# na6 v1.2 manual pages

## Description

This tool is part of the IPv6 Toolkit v1.2: a security assessment suite for the IPv6 Protocol developed by the UK CPNI. It allows the assessment of IPv6 implementations with respect to a variety of attack vectors based on ICMPv6 Neighbor Advertisement messages.

## Modes of Operation

This tool has two modes of operation: active and passive. In active mode, the tool attacks a specific target, while in passive mode the tool listens to traffic on the local network, and launches an attack in response to such traffic. Active mode is employed if a destination address (IPv6 Destination Address or Ethernet Destination Address) and a Target Address are specified. Passive mode is employed if the "-L" option (or its long counterpart "--listen") is set. If both an attack target and the "-L" option are set, the attack is launched against the specified target, and then the tool enters passive mode to respond incoming Neighbor Solicitation messages with Neighbor Advertisement (attack) packets.

The tool supports filtering of incoming Neighbor Solicitation messages based on the Ethernet Source Address, the Ethernet Destination Address, the IPv6 Source Address, the IPv6 Destination Address, and the Neighbor Solicitation Target Address. There are two types of filters: "block filters" and "accept filters". If any "block filter" is specified, and the incoming Neighbor Solicitation message matches any of those filters, the message is discarded (and thus no Neighbor Advertisements are sent in response). If any "accept filter" is specified, incoming Neighbor Solicitation messages must match the specified filters in order for the na6 tool to respond with Neighbor Advertisement messages.

## Options

The na6 tool takes it parameters as command-line options. Each of the options can be specified with a short name (one character preceded with the hyphen character, as e.g. "-i") or with a long name (a string preceded with two hyphen characters, as e.g. "--interface").

Depending on the amount of information (i.e., options) to be conveyed into the Neighbor Advertisements, it may be necessary for the na6 tool to split that information into more than one Neighbor Advertisement message. Also, if the tool is instructed to flood the victim with Neighbor Advertisements from different sources ("--flood-sources" option), multiple packets may need to be generated. na6 supports IPv6 fragmentation, which may be of use if a large amount of information needs to be conveyed within a single Neighbor Advertisement message. However, IPv6 fragmentation is not enabled by default, and must be explicitly enabled with the "-y" option.

`--interface`, `-i`

This option specifies the network interface that the tool will use. The network interface must be specified (i.e., the tool does not select any network interface "by default").

`--src-address`, `-s`

This option specifies the IPv6 source address (or IPv6 prefix) to be used for the Source Address of the attack packets. If left unspecified, a random link-local unicast address (fe80::/64) is selected.

If the "-T" ("--flood-targets") option is specified, this option includes an IPv6 prefix. See the description of the "-T" option for further information on how the "-s" option is processed in that specific case.

`--dst-address`, `-d`

This option specifies the IPv6 Destination Address of the victim. If left unspecified, but the Ethernet Destination Address is specified, the "all-nodes link-local multicast" address (ff02::1) is selected as the IPv6 Destination Address.

When operating in passive mode ("-L" option), the IPv6 Destination Address is selected according to the IPv6 Source Address of the incoming Neighbor Solicitation message. If the IPv6 Source Address of the Neighbor Solicitation is the unspecified address (::), the "all-nodes link-local multicast" address (ff02::1) is used as the IPv6 Destination Address. Otherwise, the IPv6 Source Address of the incoming Neighbor Solicitation message is used as the IPv6 Destination Address of the outgoing Neighbor Advertisement (attack) messages.

`--hop-limit, -A`

This option specifies the Hop Limit to be used for the Neighbor Advertisement messages. It defaults to 255. Note that IPv6 nodes are required to check that the Hop Limit of incoming Neighbor Advertisement messages is 255. Therefore, this option is only useful to assess whether an IPv6 implementation fails to enforce the aforementioned check.

`--frag-hdr`, `-y`

This option specifies that the resulting packet must be fragmented. The fragment size must be specified as an argument to this option.

`--dst-opt-hdr`, `-u`

This option specifies that a Destination Options header is to be included in the resulting packet. The extension header size must be specified as an argument to this option (the header is filled with padding options). Multiple Destination Options headers may be specified by means of multiple "-u" options.

`--dst-opt-u-hdr`, `-U`

This option specifies a Destination Options header to be included in the "unfragmentable part" of the resulting packet. The header size must be specified as an argument to this option (the header is filled with padding options). Multiple Destination Options headers may be specified by means of multiple "-U" options. This option is only valid if the "-y" option is specified (as the concept of "unfragmentable part" only makes sense when fragmentation is employed).

`--hbh-opt-hdr`, `-H`

This option specifies that a Hop-by-Hop Options header is to be included in the resulting packet. The header size must be specified as an argument to this option (the header is filled with padding options). Multiple Hop-by-Hop Options headers may be specified by means of multiple "-H" options.

`--src-link-address`, `-S`

This option specifies the link-layer Source Address of the Neighbor Advertisement messages (currently, only Ethernet is supported). If left unspecified, the link-layer Source Address is randomized.

When operating in passive mode, the link-layer Source Address is selected according to the IPv6 Destination Address of the incoming Neighbor Solicitation message.
If the IPv6 Destination Address of the incoming Neighbor Solicitation message is a multicast address (usually a solicited-node multicast address), the link-layer Source Address is set to the address specified by the "-S" option (or to a random address if the "-S" option was left unspecified).
If the IPv6 Destination Address of the incoming Neighbor Solicitation is not a multicast address (i.e., it is a unicast address), the link-layer Source Address is set to the Ethernet Destination Address of the incoming Neighbor Solicitation message.

`--link-dst-address`, `-D`

This option specifies the link-layer Destination Address of the Neighbor Advertisement messages (currently, only Ethernet is supported). If left unspecified, it is set to the "all-nodes link-local multicast" address (ff02::1).

When operating in passive mode, the link-layer Destination Address is set according to the IPv6 Source Address of the incoming Neighbor Solicitation message.
If the IPv6 Source Address of the incoming Neighbor Solicitation message is the unspecified address (::), the link-layer destination address is set to “33:33:00:00:00:01” (the Ethernet multicast address corresponding to the IPv6 “all-nodes link-local multicast” address). Otherwise, the link-layer Destination Address is set to the link-layer Source Address of the incoming Neighbor Solicitation message.

`--router`, `-r`

This option instructs the na6 tool to set the “R” (Router) bit in the Neighbor Advertisement messages that it sends. The “R” bit indicates that the node sending the message is a router. If left unspecified, the “R” bit is not set.

`--solicited`, `-c`

This option instructs the na6 tool to set the “S” (“Solicited”) bit in the Neighbor Advertisement messages that it sends. When operating in passive mode (“-L” option), the “Solicited” flag is forced to 1 in all responses sent to unicast IPv6 addresses.

`--override`, `-o`

This option instructs the na6 tool to set the ‘O’ (“Override”) bit in the Neighbor Advertisement messages that it sends. If this option is left unspecified, the ‘O’ bit is not set.

`--target`, `-t`

This option specifies the IPv6 Target Address of the Neighbor Advertisement messages.

If the “-T” (“--flood-targets”) option is specified, this option specifies an IPv6 prefix in the form “-t prefix/prefixlen”. See the description of the “-T” option for further information on how the “-t” option is processed in that specific case.

`--target-lla-opt`, `-E`

This option specifies the contents of a target link-layer address option to be included in the Neighbor Advertisement messages. If a single option is specified, it is included in all the outgoing Neighbor Advertisement messages. If more than one target link-layer address is specified (by means of multiple “-E” options), and all the resulting options cannot be conveyed into a single Neighbor Advertisement message, multiple Neighbor Advertisements will be sent as needed.

`--add-tlla-opt`, `-e`

This option instructs the na6 tool to include a target link-layer address option in the Neighbor Advertisement messages that it sends. The target link-layer address included in the option is the same as the Ethernet Source Address used for the outgoing Neighbor Advertisement messages. The difference between this option and the “-E” option is that the “-e” option does not specify the actual value of the option, but just instructs the tool to include a target link-layer address option (the actual value of the option is selected as explained before).

`--block-src`, `-j`

This option sets a block filter for the incoming Neighbor Solicitation messages, based on their IPv6 Source Address. It allows the specification of an IPv6 prefix in the form “-j prefix/prefixlen”. If the prefix length is not specified, a prefix length of “/128” is selected (i.e., the option assumes that a single IPv6 address, rather than an IPv6 prefix, has been specified).

`--block-dst`, `-k`

This option sets a block filter for the incoming Neighbor Solicitation messages, based on their IPv6 Destination Address. It allows the specification of an IPv6 prefix in the form “-k prefix/prefixlen”. If the prefix length is not specified, a prefix length of “/128” is selected (i.e., the option assumes that a single IPv6 address, rather than an IPv6 prefix, has been specified).

`--block-link-src`, `-J`

This option sets a block filter for the incoming Neighbor Solicitation messages, based on their link-layer Source Address. The option must be followed by a link-layer address (currently, only Ethernet is supported).

`--block-link-dst`, `-K`

This option sets a block filter for the incoming Neighbor Solicitation messages, based on their link-layer Destination Address. The option must be followed by a link-layer address (currently, only Ethernet is supported).

`--block-target`, `-w`

This option sets a block filter for the incoming Neighbor Solicitation messages, based on their Target Address. It allows the specification of an IPv6 prefix in the form “-w prefix/prefixlen”. If the prefix length is not specified, a prefix length of “/128” is selected (i.e., the option assumes that a single IPv6 address, rather than an IPv6 prefix, has been specified).

`--accept-src`, `-b`

This option sets an accept filter for the incoming Neighbor Solicitation messages, based on their IPv6 Source Address. It allows the specification of an IPv6 prefix in the form “-b prefix/prefixlen”. If the prefix length is not specified, a prefix length of “/128” is selected (i.e., the option assumes that a single IPv6 address, rather than an IPv6 prefix, has been specified).

`--accept-dst`, `-g`

This option sets a accept filter for the incoming Neighbor Solicitation messages, based on their IPv6 Destination Address. It allows the specification of an IPv6 prefix in the form “-g prefix/prefixlen”. If the prefix length is not specified, a prefix length of “/128” is selected (i.e., the option assumes that a single IPv6 address, rather than an IPv6 prefix, has been specified).

`--accept-link-src`, `-B`

This option sets an accept filter for the incoming Neighbor Solicitation messages, based on their link-layer Source Address. The option must be followed by a link-layer address (currently, only Ethernet is supported).

`--accept-link-dst`, `-K`

This option sets an accept filter for the incoming Neighbor Solicitation messages, based on their link-layer Destination Address. The option must be followed by a link-layer address (currently, only Ethernet is supported).

`--accept-target`, `-W`

This option sets a accept filter for the incoming Neighbor Solicitation messages, based on their Target Address. It allows the specification of an IPv6 prefix in the form “-W prefix/prefixlen”. If the prefix length is not specified, a prefix length of “/128” is selected (i.e., the option assumes that a single IPv6 address, rather than an IPv6 prefix, has been specified).

`--flood-targets`, `-T`

This option instructs the na6 tool to send Neighbor Advertisements for multiple Target Addresses. The number of different Target Addresses is specified as “-T number”. The Target Address of each packet is randomly selected from the prefix fe80::/64, unless a different prefix has been specified by means of the “-t” option. The IPv6 Source Address of each Neighbor Advertisement message is set according to the IPv6 address or prefix specified with the “-s” option, and defaults to a random link-local unicast address (fe80::/64) if the “-s” option is left unspecified.

`--flood-sources`, `-F`

This option instructs the tool to send multiple Neighbor Advertisement messages with different Source Addresses. The number of different sources is specified as “-F number”. The Source Address of each Neighbor Advertisement is randomly selected from the prefix specified by the “-s” option. If the “-F” option is specified but the “-s” option is left unspecified, the Source Address of the packets is randomly selected from the prefix fe80::/64 (link-local unicast). It should be noted that hosts are required to discard Router Advertisement messages that do not have a link-local unicast address as the Source Address.

`--loop, -l`

This option instructs the na6 tool to send periodic Neighbor Advertisements to the victim node. The amount of time to pause between sending Neighbor Advertisements can be specified by means of the “-z” option, and defaults to 1 second. Note that this option cannot be set in conjunction with the “-L” (“--listen”) option.

`--sleep`, `-z`

This option specifies the amount of time to pause between sending Neighbor Solicitations (when the “--loop” option is set). If left unspecified, it defaults to 1 second.

`--listen`, `-L`

This instructs the na6 tool to operate in passive mode (possibly after attacking a given node, if the ‘-d’ or ‘-D’ options were specified). Note that this option cannot be used in conjunction with the “-l” (“--loop”) option.

`--verbose`, `-v`

This option instructs the na6 tool to be verbose. When the option is set twice, the tool is “very verbose”, and the tool also informs which packets have been accepted or discarded as a result of applying the specified filters.

`--help`, `-h`

Print help information for the na6 tool.

## Examples

### Example #1

```
# ./na6 -i eth0 -d fe80::1 -t 2001:db8::1 -c -o -e
```

Use the network interface “eth0” to send a Neighbor Advertisement using a random link-local unicast IPv6 Source Address and a random Ethernet Source Address, to the IPv6 Destination address ffe80::1 and the Ethernet Destination Address 33:33:00:00:00:01 (selected by default). The target of the Neighbor Advertisement is 2001:db8::1, and the message has both the “Override” and the “Solicited” flags set. The Neighbor Advertisement also includes a target link-layer address option that contains the same Ethernet address as that used for the Ethernet Source Address of the packet.

### Example #2

```
# ./na6 -i eth0 -j fe80::1 -j 2001:db8::/32 -W fe80::/64 -c -o -e -L -v
-v
```

Listen for incoming Neighbor Solicitation messages on the interface “eth0”. Discard those messages that have an IPv6 Source Address equal to fe80::1, an IPv6 Source Address that belongs to the prefix 2001:db8::/32, or a Target Address that does not belong to the prefix fe80::/64. Respond (to those messages that are accepted) with a Neighbor Advertisement with a randomized Ethernet Source Address and a randomized link-local unicast IPv6 Source Address (unless the Destination Address of the Neighbor Solicitation was a unicast address), the IPv6 Destination Address set to the Source Address of the incoming NS message (unless it was the unspecified address), the Target Address set to the same value as the Target Address of the incoming NS, and the “Solicited” and “Override” flags set. Be very verbose (“-v -v” options).

## Credits

The na6 tool v1.2 and related manuals were produced by Fernando Gont <fgont@si6networks.com> on behalf of the UK Centre for the Protection of National Infrastructure (CPNI) <http://www.cpni.gov.uk>.

## License