IPv6 Security - Opportunities and Challenges

Thomas Scheffler

Beuth Hochschule Berlin, Germany
{scheffler@beuth-hochschule.de}

BEUTH HOCHSCHULE
FÜR TECHNIK
BERLIN
University of Applied Sciences

Agenda

1. The Basics
   - IPv6 Network Security
   - ICMPv6 / Autoconfiguration / Extension Header
2. Security problems in IPv6
   - Stateless Autoconfiguration
   - Secure Neighbor Discovery
   - Source Routing in IPv6
3. Firewalls & IPv6 Security Policies
   - ip6tables
   - Host Security
4. Literature

IPv6 Implications for Network Security

IPv6 introduces changes, that have a positive effect on network security:

- Inherent support for IPsec
- Very large subnet sizes

but:

- Implementations are relatively new and untested
- IPv6 also has a number of features that open new attack vectors

It is essential for the success of IPv6 to identify potential problem areas as early as possible and develop adequate protection measures.

3 Phases in the Debate About IPv6 Security

1. IPv6 is the secure network protocol, because it has inherent IPsec-support.
   No additional tools are needed.

2. IPv6-networks need the same protection as IPv4-networks.
   We need identical feature-sets in tools such as Firewalls.

3. IPv6 is a new network protocol. Features such as Extension Headers, address autoconfiguration, etc. that allow new attacks.
   New protection tools are needed!

Network Security IPv6 - Subnet-Size

The size of a single IPv6 subnet defaults to: $2^{64}(1.8 \times 10^{19}$ **hosts)** – **the size of the Interface ID of an IPv6-address**

- Current Internet worm-attacks use subnet scanning techniques such as Ping-Sweeps, to identify potential targets.

Ping-Sweeping an IPv6 subnet:

- Assume a subnet which is populated with 10,000 hosts using randomly distributed addresses.
- Probing this subnet with 1 Million requests per second (ca. 500 Mbit/s) it takes 29 years (on average), until the first host has been found!

Network Security IPv6 - Subnet-Size

But: Attacks become easier, if:

- the Host-ID is based on the MAC-Address.
- Admins use manually configured Interface-IDs, that are easy to remember (::10, ::20, embedded IPv4-addresses, etc.).
- Host name resolution via DNS is available.

Attacks become trivial, when the Attacker has local network access:

- IPv6 uses well-known Multicast addresses (RFC 2375): All-Nodes (FF02::1), All-Routers (FF05::2), All-DHCP Server (FF05::3).
- Through the generation of a fake Router Advertisement and the sniffing of all Duplicate Address Detection (DAD) messages, harvesting of addresses becomes easy.

ICMPv6

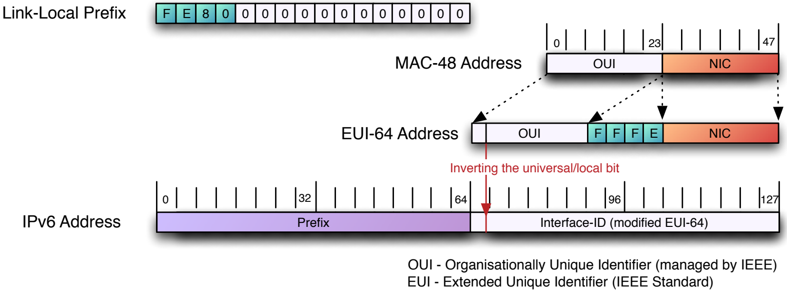
The ICMPv6 protocol is a central protocol for the deployment and use of IPv6. It provides a number of functions that, either did not exist in IPv4, or where provided through other protocols:

- Stateless Address Autoconfiguration and Router Discovery
- L2-address resolution through the ICMPv6 Neighbour Discovery Protocol (NDP). IPv4 uses the ARP protocol on Layer 2.
- Determination of reachability and parameters of the transmission path: Echo Request/Response, Path MTU Discovery.
- Management of multicast group membership through the Multicast Listener Discovery und Multicast Router Discovery. IPv4 uses here the IGMP protocol.

Address Autoconfiguration

- Address Autoconfiguration is used, in order to automatically assign IPv6 addresses to hosts. This allows the hosts in a network to communicate without explicit configuration.
- There exist two methods for address configuration. Stateless autoconfiguration is the default:
  - Stateless Autoconfig: In order to build a valid IP address, the host uses available prefix information (e.g. from the Router Discovery Process) and subsequently tests this address for uniqueness, using Duplicate Address Detection (DAD).
  - DHCPv6 is a stateful mechanism, that provides additional features. DHCPv6 has not been implemented for all operating systems.

Stateless Address Autoconfiguration



OUI - Organisationally Unique Identifier (managed by IEEE)
EUI - Extended Unique Identifier (IEEE Standard)

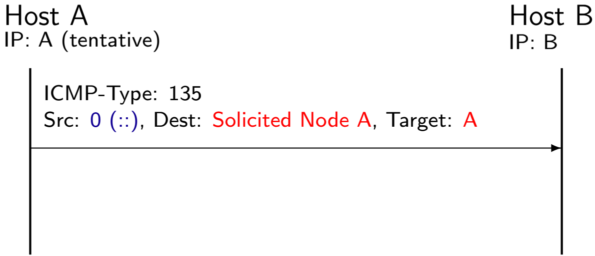
- Each interface needs to have at least a Link-Local Unicast Address.
- The Interface ID (last 64 Bit) of the address must be unique only in the respective subnet and will be derived from the MAC-address of the interface.

Stateless Address Autoconfiguration

- Autoconfiguration is used only for hosts, not for routers.
- IPv6 addresses have an associated lifetime: valid addresses are preferred. Addresses, that *soon* expire are in the state deprecated. Latter addresses will not be used for new connections - existing connections will continue to work.
- Duplicate Address Detection: After an address has been generated, it is in the state tentative. Its uniqueness on the link is verified through a Neighbour Soliciting Message.
  If this address already exists, the owner of this adress sends a respective Neighbour Advertising Message and address autoconfiguration is abborted.

Stateless Address Autoconfiguration

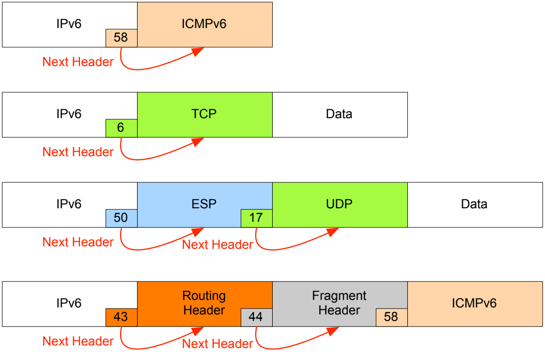
Duplicate Address Detection



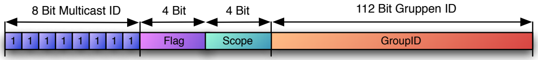
- If the IPv6-Address generated by Host A is already used on the link, it can not be assigned to the interface.
- Given the large address space and the particular address generation mechanism this is a very unlikely event.

IPv6 Extension Header

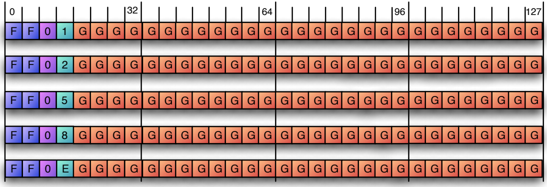
- IPv6 uses a flexible mechanism for potential protocol extensions. Additional header (Extension Header) will be inserted between the IPv6 and the L4-Header.



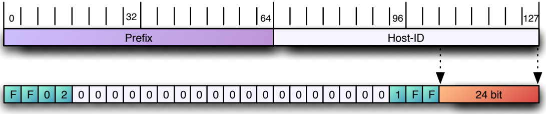
IPv6 Scoped Multicast-Addresses



Flag - 'well-known'/'transient' Adresse, u.a.
Scope - Reichweite der Multicast Gruppe



Node-Local Multicast	F	F	0	1	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G
Link-Local Multicast	F	F	0	2	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G
Site-Local Multicast	F	F	0	5	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G
Organisation-Local Multicast	F	F	0	8	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G
Global Multicast	F	F	0	E	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G



IPv6 Address: Prefix | Host-ID

Solicited Node Address	F	F	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	F	F	24 bit

Agenda

1 The Basics
- IPv6 Network Security
- ICMPv6 / Autoconfiguration / Extension Header

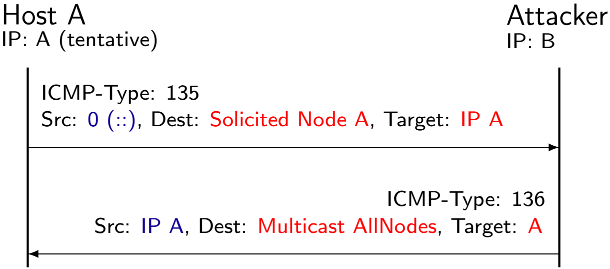
2 Security problems in IPv6
- Stateless Autoconfiguration
- Secure Neighbor Discovery
- Source Routing in IPv6

3 Firewalls & IPv6 Security Policies
- ip6tables
- Host Security

4 Literature

Stateless Address Autoconfiguration

DoS-Attack against Duplicate Address Detection


Host A
IP: A (tentative)
Attacker
IP: B
ICMP-Type: 135
Src: 0 (::), Dest: Solicited Node A, Target: IP A
ICMP-Type: 136
Src: IP A, Dest: Multicast AllNodes, Target: A

An attacker falsely and repeatedly answers the DAD-Request from Host A. The attacker effectively denies Host A the configuration of a valid IPv6 address.

Stateless Address Autoconfiguration

Problem:

- Each host can access the network and receives a valid address!
- Duplicate Address Detection can easily be exploited for DoS-attacks.
- Router Advertisements and Neighbor Solicitation Nachrichten can be spoofed (similar to ARP-Spoofing in IPv4)

Proposed remedy:

1. Authenticated Neighbour Discovery Messages (using IPsec Authentication-Header as defined by RFC 4302)
2. Usage of the Secure Neighbor Discovery Protocol (RFC 3971)

Problems in the Interworking of ICMPv6 and IPsec IKE

The IPv6 security architecture proposes the use of IPsec, for the protection of IP traffic, including ICMPv6 messages.

However,

there exists a Bootstrap-problem for address configuration!

- In order to use IKE for the establishment of a Security Association (SA) the hosts needs to have a valid IP address.
- IPsec itself is able to protect Unicast und Multicast traffic, but SAs can only be established for Unicast traffic through IKE.

  The following ICMPv6 messages would need to use manually configured SAs:
  Router & Neighbor Solicitations, Router & Neighbor Advertisements.

Securing Neighbor Discovery using SEND

- The specification of the Neighbor Discovery Protocol (RFC4861) recommends the use of IPsec for the protection of NDP messages only for smaller networks.
- The SEcure Neighbor Discovery (SEND) protocol has been designed to protect networks from attacks against NDP.
- The protocol uses cryptographically generated addresses, that bind the IP adress to the generating node. The protocol has been designed to be compatible with IPv6 address autoconfiguration.

but:

- only marginal OS support: Linux - experimental; Windows - none; Cisco IOS supports SEND (starting with 12.4).
- There exists very limited practical experience. Implementations might be vulnerable against resource exhaustion attacks.

Source Routing

- The sender of an IPv6-packet can use the Routing Header **RH0** to determine the path this packet should take through the network.
- Source-Routing was mandated for IPv6 in the Internet Standard RFC2460 and also implemented for end-systems (IPv6-Nodes).
- Liberal rules for header-processing: "IPv6 nodes must attempt to process extension headers in any order and occurring any number of times in the same packet..."

Deprecation of Source Routing:

RFC5095 has deprecated Source Routing and classified Routing Header **RH0** as potentially malicious. Packet that carry this routing header should be discarded.

Agenda

1. The Basics
   - IPv6 Network Security
   - ICMPv6 / Autoconfiguration / Extension Header
2. Security problems in IPv6
   - Stateless Autoconfiguration
   - Secure Neighbor Discovery
   - Source Routing in IPv6
3. Firewalls & IPv6 Security Policies
   - ip6tables
   - Host Security
4. Literature

IPv6 Firewall with ip6tables I

IPv6 firewalls can be build using ip6tables running on Linux.

- The rule-syntax is simular to iptables for IPv4.
- There exist a number of modules for IPv6 specific functions, eg. treatment of Extension Headers.

Firewall-Rule Syntax

```
ip6tables [-t table] -I chain [rulenum] rule-specification
[options]
```

IPv6 Firewall with ip6tables II

IPv6-specific modules

- `ah` - IPsec Authentication Header
- `esp` - IPsec ESP Header
- `dst` - Destination Header
- `hbh` - Hop-by-Hop Header
- `rt` - Routing Header
- `icmpv6` - ICMPv6

Modules can be loaded in two different ways:

- Implicitly - when a protocol is specified with **-p** or –**protocol**
- Explicitly - with the **-m** or –**match** option

Firewalls & IPv6 Security Policies I

IPv4 Firewall - ICMP Filtering

"Current best practice for IPv4 firewalling of ICMP is sometimes debated, but it is generally accepted that stringent ICMP filtering is a best practice."

Sean Convery, Darrin Miller (CISCO)
IPv6 and IPv4 Threat Comparison and Best-Practice Evaluation

Firewalls & IPv6 Security Policies II

An IPv6 firewall should discard ICMPv6-messages from the Internet except the following:

IPv6 Firewall - loose ICMPv6 Filtering

- Echo Request, Echo Reply
- No Route to Destination
- (optionally) Multicast Listener Messages
- (optionally) Router Solicitation & Advertisement, Neighbor Solicitation & Advertisement

Firewalls & IPv6 Security Policies III

IPv6 Firewall - strict ICMP Filtering

ICMPv6-messages that always need to pass through the firewall:

- Packet Too Big (Type 2 message)
- Parameter Problem (Typ 4 message)

Filtering of ICMPv6 Messages - **Permit**

ICMPv6 Typ	Description	Direction	Action
1	Destination Unreachable	In	Permit
2	Packet Too Big	In/Out	Permit
3	Time Exceeded	In/Out	Permit
4	Parameter Problem	In/Out	Permit
128	Echo Request	Out	Permit
129	Echo Reply	In	Permit
133, 134	Router Discovery	In/Out	Permit
135, 136	Neighbor Discovery	In/Out	Permit
130, 131, 132, 143	MLD messages	In/Out	Permit

Filtering of ICMPv6 Messages - **Drop**

ICMPv6 Typ	Description	Direction	Action
100, 101	Private Experimentation	In/Out	Drop
200, 201	Private Experimentation	In/Out	Drop
137	Redirect	In/Out	Drop
138	Router Renumbering	In/Out	Drop
139	ICMP Node Information Query	In	Drop
140	ICMP Node Information Response	Out	Drop
	currently not assigned/used ICMP message types	In/Out	Drop

http://www.iana.org/assignments/icmpv6-parameters

Filtering of Routing Header Typ 0

According to RFC 5095 packets with Routing Header Typ 0 (Source Routing) should be silently dropped, because they constitute a major security risk.

Firewall-Rule

```
ip6tables -A INPUT -m rt -rt-type 0 -j DROP
```

Filtering NDP Messages I

Neighbor Discovery (RFC4861) opens a number of potential attack posibilities.

- In order to prevent 'non-local' attacks on the protocol, implementations are required to *not* process NDP messages with a Hop-Count < 255
- Additionally these ICMP messages could be filtered at the network border.

Filtering NDP Messages II

Drop NDP messages with Hop Count < 255

```
ip6tables -I INPUT -p icmpv6 -icmpv6-type XXX -m hl -hl-lt
255 -j DROP
```

Local ICMP messages

- RS: Type 133, RA: Type 134
- NS: Type 135, NA: Type 136
- Redirect: Type 137
- Inverse NS: Type 141, Inverse NA: Type 142
- Send Path Solicitation/Advertisement: Type 148 / 149

General Recommendations for IPv6 Firewalls

- Configure identical firewall policies for IPv4 and IPv6!
- Filter protocols and address space that is currently not assigned and used.
- IPv6 requires defence in depth: deployment of host + network firewalls is reasonable.
- Detection and blocking of tunneled IPv6 traffic can be difficult.

Egress-filtering

Filter outgoing IPv6 traffic. Drop the following packtes in order to maintain a threat-free network:

- Packets with non-local Source-Addresses.
- Packets with Multicast-Source Addresses.
- ICMP-Packets with non existing type-numbers, autoconf, etc.

Other Potential Problem Areas:

- IPv6 transition mechanisms (automatic tunneling, 6to4, ...)
- Fragmentation and IPv6 Extension Header processing
- Network renumbering
- Scoped multicast
- Mobile IPv6
- ...

Conclusion:

- IPv6 is a new and interesting network protocol with a number of unique features.
- A thorough understanding of the protocol is necessary in order to build secure IPv6 networks.
    - Experience arises from practical application - IPv6 deployment and usage needs to rise!
- Tool support has improved in the last years. However, what is still missing is a reliable, easy-to-use test framework for the ordinary network administrator.

Challenge

New protocols bring new functionality to the network - but also new possibilities for exploits.

Agenda

1. The Basics
   - IPv6 Network Security
   - ICMPv6 / Autoconfiguration / Extension Header
2. Security problems in IPv6
   - Stateless Autoconfiguration
   - Secure Neighbor Discovery
   - Source Routing in IPv6
3. Firewalls & IPv6 Security Policies
   - ip6tables
   - Host Security
4. Literature

J. Abley, P. Savola, and G. Neville-Neil.
Deprecation of Type 0 Routing Headers in IPv6.
RFC 5095 (Proposed Standard), December 2007.

Philippe Biondi and Arnaud Ebalard.
IPv6 Routing Header Security.
CanSecWest, 2007.

Sean Convery and Darrin Miller.
IPv6 and IPv4 Threat Comparison and Best-Practice Evaluation (v1.0).
Cisco Systems Technical Report, March 2004.

Scott Hogg and Eric Vyncke.
IPv6 Security.
Cisco Press, 2008.

Questions?

BEUTH HOCHSCHULE
FÜR TECHNIK
BERLIN
University of Applied Sciences