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

$ 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

| gcm-aes-xpn-128 | gcm-aes-xpn-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] [offload { off | phy | mac }]

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 offload DEV { off | phy | mac }

ip macsec show [DEV]

OPTS := [pn { 1..2^32-1 } | xpn { 1..2^64-1 }] [salt SALT] [ssci <u32>] [on | off]

SCI := { sci <u64> | port PORT address <lladdr> }

PORT := { 1..2^16-1 }

SALT := 96-bit hex string

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 (offload is disabled by default)

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 81818181818181818181818181818181

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 82828282828282828282828282828282

Display MACsec configuration

ip macsec show

Configure offloading on an interface

ip macsec offload macsec0 phy

Configure offloading upon MACsec device creation

ip link add link eth0 macsec0 type macsec port 11 encrypt on offload mac

EXTENDED PACKET NUMBER EXAMPLES

Create a MACsec device on link eth0 with enabled extended packet number (offload is disabled by default)

ip link add link eth0 macsec0 type macsec port 11 encrypt on cipher gcm-aes-xpn-128

Configure a secure association on that device

ip macsec add macsec0 tx sa 0 xpn 1024 on salt 838383838383838383838383 ssci 123 key 01 8181818181818181818181818181818181

Configure a receive channel

ip macsec add macsec0 rx port 11 address c6:19:52:8f:e6:a0

Configure a receive association

ip macsec add macsec0 rx port 11 address c6:19:52:8f:e6:a0 sa 0 xpn 1 on salt 838383838383838383838383 ssci 123 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) de? rived 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 man? agement is 802.1X-2010, which is implemented by wpa_supplicant.

EXTENDED PACKET NUMBER NOTES

Passing cipher gcm-aes-xpn-128 or gcm-aes-xpn-256 to ip link add com? mand using the macsec type requires using the keyword 'xpn' instead of 'pn' in addition to providing a salt using the 'salt' keyword and ssci using the 'ssci' keyword when using the ip macsec command.

SEE ALSO

ip-link(8) wpa_supplicant(8)

AUTHOR

Sabrina Dubroca <sd@queasysnail.net>