

# O tráfego MACSec XPN falha entre o Catalyst 9500 e o Nexus 9000 com o aumento de pacotes inválidos e erros de FCS

## Contents

---

## Problema

Quando o MACSec XPN é habilitado entre um Catalyst 9500-28C8D e um Nexus N9K-C93180YC-FX, a sessão MKA é estabelecida com êxito, mas nenhum tráfego de dados passa pelo link. O Catalyst 9500 relata o aumento de "pacotes inválidos" em estatísticas de SA e erros de entrada de FCS na interface física. Especificamente, estes sintomas foram observados:

- Sem conectividade após MACSec ser habilitado
- A sessão MKA mostra como estabelecida, mas o lado do Catalyst 9500 mostra as estatísticas SA com "pacotes não válidos 118" aumentando e "pacotes válidos: 0"
- Os erros de entrada de FCS são incrementados na interface física do Catalyst 9500
- A remoção da configuração MACSec restaura imediatamente a conectividade e interrompe os erros de FCS

As sessões MKA foram estabelecidas em ambos os dispositivos e negociaram com sucesso a cifra GCM-AES-XPN-256. O lado do Nexus mostrou a criptografia como ativa, mas o Catalyst 9500 recebeu pacotes criptografados e os rejeitou devido à incompatibilidade de validação, resultando em nenhum pacote válido sendo aceito.

## Ambiente

- Catalyst 9500-28C8D executando o Cisco IOS®
- Nexus N9K-C93180YC-FX
- Configuração MACSec XPN usando o conjunto de cifras GCM-AES-XPN-256

- Interface 400 Gigabit Ethernet (FourHundredGigE1/0/15 no Catalyst, Ethernet1/52 no Nexus)
- Catalyst 9500 configurado como prioridade de servidor de chave 1, Nexus configurado como prioridade de servidor de chave 100
- Algoritmo criptográfico AES-256-CMAC para chaves pré-compartilhadas

## Resolução

O problema foi resolvido com a implementação de uma solução alternativa que altera a atribuição da função de servidor-chave entre os dispositivos. A resolução recomendada envolve estas etapas:

### Passo 1: Identificar o problema de configuração do servidor de chaves

Verifique a configuração atual da prioridade do servidor de chaves em ambos os dispositivos. A configuração problemática mostrou:

Configuração do Catalyst 9500:

```
mka policy MEHEALTH-ORG-XPN
  key-server priority 1
  macsec-cipher-suite gcm-aes-xpn-256
```

Configuração do Nexus:

```
macsec policy MEHEALTH-ORG-XPN
  key-server-priority 100
```

### Passo 2: Implementar Solução Alternativa para Função de Servidor-Chave

Configure o dispositivo Nexus como o servidor de chaves MACSec em vez do Catalyst 9500. Isso envolve o ajuste dos valores de prioridade do servidor de chaves para que o Nexus assuma a função do servidor de chaves.

Modifique a configuração do Nexus para ter um valor de prioridade de servidor de chave mais baixo (valores mais baixos têm prioridade mais alta):

```
macsec policy MEHEALTH-ORG-XPN
  key-server-priority 1
```

Modifique a configuração do Catalyst 9500 para ter um valor de prioridade de servidor de chave mais alto:

```
mka policy MEHEALTH-ORG-XPN
  key-server priority 100
  macsec-cipher-suite gcm-aes-xpn-256
```

### Passo 3: Verificar operação MACSec

Após implementar a alteração da função de servidor de chaves, verifique se:

- As sessões MKA são estabelecidas com êxito em ambos os dispositivos
- O tráfego de dados passa pelo link habilitado para MACSec
- Nenhum "pacote inválido" está aumentando nas estatísticas do Catalyst 9500 SA
- Os erros de entrada de FCS não estão ocorrendo na interface física

Essa solução alternativa permite que a configuração do MACSec XPN funcione corretamente até que a investigação da plataforma e o planejamento de atualização de software possam ser concluídos.

## Causa

A causa raiz desse problema está relacionada ao bug da Cisco ID CSCvs00410, que descreve um cenário em que as sessões do MKA são estabelecidas com êxito, mas os dados não podem passar pelo link ao usar AES-256-XPB com um Catalyst 9500 na função de servidor-chave sob certas condições de interoperabilidade com dispositivos Nexus. O comportamento se manifesta como uma incompatibilidade de validação onde o Catalyst 9500 rejeita pacotes criptografados do Nexus, resultando no aumento de contagens de pacotes inválidos e erros de FCS. Houve uma discrepância observada em relação ao Cisco IOS estar listado como corrigido para este defeito, exigindo investigação adicional pela equipe da plataforma Catalyst.

## Conteúdo relacionado

- ID de bug Cisco CSCvs00410 - sessão MKA ativada, mas incapaz de passar dados pelo link ao usar AES-256-XPB com a função de servidor-chave do Catalyst 9500

### 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.