

# Dépannage de WAN MACSEC sur les routeurs

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Topologie](#)

[Présentation de MACSEC pour le dépannage](#)

[Format de paquet MACsec](#)

[WAN-MACSEC](#)

[Format de paquet MACSEC WAN](#)

[Terminologie WAN MACSEC](#)

[MACSEC Key Agreement Protocol \(MKA\) et présentation de la cryptographie](#)

[Clés pré-partagées](#)

[802.1x/EAP](#)

[Dépannage de WAN MACSEC](#)

[Configuration](#)

[Problèmes opérationnels](#)

[Informations connexes](#)

---

## Introduction

Ce document décrit le protocole MACSEC WAN de base pour comprendre le fonctionnement et le dépannage des routeurs Cisco IOS® XE.

## Conditions préalables

### Exigences

Aucune condition préalable spécifique n'est requise pour ce document.

### Composants utilisés

Les informations de ce document sont spécifiques aux routeurs Cisco IOS XE tels que les gammes ASR 1000, ISR 4000 et Catalyst 8000. Recherchez le support matériel et logiciel MACSEC spécifique.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

# Topologie



Schéma de topologie

## Présentation de MACSEC pour le dépannage

MACsec est un cryptage de couche 2 saut par saut basé sur la norme IEEE 802.1AE qui fournit la confidentialité des données, l'intégrité des données et l'authentification de l'origine des données pour les protocoles indépendants de l'accès au support avec le cryptage AES-128. Seules les liaisons faisant face à l'hôte (les liaisons entre les périphériques d'accès réseau et les périphériques d'extrémité tels qu'un PC ou un téléphone IP) peuvent être sécurisées à l'aide de MACsec.

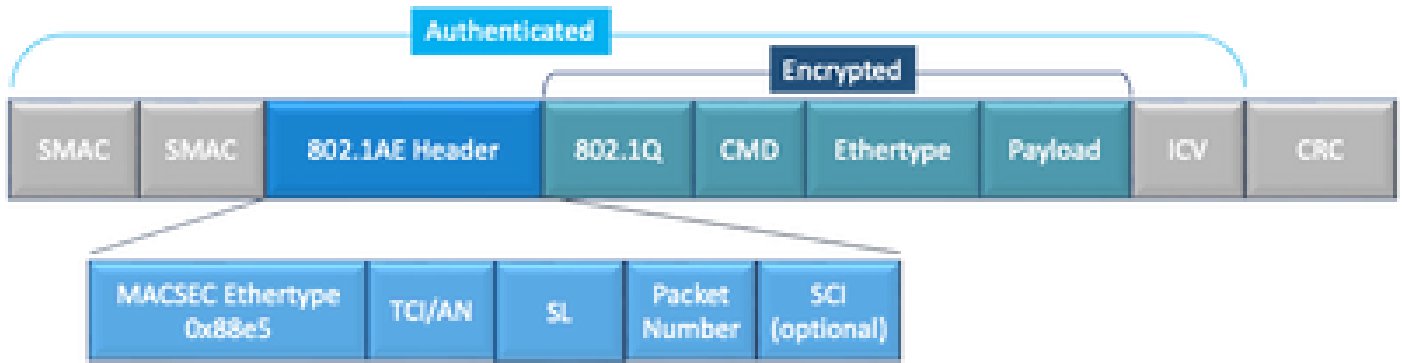
- Les paquets sont décryptés sur le port d'entrée.
- Les paquets sont effacés dans le périphérique.
- Les paquets sont chiffrés sur le port de sortie.

MACsec permet une communication sécurisée sur les réseaux locaux câblés. Lorsque MACsec est utilisé pour sécuriser la communication entre les points d'extrémité d'un réseau local, chaque paquet du réseau est chiffré à l'aide d'une cryptographie à clé symétrique, de sorte que la communication ne peut pas être surveillée ou modifiée sur le réseau local. Lorsque MACsec est utilisé avec des balises de groupe de sécurité (SGT), il fournit une protection pour la balise ainsi que pour les données contenues dans la charge utile de la trame.

MACsec assure le chiffrement de la couche MAC sur les réseaux câblés en utilisant des méthodes hors bande pour la clé de chiffrement.

### Format de paquet MACsec

Avec 802.1AE (MACsec), les trames sont chiffrées et protégées par une valeur de contrôle d'intégrité (ICV) sans impact sur la MTU IP ou la fragmentation et avec un impact minimal sur la MTU L2 : ~40 octets (moins que la trame baby giant).



Exemple de format de paquet MACSEC

- EtherType MACsec : 0x88e5, indique que la trame est une trame MACsec.
- TCI/AN : informations de contrôle TAG/numéro d'association. Est le numéro de version MACsec si la confidentialité ou l'intégrité sont utilisées seules.
- SL : longueur des données chiffrées.
- PN : numéro de paquet utilisé pour la protection de relecture.
- SCI : Secure Channel Identifier. Chaque association de connectivité (CA) est un port virtuel (adresse MAC de l'interface physique plus ID de port 16 bits).
- ICV : valeur de contrôle d'intégrité.

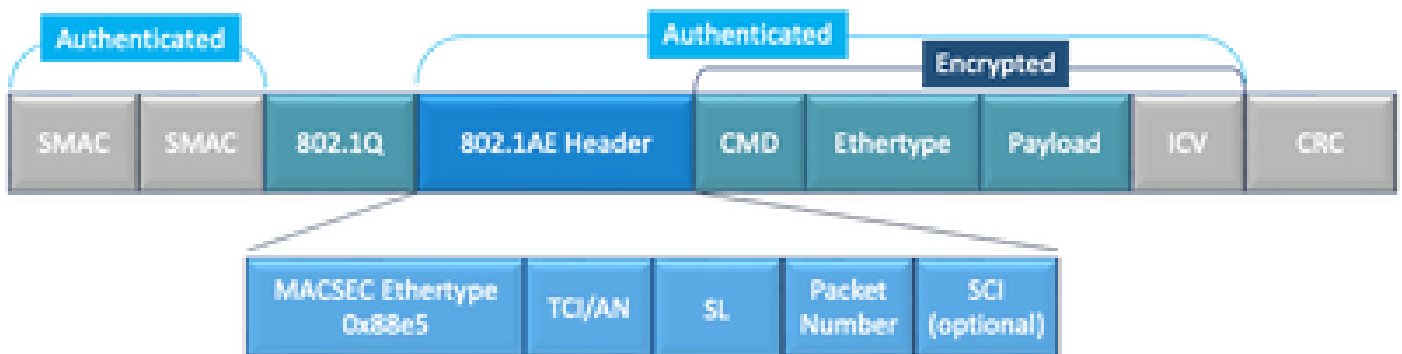
## WAN-MACSEC

Ethernet a évolué au-delà d'un transport LAN privé, pour inclure une variété d'options de transport WAN ou MAN. WAN MACSEC fournit un cryptage de bout en bout sur le service WAN Ethernet de couche 2, point à point ou point à multipoint, à l'aide d'AES 128 ou 256 bits.

WAN MACsec est basé sur (LAN) MACsec, d'où son nom (et séparé d'IPsec), mais offre plusieurs fonctionnalités supplémentaires qui n'étaient pas disponibles auparavant.

### Format de paquet MACSEC WAN

Il est possible que le fournisseur de services ne prenne pas en charge l'ethertype MACsec et ne puisse pas différencier le service L2 si l'étiquette est chiffrée, de sorte que WAN MACSEC chiffre toute la trame après les en-têtes 802.1Q :



Exemple de balise WAN MACSEC 802.1Q dans le format Clear Packet

L'une des nouvelles améliorations inclut les balises 802.1Q dans Clear (ou ClearTag). Cette

amélioration permet d'exposer la balise 802.1Q en dehors de l'en-tête MACsec chiffré. L'exposition de ce champ fournit plusieurs options de conception avec MACsec, et dans le cas des fournisseurs de transport Ethernet opérateur public, il est nécessaire d'exploiter certains services de transport.

La prise en charge de la fonctionnalité MKA fournit des informations de tunnellation telles que l'étiquette VLAN (étiquette 802.1Q) en clair, de sorte que le fournisseur de services peut fournir un multiplexage de services de sorte que plusieurs services point à point ou multipoints peuvent coexister sur une interface physique unique et différenciés sur la base de l'ID de VLAN désormais visible.

En plus du multiplexage de service, l'étiquette VLAN en clair permet également aux fournisseurs de services de fournir une qualité de service (QoS) au paquet Ethernet chiffré sur le réseau SP en fonction du champ 802.1P (CoS) qui est maintenant visible dans le cadre de l'étiquette 802.1Q.

## Terminologie WAN MACSEC

MKA	Accord de clé MACSec, défini dans IEEE 802.1XREV-2010 - Protocole d'accord de clé pour la détection des homologues MACSec et la négociation des clés.
MASQUE	Clé de session principale, générée lors de l'échange EAP. Le demandeur et le serveur d'authentification utilisent le MSK pour générer le CAK
GÂTEAU	La clé d'association de connectivité provient de MSK. Est une clé principale à longue durée de vie utilisée pour générer toutes les autres clés utilisées pour MACSec.
CKN	Connectivity Association Key Name : identifie le CAK.
SAK	Secure Association Key (Clé d'association sécurisée) : provient de la clé CAK et est la clé utilisée par le demandeur et le commutateur pour chiffrer le trafic pour une session donnée.
KS	<p>Serveur de clés responsable de :</p> <ul style="list-style-type: none"> <li>• Sélection et annonce d'une suite de chiffrements</li> <li>• Génération du SAK à partir du CAK.</li> </ul>
QUEUE	Clé de chiffrement de clé : utilisée pour protéger les clés MACsec (SAK)

## MACSEC Key Agreement Protocol (MKA) et présentation de la cryptographie

MKA est le mécanisme de plan de contrôle utilisé par WAN MACsec. Il est spécifié dans la norme IEEE 802.1X qui détecte les homologues MACsec mutuellement authentifiés, ainsi que les actions suivantes :

- Établit et gère une CA (Connectivity Association).
- Gère la liste des homologues actifs/potentiels.
- Négociation de la suite de chiffrement.
- Sélectionne le serveur de clés (KS) parmi les membres d'une autorité de certification.

- Dérivation et gestion de la clé d'association sécurisée.
- Distribution sécurisée des clés.
- Installation de la clé.
- Retouche.

Un membre est sélectionné comme serveur de clés en fonction de la priorité clé-serveur configurée (la plus basse). Si la priorité KS est la même parmi les homologues, la valeur SCI la plus basse l'emporte.

KS génère un SAK uniquement après que tous les homologues potentiels sont devenus actifs et qu'il existe au moins un homologue actif. Il distribue le SAK et le chiffre utilisé aux autres participants à l'aide de la MKA PDU ou de la MKPDU dans un format chiffré.

Les participants vérifient le chiffrement envoyé par le SAK et l'installent s'il est pris en charge, en l'utilisant sur chaque MKPDU pour indiquer la dernière clé dont ils disposent ; sinon, ils rejettent le SAK

Lorsqu'aucune MKPDU n'est reçue d'un participant après 3 pulsations (chaque pulsation est de 2 secondes par défaut), les homologues sont supprimés de la liste d'homologues en direct ; par exemple, si un client se déconnecte, le participant sur le commutateur continue à utiliser MKA jusqu'à ce que 3 pulsations se soient écoulées après la réception de la dernière MKPDU par le client.

Pour ce processus, il existe deux méthodes pour piloter les clés de chiffrement :

- Clés pré-partagées
- 802.1x/EAP

### Clés pré-partagées

Si vous utilisez des clés pré-partagées, CAK=PSK et CKN doivent être entrés manuellement. Pendant la durée de vie de la clé, assurez-vous que vous disposez d'une substitution et d'un chevauchement de clés pendant la période de renouvellement de la clé pour :

- Échangez et installez une nouvelle clé SAK et liez-la à la SA inactive.
- Purgez l'ancienne clé SAK et attribuez une nouvelle SA inactive.

Exemple de configuration :

```
<#root>
```

```
key chain
```

```
  M_Key
```

```
    macsec
```

```
key 01
```

```
  cryptographic-algorithm
```

```
aes-128-cmac
  key-string
12345678901234567890123456789001
  lifetime 12:59:59 Oct 1 2023 duration 5000
key 02
  cryptographic-algorithm aes-128-cmac
  key-string 12345678901234567890123456789002
  lifetime 14:00:00 Oct 1 2023 16:15:00 Oct 1 2023
key 03
  cryptographic-algorithm aes-128-cmac
  key-string 12345678901234567890123456789003
  lifetime 16:15:00 Oct 1 2023 17:15:00 Oct 1 2023
key 04
  cryptographic-algorithm aes-128-cmac
  key-string 12345678901234567890123456789012
  lifetime 17:00:00 Oct 1 2023 infinite
```

Lorsque les mots en gras font référence à :

**M\_Key** : nom de la chaîne de clés.

**key 01** : nom de la clé d'association de connectivité (identique à CKN).

**aes-128-cmac** : chiffrement d'authentification MKA.

**12345678901234567890123456789012** : clé d'association de connectivité (CAK).

Définir une stratégie :


```
<#root>
```

```
mka policy example
  macsec-cipher-suite
```

```
gcm-aes-256
```

Where **gcm-aes-256** fait référence aux suites de chiffrement pour la dérivation de la clé d'association sécurisée (SAK).

---

 Remarque : il s'agit d'une configuration de stratégie de base. D'autres options, telles que `privacy-offset`, `sak-rekey`, `include-icv-indicator` et d'autres sont disponibles en fonction de la mise en oeuvre.


---

Interface:

```
interface TenGigabitEthernet0/1/2
```

```
mtu 2000
ip address 198.51.100.1 255.255.255.0
ip mtu 1468
eapol destination-address broadcast-address
mka policy example
mka pre-shared-key key-chain M_Key
macsec
end
```

---


 Remarque : si aucune stratégie mka n'est configurée ou appliquée, la stratégie par défaut est activée et peut être révisée via `show mka default-policy detail`.

---

## 802.1x/EAP

Si vous utilisez la méthode EAP, toutes les clés sont générées à partir de la clé de session principale (MSK). Avec le cadre EAP (Extensible Authentication Protocol) IEEE 802.1X, MKA échange des trames EAPoL-MKA entre les périphériques, le type Ether des trames EAPoL est 0x888E tandis que le corps du paquet dans une unité de données de protocole (PDU) EAPoL est appelé unité de données de protocole (MKPDU) MACsec. Ces trames EAPoL contiennent le CKN de l'expéditeur, la priorité du serveur clé et les fonctionnalités MACsec.

---

 Remarque : par défaut, les commutateurs traitent les trames EAPoL-MKA mais ne les transmettent pas.

---

Exemple de configuration du chiffrement MACsec basé sur des certificats :

Inscription du certificat (requiert l'autorité de certification) :

```
crypto pki trustpoint EXAMPLE-CA
  enrollment terminal
  subject-name CN=ASR1000@user.example, C=IN, ST=KA, OU=ENG,O=Example
  revocation-check none
  rsakeypair mkaioscarsa
  storage nvram:
```

```
crypto pki authenticate EXAMPLE-CA
```

Authentification 802.1x et configuration AAA requises :

```
aaa new-model
dot1x system-auth-control
radius server ISE
  address ipv4 auth-port 1645 acct-port 1646
  automate-tester username dummy
  key dummy123
  radius-server deadtime 2
```

```
!  
aaa group server radius ISEGRP  
  server name ISE  
!  
aaa authentication dot1x default group ISEGRP  
aaa authorization network default group ISEGRP
```

## Profil EAP-TLS et références 802.1X :

```
eap profile EAPTLS-PROF-IOSCA  
  method tls  
  pki-trustpoint EXAMPLE-CA  
!  
dot1x credentials EAPTLSCRED-IOSCA  
  username asr1000@user.example  
  pki-trustpoint EXAMPLE-CA  
!
```

## Interface:

```
interface TenGigabitEthernet0/1/2  
  macsec network-link  
  authentication periodic  
  authentication timer reauthenticate  
  access-session host-mode multi-host  
  access-session closed  
  access-session port-control auto  
  dot1x pae both  
  dot1x credentials EAPTLSCRED-IOSCA  
  dot1x supplicant eap profile EAPTLS-PROF-IOSCA  
  service-policy type control subscriber DOT1X_POLICY_RADIUS
```

## Dépannage de WAN MACSEC

### Configuration

Vérifier la configuration et la mise en oeuvre appropriées en fonction de la plate-forme ; les clés et les paramètres doivent correspondre. Les journaux suivants permettent d'identifier les problèmes de configuration : (en anglais)

```
%MKA-3-INVALID_MACSEC_CAPABILITY : Terminating MKA Session because no peers had the required MACsec Cap
```

Vérifiez la capacité MACsec du matériel des homologues ou réduisez la configuration requise



pour la capacité MACsec en modifiant la configuration MACsec de l'interface.

```
%MKA-3-INVALID_PARAM_SET : %s, Local-TxSCI %s, Peer-RxSCI %s, Audit-SessionID %s
```

Il existe certains paramètres facultatifs que le routeur peut attendre ou non en fonction de la configuration et des différents paramètres par défaut de la plate-forme. Veillez à inclure ou à ignorer la configuration.

```
%MKA-4-MKA_MACSEC_CIPHER_MISMATCH: Lower/Higher strength MKA-cipher than macsec-cipher for RxSCI %s, Au
```

Il y a une incohérence de configuration sur la suite de chiffrement de stratégie. Assurez-vous que la correspondance est correcte.

```
%MKA-3-MKPDU_VALIDATE_FAILURE : MKPDU validation failed for Local-TxSCI %s, Peer-RxSCI %s, Audit-Session
```

MKPDU a échoué à un ou plusieurs des contrôles de validation suivants :

- Valid MAC Address et EAPOL Header : vérifiez la configuration des deux interfaces, la capture de paquets sur l'interface d'entrée peut corroborer les valeurs actuelles.
- Agilité CKN et algorithme valide : assurez-vous que les clés et les suites d'algorithmes sont valides.
- Vérification ICV : la vérification ICV est un paramètre facultatif, la configuration des deux extrémités doit correspondre.
- Existence de charges utiles MKA dans l'ordre correct : problème d'interopérabilité possible.
- Vérification MI si des homologues existent : vérification de l'identificateur de membre, unique pour chaque participant.
- Vérification MN si des homologues existent : vérification du numéro de message, unique sur chaque MKPDU transmise et incrémentée sur chaque transmission.

## Problèmes opérationnels

Une fois la configuration définie, vous pouvez voir le message %MKA-5-SESSION\_START mais vous devez vérifier si la session démarre. Une bonne commande pour commencer est `show mka sessions [interface interface_name]` :

```
<#root>
```

```
Router1#
```

```
show mka sessions
```

```
Total MKA Sessions..... 1
Secured Sessions... 1
Pending Sessions... 0
```

Interface Port-ID	Local-TxSCI Peer-RxSCI	Policy-Name MACsec-Peers	Inherited Status	Key-Server CKN
Te0/1/2	40b5.c133.0e8a/0012			

**Example**

NO

NO

18 40b5.c133.020a/0012 1

**Secured**

01

L'état fait référence à la session du plan de contrôle ; Sécurisé signifie que Rx et Tx SAK sont installés, sinon, il s'affiche comme Non sécurisé.

- Si l'état reste sur Init, vérifiez l'état de l'interface physique, la connectivité via ping pour les homologues et la correspondance de configuration. À ce stade, il n'y a pas de MKPDU reçu et d'homologues actifs, certaines plates-formes font du remplissage alors que d'autres ne le font pas ; considérez jusqu'à 32 octets de surcharge d'en-tête et assurez-vous d'une MTU plus grande pour un fonctionnement correct.
- Si l'état reste sur En attente, vérifiez si les MKPDU sont abandonnées en entrée ou en sortie dans le plan de contrôle ou si les interfaces présentent des erreurs/abandons.
- Si l'état reste Non sécurisé, que l'interface MKA est activée et que des unités MKPDU sont en cours d'exécution, mais que SAK n'est pas installé, le journal suivant s'affiche dans ce cas :

```
%MKA-5-SESSION_UNSECURED : MKA Session was not secured for Local-TxSCI %s, Peer-RxSCI %s, Audit-Session
```

Cela est dû à l'absence de prise en charge MACsec, à une configuration MACsec non valide ou à une autre défaillance MKA sur le côté local ou homologue avant l'établissement d'un canal sécurisé (SC) et l'installation d'associations sécurisées (SA) dans MACsec. Vous pouvez utiliser la commande detail pour plus d'informations sur show mka session [interface interface\_name] detail :

<#root>

Router1#

show mka sessions detail

MKA Detailed Status for MKA Session

=====

Status: SECURED - Secured MKA Session with MACsec

Local Tx-SCI..... 40b5.c133.0e8a/0012  
Interface MAC Address.... 40b5.c133.0e8a  
MKA Port Identifier..... 18  
Interface Name..... TenGigabitEthernet0/1/2  
Audit Session ID.....

CAK Name (CKN)..... 01

Member Identifier (MI)... DC5F7E3E38F4210925AAC8CA  
Message Number (MN)..... 14462  
EAP Role..... NA  
Key Server..... NO

MKA Cipher Suite..... AES-128-CMAC

Latest SAK Status..... Rx & Tx  
Latest SAK AN..... 0  
Latest SAK KI (KN)..... 272DA12A009CD0A3D313FADF00000001 (1)  
Old SAK Status..... FIRST-SAK  
Old SAK AN..... 0  
Old SAK KI (KN)..... FIRST-SAK (0)

SAK Transmit Wait Time... 0s (Not waiting for any peers to respond)  
SAK Retire Time..... 0s (No Old SAK to retire)  
SAK Rekey Time..... 0s (SAK Rekey interval not applicable)

MKA Policy Name..... Example  
Key Server Priority..... 2  
Delay Protection..... NO  
Delay Protection Timer..... 0s (Not enabled)

Confidentiality Offset... 0  
Algorithm Agility..... 80C201  
SAK Rekey On Live Peer Loss..... NO  
Send Secure Announcement.. DISABLED  
SCI Based SSCI Computation... NO  
SAK Cipher Suite..... 0080C20001000002 (GCM-AES-256)  
MACsec Capability..... 3 (MACsec Integrity, Confidentiality, & Offset)  
MACsec Desired..... YES

# of MACsec Capable Live Peers..... 1  
# of MACsec Capable Live Peers Responded.. 0

Live Peers List:

MI	MN	Rx-SCI (Peer)	KS Priority	RxSA Installed	SSCI
272DA12A009CD0A3D313FADF	14712	40b5.c133.020a/0012	1	YES	0

Potential Peers List:

MI	MN	Rx-SCI (Peer)	KS Priority	RxSA Installed	SSCI
----	----	---------------	----------------	-------------------	------

---

Recherchez les informations SAK sur les homologues et les données pertinentes mises en surbrillance pour mieux comprendre la situation. Si SAK différent est en place, examinez la clé utilisée et les options de durée de vie ou de renouvellement de clé SAK configurées. Si des clés pré-partagées sont utilisées, vous pouvez utiliser show mka keychains :

```
<#root>
```

```
Router1#
```

```
show mka keychains
```

```
MKA PSK Keychain(s) Summary...
```

Keychain Name	Latest CKN Latest CAK	Interface(s) Applied
------------------	--------------------------	-------------------------

---

```
Master_Key
```

```
01
```

```
Te0/1/2
```

```
<HIDDEN>
```

CAK n'est jamais affiché, mais vous pouvez corroborer le nom de la chaîne de clés et CKN.

Si la session a été établie mais que vous avez des flaps ou un flux de trafic intermittent, vous devez vérifier si les MKPDU circulent correctement entre les homologues, s'il y a un délai d'attente, vous pouvez voir le message suivant :

```
%MKA-4-KEEPALIVE_TIMEOUT : Keepalive Timeout for Local-TxSCI %s, Peer-RxSCI %s, Audit-SessionID %s, CKN
```

S'il y a un homologue, la session MKA est terminée, si vous avez plusieurs homologues et que MKA n'a pas reçu de MKPDU de l'un de ses homologues pendant plus de 6 secondes, l'homologue en direct est supprimé de la liste des homologues en direct, vous pouvez commencer par show mka statistics [interface interface\_name] :

```
<#root>
```

```
Router1#
```

```
show mka statistics interface TenGigabitEthernet0/1/2
```

```
MKA Statistics for Session
=====
Reauthentication Attempts.. 0
```

```
CA Statistics
  Pairwise CAKs Derived... 0
  Pairwise CAK Rekeys..... 0
  Group CAKs Generated.... 0
  Group CAKs Received..... 0
```

```
SA Statistics
  SAKs Generated..... 0
  SAKs Rekeyed..... 0
  SAKs Received..... 1
  SAK Responses Received.. 0
```

```
MKPDU Statistics
```

```
MKPDUs Validated & Rx... 11647
  "Distributed SAK".. 1
  "Distributed CAK".. 0
```

```
MKPDUs Transmitted..... 11648
  "Distributed SAK".. 0
  "Distributed CAK".. 0
```

Les MKPDU transmises et reçues doivent avoir des numéros similaires pour un homologue, assurez-vous qu'elles augmentent à Rx et Tx aux deux extrémités, pour déterminer ou guider la direction problématique, s'il y a des différences, vous pouvez activer debug mka linksec-interface frames aux deux extrémités :


```
*Sep 20 21:14:10.803: MKA-LLI-MKPDU: Received CKN length (2 bytes) from Peer with CKN 01
*Sep 20 21:14:10.803: MKA-LLI-MKPDU: MKPDU Received: Interface: [Te0/1/2 : 18] Peer MAC: 40:B5:C1:33:02
*Sep 20 21:14:12.101: MKA-LLI-MKPDU: MKPDU transmitted: Interface [Te0/1/2: 18] with CKN 01
*Sep 20 21:14:12.803: MKA-LLI-MKPDU: Received CKN length (2 bytes) from Peer with CKN 01
*Sep 20 21:14:12.803: MKA-LLI-MKPDU: MKPDU Received: Interface: [Te0/1/2 : 18] Peer MAC: 40:B5:C1:33:02
```

Si aucune MKPDU n'est reçue, recherchez les erreurs ou les abandons d'interface entrants, l'état des interfaces homologues et la session MKPDU ; si les deux routeurs envoient mais ne reçoivent pas, les MKPDU sont perdues sur le support et doivent vérifier les périphériques intermédiaires pour un transfert correct.

Si vous n'envoyez pas de MKPDU, vérifiez l'état de l'interface physique (ligne et erreurs/abandons) et la configuration ; examinez si vous générez ces paquets au niveau du plan de contrôle, FIA trace et Embedded Packet Capture (EPC) sont des outils fiables à cet effet. Référez-vous à [Dépannage avec la fonctionnalité Cisco IOS XE Datapath Packet Trace](#)

Vous pouvez utiliser debug mka events et rechercher des raisons peuvent guider les étapes suivantes.

---

 Remarque : utilisez avec prudence les diagnostics debug mka et debug mka car ils affichent des informations très détaillées sur la machine d'état et qui peuvent entraîner des problèmes de plan de contrôle sur le routeur.

---

Si la session est sécurisée et stable mais que le trafic ne circule pas, recherchez le trafic chiffré qui envoie les deux homologues :

```
<#root>
```

```
Router1#
```

```
show macsec statistics interface TenGigabitEthernet 0/1/2
```

```
MACsec Statistics for TenGigabitEthernet0/1/2
```

```
SecY Counters
```

```
Ingress Untag Pkts:      0
Ingress No Tag Pkts:    0
Ingress Bad Tag Pkts:   0
Ingress Unknown SCI Pkts: 0
Ingress No SCI Pkts:    0
Ingress Overrun Pkts:   0
Ingress Validated Octets: 0
```

```
Ingress Decrypted Octets: 98020
```

```
Egress Untag Pkts:      0
Egress Too Long Pkts:   0
Egress Protected Octets: 0
```

```
Egress Encrypted Octets: 98012
```

```
Controlled Port Counters
```

```
IF In Octets:      595380
IF In Packets:     5245
IF In Discard:     0
IF In Errors:      0
IF Out Octets:     596080
IF Out Packets:    5254
IF Out Errors:     0
```

```
Transmit SC Counters (SCI: 40B5C1330E8B0013)
```

```
Out Pkts Protected: 0
```

```
Out Pkts Encrypted:      970
```

```
Transmit SA Counters (AN 0)
```

```
Out Pkts Protected:     0
```

```
Out Pkts Encrypted:      970
```

Receive SA Counters (SCI: 40B5C133020B0013 AN 0)

In Pkts Unchecked: 0  
In Pkts Delayed: 0

In Pkts OK: 967

In Pkts Invalid: 0

In Pkts Not Valid: 0  
In Pkts Not using SA: 0  
In Pkts Unused SA: 0  
In Pkts Late: 0

Les compteurs SecY sont des paquets actuels sur l'interface physique, tandis que les autres sont associés au canal sécurisé Tx signifie que les paquets sont chiffrés et transmis et que l'association sécurisée Rx signifie que les paquets valides sont reçus sur l'interface.

Plus de débogages tels que les erreurs debug mka et les paquets debug mka aident à identifier les problèmes, veuillez utiliser ce dernier avec précaution car cela peut induire une journalisation lourde.

## Informations connexes

- [Guide de configuration MACsec et MKA](#)
- [Assistance technique et téléchargements Cisco](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.