



## ***Rocky Enterprise Linux 9.2 Manual Pages on command 'ip-macsec.8'***

**C:\>man ip-macsec.8**

IP-MACSEC(8)                      Linux                      IP-MACSEC(8)

### NAME

ip-macsec - MACsec device configuration

### SYNOPSIS

```
ip link add link DEVICE name NAME type macsec [ [ address <lladdr> ] port PORT |
sci <u64> ] [ cipher { default | gcm-aes-128 | gcm-aes-256"}][ " icvlen ICVLEN ] [
encrypt { on | off } ] [ send_sci { on | off } ] [ end_station { on | off } ] [ scb
{ on | off } ] [ protect { on | off } ] [ replay { on | off } ] [ window WINDOW ] [
validate { strict | check | disabled } ] [ encodingsa SA ]
ip macsec add DEV tx sa { 0..3 } [ OPTS ] key ID KEY
ip macsec set DEV tx sa { 0..3 } [ OPTS ]
ip macsec del DEV tx sa { 0..3 }
ip macsec add DEV rx SCI [ on | off ]
ip macsec set DEV rx SCI [ on | off ]
ip macsec del DEV rx SCI
ip macsec add DEV rx SCI sa { 0..3 } [ OPTS ] key ID KEY
ip macsec set DEV rx SCI sa { 0..3 } [ OPTS ]
ip macsec del DEV rx SCI sa { 0..3 }
ip macsec show [ DEV ]
OPTS := [ pn { 1..2^32-1 } ] [ on | off ]
SCI := { sci <u64> | port PORT address <lladdr> }
PORT := { 1..2^16-1 }
```

## DESCRIPTION

The `ip macsec` commands are used to configure transmit secure associations and receive secure channels and their secure associations on a MACsec device created with the `ip link add` command using the `macsec` type.

## EXAMPLES

Create a MACsec device on link `eth0`

```
# ip link add link eth0 macsec0 type macsec port 11 encrypt on
```

Configure a secure association on that device

```
# ip macsec add macsec0 tx sa 0 pn 1024 on key 01 818181818181818181818181818181
```

Configure a receive channel

```
# ip macsec add macsec0 rx port 1234 address c6:19:52:8f:e6:a0
```

Configure a receive association

```
# ip macsec add macsec0 rx port 1234 address c6:19:52:8f:e6:a0 sa 0 pn 1 on key 00
```

```
8282828282828282828282828282828282
```

Display MACsec configuration

```
# ip macsec show
```

## NOTES

This tool can be used to configure the 802.1AE keys of the interface. Note that 802.1AE uses GCM-AES with a initialization vector (IV) derived from the packet number. The same key must not be used with the same IV more than once. Instead, keys must be frequently regenerated and distributed. This tool is thus mostly for debugging and testing, or in combination with a user-space application that reconfigures the keys. It is wrong to just configure the keys statically and assume them to work indefinitely. The suggested and standardized way for key management is 802.1X-2010, which is implemented by `wpa_supplicant`.

## SEE ALSO

`ip-link(8)` `wpa_supplicant(8)`

## AUTHOR

Sabrina Dubroca <[sd@queasysnail.net](mailto:sd@queasysnail.net)>

`iproute`

07 Mar 2016

IP-MACSEC(8)