitigation

- **MOSTLY GOOD NEWS**: dynamic ARP inspection for IPv6 is available (but not yet on all platforms)
  - First phase (Port ACL & RA Guard) available since Summer 2010
  - Second phase (NDP & DHCP snooping) starting to be available since Summer 2011

- **GOOD NEWS**: Secure Neighbour Discovery
  - SeND = NDP + crypto
  - IOS 12.4(24)T
  - But not in Windows Vista, 2008 and 7, Mac OS/X, iOS, Android
  - Crypto means slower...

- Other **GOOD NEWS**:
  - Private VLAN works with IPv6
  - Port security works with IPv6
  - IEEE 801.X works with IPv6 (except downloadable ACL)
Mitigating Rogue RA: Host Isolation

- Prevent Node-Node Layer-2 communication by using:
  - Private VLANs (PVLAN) where nodes (isolated port) can only contact the official router (promiscuous port)
  - WLAN in ‘AP Isolation Mode’
  - 1 VLAN per host (SP access network with Broadband Network Gateway)

- Link-local multicast (RA, DHCP request, etc) sent only to the local official router: no harm
  - Side effect: breaks DAD
Secure Neighbour 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 neighbour and router discovery

- Timestamp and nonce options
  - Prevent replay attacks

- Requires IOS 12.4(24)T (and crypto image/license)
Cryptographically Generated Addresses
CGA RFC 3972 (Simplified)

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

<table>
<thead>
<tr>
<th>Subnet</th>
<th>Prefix</th>
<th>Interface Identifier</th>
<th>Modifier</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Public Key</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Subnet Prefix</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Signature</td>
</tr>
</tbody>
</table>

SeND Messages -> Crypto. Generated Address

SHA-1
Securing Neighbour and Router Advertisements with SeND

- Adding a X.509 certificate to RA
- Subject Name contains the list of authorised IPv6 prefixes
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
First Hop Security: RAguard since 2010

- **Port ACL** blocks all ICMPv6 RA from hosts
  
  ```
  interface FastEthernet0/2
  ipv6 traffic-filter ACCESS_PORT in
  access-group mode prefer port
  ```

- **RA-guard lite** (12.2(33)SX14 & 12.2(54)SG): also dropping all RA received on this port
  
  ```
  interface FastEthernet0/2
  ipv6 nd raguard
  access-group mode prefer port
  ```

- **RA-guard** (12.2(50)SY, 15.0(2)SE)
  
  ```
  ipv6 nd raguard policy HOST device-role host
  ipv6 nd raguard policy ROUTER device-role router
  ipv6 nd raguard attach-policy HOST vlan 100
  interface FastEthernet0/0
  ipv6 nd raguard attach-policy ROUTER
  ```
RA-Guard

Goal: mitigate against rogue RA

- Configuration-based
- Learning-based
- Challenge-based

I am the default gateway

Router Advertisement Option: prefix(s)

Switch selectively accepts or rejects RAs based on various criteria’s
- Can be ACL based, learning based or challenge (SeND) based.
- Hosts see only allowed RAs, and RAs with allowed content
First Hop Security in June 2012

- IPv6 port ACL & RA Guard lite: 12.2(54)SG, 3.2.0SG, 15.0(2)SG, 12.2(33)SXI4

- NDP inspection (binding integrity guard): 12.2(50)SY, 15.0(1)SY, 15.0(2)SE

For more Information:
# IPv6 and the LAN Access

<table>
<thead>
<tr>
<th>IPv6 FHS</th>
<th>C6K</th>
<th>C4K</th>
<th>C3K</th>
<th>C2K</th>
<th>WLC</th>
</tr>
</thead>
<tbody>
<tr>
<td>RA Guard</td>
<td>12.2(50)SY and 15.0(1)SY</td>
<td>12.2(54)S G</td>
<td>15.0(2)S E</td>
<td>15.0(2)S E</td>
<td>7.2</td>
</tr>
<tr>
<td>DHCP Guard</td>
<td>2013</td>
<td>Q4 CY12</td>
<td>15.0(2)S E</td>
<td>15.0(2)S E</td>
<td>7.2</td>
</tr>
<tr>
<td>Binding Integrity Guard</td>
<td>2013</td>
<td>Q4 CY12</td>
<td>15.0(2)S E</td>
<td>15.0(2)S E</td>
<td>7.2</td>
</tr>
<tr>
<td>Source Guard</td>
<td>2013</td>
<td>MID 2013</td>
<td>15.0(2)S E</td>
<td>15.0(2)S E</td>
<td>7.2</td>
</tr>
<tr>
<td>Destination Guard</td>
<td>2013</td>
<td>Q4 CY12</td>
<td>15.0(2)S E</td>
<td>15.0(2)S E</td>
<td>7.2</td>
</tr>
</tbody>
</table>
**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></td>
<td>X</td>
</tr>
<tr>
<td>Address Resolution</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Router Discovery</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Multicast Group Management</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Mobile IPv6 Support</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

=> ICMP policy on firewalls needs to change
### 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>

![Diagram of Internet, Internet Server A, and Firewall](image)
### Equivalent ICMPv6

**RFC 4890: 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—HL 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>
Potential Additional ICMPv6

RFC 4890: 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>4</td>
<td>0</td>
<td>Parameter Problem</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>135/136</td>
<td>0</td>
<td>Neighbour Solicitation and Advertisement</td>
</tr>
<tr>
<td>Deny</td>
<td>Any</td>
<td>Any</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Information Leak with Hop-Limit

- IPv6 hop-limit has identical semantics as IPv4 time-to-live
- Can be leveraged by design
  - To ensure packet is local iff hop-limit = 255
  - Notably used by Neighbour Discovery
- Can be leveraged by malevolent people
  - Guess the remote OS: Mac OS/X always set it to 64
  - Evade inspection: hackers send some IPv6 packets analysed by the IPS but further dropped by the network before reaching destination… Could evade some IPS
  - Threat: low and identical to IPv4
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 rely on transport mode IPsec (for authentication and confidentiality)
  - But see draft-ietf-ospf-auth-trailer-ospfv3

- IPv6 routing attack best practices
  - Use traditional authentication mechanisms on BGP and IS-IS
  - Use IPsec to secure protocols such as OSPFv3
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 2011 12:00:00 Jan 1 2012
send-lifetime local 00:00:00 Jan 1 2012 23:59:59 Dec 31 2013

No crypto maps, no ISAKMP: transport mode with static session keys
IPv6 Attacks with Strong IPv4 Similarities

- **Sniffing**
  - IPv6 is no more or less likely to fall victim to a sniffing attack than IPv4

- **Application layer attacks**
  - The majority of vulnerabilities on the Internet today are at the application layer, something that IPSec will do nothing to prevent

- **Rogue devices**
  - Rogue devices will be as easy to insert into an IPv6 network as in IPv4

- **Man-in-the-Middle Attacks (MITM)**
  - Without strong mutual authentication, any attacks utilising 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 were new and could be buggy
- Some examples

<table>
<thead>
<tr>
<th>CVE-2011-2393</th>
<th>Feb 2012</th>
<th>FreeBSD, OpenBSD, NetBSD and others</th>
<th>Local users DoS with RA flooding</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2010-4563</td>
<td>Feb 2012</td>
<td>Linux</td>
<td>Remote detection of promiscuous mode</td>
</tr>
<tr>
<td>CVE-2011-2059</td>
<td>Oct 2011</td>
<td>IOS</td>
<td>Remote OS detection with ICMP + HbH</td>
</tr>
<tr>
<td>CVE-2008-1576</td>
<td>Jun 2008</td>
<td>Apple Mac OS X</td>
<td>Buffer overflow in Mail over IPv6</td>
</tr>
<tr>
<td>CVE-2010-4669</td>
<td>Jan 2011</td>
<td>Microsoft</td>
<td>Flood of forged RA DoS</td>
</tr>
</tbody>
</table>

Source: [http://cve.mitre.org/cve/](http://cve.mitre.org/cve/)
Specific IPv6 Issues
IPv6 Privacy Extensions (RFC 4941)

- Temporary addresses for IPv6 host client application, e.g. web browser
  - Inhibit device/user tracking
  - Random 64 bit interface ID, then run Duplicate Address Detection before using it
  - Rate of change based on local policy
- Enabled by default in Windows, Android, iOS 4.3, Mac OS/X 10.7

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

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

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

- Alternatively disabling stateless auto-configuration and force DHCPv6
  - Send Router Advertisements with
  - all prefixes with A-bit set to 0 (disable SLAAC)
  - M-bit set to 1 to force stateful DHCPv6
  - Use DHCP to a specific pool + ingress ACL allowing only this pool

  ```
  interface fastEthernet 0/0
  ipv6 nd prefix default no-autoconfig
  ipv6 dhcp server . . . (or relay)
  ipv6 nd managed-config-flag
  ```
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?
  - Mitigation: a firewall such as ASA which can filter on headers

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 => MATCH
  - Or unknown extension header/layer 4 header found... => NO MATCH
In IPv6 fragmentation is done only by the end system
- Tunnel end-points are end systems => Fragmentation / re-assembly can happen inside the network
- Reassembly done by end system like in IPv4
- RFC 5722: overlapping fragments => MUST drop the packet. Most OS implement it in 2012
- 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 must be fragmented!
- RFC 3128 is not applicable to IPv6
- Layer 4 information could be in 2nd fragment

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

Layer 4 header is in 2nd fragment
 Parsing the Extension Header Chain Fragments and Stateless Filters

- RFC 3128 is not applicable to IPv6
- Layer 4 information could be in 2nd fragment
- But, stateless firewalls could not find it if a previous extension header is fragmented

IPv6 hdr | HopByHop | Routing | Fragment1 | Destination …
---------|----------|---------|-----------|--------------

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

Layer 4 header is in 2nd fragment, Stateless filters have no clue where to find it!
IPv6 Fragmentation & 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)

- underdetermined-transport keyword does not match
  - TCP/UDP/SCTP and ports are in the fragment
  - ICMP and type and code are in the fragment
  - Everything else matches (including OSPFv3, …)
  - Only for deny ACE
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.

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
Enabling IPv6 in the IPv4 Data Centre
The Fool’s Way

1) I want IPv6, send RA

2) Sending RA with prefix for auto-configuration

3) Yahoo! IPv6 ☑

4) Default protection…

IPv6 Protection:
No ip6tables ✗

IPv6 Protection:
No ip6fw ✗

IPv6 Protection:
Security Centre ✓
Enabling IPv6 in the IPv4 Data Centre
The Right Way

1) I want IPv6, send RA

2) Sending RA with “no auto-config”

3) Yahoo! Static IPv6 address

3) No IPv6 SLAAC

IPv4 protection: iptables

IPv4 Protection: Security Centre

IPv4 protection: ipfw

Mac
IPv6 Tunneling Summary

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

- Only allow authorised endpoints to establish tunnels
- Static tunnels are deemed as “more secure,” but less scalable
- Automatic tunnelling 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
- And more to come to transport IPv4 over IPv6…
L3-L4 Spoofing in IPv6 When Using IPv6 over IPv4 Tunnels

- Most IPv4/IPv6 transition mechanisms have no authentication built in
- \( \Rightarrow \) an IPv4 attacker can inject traffic if spoofing on IPv4 and IPv6 addresses

IPv6 ACLs Are Ineffective since IPv4 & IPv6 are spoofed
Tunnel termination forwards the Inner IPv6 Packet
Looping Attack Between 2 ISATAP Routers (RFC 6324)

- **Root cause**
  - ISATAP routers ignore each other

- **ISATAP router:**
  - accepts native IPv6 packets
  - forwards it inside its ISATAP tunnel
  - Other ISATAP router decaps and forward as native IPv6

1. Spoofed IPv6 packet
   S: 2001:db8:2::200:5efe:c000:201
   D: 2001:db8:1::200:5efe:c000:202

2. IPv4 ISATAP packet to 192.0.0.2 containing
   S: 2001:db8:2::200:5efe:c000:201
   D: 2001:db8:1::200:5efe:c000:202

3 IPv6 packet
   S: 2001:db8:2::200:5efe:c000:201
   D: 2001:db8:1::200:5efe:c000:202

- **Mitigation:**
  - IPv6 anti-spoofing everywhere
  - ACL on ISATAP routers accepting IPv4 from valid clients only
  - Within an enterprise, block IPv4 ISATAP traffic between ISATAP routers
  - Within an enterprise block IPv6 packets between ISATAP routers

Repeat until Hop Limit == 0
ISATAP/6to4 Tunnels Bypass ACL

Direct tunneled traffic ignores hub ACL
TEREDO?

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

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

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

- **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)

Note: on Windows Teredo is:
- Disabled when firewall is disabled
- Disabled when PC is part of Active Directory domain
- Else enabled
- User can override this protection
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 registry
  - HKLM\SYSTEM\CurrentControlSet\Services\tcpip6\Parameters\DisabledComponents
  - But Microsoft does not test any Windows application with IPv6 disabled
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)
Enforcing a Security Policy
PCI DSS Compliance and IPv6

- Payment Card Industry Data Security Standard (latest revision October 2010):
  - **Requirement 1.3.8** Do not disclose private IP addresses and routing information to unauthorised parties.
  - Note: Methods to obscure IP addressing may include, but are not limited to:
    - Network Address Translation (NAT)

- There is no NAT n:1 IPv6 <-> IPv6 in most of the firewalls
  - RFC 6296 Network Prefix Translation for IPv6 (NPT6) is stateless 1:1 where inbound traffic is always mapped.
  - RFC 6296 is mainly for multi-homing and does not have any security benefit (not that NAT n:1 has any…)

- Use application proxies to comply with PCI DSS

- PCI DSS 2.0 Third Edition (December 2012) should be IPv6 aware
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:
  - VLAN ACL only in 15.0(1)SY
  - Port ACL on Nexus-7000, Cat 3750 (12.2(46)SE not in base image), Cat 4K (12.2(54)SG), Cat 6K (12.3(33)SX14)
IOS IPv6 Extended ACL

- Can match on
  - Upper layers: TCP, UDP, SCTP port numbers, ICMPv6 code and type
  - TCP flags SYN, ACK, FIN, PUSH, URG, RST
  - 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 destination options
  - auth matches AH
  - hbh matches hop-by-hop (since 15.2(3)T)

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

- undetermined-transport keyword does not match
  - TCP/UDP/SCTP and ports are in the fragment
  - ICMP and type and code are in the fragment
  - Everything else matches (including OSPFv3, …)
  - Only for deny ACE

Check your platform & release as your mileage can vary…
IPv6 ACL Implicit Rules
RFC 4890

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

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

- Nexus 7000 also allows RS & RA
IPv6 ACL Implicit Rules – Cont.

Adding a deny-log

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

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

- Solution, explicitly add the implicit ACE

```
! Now log all denied packets
permit icmp any any nd-na
permit icmp any any nd-ns
deny ipv6 any any log
```
Example: Rogue RA & DHCP Port ACL

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

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

Note: PACL replaces RACL for the interface (or is merged with RACL 'access-group mode prefer port')
In August 2010, Nexus-7000, Cat 3750 12.2(46)SE, Cat 4500 12.2(54)SG and Cat 6500 12.2(33)SXI4
IPv6 ACL to Protect VTY

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

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

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

Does not exist for protecting HTTP server => use ACL
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)

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

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

```
mls rate-limit all ttl-failure 1000
mls rate-limit unicast cef glean 1000
```
ASA Firewall IPv6 Support

- Since version 7.0 (April 2005)
- Dual-stack, IPv6-only, IPv4-only
- Extended IP ACL with stateful inspection
- Application awareness: TTP, FTP, telnet, SMTP, TCP, SSH, UDP
- uRPF and v6 Frag guard
- IPv6 header security checks (length & order)
- Management access via IPv6: Telnet, SSH, HTTPS
- ASDM support (ASA 8.2)
- Routed & transparent mode (ASA 8.2)
- Fail-over support (ASA 8.2.2)
- Selective permit/deny of extension headers (ASA 8.4.2)
- OSPFv3, DHCPv6 relay, stateful NAT64/46/66 (ASA 9.0)
ASA 8.4.2 : IPv6 Extension Header Filtering
## ASA 9.0 Mixed Mode Objects

### Configuration > Firewall > Objects > Network Objects/Groups

<table>
<thead>
<tr>
<th>Name</th>
<th>IP Address</th>
<th>Netmask</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>any</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2001:e00::0/64</td>
<td>2001:e00::0/64</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12eb:00:00:cd30:123:4567:89eb:cd6f</td>
<td>12eb:00:00:cd30:123:4567:89eb:cd6f</td>
<td></td>
<td></td>
</tr>
<tr>
<td>my_host</td>
<td>192.168.1.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>my_host_ipv6</td>
<td>2620:144:b20:200</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Configuration > Firewall > Objects > Network Object Groups

<table>
<thead>
<tr>
<th>Name</th>
<th>IP Address</th>
<th>Netmask</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>my_host</td>
<td>192.168.1.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>my_host_ipv6</td>
<td>2620:144:b20:200</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
IPS Supports IPv6

- Since IPS 6.2 (November 2008)
- Engines
  - Specific to IPv6
  - Common to IPv4 and IPv6
  - TCP reset works over IPv4
- **IPS Manager Express** can view IPv6 events
- **IPS Device Manager** can configure IPv6
- All management plane is over IPv4 only
  - Not critical for most customers
Dual-Stack IPS Engines

Service HTTP

<table>
<thead>
<tr>
<th>Sig. Name</th>
<th>Sig. ID</th>
<th>Attacker IP</th>
<th>Victim IP</th>
<th>Victim Port</th>
<th>Th.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dot Dot Slash in URI</td>
<td>5256/0</td>
<td>192.168.200.46</td>
<td>192.168.200.38</td>
<td>80</td>
<td></td>
</tr>
<tr>
<td>Dot Dot Slash in URI</td>
<td>5256/0</td>
<td>2001:db8:0:0:0:0:0:46</td>
<td>2001:db8:0:0:0:0:0:38</td>
<td>80</td>
<td></td>
</tr>
</tbody>
</table>
Dual-Stack Engine
String TCP with Custom Signature

- Yet another example of an engine supporting both IPv4 and IPv6
IPv6-Only Engines

- Atomic IPv6 (mostly obsolete)
- Atomic IP Advanced
  - Routing Header type 0
  - Hop-by-Hop
  - ...
- Missing
  - Rogue RA
  - Rogue NA
Summary of Cisco IPv6 Security Products

- **ASA Firewall**
  - Since version 7.0 (released 2005)
  - Flexibility: Dual stack, IPv6 only, IPv4 only
  - SSL VPN for IPv6 over IPv4 (ASA 8.0) over IPv6 (ASA 9.0)
  - Stateful-Failover (ASA 8.2.2)
  - Extension header filtering and inspection (ASA 8.4.2)
  - Dual-stack ACL & object grouping (ASA 9.0)

- **ASA-SM**
  - Leverage ASA code base, same features ;-) 16 Gbps of IPv6 throughput

- **FWSM**
  - IPv6 in software... 80 Mbps … Not an option (put an IPv6-only ASA in parallel or migrate to ASA-SM)

- **IOS Firewall**
  - IOS 12.3(7)T (released 2005)
  - Zone-based firewall on IOS-XE 3.6 (2012)

- **IPS**
  - Since 6.2 (released 2008)

- **Email Security Appliance (ESA)** under beta testing since 2010, IPv6 support since 7.6.1 (May 2012)

- **Web Security Appliance (WSA)** with explicit proxy then transparent mode, work in progress (end of 2013)

- **ScanSafe** expected to be available in 2012
Security IPv6 Connectivity
## 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>
</table>
| IPv4           | • 6in4/GRE Tunnels Protected by IPsec  
                • DMVPN 12.4(20)T | • ISATAP Protected by RA IPsec  
                • SSL VPN Client AnyConnect |
| IPv6           | • IPsec VTI 12.4(6)T  
                • DMVPN 15.2(1)T | • AnyConnect 3.1 & ASA 9.0 |
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)
  - In IOS-XE release 3.5 (end 2011)
  - 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

```conf
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 3.0 (Windows, Android, iPhone)
  - Can transfer IPv4+IPv6 traffic over public IPv4
    - DNS is still IPv4-only, no split tunnelling only
  - Mid-2012 with ASA and AnyConnect, IPv4+IPv6 traffic over public IPv6 and over IPsec or SSL (roadmap, date can change)
Secure RA IPv6 Traffic over IPv4 Public Network: ISATAP in IPSec

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

IPv6 PC
IPv6 Network
IPv4
ISATAP Tunnel server on dual stack router
Enterprise VPN head-end (ASA, IOS, ...)

IPsec with NAT-T can traverse NAT
ISATAP encapsulates IPv6 into IPv4
Secure RA IPv* over IPv* Public Network: AnyConnect SSL VPN Client 3.1 & ASA 9.0
Summary
Key Take Away

- So, nothing really new in IPv6
  - Reconnaissance: address enumeration replaced by DNS enumeration
  - Spoofing & bogons: uRPF is our IP-agnostic friend
  - NDP spoofing: RA guard and more feature coming
  - ICMPv6 firewalls need to change policy to allow NDP
  - Extension headers: firewall & ACL can process them
  - Amplification attacks by multicast mostly impossible
  - Potential loops between tunnel endpoints: ACL must be used

- Lack of operation experience may hinder security for a while: training is required

- Security enforcement is possible
  - Control your IPv6 traffic as you do for IPv4

- Leverage IPsec to secure IPv6 when suitable
Is IPv6 in My Network?

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

IPv6 Security
Information assurance for the next-generation Internet Protocol

IPv6 for Enterprise Networks

Cisco Firewalls
Concepts, design and deployment for Cisco Stealthy Firewall solutions
Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2013 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site [www.ciscoliveaustralia.com/mobile](http://www.ciscoliveaustralia.com/mobile)
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 8 March 12:00pm-2:00pm

Don’t forget to activate your Cisco Live 365 account for access to all session material, communities, and on-demand and live activities throughout the year. Log into your Cisco Live portal and click the "Enter Cisco Live 365" button.