

## icmp6 v1.1 manual pages

### Description

This tool is part of the IPv6 Toolkit v1.1: 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 error messages.

### Modes of Operation

This tool has two modes of operation: “active” and “listening”. In active mode, the tool attacks a specific target without listening to any incoming traffic, while in “listening” mode the tool listens to traffic on the local network, and launches an attack in response to such traffic. Active mode is employed if an IPv6 Destination Address is specified. “Listening” mode is employed if the “-L” option (or its long counterpart “--listen”) is set. If both an attack target and the “-L” option are specified, the attack is launched against the specified target, and then the tool enters “listening” mode to respond incoming packets with ICMPv6 error messages.

The tool supports filtering of incoming packets based on the Ethernet Source Address, the Ethernet Destination Address, the IPv6 Source Address, and the IPv6 Destination Address. There are two types of filters: “block filters” and “accept filters”. If any “block filter” is specified, and the incoming packet matches any of those filters, the message is discarded (and thus no ICMPv6 error messages are sent in response). If any “accept filter” is specified, incoming packets must match the specified filters in order for the tool to respond with ICMPv6 error messages.

### Options

The icmp6 tool takes its 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”).

The icmp6 tool supports IPv6 fragmentation, which might be of use to circumvent layer-2 filtering and/or Network Intrusion Detection Systems (NIDS). 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 a prefix is specified, the Source Address is randomly selected from that prefix. If this option is left unspecified, the IPv6 Source Address of the attack packets is randomly selected from the prefix ::/0.

--dst-address, -d

This option specifies the IPv6 Destination Address of the victim. It can be left unspecified only if the “-L” option is selected (that is, if the tool is to operate in “listening” mode).

When operating in “listening” mode (“-L” option), the IPv6 Destination Address is selected according to the IPv6 Source Address of the incoming packet.

--hop-limit, -c

This option specifies the Hop Limit to be used for the Redirect messages. If this option is left unspecified, the Hop Limit is randomized to a value between 64 and 243.

--frag-hdr, -y

This option specifies that the ICMPv6 error messages 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 attack packets. 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 attack packets. 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 attack packets (currently, only Ethernet is supported). If left unspecified, the link-layer Source Address is randomized.

--link-dst-address, -D

This option specifies the link-layer Destination Address of the attack packets (currently, only Ethernet is supported). If left unspecified, it is set to that of the local router (for non-local destinations) or to that corresponding to the destination host (for local hosts).

When operating in “listening” mode, the link-layer Destination Address is set to the link-layer Source Address of the incoming packet.

--icmp6, -t

This option specifies the Type and Code of the ICMPv6 error message in the form “--icmp6 TYPE:CODE”. If left unspecified, the ICMPv6 error message defaults to “Parameter Problem, Erroneous header field encountered” (Type 4, Code 0).

Note: Other options (such as “--icmp6-unreachable”) provide an alternative for setting the ICMPv6 Type and Code.

--icmp6-dest-unreach, -e

This option sets the ICMPv6 Type to “1” (Destination Unreachable), and allows the user to specify the ICMPv6 Code, in the form “--icmp6-dest-unreach CODE”.

Note: this option is an alternative to the “-t” option for setting the ICMPv6 Type and Code.

--icmp6-packet-too-big, -E

This option sets the ICMPv6 Type to “1”, and the ICMPv6 Code to “0” (Packet Too Big).

Note: this option is an alternative to the “-t” option for setting the ICMPv6 Type and Code.

`--icmp6-time-exceeded, -A`

This option sets the ICMPv6 Type to “3” (Time Exceeded), and allows the user to specify the ICMPv6 Code, in the form “--icmp6-time-exceeded CODE”.

Note: this option is an alternative to the “-t” option for setting the ICMPv6 Type and Code.

`--icmp6-param-problem, -R`

This option sets the ICMPv6 Type to “4” (Parameter Problem), and allows the user to specify the ICMPv6 Code, in the form “--icmp6-param-problem CODE”.

Note: this option is an alternative to the “-t” option for setting the ICMPv6 Type and Code.

`--mtu, -m`

This specifies the value of the “MTU” field of ICMPv6 Packet Too Big error messages.

`--pointer, -O`

This option specifies the value of the “Pointer” field of ICMPv6 Parameter Problem error messages.

`--payload-type, -p`

This option specifies the payload type to be included in the ICMPv6 Payload. Currently supported payloads are “TCP”, “UDP”, and “ICMP6”. The payload-type defaults to “TCP”.

When the tool operates in “Listening” mode, this option specifies the type of packets the tool will listen to. In listening mode, an additional type can be specified: “IP6”; this will cause the tool to listen to all IPv6 traffic.

`--payload-size, -P`

Size of the payload to be included in the ICMPv6 Payload (with the payload type being specified by the “-p” option). By default, as many bytes as possible are included, without exceeding the minimum IPv6 MTU (1280 bytes).

`--no-payload, -n`

This option specifies that no payload should be included within the ICMPv6 error message.

`--ipv6-hlim, -C`

This option specifies the Hop Limit of the IPv6 packet included in the payload of the ICMPv6 error message. If this option is left unspecified, the Hop Limit is randomized to a value between 64 and 243.

`--target-addr, -r`

This option specifies the Source Address of the IPv6 packet that is embedded in the ICMPv6 error message. If left unspecified, it is set to the same address as the IPv6 Destination Address of the outer packet.

When operating in “Listening mode”, the tool automatically embeds a piece of the received packet (unless otherwise specified by the “-n” option), and hence the IPv6 Source Address of the embedded IPv6 packet is set accordingly.

`--peer-addr, -x`

This option specifies the Destination Address of the IPv6 packet that is embedded in the ICMPv6 error message. If left unspecified, it is set to a random value.

When operating in “Listening mode”, the tool automatically embeds a piece of the received packet (unless otherwise specified by the “-n” option), and hence the IPv6 Destination Address of the embedded IPv6 packet is set accordingly.

Note: since the victim host is expected to check that the ICMPv6 error message corresponds to an ongoing communication instance, when operating in “active mode”, this option should be set to a value that corresponds to an ongoing communication instance.

`--target-port, -o`

This option specifies the Source Port of the TCP or UDP packet contained in the ICMPv6 Payload. If a port range is specified in the form “-o LOWPORT:HIGHPORT” the tool will send one ICMPv6 error message for each port in that range.

Note: This option is meaningful only if “TCP” or “UDP” have been specified (with the “-p” option).

`--peer-port, -a`

This option specifies the Destination Port of the TCP or UDP packet contained in the ICMPv6 Payload. If a port range is specified in the form “-o LOWPORT:HIGHPORT” the tool will send one ICMPv6 error message for each port in that range.

Note: This option is meaningful only if “TCP” or “UDP” have been specified (with the “-p” option).

--tcp-flags, -X

This option specifies the flags of the TCP header contained in the ICMPv6 Payload. The flags are specified as “F” (FIN), “S” (SYN), “R” (RST), “P” (PSH), “A” (ACK), “U” (URG), “X” (no flags). If left unspecified, only the “ACK” bit is set.

Note: This option is meaningful only if “TCP” has been specified (with the “-p” option).

--tcp-seq, -q

This option specifies the Sequence Number of the TCP header contained in the ICMPv6 Payload. If left unspecified, the Sequence Number is randomized.

Note: This option is meaningful only if “TCP” has been specified (with the “-p” option).

--tcp-ack, -Q

This option specifies the Acknowledgment Number of the TCP header contained in the ICMPv6 Payload. If left unspecified, the Acknowledgment Number is randomized.

Note: This option is meaningful only if “TCP” has been specified (with the “-p” option).

--tcp-urg, -V

This option specifies the Urgent Pointer of the TCP header contained in the ICMPv6 Payload. If left unspecified, the Urgent Pointer is set to 0.

Note: This option is meaningful only if “TCP” has been specified (with the “-p” option).

--tcp-win, -w

This option specifies the Window of the TCP header contained in the ICMPv6 Payload. If left unspecified, the Window is randomized.

Note: This option is meaningful only if “TCP” has been specified (with the “-p” option).

`--block-src, -j`

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

`--accept-src, -b`

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

`--sanity-filters, -f`

This option automatically adds a “block filter” for the IPv6 Source Address of the packets.

Note: This option may be desirable when the tool operates in “Listening mode” and is instructed to listen to “ICMP6” or “IP6” packets (thus possibly avoiding packet loops).

`--loop, -l`

This option instructs the icmp6 tool to send periodic ICMPv6 error messages to the victim node. The amount of time to pause between sending ICMPv6 error messages 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 ICMPv6 error messages (when the “--loop” option is set). If left unspecified, it defaults to 1 second.

`--listen, -L`

This instructs the icmp6 tool to operate in “Listening” mode (possibly after attacking a given node). Note that this option cannot be used in conjunction with the “-l” (“--loop”) option.

`--verbose, -v`

This option instructs the icmp6 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 icmp6 tool.

## Examples

### Example #1

```
# ./icmp6 -i eth0 -L -p TCP -v
```

The tool uses the network interface “eth0”, and operates in “Listening” mode (“-L” option). Each ICMPv6 error message will contain the ICMPv6 Payload as many bytes from the captured packet without exceeding the minimum IPv6 MTU (1280 bytes). The tool will print detailed information about the attack (“-v” option).

### Example #2

```
# ./icmp6 -i eth0 --icmp6-packet-too-big -p ICMP6 -d 2001:db8:10::1  
--peer-addr 2001:db8:11::2 -m 1240 -v
```

The tool uses the network interface “eth0” to send an ICMPv6 Packet Too Big error message that advertises an MTU of 1240 bytes. The ICMPv6 error message will be sent to the address “2001:db8:10::1”. The ICMPv6 error message will embed an ICMPv6 Echo Request message with the Source Address set to “2001:db8:10::1” (i.e., Destination Address of the error message), and the Destination Address set to “2001:db8:11::2” (“--peer-addr” option). The value of the “Identifier” and “Sequence Number” fields of the embedded ICMPv6 Echo Request message randomized. The tool will provide detailed information about the attack (“-v” option).

## Credits

The IPv6 Toolkit version 1.1 and related manual were produced by Fernando Gont <[fgont@si6networks.com](mailto:fgont@si6networks.com)> on behalf of the UK Centre for the Protection of National Infrastructure (CPNI) <<http://www.cpni.gov.uk>>.

## License

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.3 or any later version published by the Free Software Foundation; with the Invariant Sections being just "Credits", with no Front-Cover Texts, and with no Back-Cover Texts. A copy of the license is available at <<http://www.gnu.org/licenses/fdl.html>>.