

Captura de pacote de informação encaixada para o Cisco IOS e o exemplo de configuração IOS-XE

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Exemplo da configuração do IOS da Cisco](#)

[Configuração básica do EPC](#)

[Exemplo de configuração do Cisco IOS XE](#)

[Configuração básica do EPC](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve a característica encaixada da captura de pacote de informação (EPC) no software do [®] do Cisco IOS.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

[Componentes Utilizados](#)

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco IOS Release 12.4(20)T ou Mais Recente
- Liberação 15.2(4)S do Cisco IOS XE - 3.7.0 ou mais atrasado

A informação neste documento foi criada dos dispositivos em um ambiente de laboratório. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

Quando permitido, o roteador captura os pacotes enviados e recebidos. Os pacotes são armazenados dentro de um buffer no DRAM e não são assim persistentes através de um reload. Uma vez que os dados são capturados, podem ser examinados em um sumário ou em uma vista detalhada no roteador. Além, os dados podem ser exportados como um arquivo da captura de pacote de informação (PCAP) para permitir um exame mais adicional. A ferramenta é configurada no modo exec e considerada uma ferramenta provisória do auxílio. Em consequência, a configuração da ferramenta não é armazenada dentro da configuração de roteador e não permanecerá no lugar após um recarregamento do sistema.

A ferramenta do [gerador e do analisador da configuração da captura de pacote de informação](#) está disponível para que os clientes Cisco ajudem na configuração, na captação, e na extração das capturas de pacote de informação.

Exemplo da configuração do IOS da Cisco

Configuração básica do EPC

1. Defina da “um buffer captação”, que seja um buffer provisório que os pacotes capturados estão armazenados dentro. Há as várias opções que podem ser selecionadas quando o buffer é definido; como o tamanho, o tamanho do pacote do maxium, e o circular/o Linear:

```
monitor capture buffer BUF size 2048 max-size 1518 linear
```

2. Um filtro pode igualmente ser aplicado para limitar a captação ao tráfego desejado. Defina um Access Control List (ACL) dentro do modo de configuração e aplique o filtro ao buffer:

```
ip access-list extended BUF-FILTER
permit ip host 192.168.1.1 host 172.16.1.1
permit ip host 172.16.1.1 host 192.168.1.1
monitor capture buffer BUF filter access-list
BUF-FILTER
```

3. Defina da “um ponto captação”, que defina o lugar onde a captação ocorre. O ponto da captação igualmente define se a captação ocorre para o IPv4 ou o IPv6 e em que trajeto de switching (processo contra o cef):

```
monitor capture point ip cef POINT fastEthernet 0 both
```

4. Anexe o buffer ao ponto da captação:

```
monitor capture point associate POINT BUF
```

5. Comece a captação:

```
monitor capture point start POINT
```

6. A captação é agora ativa. Permita a coleção dos dados necessários.

7. Pare a captação:

```
monitor capture point stop POINT
```

8. Examine o buffer na unidade:

```
show monitor capture buffer BUF dump
```

Nota: Esta saída mostra somente a cópia parcial da memória de HEX das capturas dos pacotes. A fim ver em compreensível para o utilizador lá são duas maneiras. Exporte o buffer do roteador para a análise mais aprofundada:

```
monitor capture buffer BUF export tftp://10.1.1.1/BUF.pcap
```

Dica: A requisição de aprimoramento [CSCuw77601](#) foi arquivada a fim adicionar a opção de exportação assim que você pode enviar por correio eletrônico o buffer diretamente a uma email-identificação. Contudo o método anterior não é sempre prático como ele exigiu o acesso T/FTP ao roteador. Em tais situações, você pode tomar uma cópia da cópia parcial da memória de HEX e para usar todo o em linha encantar-pcap o conversor a fim ver os arquivos.

9. Uma vez que os dados necessários foram recolhidos, suprima da “do ponto captação” e “capture o buffer”:

```
no monitor capture point ip cef POINT fastEthernet 0 both  
no monitor capture buffer BUF
```

Notas:

- Nas liberações mais cedo do que o Cisco IOS Release 15.0(1)M, o tamanho de buffer foi limitado a 512K.
- Nas liberações mais cedo do que o Cisco IOS Release 15.0(1)M, o tamanho do pacote capturado foi limitado a 1024 bytes.
- O buffers de pacotes é armazenado no DRAM e não persistirá através dos reloads.
- A configuração da captação não é armazenada no NVRAM e não persistirá através dos reloads.
- O ponto da captação pode ser definido para capturar no cef ou nos caminhos de switching do processo.
- O ponto da captação pode ser definido para capturar somente em uma relação ou globalmente.
- Quando o buffer da captação é exportado no formato PCAP, a informação L2 (tal como a encapsulation do Ethernet) não está preservada.
- [See Best pratica procurando comandos](#) a fim obter mais informação nos comandos usados nesta seção.

Exemplo de configuração do Cisco IOS XE

A característica encaixada da captura de pacote de informação foi introduzida na liberação 3.7 do Cisco IOS XE - 15.2(4)S. A configuração da captação é diferente do que o Cisco IOS porque adiciona mais características.

Configuração básica do EPC

1. Defina o lugar onde a captação ocorrerá:

```
monitor capture CAP interface GigabitEthernet0/0/1 both
```

2. Associe um filtro. O filtro pode ser especificado inline, ou um ACL ou o mapa de classe podem ser providos:

```
monitor capture CAP match ipv4 protocol tcp any any
```

3. Comece a captação:

```
monitor capture CAP start
```

4. A captação é agora ativa. Permita que recolha os dados necessários.

5. Pare a captura:

```
monitor capture CAP stop
```

6. Examine a captura em uma vista sumária:

```
show monitor capture CAP buffer brief
```

7. Examine a captura em uma vista detalhada:

```
show monitor capture CAP buffer detailed
```

8. Além, exporte a captura no formato PCAP para a análise mais aprofundada:

```
monitor capture CAP export ftp://10.0.0.1/CAP.pcap
```

9. Uma vez que os dados necessários foram recolhidos, remova a captura:

```
no monitor capture CAP
```

Notas:

- A captura pode ser executada em interfaces física, em subinterfaces, e em interfaces de túnel.
- O Network Based Application Recognition (NBAR) baseou filtros, esse uso o **comando match protocol** sob o mapa de classe, não é apoiado atualmente.
- Veja [melhores prática procurando comandos](#) a fim obter mais informação nos comandos usados nesta seção.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Para o EPC que é executado no Cisco IOS XE, este comando debug pode ser usado para assegurar-se de que o EPC se estabeleça corretamente:

```
no monitor capture CAP
```

Informações Relacionadas

- [Captura de pacote de informação encaixada - Cisco IOS XE](#)
- [Captura de pacote de informação encaixada - Cisco IOS](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)