IPv6 Security

Training Course

January 2023
Please Follow Our Safety Measures

- **Self-test**
  Please test yourself and keep everyone safe

- **Get a mask**
  Use a mask if this is required at the location

- **Sanitise your hands**
  Particularly when entering and leaving rooms

- **Respect each other's space**
  - **Red sticker:** Please keep 1.5 m distance
  - **Yellow sticker:** Elbow bumps only please
  - **Green sticker:** You can stand closer
Copyright Statement

[...]

The RIPE NCC Materials may be used for **private purposes**, for public non-commercial purpose, for research, for educational or demonstration purposes, or if the materials in question specifically state that use of the material is permissible, and provided the RIPE NCC Materials are not modified and are properly identified as RIPE NCC documents. Unless authorised by the RIPE NCC in writing, any use of the RIPE NCC Materials for advertising or marketing purposes is strictly forbidden and may be prosecuted. The RIPE NCC should be notified of any such activities or suspicions thereof.

[...]
09:00 - 09:30  Coffee, Tea
11:00 - 11:15  Break
13:00 - 14:00  Lunch
15:30 - 15:45  Break
17:30  End
Introductions

- Name
- Experience with Security and IPv6
- Goals
## Introduction

### Basic IPv6 Protocol Security
Basic header, Extension Headers, Addressing

### IPv6 Associated Protocols Security
ICMPv6, NDP, MLD, DNS, DHCPv6

### Internet-wide IPv6 Security
Filtering, DDoS, Transition Mechanisms

### Tips and Tools
Up-to-date information, Security Tools, Device features
Legend

- **Legend**
  - **Attacker**
  - **Learning / Understanding**
  - **Protecting**
Introduction to IPv6 Security

Section 1
IPv6 is Happening...

<table>
<thead>
<tr>
<th>RANK</th>
<th>IPV6%</th>
<th>COUNTRY / REGION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>59.3%</td>
<td>India</td>
</tr>
<tr>
<td>2</td>
<td>57.2%</td>
<td>Belgium</td>
</tr>
<tr>
<td>3</td>
<td>53.9%</td>
<td>Germany</td>
</tr>
<tr>
<td>4</td>
<td>52.1%</td>
<td>Saudi Arabia</td>
</tr>
<tr>
<td>5</td>
<td>51%</td>
<td>Montserrat</td>
</tr>
<tr>
<td>6</td>
<td>50.5%</td>
<td>Uruguay</td>
</tr>
<tr>
<td>7</td>
<td>50.4%</td>
<td>Malaysia</td>
</tr>
<tr>
<td>8</td>
<td>49.6%</td>
<td>France</td>
</tr>
<tr>
<td>9</td>
<td>48.1%</td>
<td>Viet Nam</td>
</tr>
<tr>
<td>10</td>
<td>47.9%</td>
<td>Japan</td>
</tr>
<tr>
<td>11</td>
<td>47.8%</td>
<td>Greece</td>
</tr>
<tr>
<td>12</td>
<td>46.6%</td>
<td>Luxembourg</td>
</tr>
<tr>
<td>13</td>
<td>45.1%</td>
<td>Switzerland</td>
</tr>
<tr>
<td>14</td>
<td>43.8%</td>
<td>Mexico</td>
</tr>
</tbody>
</table>

... and So Are IPv6 Security Threats!
IPv6 Security Statements

- IPv6 is more secure than IPv4
- IPv6 has better security and it’s built in

Reason:
- RFC 4294 - IPv6 Node Requirements: IPsec MUST

Reality:
- RFC 8504 - IPv6 Node Requirements: IPsec SHOULD
- IPsec available. Used for security in IPv6 protocols
### IPv6 Security Statements

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>IPv6 has no NAT. Global addresses used</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>I’m exposed to attacks from Internet</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Reason:**

- End-2-End paradigm. Global addresses. No NAT

**Reality:**

- Global addressing does not imply global reachability
- You are responsible for reachability (filtering)
IPv6 Security Statements

- IPv6 Networks are too big to scan

**Reason:**
- Common LAN/VLAN use /64 network prefix
- 18,446,744,073,709,551,616 hosts

**Reality:**
- Brute force scanning is not possible [RFC5157]
- New scanning techniques
IPv6 Security Statements

• IPv6 is too new to be attacked

Reason:

• Lack of knowledge about IPv6 (it’s happening!)

Reality:

• There are tools, threats, attacks, security patches, etc.
• You have to be prepared for IPv6 attacks
### IPv6 Security Statements

**Reason:**
- Routing and switching work the same way

**Reality:**
- Whole new addressing architecture
- Many associated new protocols

- IPv6 is just IPv4 with 128 bits addresses
- There is nothing new
IPv6 Security Statements

Reason:

• Question: “Does it support IPv6?”
• Answer: “Yes, it supports IPv6”

Reality:

• IPv6 support is not a yes/no question
• Features missing, immature implementations, interoperability issues
### IPv6 Security Statements

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
</table>

- IPv6 is not a security problem in my IPv4-only network

**Reason:**
- Networks only designed and configured for IPv4

**Reality:**
- IPv6 available in many hosts, servers, and devices
- Unwanted IPv6 traffic. Protect your network
IPv6 Security Statements

Reason:
• Considering IPv6 completely different than IPv4
• Think there are no BCPs, resources or features

Reality:
• Use IP independent security policies
• There are BCPs, resources and features
Conclusions

A change of mindset is necessary

- IPv6 is not more or less secure than IPv4
- Knowledge of the protocol is the best security measure
Basic IPv6 Protocol
Security
Section 2
IPv6 Basic Header and Extension Headers

Section 2.1
Basic IPv6 Header: Threat #1

<table>
<thead>
<tr>
<th>Version</th>
<th>Traffic Class</th>
<th>Flow Label</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Payload Length</td>
<td>Next Header</td>
<td>Hop Limit</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Source Address</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Destination Address</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Basic IPv6 Header: Threat #1

**IP spoofing:**
Using a fake IPv6 source address

**Solution:**
Ingress filtering and RPF (*reverse path forwarding*)
## Basic IPv6 Header: Threat #2

<table>
<thead>
<tr>
<th>Version</th>
<th>Traffic Class</th>
<th>Flow Label</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Payload Length</td>
<td>Next Header</td>
<td>Hop Limit</td>
</tr>
<tr>
<td>Source Address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Destination Address</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Basic IPv6 Header: Threats #2

Covert Channel:
Using Traffic Class and/or Flow Label

Solution:
Inspect packets (IDS / IPS)
Expected values:
- Traffic Class: 0 (unless QoS is used)
- Flow Label: 0
IPv6 Extension Headers

Basic IPv6 Header → Hop-by-hop Options → Routing → Fragment → IPsec: AH → IPsec: ESP → Destination Options** → Upper Layer

* Options for IPs in routing header
** Options for destination IP
# Extension Headers Properties

<table>
<thead>
<tr>
<th></th>
<th>Property</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>Flexible</strong> <em>(use is optional)</em></td>
</tr>
<tr>
<td>2</td>
<td><strong>Only appear once</strong> <em>(except Destination options)</em></td>
</tr>
<tr>
<td>3</td>
<td><strong>Fixed</strong> <em>(types and order)</em></td>
</tr>
<tr>
<td>4</td>
<td><strong>Processed only at endpoints</strong> <em>(except Hop-by-Hop and Routing)</em></td>
</tr>
</tbody>
</table>
• Flexibility means **complexity**

• Security devices / software must process the **full chain of headers**

• Firewalls must be able to filter based on **Extension Headers**
Routing Header

Includes one or more IPs that should be “visited” in the path

- Processed by the **visited routers**

<table>
<thead>
<tr>
<th>8 bits</th>
<th>8 bits</th>
<th>8 bits</th>
<th>8 bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next Header</td>
<td>Length</td>
<td>Routing Type</td>
<td>Segments Left</td>
</tr>
</tbody>
</table>

Specific data of that Routing Header type
Routing Header Threat

• Routing Header (Type 0):
  - RH0 can be used for traffic amplification over a remote path

• RH0 Deprecated [RFC5095]
  - RH1 deprecated. RH2 (MIPv6), RH3 (RPL) and RH4 (SRH) are valid

Basic Hdr  
S | D  
Segs = 127

Addr[1] = A  
Addr[2] = B  
Addr[126] = B  
Addr[127] = A

Basic Hdr  
S | A  
Segs = 127

Addr[1] = B  
Addr[2] = A  
Addr[126] = A  
Addr[127] = D

Basic Hdr  
S | B  
Segs = 126

Attacker  
S

Basic Hdr  
S | D  
Segs = 125

Basic Hdr  
S | B  
Segs = 124

Basic Hdr  
S | A  
Segs = 125

Basic Hdr  
S | B  
Segs = 124

Basic Hdr  
S | A  
Segs = 1

Basic Hdr  
S | B  
Segs = 0

Basic Hdr  
S | D  
Segs = 0

Target  
D
Extension Headers Solutions

- Require security tools to inspect Header Chain properly

Use of RH0

Deprecated [RFC5095]
Do not use or allow
**Fragment Header**

- Used by IPv6 source node to send a packet **bigger than path MTU**
- **Destination host** processes fragment headers

<table>
<thead>
<tr>
<th>8 bits</th>
<th>8 bits</th>
<th>13 bits</th>
<th>2 bits</th>
<th>1 bit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next Header</td>
<td>Reserved</td>
<td>Fragment Offset</td>
<td>Res</td>
<td>M</td>
</tr>
</tbody>
</table>

**Identification**

32 bits

**M Flag:**
1 = more fragments to come;
0 = last fragment
EH Threats: Fragmentation

- Overlapping Fragments
- Not Sending Last Fragment
- “Atomic” Fragments

Fragments that overlap because of wrong “fragment offset”
Waiting for last fragment Resource consumption
Packet with Frag. EH is the only fragment (Frag. Offset and M = 0)
EH Solutions: Fragmentation

- **Overlapping Fragments**: Not allowed in IPv6 [RFC5722]. Packets are discarded.

- **Not Sending Last Fragment**: Timer and discard packets (default 60 secs).

- **“Atomic” Fragments**: Processed in isolation from any other packets/fragments [RFC6946].
# Bypassing RA Filtering/RA-Guard

Using **any** Extension Header

<table>
<thead>
<tr>
<th>Basic IPv6 Header</th>
<th>Destination Options</th>
<th>ICMPv6: RA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next Header = 60</td>
<td>Next Header = 58</td>
<td></td>
</tr>
</tbody>
</table>

If it only looks at Next Header = 60, it **does not detect** the RA
Bypassing RA Filtering/RA-Guard

Using **Fragment** Extension Header

<table>
<thead>
<tr>
<th>Basic IPv6 Header</th>
<th>Fragment</th>
<th>Destination Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next Header = 44</td>
<td>Next Header = 60</td>
<td>Next Header = 58</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Basic IPv6 Header</th>
<th>Fragment</th>
<th>Destination Options</th>
<th>ICMPv6: RA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next Header = 44</td>
<td>Next Header = 60</td>
<td>Next Header = 58</td>
<td></td>
</tr>
</tbody>
</table>

**Needs all fragments to detect the RA**
Extension Headers Solutions

- **Fragmented NDP packets**
  - **Forbidden [RFC6980]**
    - Do not use or allow

- **Other attacks based on Extension Headers**
  - **Header chain should go in the first fragment [RFC7112]**
  - **Recommendations to avoid the problem [RFC7113]**

- **Require** security tools to inspect Header Chain properly
IPsec - Security Protocols

Authentication Header (AH)
- Provides Integrity
  - MAY be implemented

Encapsulating Security Payload (ESP)
- Provides Confidentiality and Integrity
  - MUST be implemented
**IPsec**

**Security Policy Database** indicates what to do with packets

**Security Association:** info needed for IPsec with 1 host, 1 direction

**Internet Key Exchange** allows automatic creation of SAs
IPsec Modes

Tunnel Mode
IPv6 | IPsec IPv6 | Upper Layers

Transport Mode
IPv6 | IPsec Upper Layers
IPsec: Authentication Header

Unprotected IPv6

IPv6 | EHs | Upper Layers

AH in Transport Mode

IPv6 | EH1 | AH | EH2 | Upper Layers

EH1 = Hop-by-Hop, Dest. Options*, Routing, Fragment

EH2 = Destination Options**

AH in Tunnel Mode

IPv6 | EHs | AH | IPv6 | EHs | Upper Layers

* Options for IPs in routing header

** Options for destination IP
IPsec: ESP

Unprotected IPv6

IPv6  EHs  Upper Layers

ESP in Transport Mode

IPv6  EH1  ESP  EH2  Upper Layers  ESP Trailer  ICV

ESP in Tunnel Mode

IPv6  EHs  ESP  IPv6  EHs  Upper Layers  ESP Trailer  ICV

EH1 = Hop-by-Hop, Dest. Options*, Routing, Fragment
EH2 = Destination Options**

* Options for IPs in routing header
** Options for destination IP
IPv6 Packet Generation

Exercise 2.1
Exercise 2.1: IPv6 Packet Generation

- **Description**: Use Scapy to generate IPv6 packets
- **Goals**:
  - Get familiar with lab environment
  - Learn the basics of Scapy tool
  - Learn to generate tailor made IPv6 packets
- **Time**: 30 minutes
- **Tasks**:
  - Login in to the lab environment
  - Generate IPv6 packets following instructions in Exercise Booklet
Exercise 2.1: Lab network

HOST A
HOST B
HOST C

ROUTER

USER X
Network Prefix:
2001:DB8:F::/64

eth0
::1
IPv6 Addressing
Architecture
Section 2.2
340,282,366,920,938,463,463,374,607,431,768,211,456

End-to-end

Multiple Addresses
- Link-local
- Global (GUA)
- Multicast
IPv6 Address Scope

fe80::a:b:100  ff01::2  2001:67c:2e:1::c1

fd00:a:b::100  ff05::1:3  ff02::1
IPv6 Network Scanning

Network Prefix determination (64 bits)
- Common patterns in addressing plans
- DNS direct and reverse resolution
- Traceroute

Interface ID determination (64 bits)
- "brute force" no longer possible
IID Generation Options

64 bits

Interface ID (IID)

- Modified EUI-64 (uses MAC address)
- Stable, semantically opaque [RFC7217]
- Temporary Address Extensions [RFC8981]
- DHCPv6
- Manually
- Others (CGA, HBA)

“stable” IID for SLAAC

“temporary” IID for SLAAC
SLAAC IIDs Currently

• Consider IID bits “opaque”, no value or meaning [RFC7136]

How to generate IIDs [RFC7217]

Different for each interface in the same network prefix

Not related to any fixed interface identifier

Always the same when same interface connected to same network

• Widely used and standardised for “stable” addresses [RFC8064]
Guessing IID

64 bits = 18,446,744,073,709,551,616 Addresses

- EUI-64
  - OUI: 24 bits
  - FF: 16 bits
- IPv4-based
  - 2001:db8:1::10.0.0.5
- Sequential
- Low-bits / Trivial (::1)
- Service port
  - 2001:db8:1::80
- Wordy Address
  - 2001:db8::bad:cafe
Locally Scanning IPv6 Networks

- Traffic Snooping
- Dual-stack
- Routing Protocols
- Local Protocols
- Local Scanning

LLMNR [RFC4795]
Multicast DNS (mDNS) [RFC6762]
DNS Service Discovery (DNS-SD) [RFC6763]
## Special / Reserved IPv6 Addresses

<table>
<thead>
<tr>
<th>Name</th>
<th>IPv6 Address</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unspecified</td>
<td>::/128</td>
<td>When no address available</td>
</tr>
<tr>
<td>Loopback</td>
<td>::1/128</td>
<td>For local communications</td>
</tr>
<tr>
<td>IPv4-mapped</td>
<td>::ffff:0:0/96</td>
<td>For dual-stack sockets. Add IPv4 address 32 bits</td>
</tr>
<tr>
<td>Documentation</td>
<td>2001:db8::/32</td>
<td>RFC 3849</td>
</tr>
<tr>
<td>IPv4/IPv6 Translators</td>
<td>64:ff9b::/96</td>
<td>RFC 6052</td>
</tr>
<tr>
<td>Discard-Only Address Block</td>
<td>100::/64</td>
<td>RFC 6666</td>
</tr>
<tr>
<td>Teredo</td>
<td>2001::/32</td>
<td>IPv6 in IPv4 Encapsulation Transition Mechanism</td>
</tr>
<tr>
<td>6to4</td>
<td>2002::/16</td>
<td>IPv6 in IPv4 Encapsulation Transition Mechanism</td>
</tr>
<tr>
<td>ORCHID</td>
<td>2001:10::/28</td>
<td>Deprecated RFC 5156</td>
</tr>
<tr>
<td>Benchmarking</td>
<td>2001:2::/48</td>
<td>RFC 5180</td>
</tr>
<tr>
<td>Link-local</td>
<td>fe80::/10</td>
<td>RFC 4291</td>
</tr>
<tr>
<td>Unique-local</td>
<td>fc00::/7</td>
<td>RFC 4193</td>
</tr>
<tr>
<td>6Bone</td>
<td>3ffe::/16, 5f00::/8</td>
<td>Deprecated RFC 3701</td>
</tr>
<tr>
<td>IPv4-compatible</td>
<td>::/96</td>
<td>Deprecated RFC 5156</td>
</tr>
</tbody>
</table>

[http://www.iana.org/assignments/iana-ipv6-special-registry/](http://www.iana.org/assignments/iana-ipv6-special-registry/)
Security Tips

- Use hard to guess IIDs
  - RFC 7217 better than Modified EUI-64
  - RFC 8064 establishes RFC 7217 as the default
- Use IPS/IDS to detect scanning
- Filter packets where appropriate
- Be careful with routing protocols
- Use "default" /64 size IPv6 subnet prefix
Exercise 2.2: IPv6 Network Scanning

• **Description:** Use available toolsets to scan a subnet

• **Goals:**
  - Know about two new toolsets: THC-IPV6 and The IPv6 Toolkit
  - Learn how to use them to scan a subnet

• **Time:** 10 minutes

• **Tasks:**
  - Use The IPv6 Toolkit to scan your lab’s subnet
  - Use THC-IPV6 to scan your lab’s subnet
IPv6 Associated Protocols Security
Section 3
ICMPv6 [RFC4443] is an integral part of IPv6

**Error Messages**
- Destination Unreachable
- Packet Too Big
- Time Exceeded
- Parameter Problem

**Informational Messages**
- Echo Request
- Echo Reply
- NDP
- MLD
# ICMPv6 Format

- **General Format**

<table>
<thead>
<tr>
<th>8 bits</th>
<th>8 bits</th>
<th>16 bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Code</td>
<td>Checksum</td>
</tr>
</tbody>
</table>

  **Message Body**

- **Extended Format** \([RFC4884]\)

  **Used by:**
  - Destination Unreachable
  - Time Exceeded
## ICMPv6 Error Messages

<table>
<thead>
<tr>
<th>Type</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Destination Ureachable (1)</strong></td>
<td>No route to destination (0)</td>
</tr>
<tr>
<td></td>
<td>Communication with destination administratively prohibited (1)</td>
</tr>
<tr>
<td></td>
<td>Beyond scope of source address (2)</td>
</tr>
<tr>
<td></td>
<td>Address Unreachable (3)</td>
</tr>
<tr>
<td></td>
<td>Port Unreachable (4)</td>
</tr>
<tr>
<td></td>
<td>Source address failed ingress/egress policy (5)</td>
</tr>
<tr>
<td></td>
<td>Reject route to destination (6)</td>
</tr>
<tr>
<td></td>
<td>Error in Source Routing Header (7)</td>
</tr>
<tr>
<td><strong>Packet Too Big (2)</strong></td>
<td>Packet Too Big (0)</td>
</tr>
<tr>
<td>Parameter = next hop MTU</td>
<td></td>
</tr>
<tr>
<td><strong>Time Exceeded (3)</strong></td>
<td>Hop Limit Exceeded in Transit (0)</td>
</tr>
<tr>
<td></td>
<td>Fragment Reassembly Time Exceeded (1)</td>
</tr>
<tr>
<td><strong>Parameter Problem (4)</strong></td>
<td>Erroneous Header Field Encountered (0)</td>
</tr>
<tr>
<td>Parameter = offset to error</td>
<td>Unrecognized Next Header Type (1)</td>
</tr>
<tr>
<td></td>
<td>Unrecognized IPv6 Option (2)</td>
</tr>
<tr>
<td></td>
<td>IPv6 First Fragment has incomplete IPv6 Header Chain (3)</td>
</tr>
</tbody>
</table>
FILTER ICMPv6 CAREFULLY!

Used in many IPv6 related protocols
ICMPv6 Security

Packet with MULTICAST destination address

- No ICMPv6 Error message allowed as a response
- Echo Reply responding an Echo Request is Optional

avoids
- Hosts Discovery
- Amplification Attacks

not recommended
- Smurf Attacks
NDP

Section 3.2
NDP [RFC4861] is used on a link

**Messages**
- Neighbour Solicitation
- Neighbour Advertisement
- Router Solicitation
- Router Advertisement
- Redirect

**Used for:**
- Discovery: routers, prefixes, network parameters
- Autoconfiguration
- DAD
- NUD
- Address Resolution
Hop Limit = 255

if not then discard

NDP has vulnerabilities

[RFC3756]
[RFC6583]

Specification says to use IPsec

impractical, it’s not used

SEND [RFC3971]
(SEcure Neighbour Discovery)

Not widely available
NDP Threats

- Neighbor Solicitation/Advertisement Spoofing

- Can be done sending:
  1. **NS** with “source link-layer” option changed
  2. **NA** with “target link-layer” option changed
     - Can send unsolicited **NA** or as an answer to **NS**

- Redirection/DoS attack

- Could be used for a “**Man-In-The-Middle**” attack
NS Spoofing (Redirection / DoS)

### Neighbour Cache

<table>
<thead>
<tr>
<th>IP</th>
<th>MAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP1</td>
<td>11:11:11:11:11:11</td>
</tr>
<tr>
<td>IPr</td>
<td>12:34:56:78:9a:bc</td>
</tr>
<tr>
<td>IP2</td>
<td>aa:aa:aa:aa:aa:aa</td>
</tr>
</tbody>
</table>

### Neighbour Cache

<table>
<thead>
<tr>
<th>IP</th>
<th>MAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP1</td>
<td>11:11:11:11:11:11</td>
</tr>
<tr>
<td>IPr</td>
<td>12:34:56:78:9a:bc</td>
</tr>
<tr>
<td>IP2</td>
<td>aa:aa:aa:aa:aa:aa</td>
</tr>
</tbody>
</table>

### IPv6

<table>
<thead>
<tr>
<th>IPv6 Source IPv6</th>
<th>IPv2</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 Destination IPv6</td>
<td>IP1</td>
</tr>
<tr>
<td>NS.Target Addr</td>
<td>IP1</td>
</tr>
<tr>
<td>NS.Src Link-layer Addr</td>
<td>aa:aa:aa:aa:aa:aa</td>
</tr>
</tbody>
</table>

### ICMPv6 NS

IPa MACa = aa:aa:aa:aa:aa:aa

IPr MACr = 12:34:56:78:9a:bc

IP1 MAC1 = 11:11:11:11:11:11

Unsolicited NA (Redirection / DoS)

**IP1**
11:11:11:11:11:11

**IPr**
12:34:56:78:9a:bc

**IP2**
aa:aa:aa:aa:aa:aa

**IPv6**
**ICMPv6 NA**

**NA.Target Addr**
IP2

**NA.Target Link-layer Addr**
aa:aa:aa:aa:aa:aa

**IP1**
MAC1 = 11:11:11:11:11:11

**IPr**
MACr = 12:34:56:78:9a:bc

**IP2**

**IPa**
MACa = aa:aa:aa:aa:aa:aa
NUD Failure (DoS attack)
DAD (DoS Attack)

Answer to NS

NA

Answer to NS

NS

NS

DAD for IP before configuring it
NDP

Exercise 3.2-a
Exercise 3.2-a NDP

- **Description:** Create packets to poison neighbor cache
- **Goals:**
  - Practice with Scapy tool
  - Learn how to modify the neighbor cache of another host in the same network
- **Time:** 15 minutes
- **Tasks** (at least one of them):
  - Generate NS packets that change other host’s neighbor cache
  - Generate NA packets that change other host’s neighbor cache
3.2-a: Neighbor cache attack using NS

Neighbor Cache

# ip neighbour show


IPb | cc:cc:cc:cc:cc:cc

IPa | aa:aa:aa:aa:aa:aa
MACa = aa:aa:aa:aa:aa:aa

IPv6 | ICMPv6 NS

IPv6.Source IPv6 | IPb
IPv6.Destination IPv6 | IPa
NS.Target Addr | IPa
NS.Src Link-layer Addr | cc:cc:cc:cc:cc:cc


IPc | cc:cc:cc:cc:cc:cc
MACc = cc:cc:cc:cc:cc:cc

B

A

C
3.2-a: Neighbor cache attack using NA

Neighbor Cache

# ip neighbour show


IPb | cc:cc:cc:cc:cc:cc

IPa
MACa = aa:aa:aa:aa:aa:aa

IPb
MACb = bb:bb:bb:bb:bb:bbb

IPc
MACc = cc:cc:cc:cc:cc:cc

IPv6
ICMPv6 NA

NA.Target Addr | IPb
NA.Target Link-layer Addr | cc:cc:cc:cc:cc:cc
Malicious Last Hop Router

![Diagram of Malicious Last Hop Router]

- Periodic RAs
- Answer to RS (lifetime = 0)
- RS
Bogus On-Link Prefix

Prefixes on the Link
- google
- facebook
- amazon

DoS
- google is on the link
Bogus Address Configuration Prefix

this is your global prefix
2001:db8:bad:bad::/64

DoS
Parameter Spoofing: Hop Limit

Current Hop Limit: 3
Parameter Spoofing: DHCPv6

ATTACKER’S DHCP SERVER

M: 1
O: 1

DoS
Spoofed Redirect Message

Routes on Host 1:
::/0 - fe80::a:b:c
2001:db8::face:b00c - fe80::a

IPv6
IPv6.Source IPv6
IPv6.Destination IPv6
Redirect.Target Addr
Redirect.Dst Addr.

ICMPv6 Redirect

IPr = fe80::a:b:c
MACr = 12:34:56:78:9a:bc
IPa = fe80::a
MACa = aa:aa:aa:aa:aa:aa

IP1
MAC1 = 11:11:11:11:11:11

IP1
IPr = fe80::a:b:c
MACr = 12:34:56:78:9a:bc

11:11:11:11:11:11
12:34:56:78:9a:bc
Neighbour Discovery DoS Attack

Router Neighbour Cache

| IPa | aa:aa:aa:aa:aa:aa     |
| IPr | 12:34:56:78:9a:bc     |
| IP1 | ???                   |
| IPn | ???                   |

IPa (Pa) 2001:db8:a:b::/64

IPb (Pb)

Network Prefix (P) 2001:db8:a:b::/64

IPr = fe80::a:b:c
MACr = 12:34:56:78:9a:bc

IP1 = P::1
IP2 = P::2
IP3 = P::3
IPn = P::n
NDP

Exercise 3.2-b
Exercise 3.2-b NDP

- **Description**: Send RA messages to perform attacks

- **Goals**:
  - Practice with Scapy tool
  - Use RA messages to perform attacks on a link

- **Time**: 20 minutes

- **Tasks**:
  - Send RA messages with bogus address configuration prefix
First Hop Security

- Security implemented **on switches**
- There is a number of techniques available:
  - RA-GUARD
  - IPv6 Snooping (*ND inspection* + *DHCPv6 Snooping*)
  - IPv6 Source / Prefix Guard
  - IPv6 Destination Guard (*or ND Resolution rate limiter*)
  - MLD Snooping
  - DHCPv6 Guard
IPv6 Snooping
IPv6 Source / Prefix Guard
IPv6 Destination Guard
Rogue Router Advertisements
Rogue RA Solutions

1. Link Monitoring
2. SEND
3. MANUAL CONFIGURATION
   + Disable Autoconfig
4. Host Packet Filtering
5. Router Preference Option
   [RFC4191]
6. ACLs on Switches
7. RA Snooping on Switches (RA GUARD)
RA-GUARD \[RFC6105\]

- Easiest available solution
- Only allows RAs on legitimate ports on L2 switches
Implementing RA-GUARD

Stateless RA Guard
Decision based on RA message or static configuration

Stateful RA Guard
Learns dynamically
Filtering

- Use Access Control Lists (ACLs) in switches

Switches need to understand

<table>
<thead>
<tr>
<th>Ethernet</th>
<th>IPv6</th>
<th>ICMPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethertype 0x86DD for IPv6</td>
<td>Version 6</td>
<td>ICMPv6 Type and Code</td>
</tr>
<tr>
<td>Source/destination MAC address</td>
<td>Source/destination IPv6 address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Next Header</td>
<td></td>
</tr>
</tbody>
</table>
Filtering Example

(config)#ipv6 access-list RA-GUARD
(config-ipv6-acl)#sequence 3 deny icmp any any router-advertisement
(config-ipv6-acl)#sequence 6 permit ipv6 any any

(config-ipv6-acl)#exit

(config)#interface FastEthernet0/5
(config-if)#ipv6 traffic-filter RA-GUARD in
Conclusions / Tips

• NDP is an important, powerful and vulnerable protocol

• **Recommended**: use available solutions to protect NDP

• Detection (IDS/IPS) can be easier and recommended
• MLD (Multicast Listener Discovery) is:
  - Multicast related protocol, used in the local link
  - Two versions: MLDv1 and MLDv2
  - Uses ICMPv6
  - Required by NDP and “IPv6 Node Requirements”
  - IPv6 nodes use it when joining a multicast group
MLDv1

**QUERY**
Router asks for listeners

**REPORT**
Listeners report themselves

**DONE**
Listeners indicate that they're done

- General
- Specific
**QUERY**

**Src:** fe80::a  
**Dst:** FF02::1

**REPORT**

**Src:** fe80::2  
**Dst:** SolicitedNode(2)

**Src:** fe80::2  
**Dst:** SolicitedNode(2)
MLDv2

- Mandatory for all IPv6 nodes *(MUST)* [RFC8504]
- **Interoperable** with MLDv1
- Adds Source-Specific Multicast filters:
  - Only accepted sources
  - Or all sources accepted *except* specified ones
MLDv2

**QUERY**

- Router asks for listeners
  - General
  - Specific Multicast Address
  - Specific Multicast Address and Source

**REPORT-v2**

- Current state
- State change (filter/sources)
  - Sent to FF02::16
MLD Details

- Nodes **MUST** process QUERY to any of its unicast or multicast addresses
- MLDv2 **needs all nodes** using MLDv2
- **All OSs join** (REPORT) to the Solicited Node addresses
MLD Flooding

- Rate limit MLD messages
- Limit MLD states
- Disable MLD *(if not needed)*
MLD Traffic amplification

Several REPORTs for each QUERY
MLD Traffic amplification

Rate limit MLD messages

Disable MLD *(if not needed)*
Passive MLD Scanning

QUERY

REPORT

DONE
Active MLD Scanning

- **QUERY**
  - **All Nodes** (FF02::1)
  - **Routers** (FF02::2, FF02::16)

- REPORT
  - REPORT
  - REPORT
  - REPORT
## Built-in MLD Security

<table>
<thead>
<tr>
<th>MLD Message</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Source:</strong> Link local address <strong>only</strong></td>
</tr>
<tr>
<td><strong>Hop Limit = 1</strong></td>
</tr>
<tr>
<td><strong>Router Alert</strong> option in Hop-by-Hop EH</td>
</tr>
</tbody>
</table>

Discard non-compliant messages
MLD Snooping
RFC4541

Only allow multicast traffic on ports with listeners

QUERY
MLD Protection on Switches

Only allow **QUERIES** on router’s port

```
deny icmp any any any mld-query
```
Exercise 3.3 MLD

• **Description**: Network scanning using MLD

• **Goals**:
  - Know about a new tool: Chiron
  - Learn how to use Chiron to scan a network using MLD

• **Time**: 10 minutes

• **Tasks**:
  - Scan your network using MLD Query message
Attacker becomes the DNS server of the victim using:

**NDP**
- Man-in-the-Middle
- Neighbor Cache Poisoning

**Autoconfiguration**
- SLAAC
- DHCPv6
IPv6 DNS Configuration Attacks

Depending on answers to DNS queries

- Man-in-the-Middle
- DoS Attack
Introduction

Similar to IPv4

- Client / Server
- UDP
- Uses Relays

Message names change

- SOLICIT
- ADVERTISE
- REQUEST
- REPLY
- ...

Uses Relays

Similar to IPv4

Client / Server

UDP

Uses Relays

Message names change

SOLICIT

ADVERTISE

REQUEST

REPLY

...
### Multicast in DHCPv6

Servers and relays listen on multicast addresses

<table>
<thead>
<tr>
<th>Group</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>All DHCP Relay Agents and Servers</td>
<td>FF02::1:2</td>
</tr>
<tr>
<td>All DHCP Servers</td>
<td>FF05::1:3</td>
</tr>
</tbody>
</table>
Triggering the use of DHCP

Looks like I’ll need a DHCP server to know
- where is the DNS Server
CLIENT
fe80::a

DHCPv6 RELAY
fe80::f

DHCPv6 SERVER

SOLICIT
Dst: FF02::1:2
Src: FE80::a

R-F (SOLICIT)

ADVERTISE
Dst: FE80::a
Src: FE80::f

R-R (ADVERTISE)

REQUEST
Dst: FF02::1:2
Src: FE80::a

R-F (REQUEST)

REPLY
Dst: FE80::a
Src: FE80::f

R-R (REPLY)
Privacy Considerations

Client information can be obtained from IDs like the MAC from Client-ID
Privacy Considerations

Server address assignment strategies:
- **Iterative**: scanning easier
- **Identifier-based**: easier to track activity
- **Hash**: better, but still allows activity tracking
- **Random**: better privacy
Rogue DHCP Server

Answers before legitimate server
Rogue DHCP Server

DHCP Exhaustion Attack

Address Pool: EMPTY
Rogue DHCP Server

DHCP Reply Injection
DHCPv6 Solutions

RFC8415 - Security Considerations recommends RFC8213 - IPSec with Encryption

RFC8415 - Security Considerations recommends RFC8213 - IPSec with Encryption
Secure DHCPv6 *(with encryption)*

End-to-end encryption
Public key cryptography
Authentication
DHCPv6 Shield

RFC7610

- Protects clients only
- Implemented on L2 switches
- DHCPv6 Guard is vendor implementation
Filtering IPv6 Traffic

Section 4.1
Filtering in IPv6 is very Important!

- Global Unicast Addresses
- A good **addressing plan**

**Easier** filtering!
New Filters to Take Into Account

- ICMPv6
- IPv6 Extension Headers
- Fragments Filtering
- Transition mechanisms (TMs) / Dual-Stack
# Filtering ICMPv6

<table>
<thead>
<tr>
<th>Type - Code</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type 1 - all</td>
<td>Destination Unreachable</td>
<td>ALLOW</td>
</tr>
<tr>
<td>Type 2</td>
<td>Packet Too Big</td>
<td>ALLOW</td>
</tr>
<tr>
<td>Type 3 - Code 0</td>
<td>Time Exceeded</td>
<td>ALLOW</td>
</tr>
<tr>
<td>Type 4 - Code 0, 1 &amp; 2</td>
<td>Parameter Problem</td>
<td>ALLOW</td>
</tr>
<tr>
<td>Type 128</td>
<td>Echo Reply</td>
<td>ALLOW for troubleshoot and services. Rate limit</td>
</tr>
<tr>
<td>Type 129</td>
<td>Echo Request</td>
<td>ALLOW for troubleshoot and services. Rate limit</td>
</tr>
<tr>
<td>Types 131,132,133, 143</td>
<td>MLD</td>
<td>ALLOW if Multicast or MLD goes through FW</td>
</tr>
<tr>
<td>Type 133</td>
<td>Router Solicitation</td>
<td>ALLOW if NDP goes through FW</td>
</tr>
<tr>
<td>Type 134</td>
<td>Router Advertisement</td>
<td>ALLOW if NDP goes through FW</td>
</tr>
<tr>
<td>Type 135</td>
<td>Neighbour Solicitation</td>
<td>ALLOW if NDP goes through FW</td>
</tr>
<tr>
<td>Type 136</td>
<td>Neighbour Advertisement</td>
<td>ALLOW if NDP goes through FW</td>
</tr>
<tr>
<td>Type 137</td>
<td>Redirect</td>
<td>NOT ALLOW by default</td>
</tr>
<tr>
<td>Type 138</td>
<td>Router Renumbering</td>
<td>NOT ALLOW</td>
</tr>
</tbody>
</table>

Filtering Extension Headers

• **Firewalls** should be able to:
  1. Recognise and filter some **EHs** (example: **RH0**)
  2. Follow the **chain of headers**
  3. Not allow **forbidden combinations** of headers
Filtering Fragments

- Upper layer info not in 1st fragment
  - Creates many tiny fragments to go through filtering / detection

- Fragments inside fragments
  - Several fragment headers

- Fragmentation inside a tunnel
  - External header hides fragmentation
Filtering Fragments

Upper layer info not in 1\textsuperscript{st} Fragment

All header chain should be in the 1\textsuperscript{st} fragment [RFC7112]

Fragments inside fragments

Should not happen in IPv6. Filter them

Fragmentation inside a tunnel

FW / IPS / IDS should support inspection of encapsulated traffic
# Filtering TMs / Dual-stack

<table>
<thead>
<tr>
<th>Technology</th>
<th>Filtering Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>Native IPv6</td>
<td>EtherType 0x86DD</td>
</tr>
<tr>
<td>6in4</td>
<td>IP proto 41</td>
</tr>
<tr>
<td>6in4 (GRE)</td>
<td>IP proto 47</td>
</tr>
<tr>
<td>6in4 (6-UDP-4)</td>
<td>IP proto 17 + IPv6</td>
</tr>
<tr>
<td>6to4</td>
<td>IP proto 41</td>
</tr>
<tr>
<td>6RD</td>
<td>IP proto 41</td>
</tr>
<tr>
<td>ISATAP</td>
<td>IP proto 41</td>
</tr>
<tr>
<td>Teredo</td>
<td>UDP Dest Port 3544</td>
</tr>
<tr>
<td>Tunnel Broker with TSP</td>
<td>(IP proto 41)</td>
</tr>
<tr>
<td>AYIYA</td>
<td>UDP dest port 5072</td>
</tr>
</tbody>
</table>


IANA Protocol Numbers - [https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml](https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml)
IPv6 Packet Filtering

- Much more important in IPv6
- Common IPv4 Practices
- New IPv6 Considerations
  - End to End needs filtering
  - ICMPv6 should be wisely filtered
  - Filtering adapted to IPv6: EHs, TM
Filtering IPv6 Traffic

Exercise 4.1
Exercise 4.1 IPv6 Packet Filtering

- **Description**: Configure IPv6 packet filters

- **Goals**:
  - Understand IPv6 packet filtering
  - Learn how to use ip6tables on Linux hosts

- **Time**: 20 minutes

- **Tasks**:
  - Configure IPv6 packet filtering rules
4.1: IPv6 Packet Filtering - Redirect

**IPv6**
- **IPv6.Source**: fe80::a:b:c
- **IPv6.Destination**: IPa
- **Redirect.Target Addr**: fe80::a
- **Redirect.Dst Addr**: 2001:db8:bad:dad::1

**ICMPv6 Redirect**
- **IPa**: MACa = aa:aa:aa:aa:aa:aa
- **IPb**: MACb = bb:bb:bb:bb:bb:bb
- **IPc**: MACc = cc:cc:cc:cc:cc:cc

**Routes on Host A**
- ::/0: fe80::a:b:c
- 2001:db8:bad:dad::1: fe80::a

# ip -6 route show cache

**IPr** = fe80::a:b:c
**MACr** = 12:34:56:78:9a:bc

**IPv6**
- **IPv6.Source**: fe80::a:b:c
- **IPv6.Destination**: IPa
- **Redirect.Target Addr**: fe80::a
- **Redirect.Dst Addr**: 2001:db8:bad:dad::1
Internet Wide IPv6 Security
Section 5
DDoS

Section 5.1
DDoS attacks in IPv6?

First IPv6 Distributed Denial of Service Internet attacks seen

You know IPv6 must finally be making it: The first IPv6 Distributed Denial of Service Internet attacks have been spotted in the wild.

By Steven J. Vaughan-Nichols for Networking February 20, 2012 - 14:48 GMT (14:48 GMT) | Topic: Networking

It's begun: 'First' IPv6 denial-of-service attack puts IT bods on notice

Internet engineers warn this is only the beginning

Kieren McCarthy in San Francisco Sat 3 Mar 2018 // 09:30 UTC
DDoS factors related with IPv6

- Using lots of hosts
- Using outdated firmware
- Poor (or no) security measures
## DDoS factors related with IPv6

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Filter Traffic" /></td>
<td>Filter traffic&lt;br&gt;Don’t allow access to all IPv6 addresses</td>
</tr>
<tr>
<td><img src="image2.png" alt="Update Firmware" /></td>
<td>Update firmware</td>
</tr>
<tr>
<td><img src="image3.png" alt="Use Security Measures" /></td>
<td>Use security measures for IPv6</td>
</tr>
<tr>
<td><img src="image4.png" alt="Ingress/Egress Filtering" /></td>
<td>Ingress / Egress filtering and RPF</td>
</tr>
<tr>
<td><img src="image5.png" alt="Hierarchical Assignment" /></td>
<td>Hierarchical IPv6 address assignment</td>
</tr>
</tbody>
</table>
IPv6 Transition Mechanisms

Section 5.2
Temporary solution...

With security risks!
In IPv4-only infrastructure expect **dual-stack hosts**:

- VPNs or tunnels
- Undesired local IPv6 traffic
- Automatic Transition Mechanisms
- Problems with rogue RAs
## Dual-stack

<table>
<thead>
<tr>
<th>Threat</th>
<th>Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bigger attack surface</td>
<td>Protect IPv6 at the same level as IPv4</td>
</tr>
<tr>
<td>GUA Addresses</td>
<td>Filter end-to-end IPv6 properly</td>
</tr>
<tr>
<td>Use one IP version to attack the other</td>
<td>Don’t trust “IPv4-only”</td>
</tr>
</tbody>
</table>
Tunnelling

Attacker need knowledge of:

- Version of IP-1 and IP-2
- Tunnel end points addresses
- Tunneling protocol

To create tailor-made packets for:

- Traffic Injection
- Unauthorised use
- Reflection attack
- Loop attack

Solutions:

- Filtering
- Authentication
<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Security Measure</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPSec can’t be used end-to-end</td>
<td>Must support filtering</td>
</tr>
<tr>
<td>DNSSEC can’t be used with DNS64</td>
<td></td>
</tr>
<tr>
<td>Reflection attack</td>
<td>Implementations should protect themselves against exhaustion attacks</td>
</tr>
<tr>
<td>IP pool depletion attack</td>
<td></td>
</tr>
<tr>
<td>ALG (Application Level Gateway) CPU Attack</td>
<td></td>
</tr>
</tbody>
</table>
IPv6 Security Tips and Tools
Section 6
# Introduction

1. **Best security tool is knowledge**

2. **IPv6 security is a moving target**

3. **IPv6 is happening: need to know about IPv6 security**

4. **Cybersecurity challenge: Scalability**
   - **IPv6 is also responsible for Internet growth**
Tips

- IPv6 quite similar to IPv4, many reusable practices
- IPv6 security compared with IPv4:
  - No changes with IPv6
  - Changes with IPv6
  - New IPv6 issues
## Up to date information

<table>
<thead>
<tr>
<th>Information category</th>
<th>Standardisation Bodies</th>
<th>Vulnerabilities Databases</th>
<th>Security Tools</th>
<th>Cybersecurity Organisations</th>
<th>Vendors</th>
<th>Public Forums</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sub-categories</strong></td>
<td>IETF, 3GPP, Broadband Forum</td>
<td>Vulnerability ID (CVE-ID, other)</td>
<td>Vulnerability ID (CVE-ID, other)</td>
<td>CSIRTs / CERTs Gov. / LEAs</td>
<td>Vulnerability ID (CVE-ID, other)</td>
<td>Mailing Lists Groups of Interest Security Events</td>
</tr>
<tr>
<td><strong>Information in this category</strong></td>
<td>Security considerations</td>
<td>Severity (CVSS, other)</td>
<td>Severity (CVSS, other)</td>
<td></td>
<td>Severity (CVSS, other)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Protocol updates</td>
<td>Description</td>
<td>Description</td>
<td></td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Security recommendations</td>
<td>Affected systems</td>
<td>Affected systems</td>
<td></td>
<td>Affected systems</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Solutions and workarounds</td>
<td>Solutions and workarounds</td>
<td></td>
<td>Solutions and workarounds</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Affected devices in your network</td>
<td>“0 Day” vulnerabilities</td>
<td></td>
<td>“0 Day” vulnerabilities</td>
<td></td>
</tr>
<tr>
<td><strong>Examples</strong></td>
<td>RFCs, I-Ds</td>
<td>NVD, CVE</td>
<td>OpenVAS</td>
<td>CERT-EU ENISA EUROPOL/EC3</td>
<td>Cisco, Juniper, MS, Kaspersky, etc.</td>
<td>NOGs, IETF, IPv6 Hackers, Reddit, Troopers, etc.</td>
</tr>
</tbody>
</table>
Examples

CVE

cve.mitre.org/cve/search_cve_list.html
Search for: ICMPv6 windows

NVD

https://nvd.nist.gov/vuln/search
Search for: CVE-2020-16899
Go to vendor’s link

OpenVAS

<table>
<thead>
<tr>
<th>Name</th>
<th>Status</th>
<th>Reports</th>
<th>Last Report</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Workgroup Test</td>
<td>Stopped at 2 %</td>
<td>1</td>
<td>Thu, Dec 26, 2019 6:00 AM UTC</td>
<td>7.0 (High)</td>
</tr>
<tr>
<td>Windows Domain Test</td>
<td>Stopped at 2 %</td>
<td>1</td>
<td>Thu, Dec 26, 2019 6:00 AM UTC</td>
<td>7.0 (High)</td>
</tr>
<tr>
<td>DMZ Mail Scan</td>
<td>Container</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EulerOS Scan</td>
<td>Stopped at 27 %</td>
<td>74</td>
<td>Thu, Dec 26, 2019 6:00 AM UTC</td>
<td>7.0 (High)</td>
</tr>
<tr>
<td>TLS Map Scan</td>
<td>Done</td>
<td>1</td>
<td>Fri, Dec 27, 2019 1:38 PM UTC</td>
<td>0.0 (Low)</td>
</tr>
<tr>
<td>Metasploitable Test - GSM Master</td>
<td>Done</td>
<td>1</td>
<td>Fri, Jan 3, 2020 11:29 AM UTC</td>
<td>10.0 (High)</td>
</tr>
<tr>
<td>DMZ Mail Scan 2</td>
<td>Done</td>
<td>1</td>
<td>Fri, Dec 29, 2019 10:29 AM UTC</td>
<td>0.0 (Low)</td>
</tr>
<tr>
<td>system discovery</td>
<td>Done</td>
<td>1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Homework

Go to: cert.europa.eu
Select language filters
Search for IPv6
optional: configure a subscription

Go to NVD: https://nvd.nist.gov/vuln/search
Search for IPv6 + your vendor
## Security Tools

<table>
<thead>
<tr>
<th>Type</th>
<th>Can be used for</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Packet Generators</strong></td>
<td>Assessing IPv6 security, Testing implementations, Learning about protocols</td>
<td>Scapy, nmap, Ostinato, TReX</td>
</tr>
<tr>
<td></td>
<td>Proof of concept of attacks/protocols</td>
<td></td>
</tr>
<tr>
<td><strong>Packet Sniffers/Analysts</strong></td>
<td>Understanding attacks and security measures, Learning about protocols and implementations</td>
<td>tcpdump, Scapy, Wireshark, termshark</td>
</tr>
<tr>
<td></td>
<td>Troubleshooting</td>
<td></td>
</tr>
<tr>
<td><strong>Specialised Toolkits</strong></td>
<td>Assessing IPv6 security, Learning about protocols and implementations, Proof of concept of attacks/protocols</td>
<td>THC-IPV6, The IPv6 Toolkit, Ettercap</td>
</tr>
<tr>
<td></td>
<td>Learn about new attacks</td>
<td></td>
</tr>
<tr>
<td><strong>Scanners</strong></td>
<td>Finding devices and information, Proactively protect against vulnerabilities</td>
<td>nmap, OpenVAS</td>
</tr>
<tr>
<td><strong>IDS/IPS</strong></td>
<td>Understanding attacks and security measures, Learning about protocols and implementations, Assessing IPv6 security</td>
<td>Snort, Suricata, Zeek</td>
</tr>
<tr>
<td></td>
<td>Learn about new attacks</td>
<td></td>
</tr>
</tbody>
</table>
# Devices Categories (RIPE-772)

<table>
<thead>
<tr>
<th>Host</th>
<th>Switch</th>
<th>Router</th>
<th>Security Equipment</th>
<th>CPE</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IPSec (if needed)</strong></td>
<td><strong>HOST +</strong></td>
<td><strong>HOST +</strong></td>
<td><strong>HOST +</strong></td>
<td><strong>Router</strong></td>
</tr>
<tr>
<td><strong>RH0 [RFC5095]</strong></td>
<td><strong>IPv6 ACLs</strong></td>
<td><strong>Ingress Filtering and RPF</strong></td>
<td><strong>Header chain [RFC7112]</strong></td>
<td><strong>Security Equipment</strong></td>
</tr>
<tr>
<td><strong>Overlapping Frags [RFC5722]</strong></td>
<td><strong>FHS</strong></td>
<td><strong>DHCPv6 Relay [RFC8213]</strong></td>
<td><strong>Support EHS Inspection</strong></td>
<td><strong>DHCPv6 Server Privacy Issues</strong></td>
</tr>
<tr>
<td><strong>Atomic Fragments [RFC6946]</strong></td>
<td><strong>RA-Guard [RFC6105]</strong></td>
<td><strong>OSPFv3</strong></td>
<td><strong>ICMPv6 fine grained filtering</strong></td>
<td></td>
</tr>
<tr>
<td><strong>NDP Fragmentation [RFC6980]</strong></td>
<td><strong>DHCPv6 guard</strong></td>
<td><strong>Auth. [RFC4552]</strong></td>
<td><strong>Encapsulated Traffic Inspection</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Header chain [RFC7112]</strong></td>
<td><strong>IPv6 snooping</strong></td>
<td><strong>or / and [RFC7166]</strong></td>
<td><strong>IPv6 Traffic Filtering</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Stable IIDs [RFC8064][RFC7217] [RFC7136]</strong></td>
<td><strong>IPv6 source / prefix guard</strong></td>
<td><strong>IS-IS</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Temp. Address Extensions [RFC8981]</strong></td>
<td><strong>IPv6 destination guard</strong></td>
<td><strong>[RFC5310]</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Disable if not used:</strong> LLMNR, mDNS, DNS-SD, transition mechanisms</td>
<td><strong>MLD snooping [RFC4541]</strong></td>
<td><strong>or, less preferred, [RFC5304]</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>DHCPv6-Shield [RFC7610]</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>MBGP</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>TCP-AO [RFC5925]</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>MD5 Signature Option [RFC2385] Obsoleted</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>MBGP Bogon prefix filtering</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Control Plane Security

- BGP
- IGP
- NDP
- MLD
- IDS/IPS
- NDP
- DHCPv6
- MLD
- DNS*

Forwarding Plane Security

- IPv6
- IDS/IPS
- FHS
- IPv6

* All Name resolution related protocols
We want your feedback!

What did you think about this webinar?

Take our survey at:

https://www.ripe.net/feedback/v6s
We want your feedback!

What did you think about this session? Take our survey at:
Learn something new today!
academy.ripe.net
RIPE NCC Certified Professionals

IPv6 Fundamentals
Analyst

RIPE Database
Associate

BGP Security
Associate

IPv6 Security
Expert

https://getcertified.ripe.net/
END
Extra: Smurf Attack

IPv4

1 Packet
Source: Victim
Destination: Broadcast

IPv6

1 Packet
Source: Victim
Destination: Multicast (FF02::1)
Extra: DoS / DDoS

- **DoS** (Denial of Service): Type of attack that is able to make a service or protocol to stop working.

- **DDoS** (Distributed DoS): Is a type of DoS attack that is performed from several devices.

- Example: send too much traffic to a link, so that the routers can’t handle it, overloading them.
Extra: MITM

- Man-In-The-Middle attack:
  - The attacker is able to be on the path of the packets
Extra: Replay Attacks

- Replay Attacks consist in sending again a previous packet

- Solution: nonce or timestamp (makes packet unique)
Extra: Overlapping Fragments

Fragments

Normal fragments offset say where the data goes

Overlapping fragments have wrong offset values
**Extra: Hash Function**

- **Input**: Variable length bit string, for example a text

- **Output**: Fixed length bit string, represented by a series of characters

```
Input
  RIPE NCC
  RIPE NCC
  The RIPE NCC offers *many* courses
  The RIPE NCC offers *great* courses

Hash function

Hash output
  9f3j2bz5j
  4daevgi2s
  cd83jxwgl
```

- `9f3j2bz5j` is the same input that produces the same output.
- `cd83jxwgl` is nearly impossible to reverse and guess the input.

`4daevgi2s` is a fixed length output.
IPv6 Associated Protocols Security

Section 3
IPv6 Routing protocols

Section 3.6
Securing routing updates

Authentication of neighbors/peers

Route filtering

Router Hardening

THIS SECTION

NOT COVERED

SAME AS IPv4
# Neighbors/Peers Authentication

<table>
<thead>
<tr>
<th>Authentication Options</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RIPng</strong></td>
<td></td>
</tr>
<tr>
<td>- No authentication</td>
<td>- RIPv2-like MD5 no longer available</td>
</tr>
<tr>
<td>- IPsec (general recommendation)</td>
<td>- IPSec not available in practice</td>
</tr>
<tr>
<td><strong>OSPFv3</strong></td>
<td></td>
</tr>
<tr>
<td>- IPsec [RFC4552]</td>
<td>- ESP or AH. Manual keys</td>
</tr>
<tr>
<td>- Authentication Trailer [RFC7166]</td>
<td>- Hash of OSPFv3 values. Shared key</td>
</tr>
<tr>
<td><strong>IS-IS</strong></td>
<td></td>
</tr>
<tr>
<td>- HMAC-MD5 [RFC5304]</td>
<td>- MD5 not recommended</td>
</tr>
<tr>
<td>- HMAC-SHA [RFC5310]</td>
<td>- Many SHA, or any other hash</td>
</tr>
<tr>
<td><strong>MBGP</strong></td>
<td></td>
</tr>
<tr>
<td>- TCP MD5 Signature Option [RFC2385]</td>
<td>- Protects TCP. Available. Obsoleted</td>
</tr>
<tr>
<td>- TCP-AO [RFC5925]</td>
<td>- Protects TCP. Recommended</td>
</tr>
</tbody>
</table>
Securing Routing Updates

• IPsec is a general solution for IPv6 communication
  - In practice not easy to use

• OSPFv3 specifically states [RFC4552]:
  1. ESP must be used
  2. Manual Keying

• Other protocols: No options available
Conclusions

- Security options available for IPv6 routing protocols

- Try to use them:
  - Depending on the protocol you use
  - At least at the same level as IPv4
IPv6 Filtering
Section 4
# IPv6 BGP Bogon Prefix Filtering

<table>
<thead>
<tr>
<th>Use</th>
<th>Prefix</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>::/0</td>
</tr>
<tr>
<td>Unspecified Address</td>
<td>::/128</td>
</tr>
<tr>
<td>Loopback Address</td>
<td>::1/128</td>
</tr>
<tr>
<td>IPv4-mapped Addresses</td>
<td>::ffff:0.0.0.0/96</td>
</tr>
<tr>
<td>IPv4-compatible Addresses (deprecated)</td>
<td>::/96</td>
</tr>
<tr>
<td>Link-local Addresses</td>
<td>fe80::/10</td>
</tr>
<tr>
<td>Site-local Addresses (deprecated)</td>
<td>fec0::/10</td>
</tr>
<tr>
<td>Unique-local addresses</td>
<td>fc00::/7</td>
</tr>
<tr>
<td>Multicast Addresses</td>
<td>ff00::/8</td>
</tr>
<tr>
<td>Documentation addresses</td>
<td>2001:db8::/32</td>
</tr>
<tr>
<td>6Bone Addresses (deprecated)</td>
<td>3ffe::/16, 5f00::/8</td>
</tr>
<tr>
<td>ORCHID</td>
<td>2001:10::/28</td>
</tr>
</tbody>
</table>

**Team Cymru:** [https://team-cymru.com/community-services/bogon-reference/](https://team-cymru.com/community-services/bogon-reference/)
MANRS (www.manrs.org)

- Secure and Resilient Internet is a **collaborative** effort
- **Concrete actions** for: network operators, IXPs, CDN/Cloud providers
- **IPv6** and **IPv4** BGP
### MANRS Network Operators Actions

<table>
<thead>
<tr>
<th>Facilitate Global Coordination</th>
<th>Keep contact information updated: RIPE DB, LIR Portal, PeeringDB</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facilitate Routing Information Validation</td>
<td>Route Objects</td>
</tr>
<tr>
<td>Prevent IP Spoofing</td>
<td>uRPF</td>
</tr>
<tr>
<td>Prevent Incorrect Routing Information</td>
<td>Define Routing Policy</td>
</tr>
</tbody>
</table>
Internet Wide IPv6 Security
Section 5
BGP Hijacking

Section 5.3
Introduction

• BGP is a control plane protocol (application level)
• Hijack techniques same in IPv6 and IPv4
• Protection techniques as well
BGP Prefix Hijack - Fake Origin

Traffic to AS 1

1. Victim
2. Attacker
3. /32 prefix

P/29 [1]
P/29 [1,A]
P/29 [1,A,B]
P/29 [1,A,C]
P/29 [1,A,B]
P/32 [3]
P/32 [3,D]
BGP MITM - Fake AS-path

Traffic to AS 1

1. Victim

A

B

C

D

3. Attacker

P/29 [1]
P/29 [1,A]
P/29 [1,A,B]
P/32 [A,C,3,D]
P/32 [A,C,3]
P/29 [1,A]
P/29 [1,A,3]
P/29 [1,A,B]

Traffic to AS 1

P/32 [A,C,3]
P/32 [A,C,3,D]
P/29 [1,A,B]
P/29 [1,A]
P/29 [1]

Traffic to AS 1 /32 prefix

P/29 [1,A]
P/29 [1,A,B]
P/29 [1,A]
P/29 [1,3]
P/29 [1,A,3]
P/29 [1,A,B]
P/29 [1]

P/32 [A,C,3]
P/32 [A,C,3,D]
P/29 [1,A,B]
P/29 [1,A]
P/29 [1]

Traffic to AS 1 /32 prefix
BGP Hijack: Solutions

• To secure BGP for IPv6:
  1. Route Filtering
  2. RPKI
  3. BGPsec (in the future)

• Temporary: More specific announcement