

Solucionar problemas do MACSEC da WAN em roteadores

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Topologia](#)

[Visão geral do MACSEC para solucionar problemas](#)

[Formato de Pacote MACsec](#)

[WAN-MACSEC](#)

[Formato de pacote MACSEC da WAN](#)

[Terminologia MACSEC de WAN](#)

[Protocolo de Acordo de Chave \(MKA - Key Agreement Protocol\) MACSEC e Visão Geral de Criptografia](#)

[Chaves pré-compartilhadas](#)

[802.1x/EAP](#)

[Solucionar problemas do MACSEC da WAN](#)

[Configuração](#)

[Problemas operacionais](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve o protocolo básico de MACSEC de WAN para entender a operação e solucionar problemas dos roteadores Cisco IOS® XE.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são específicas para os roteadores Cisco IOS XE como as famílias ASR 1000, ISR 4000 e Catalyst 8000. Procure suporte MACSEC específico para hardware e software.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma

configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Topologia

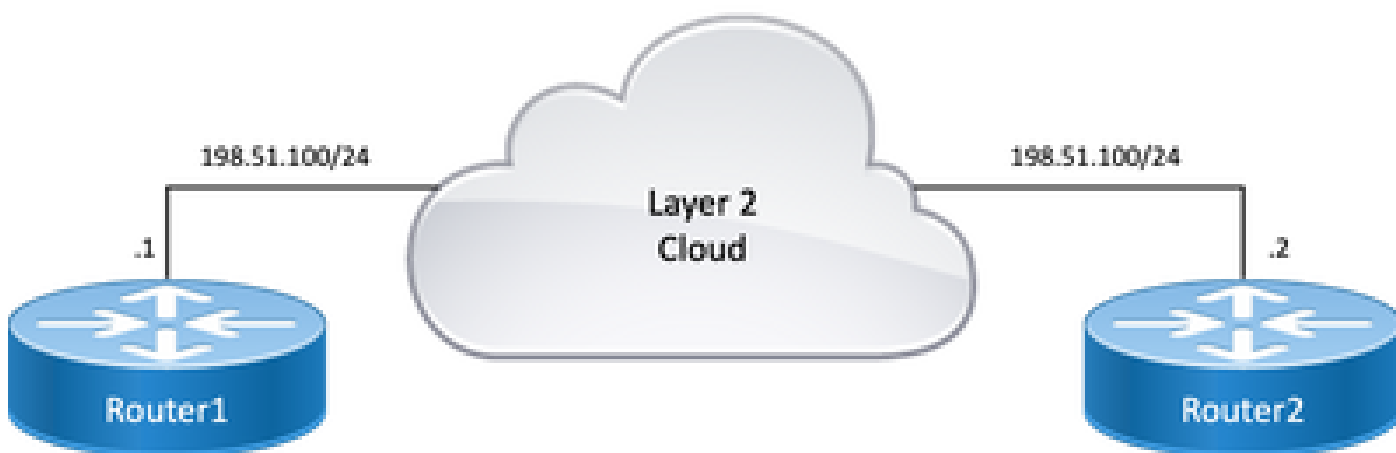


Diagrama de topologia

Visão geral do MACSEC para solucionar problemas

O MACsec é uma criptografia de Camada 2 salto por salto baseada no padrão IEEE 802.1AE que fornece confidencialidade de dados, integridade de dados e autenticação da origem de dados para protocolos independentes de acesso à mídia com criptografia AES-128, apenas links para host (links entre dispositivos de acesso à rede e dispositivos de ponto final, como um PC ou telefone IP) podem ser protegidos usando o MACsec.

- Os pacotes são descriptografados na porta de entrada.
- Os pacotes estão limpos no dispositivo.
- Os pacotes são criptografados na porta de saída.

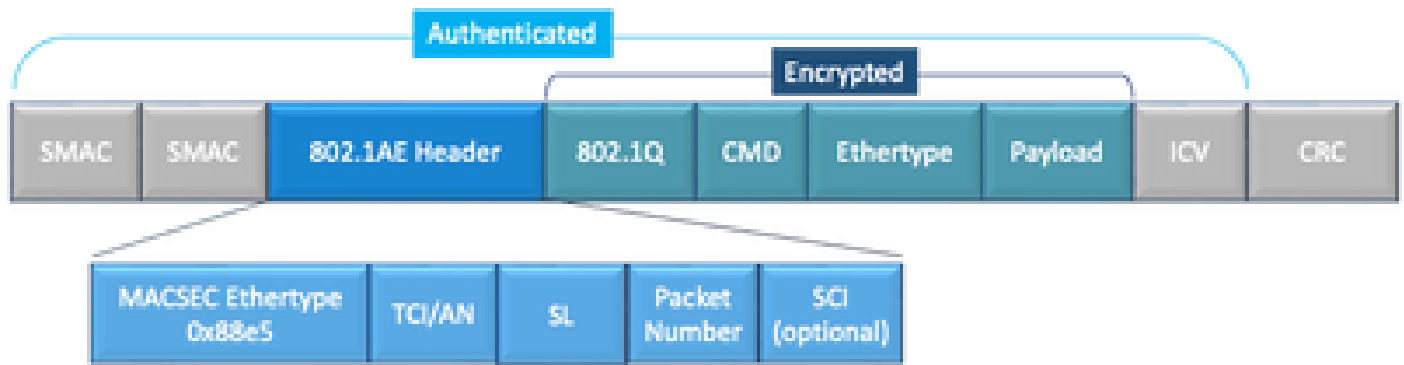
O MACsec fornece comunicação segura em LANs com fio, quando o MACsec é usado para proteger a comunicação entre pontos finais em uma LAN, cada pacote no fio é criptografado usando criptografia de chave simétrica, de modo que a comunicação não possa ser monitorada ou alterada no fio. Quando o MACsec é usado em conjunto com tags de grupos de segurança (SGTs), ele fornece proteção para a tag junto com os dados contidos no payload do quadro.

O MACsec fornece criptografia de camada MAC em redes com fio usando métodos fora de banda para chaves de criptografia.

Formato de Pacote MACsec

Com 802.1AE (MACsec), os quadros são criptografados e protegidos com um valor de verificação de integridade (ICV) sem impacto no MTU IP ou na fragmentação e impacto mínimo no MTU L2:

~40 bytes (menos que o quadro baby giant).



Exemplo de formato de pacote MACSEC

- EtherType MACsec: 0x88e5, designa que o quadro é um quadro MACsec.
- TCI/AN: TAG Control Information/Association Number (Informações de controle de TAG/Número de associação). É o número da versão do MACsec se a confidencialidade ou a integridade forem usadas sozinhas.
- SL: Comprimento dos dados criptografados.
- PN: número do pacote usado para proteção de reprodução.
- SCI: Identificador de canal seguro. Cada associação de conectividade (CA) é uma porta virtual (endereço MAC da interface física mais ID de porta de 16 bits).
- ICV: Valor de Verificação de Integridade.

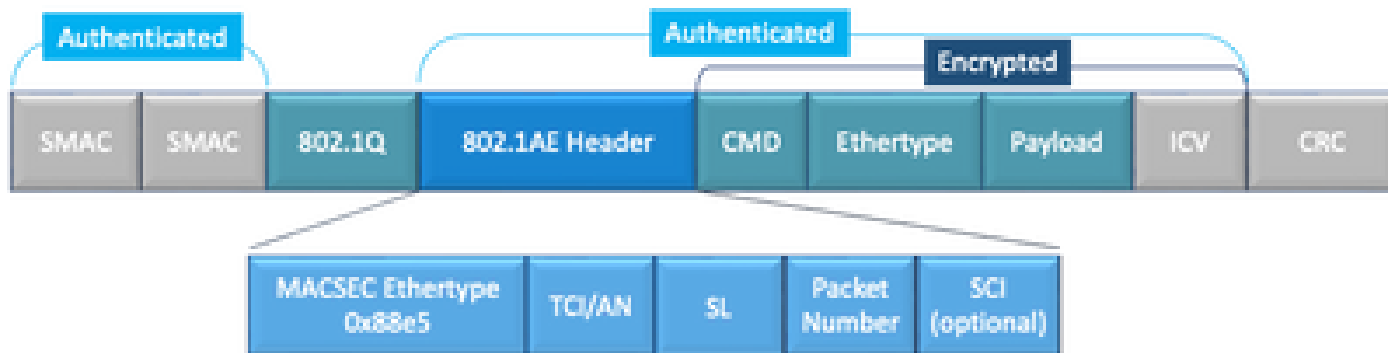
WAN-MACSEC

A Ethernet evoluiu além de um transporte LAN privado, para incluir uma variedade de opções de transporte WAN ou MAN. O WAN MACSEC fornece criptografia de ponta a ponta através do serviço WAN Ethernet de Camada 2, ponto a ponto ou ponto a multiponto, usando AES de 128 ou 256 bits.

O WAN MACsec é baseado no (LAN) MACsec, daí o nome (e separado do IPsec), mas oferece vários recursos adicionais não disponíveis anteriormente.

Formato de pacote MACSEC da WAN

É possível que o provedor de serviços não suporte o tipo Ethernet MACsec e não possa diferenciar o serviço L2 se a marca for criptografada para que o WAN MACSEC criptografe todos os quadros após os cabeçalhos 802.1Q:



Exemplo de Tag WAN MACSEC 802.1Q no formato de pacote limpo

Um dos novos aprimoramentos inclui tags 802.1Q no Clear (também conhecidas como ClearTag). Esse aprimoramento permite a capacidade de expor a marca 802.1Q fora do cabeçalho MACsec criptografado. A exposição desse campo fornece várias opções de design com o MACsec e, em para provedores de transporte públicos Carrier Ethernet, é necessário para aproveitar determinados serviços de transporte.

O suporte ao recurso MKA fornece informações de tunelamento, como a marca de VLAN (marca 802.1Q), de forma que o provedor de serviços possa fornecer multiplexação de serviço, de modo que vários serviços ponto a ponto ou multiponto possam coexistir em uma única interface física e diferenciados com base no ID de VLAN agora visível.

Além da multiplexação de serviços, a marca VLAN no espaço livre também permite que os provedores de serviços forneçam qualidade de serviço (QoS) para o pacote Ethernet criptografado através da rede SP com base no campo 802.1P (CoS) que agora é visível como parte da marca 802.1Q.

Terminologia MACSEC de WAN

MKA	Acordo-chave MACSec, definido no IEEE 802.1XREV-2010 - Protocolo de acordo-chave para descobrir pares MACSec e chaves de negociação.
MSK	Chave de Sessão Mestre, gerada durante a troca de EAP. O solicitante e o servidor de autenticação usam o MSK para gerar o CAK
CAK	A chave de associação de conectividade é derivada do MSK. É uma chave mestra de longa duração usada para gerar todas as outras chaves usadas para MACSec.
CKN	Nome da chave de associação de conectividade - identifica o CAK.
SAK	Chave de Associação Segura - Deriva do CAK e é a chave usada pelo requerente e pelo switch para criptografar o tráfego de uma determinada sessão.
KS	Servidor de chaves responsável por: <ul style="list-style-type: none"> • Selecionando e anunciando um conjunto de cifras • Gerando o SAK do CAK.
KEK	Chave de criptografia de chave - usada para proteger chaves MACsec (SAK)

Protocolo de Acordo de Chave (MKA - Key Agreement Protocol) MACSEC e Visão Geral de Criptografia

O MKA é o mecanismo de plano de controle usado pelo MACsec da WAN; especificado no padrão IEEE 802.1X, que descobre pares MACsec mutuamente autenticados mais as próximas ações:

- Estabelece e gerencia uma CA (Associação de Conectividade).
- Gerencia a lista de colegas ao vivo/em potencial.
- Negociação do conjunto de cifras.
- Escolhe o KS (Key Server, servidor de chaves) entre os membros de uma CA.
- Derivação e gerenciamento de Chave de Associação Segura (SAK).
- Distribuição segura de chaves.
- Instalação de chave.
- Rechavear.

Um membro é eleito como o servidor de chaves com base na prioridade do servidor de chaves configurado (mais baixa), se a prioridade KS for a mesma entre os pares, o SCI mais baixo ganha.

O KS gera um SAK somente depois que todos os pares em potencial se tornarem ativos e houver, pelo menos, um par ativo. Ele distribui o SAK e a cifra usada para outros participantes que usam o MKA PDU ou o MKPDU em um formato criptografado.

Os participantes verificam a cifra enviada pelo SAK e a instalam se for suportada, usando-a em cada MKPDU para indicar a chave mais recente que possuem; caso contrário, eles rejeitarão o SAK

Quando nenhum MKPDU é recebido de um participante após 3 pulsações (cada pulsação é de 2 segundos por padrão), os peers são excluídos da lista de peers ativos; por exemplo, se um cliente se desconectar, o participante no switch continuará a operar o MKA até que 3 pulsações tenham decorrido após o último MKPDU ser recebido do cliente.

Para esse processo, há dois métodos para acionar chaves de criptografia:

- Chaves pré-compartilhadas
- 802.1x/EAP

Chaves pré-compartilhadas

Se você usar chaves pré-compartilhadas, CAK=PSK e CKN deverão ser inseridos manualmente. Para o tempo de vida da chave, certifique-se de que você tenha uma substituição de chave e sobreposição durante o tempo de nova chave para:

- Troque e instale uma nova chave SAK e vincule-a à SA ociosa.
- Remova a chave SAK antiga e aloque uma nova SA ociosa.

Exemplo de configuração:

```
<#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
```

Onde negrito se refere a:

M_Key: nome da cadeia de chaves.

key 01: Nome da chave de associação de conectividade (o mesmo que CKN).


aes-128-cmac: MKA Authentication Cipher (Cifra de autenticação MKA).

12345678901234567890123456789012: Chave de Associação de Conectividade (CAK).

Definir política:


```
<#root>
mka policy example
  macsec-cipher-suite
gcm-aes-256
```

Where **gcm-aes-256** refere-se a conjuntos de cifras para derivação de chave de associação segura (SAK).

 Observação: esta é uma configuração de política básica, mais opções como `confidencialeoffset`, `sak-rekey`, `include-icv-indicator` e mais estão disponíveis para uso depende da implementação.


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
```

 Observação: se nenhuma política `mka` for configurada ou aplicada, a política padrão será ativada e poderá ser revisada por meio de `show mka default-policy detail`.

802.1x/EAP

Se você usar o método EAP, todas as chaves serão geradas a partir da MSK (Master Session Key). Com a estrutura IEEE 802.1X Extensible Authentication Protocol (EAP), o MKA troca quadros EAPoL-MKA entre dispositivos, o tipo Ether de quadros EAPoL é 0x888E, enquanto o corpo do pacote em uma unidade de dados do protocolo EAPoL (PDU) é chamado de MACsec Key Agreement PDU (MKPDU). Esses quadros EAPoL contêm o CKN do remetente, a prioridade principal do servidor e os recursos MACsec.

 Observação: por padrão, os switches processam quadros EAPoL-MKA, mas não os encaminham.

Exemplo de configuração da Criptografia MACsec com base em certificado:

Registrando o certificado (requer autoridade de certificação):

```
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
```

Autenticação 802.1x e configuração AAA necessárias:

```
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
```

Perfil EAP-TLS e credenciais 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
```

Solucionar problemas do MACSEC da WAN

Configuração

Verifique o suporte apropriado de configuração e implementação, dependendo da plataforma; as chaves e os parâmetros devem ser correspondentes. Alguns dos registros comuns para identificar se há um problema na configuração são os seguintes:

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

Verifique a capacidade MACsec do hardware dos peers ou reduza os requisitos para a capacidade MACsec alterando a configuração MACsec da interface.

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

Há alguns parâmetros opcionais que o roteador pode esperar ou não com base na configuração e em diferentes configurações padrão da plataforma. Certifique-se de incluir ou descartar na configuração.

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

Há uma incompatibilidade de configuração no conjunto de cifras de política. Verifique se a configuração está correta.

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

MKPDU falhou em uma ou mais das próximas verificações de validação:

- Endereço MAC válido e cabeçalho EAPOL: verifique a configuração de ambas as interfaces, a captura de pacotes na interface de entrada pode corroborar os valores atuais.
- CKN e agilidade de algoritmo válidos: verifique se as chaves e conjuntos de algoritmos são válidos.
- Verificação de ICV: a verificação de ICV é um parâmetro opcional; a configuração de ambas as extremidades deve corresponder.
- Correção da existência de payloads MKA: Possível problema de interoperabilidade.
- Verificação do IA se existirem pares: verificação do identificador do membro, única para cada participante.
- Verificação de MN se os pares existirem: Verificação do número da mensagem, exclusiva em cada MKPDU transmitida e incrementa em cada transmissão.

Problemas operacionais

Uma vez definida a configuração, você pode ver a mensagem %MKA-5-SESSION_START, mas precisa verificar se a sessão é ativada, um bom comando para começar é 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

Status se refere à sessão do plano de controle; Secured significa que Rx e Tx SAK estão instalados; caso contrário, ele aparece como Not Secured.

- Se o status permanecer em Init, verifique o estado da interface física, a conectividade via ping para os pares e a correspondência de configuração. Neste ponto, não há nenhum MKPDU recebido e correspondentes ativos, algumas plataformas preenchem enquanto outras não; considere até 32 bytes de sobrecarga de cabeçalho e garanta um MTU maior para a operação apropriada.
- Se o status permanecer em Pendente, verifique se a MKPDU é descartada em erros/quedas de ingresso ou saída no plano de controle ou de interfaces.
- Se o status permanecer em Não protegido, a interface MKA está ativa e os MKPDUs estão fluindo, mas o SAK não está instalado, nesse caso o próximo log é visto:

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

Isso ocorre porque não há suporte a MACsec, configuração MACsec inválida ou outra falha de MKA no lado local ou de peer antes do estabelecimento de um Secure Channel (SC) e da instalação de Associações Seguras (SA) no MACsec. Você pode usar o comando detail para obter mais informações 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
-----	-----	-----	-----	-----	-----

Procure por informações de SAK sobre pares e dados relevantes destacados para entender melhor a situação, se diferentes SAK estão em vigor, examine a chave usada e o tempo de vida ou as opções de rechaveamento de SAK configuradas, se as chaves pré-compartilhadas forem usadas, você pode usar show mka keychain:

```
<#root>
```

```
Router1#
```

```
show mka keychains
```

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

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

```
=====
```

```
Master_Key
```

```
01
```

```
<HIDDEN>
```

```
Te0/1/2
```

O CAK nunca é exibido, mas você pode confirmar o nome do conjunto de chaves e o CKN.

Se a sessão foi estabelecida, mas você tem oscilações ou fluxo de tráfego intermitente, você deve verificar se os MKPDUs estão fluindo corretamente entre os peers; se houver um tempo limite, você pode ver a próxima mensagem:

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

Se houver um correspondente, a sessão MKA será encerrada, caso você tenha vários correspondentes e o MKA não tenha recebido um MKPDU de um de seus correspondentes por mais de 6 segundos, o correspondente ao vivo será removido da lista de correspondentes ao vivo, você pode começar com `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
```


Os MKPDUs transmitidos e recebidos devem ter números semelhantes para um peer, certifique-se de que eles aumentem em Rx e Tx em ambas as extremidades, para determinar ou guiar a direção problemática, se houver diferenças você pode habilitar `debug mka linksec-interface frames` ambas as extremidades:

```
*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
```

Caso não haja MKPDU recebido, procure erros ou quedas de interface de entrada, status das interfaces de peers e sessão mka; caso você tenha ambos os roteadores enviando mas não recebendo, os MKPDUs são perdidos na mídia e precisam verificar os dispositivos intermediários para o encaminhamento correto.

Se você não estiver enviando MKPDUs, verifique o estado da interface física (linha e erros/quedas) e a configuração; examine se você está gerando esses pacotes no nível do plano de controle, o rastreamento FIA e o Embedded Packet Capture (EPC) são ferramentas confiáveis para essa finalidade. Consulte [Solução de problemas com o recurso de rastreamento de pacote de caminho de dados do Cisco IOS XE](#)

Você pode usar debug mka events e procurar por motivos que possam orientar as próximas etapas.

 Observação: use com cuidado debug mka e debug mka diagnostics pois mostram a máquina de estado e informações muito detalhadas que podem causar problemas no plano de controle no roteador.

Se a sessão estiver protegida e estável, mas o tráfego não estiver fluindo, verifique se há tráfego criptografado enviando os dois pares:

```
<#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
```

Os Contadores de SecY são pacotes atuais na interface física, enquanto os outros estão relacionados ao Canal de Segurança Tx significa que os pacotes estão sendo criptografados e transmitidos e a Associação de Segurança Rx significa que os pacotes válidos foram recebidos na interface.

Mais depurações, como debug mka errors e debug mka packets ajudam na identificação de problemas. Use esta última com precaução, pois pode induzir um registro pesado.

Informações Relacionadas

- [Guia de configuração MACsec e MKA](#)
- [Suporte técnico e downloads da Cisco](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.