MACsec encryption performance and statistics

This chapter provides comprehensive guidance on monitoring and troubleshooting MACsec performance using SecY statistics, SNMP MIBs, and CLI commands. Users can learn how to access detailed encryption and decryption metrics, retrieve MACsec interface indexes, and perform SNMP queries for secure network management and diagnostics.

MACsec SecY statistics

The MACsec SecY statistics are operational metrics that

- monitor the performance of the MAC Security (MACsec) Secure Channel (SecY) component,
- provide detailed visibility into packet and octet processing activities, and
- help identify encryption or decryption issues in secure network communication.

MACsec SecY statistics track the behavior of encrypted traffic, including packet processing, encryption, decryption, and error conditions. They serve as diagnostic indicators that allow network administrators to confirm proper MACsec operation and troubleshoot encrypted traffic flows.

Key aspects of SecY statistics include:

- Interface statistics: Track untagged packets, packets without MACsec tags, packets with invalid tags, unknown Secure Channel Identifiers (SCI), and counts of validated or decrypted octets.
- Secure Channel (SC) statistics: Include transmit (TxSC) and receive (RxSC) data, such as packets protected, encrypted, dropped for being too long, and octet encryption or decryption counts.
- Secure Association (SA) statistics: Provide detailed per-SA data for both transmit and receive directions, including packets protected, encrypted, and the next packet number (NextPN).

These statistics can be accessed using CLI commands such as **show macsec secy stats** on supported controllers or interfaces, and through SNMP queries using the IEEE8021-SECY-MIB.

Network administrators rely on these statistics to ensure that MACsec encryption is functioning correctly and to detect anomalies in encrypted traffic.

Administrators can query MACsec SecY statistics using the following methods:

- CLI – for real-time interface and controller-level statistics
- SNMP MIB – for remote monitoring and integration with network management systems

Query SNMP statistics

Administrators can query SNMP statistics through the CLI to view detailed information about MACsec SecY statistics on a specific interface.

Use the **show macsec secy statistics interface** command to display detailed MACsec SecY statistics for a specified interface.

- Example:

```
Router# show macsec secy stats interface hundredGigE 0/1/0/10 sc

Interface Stats
    InPktsUntagged     :  0
    InPktsNoTag        :  0
    InPktsBadTag       :  0
    InPktsUnknownSCI   :  0
    InPktsNoSCI        :  0
    InPktsOverrun      :  0
    InOctetsValidated  :  0
    InOctetsDecrypted  :  0
    OutPktsUntagged    :  0
    OutPktsTooLong     :  0
    OutOctetsProtected :  0
    OutOctetsEncrypted :  0

SC Stats
  TxSC Stats
    OutPktsProtected   : 0
    OutPktsEncrypted   : 0
    OutOctetsProtected : 0
    OutOctetsEncrypted : 0
    OutPktsTooLong     : 0
    TxSA Stats
      TxSA 0:
        OutPktsProtected : 0
        OutPktsEncrypted : 0
        NextPN           : 1
      TxSA 1:
        OutPktsProtected : 0
        OutPktsEncrypted : 0
        NextPN           : 0
      TxSA 2:
        OutPktsProtected : 0
        OutPktsEncrypted : 0
        NextPN           : 0
      TxSA 3:
        OutPktsProtected : 0
        OutPktsEncrypted : 0
        NextPN           : 0

  RxSC Stats
    RxSC 1: 10000742d968a00
```

```
    InPktsUnchecked     : 0
    InPktsDelayed       : 0
    InPktsLate          : 0
    InPktsOK            : 0
    InPktsInvalid       : 0
    InPktsNotValid      : 0
    InPktsNotUsingSA    : 0
    InPktsUnusedSA      : 0
    InPktsUntaggedHit   : 0
    InOctetsValidated   : 0
    InOctetsDecrypted   : 0
  RxSA Stats
    RxSA 0:
      InPktsUnusedSA      : 0
      InPktsNotUsingSA    : 0
      InPktsNotValid      : 0
      InPktsInvalid       : 0
      InPktsOK            : 0
      NextPN              : 1
    RxSA 1:
      InPktsUnusedSA      : 0
      InPktsNotUsingSA    : 0
      InPktsNotValid      : 0
      InPktsInvalid       : 0
      InPktsOK            : 0
      NextPN              : 0
    RxSA 2:
      InPktsUnusedSA      : 0
      InPktsNotUsingSA    : 0
      InPktsNotValid      : 0
      InPktsInvalid       : 0
      InPktsOK            : 0
      NextPN              : 0
    RxSA 3:
      InPktsUnusedSA      : 0
      InPktsNotUsingSA    : 0
      InPktsNotValid      : 0
      InPktsInvalid       : 0
      InPktsOK            : 0
      NextPN              : 0
```

- On Cisco 8712-MOD-M routers, all TxSC (Transmit Secure Channel) counters display a value of zero. This behavior occurs due to a hardware limitation — K100 ASIC-based systems used in these routers do not support the collection of TxSC statistics.

MACsec SNMP MIB

A MACsec SNMP MIB (IEEE8021-SECY-MIB) is a management information base that

- provides Simple Network Management Protocol (SNMP) access to the MAC Security (MACsec) entity (SecY),
- enables network administrators to query encryption, decryption, and hardware-related SecY data, and
- operates exclusively on the Controlled Port for MACsec-enabled interfaces.

The IEEE8021-SECY-MIB allows monitoring of SecY statistics on IOS XR MACsec-enabled line cards, offering visibility into the performance and status of secure data transmission. It is primarily used to retrieve real-time operational data about packet encryption and decryption within MACsec environments.

The object identifier (OID) for the IEEE8021-SECY-MIB is 1.0.8802.1.1.3.

The IEEE8021-SECY-MIB contains the following tables that specifies the detailed attributes of the MACsec Controlled Port interface index.

Table 1: IEEE8021-SECY-MIB

Tables	OID
secyIfTable	1.0.8802.1.1.3.1.1.1
secyTxSCTable	1.0.8802.1.1.3.1.1.2
secyTxSATable	1.0.8802.1.1.3.1.1.3
secyRxSCTable	1.0.8802.1.1.3.1.1.4
secyRxSATable	1.0.8802.1.1.3.1.1.5
secyCipherSuiteTable	1.0.8802.1.1.3.1.1.6
secyTxSAStatsTable	1.0.8802.1.1.3.1.2.1
secyTxSCStatsTable	1.0.8802.1.1.3.1.2.2
secyRxSAStatsTable	1.0.8802.1.1.3.1.2.3
secyRxSCStatsTable	1.0.8802.1.1.3.1.2.4
secyStatsTable	1.0.8802.1.1.3.1.2.5

- For more technical details on MACsec SNMP MIB (IEEE8021-SECY-MIB), download the IEEE8021-SECY-MIB from MIB Locator in Cisco Feature Navigator.
- For more information on the IEEE8021-SecY-MIB, see http://www.ieee802.org/1/files/public/MIBs/IEEE8021-SECY-MIB-200601100000Z.mib

Use SNMP commands to access SECY MIB

Retrieve SECY MIB information from a device using SNMP commands.

You need to query SECY MIB data for MACsec interfaces on a device with SNMP enabled.

Before you begin

Ensure you have the correct SNMP community string, management IP address, and interface ifIndex.

Follow these steps to retrieve SECY MIB data:

Procedure

Step 1 Walk the entire SECY MIB subtree to enumerate all objects.

Example:

```
snmpwalk -v2c -c <community_string> <management_IP> 1.0.8802.1.1.3
```

Step 2 Query the TxSCI value for a specific interface using its ifIndex:

Example:

```
snmpget -v2c -c <community_string> <management_IP> iso.0.8802.1.1.3.1.1.2.1.1.<ifIndex>
```

Step 3 Find the ifIndex of the MACsec controlled port by performing an SNMP walk on the IfMib:

Example:

```
snmpwalk -v2c -c <community_string> <management_IP> 1.3.6.1.2.1.31.1.1.1.1
```

Step 4 Alternatively, use the **show snmp interface** command to display SNMP interface information:

You will obtain SECY MIB data and the interface index needed for targeted SNMP queries.

Obtain the MACsec controlled port interface index

This reference describes how to identify the interface index (ifindex) for a MACsec controlled port by using SNMP and CLI commands. It helps users manage and monitor MACsec-enabled interfaces on network devices.

Use these commands to obtain the ifindex of the MACsec controlled port:

- **snmpwalk** command on IfMib [OID: 1.3.6.1.2.1.31.1.1.1]

```
rtr1.0/1/CPU0/ $ snmpwalk -v2c -c public 10.0.0.1  1.3.6.1.2.1.31.1.1.1.1
SNMPv2-SMI::mib-2.31.1.1.1.1.3 = STRING: "GigabitEthernet0/1/0/0"
SNMPv2-SMI::mib-2.31.1.1.1.1.18 = STRING: "MACSecControlled0/1/0/0"
SNMPv2-SMI::mib-2.31.1.1.1.1.19 = STRING: "MACSecUncontrolled0/1/0/0"
```

- **show snmp interface** command

```
Router# show snmp interface
.
.
ifName : MACSecControlled0/0/0/0  ifIndex : 77
ifName : MACSecControlled0/0/0/4  ifIndex : 79
ifName : MACSecControlled0/0/0/21  ifIndex : 94
ifName : MACSecControlled0/0/0/30  ifIndex : 118
ifName : MACSecControlled0/0/0/34  ifIndex : 116
ifName : MACSecUncontrolled0/0/0/0  ifIndex : 78
ifName : MACSecUncontrolled0/0/0/4  ifIndex : 80
ifName : MACSecUncontrolled0/0/0/21  ifIndex : 95
ifName : MACSecUncontrolled0/0/0/30  ifIndex : 119
ifName : MACSecUncontrolled0/0/0/34  ifIndex : 117
```

SNMP query examples

The following commands enable network administrators to access and query SECY MIB data from a router using SNMP. These examples assume the SNMP community string is set to public and the device management IP address is 10.0.0.1.

Obtaining the MACsec Controlled Port Interface Index

- To perform an SNMP walk on the entire SECY MIB:

```
snmpwalk -v2c -c public 10.0.0.1 1.0.8802.1.1.3
```

- To query the secyTxSCTable and obtain the TxSCI value for interface Gi0/1/0/0 (where the ifindex for MACsecControlled0/1/0/0 is 18):

```
snmpget -v2c -c public 10.0.0.1 iso.0.8802.1.1.3.1.1.2.1.1.18
```

These SNMP query examples help administrators retrieve security-related MIB data for monitoring and management of router interfaces.