# Configurar a captura de pacote vManage/vSmart/vEdge TCPDUMP no modo CLI

## Contents



## Introdução

Este documento descreve como configurar a captura de pacote vManage/vSmart/vEdge TCPDUMP no modo CLI.

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Rede de longa distância definida por software da Cisco (SD-WAN)

### Componentes Utilizados

As informações neste documento são baseadas no Cisco vManage versão 20.9.4

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos usados neste documento começaram com a configuração limpa (padrão). Se sua rede estiver ativa, certifique-se de que você compreende o impacto potencial de qualquer comando.

## Informações de Apoio

Na arquitetura Cisco SD-WAN, vManage, vSmart e vEdge, respectivamente, desempenham as funções principais de gerenciamento, controle e encaminhamento de dados. Para garantir a estabilidade e a segurança da rede e para solucionar problemas de falhas de rede, os engenheiros de rede frequentemente precisam realizar captura e análise de pacotes no tráfego que flui por esses dispositivos. O TCPDUMP é uma ferramenta de linha de comando leve e poderosa que pode ser usada para capturar e analisar pacotes de dados que passam pelas interfaces.

Ao configurar e usar o TCPDUMP no modo CLI, os usuários podem capturar diretamente o tráfego em tempo real no dispositivo sem a necessidade de ferramentas adicionais ou dispositivos proxy intermediários. Isso é de grande importância para a localização de problemas como anomalias de roteamento, falhas de conexão de controle, perda de pacotes e verificação de caminhos de tráfego. Como os dispositivos Cisco SD-WAN (como o vEdge) executam sistemas operacionais personalizados (como o Viptela OS), o uso do TCPDUMP pode diferir ligeiramente do uso em ambientes Linux tradicionais em alguns aspectos. Portanto, compreender sua estrutura básica de comandos e suas limitações de uso é particularmente crucial.

Esta seção explica como configurar e executar o TCPDUMP no modo CLI dos dispositivos vManage, vSmart e vEdge, a fim de ajudar os usuários na realização de análise de tráfego de rede eficaz e diagnóstico de problemas.

# Explicação dos pontos principais do TCPDUMP(Controladores)

```
tcpdump [vpn x | interface x | vpn x interface x] options " "
Usage: tcpdump [-AbdDefhHIJKlLnNOpqStuUv] [ -B size ] [ -c count ]
               [ -E algo:secret ] [ -j tstamptype ] [ -M secret ]
               [ -T type ] [ -y datalinktype ] [ expression ]
```

- Especifique uma interface (não é possível obter saída especificando somente vpn)
- Coloque as opções entre aspas ( "" ), use ctrl c para parar
- Use -n para impedir a conversão de ip em nome de host e -nn para impedir nome e porta ?
- -v mostra mais detalhes (informações de cabeçalho IP, tos, ttl, offset, flags, protocol)
- -vv e -vvv mostram mais detalhes em certos tipos de pacotes
- Proto ex - udp, tcp icmp pim igmp vrrp esp arp
- Negar! ou não, && ou and, | | ou ou, use com ( ) não (udp ou icmp)

# TCPDUMP (continuação)

- Adaptado do comando tcpdump do linux, mas não suporta todas as opções disponíveis. Os instantâneos de pacotes salvos em um buffer não podem ser exportados para um PCAP.
- É executado com a flag -p, que significa "modo não promíscuo" - o controlador captura apenas pacotes destinados à interface do controlador, incluindo pacotes de controle ou pacotes de broadcast. Não é possível capturar o tráfego do plano de dados.

- Executado com -s 128, tamanho do instantâneo em Bytes. Os primeiros x bytes do pacote são capturados.

# Usar o comando TCPDUMP

Esta seção fornece exemplos que ilustram a forma como o comando tetcpdumpé usado.

```
vmanage# tcpdump ?
Possible completions:
interface  Interface on which tcpdump listens
vpn        VPN ID
```

A saída do comando show interface description fornece informações precisas sobre o nome e o número da vpn/interface que está em uso no momento.

```
vmanage# tcpdump vpn 0 interface eth0 ?
Possible completions:
help       tcpdump help
options    tcpdump options or expression
|          Output modifiers
<cr>
```

Você pode adicionar mais condições para filtragem de captura de pacotes por meio da palavra-chave "options".

```
vmanage# tcpdump vpn 0 interface eth0 help

Tcpdump options:
help              Show usage
vpn               VPN or namespace
interface         Interface name
options           Tcpdump options like -v, -vvv, t,-A etc or expressions like port 25 and not host 10.0

e.g., tcpdump vpn 1 interface ge0/4 options "icmp or udp"

Usage: tcpdump [-AbdDefhHIJKlLnNOpqStuUv] [ -B size ] [ -c count ] [ -E algo:secret ] [ -j tstamptype ]
               [ -T type ] [ -y datalinktype ] [ expression ]
```

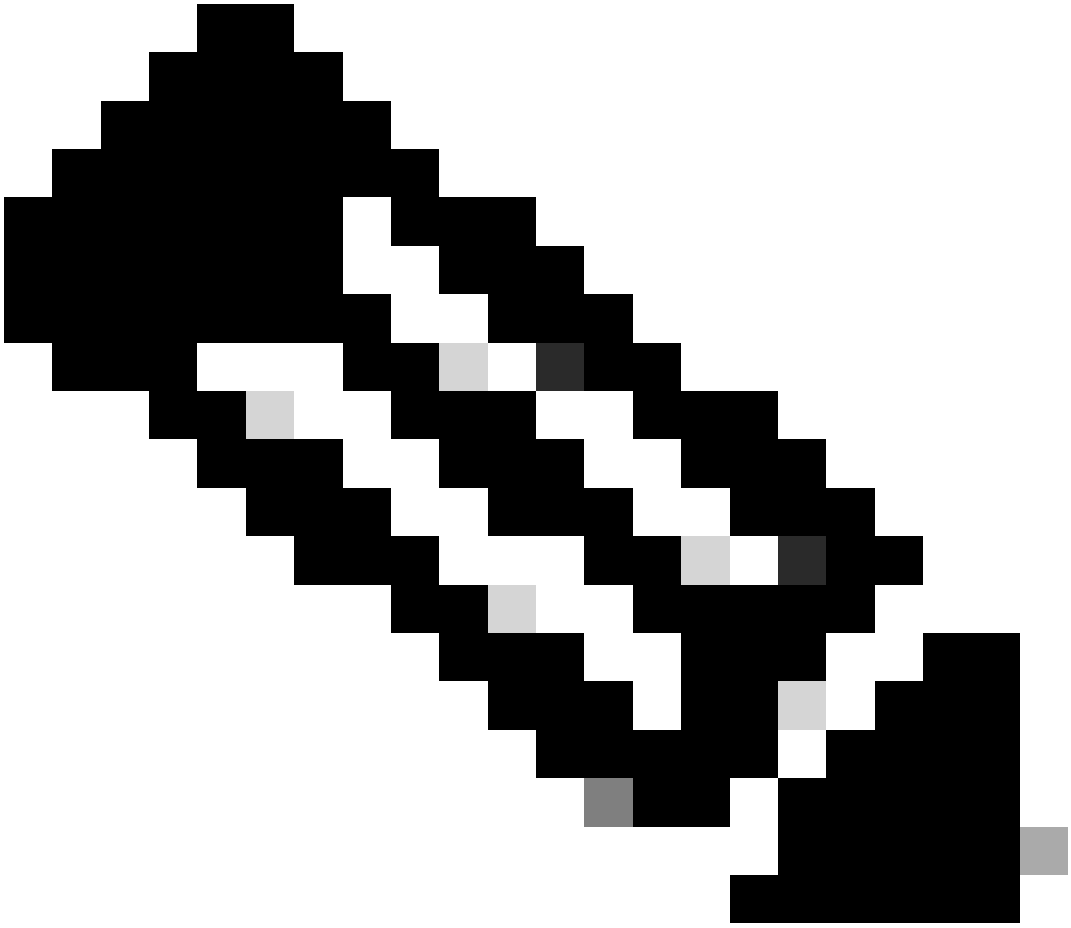
Você pode indicar a contagem do pacote específico pelo comando "-c count" das opções. Se você não indicar uma contagem de pacotes específica, uma captura contínua será executada sem limite.

```
vmanage# tcpdump vpn 0 interface eth0 options "-c 10 "
tcpdump -p -i eth0 -s 128 -c 10 in VPN 0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
```

```
listening on eth0, link-type EN10MB (Ethernet), capture size 128 bytes
04:56:55.797308 IP 50.128.76.22.12746 > softbank219168102002.bbtec.net.12366: UDP, length 237
04:56:55.797371 IP 50.128.76.22.12746 > softbank219168102002.bbtec.net.12366: UDP, length 205
04:56:55.797554 IP 50.128.76.22.12746 > softbank219168102002.bbtec.net.12366: UDP, length 173
04:56:55.797580 IP 50.128.76.22.12746 > softbank219168102002.bbtec.net.12366: UDP, length 173
04:56:55.808036 IP 50.128.76.22.12746 > softbank219168102002.bbtec.net.12366: UDP, length 173
04:56:55.917567 ARP, Request who-has 50.128.76.31 (Broadcast) tell 50.128.76.1, length 46
04:56:55.979071 IP 50.128.76.22.12346 > 50.128.76.25.12346: UDP, length 182
04:56:55.979621 IP 50.128.76.25.12346 > 50.128.76.22.12346: UDP, length 146
04:56:56.014054 IP 50.128.76.22.12746 > softbank219168102002.bbtec.net.12366: UDP, length 237
04:56:56.135636 IP 50.128.76.32.12426 > 50.128.76.22.12546: UDP, length 140
10 packets captured
1296 packets received by filter
0 packets dropped by kernel
```

Você também pode adicionar condições de filtro sobre o endereço de host e o tipo de protocolo nas opções.

```
vmanage# tcpdump vpn 0 interface eth0 options "-n host 50.128.76.27 and icmp"
tcpdump -p -i eth0 -s 128 -n host 50.128.76.27 and icmp in VPN 0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 128 bytes
05:21:31.855189 IP 50.128.76.27 > 50.128.76.22: ICMP echo reply, id 34351, seq 29515, length 28
05:21:34.832871 IP 50.128.76.22 > 50.128.76.27: ICMP echo request, id 44520, seq 29516, length 28
05:21:34.859655 IP 50.128.76.27 > 50.128.76.22: ICMP echo reply, id 44520, seq 29516, length 28
05:21:37.837244 IP 50.128.76.22 > 50.128.76.27: ICMP echo request, id 39089, seq 29517, length 28
05:21:37.866201 IP 50.128.76.27 > 50.128.76.22: ICMP echo reply, id 39089, seq 29517, length 28
05:21:40.842214 IP 50.128.76.22 > 50.128.76.27: ICMP echo request, id 24601, seq 29518, length 28
05:21:40.870203 IP 50.128.76.27 > 50.128.76.22: ICMP echo reply, id 24601, seq 29518, length 28
05:21:43.847548 IP 50.128.76.22 > 50.128.76.27: ICMP echo request, id 42968, seq 29519, length 28
05:21:43.873016 IP 50.128.76.27 > 50.128.76.22: ICMP echo reply, id 42968, seq 29519, length 28
05:21:46.852305 IP 50.128.76.22 > 50.128.76.27: ICMP echo request, id 23619, seq 29520, length 28
05:21:46.880557 IP 50.128.76.27 > 50.128.76.22: ICMP echo reply, id 23619, seq 29520, length 28
^C                                                                                <<<< Ctrl + c can inter
11 packets captured
11 packets received by filter
0 packets dropped by kernel
```

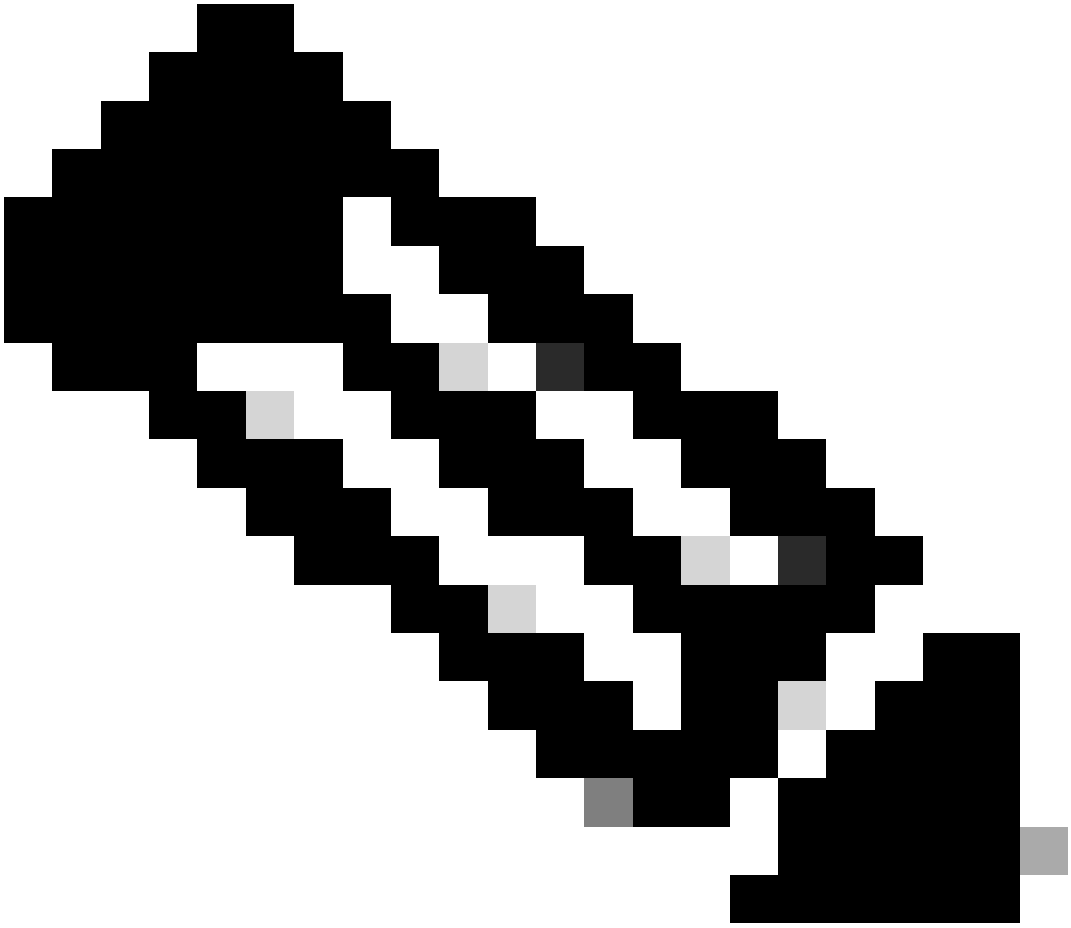


Note: No software Cisco IOS XE SD-WAN, você pode usar EPC (Embedded Packet Capture) em vez de TCPDUMP.

## Exemplos de TCPDUMP

Ouvindo pacote UDP geral:

tcpdump vpn 0 options "-vv -nnn udp"



Note: Isso também pode ser aplicado a outros protocolos... por exemplo: icmp, arp, etc.

---

Escutando uma porta específica com ICMP e UDP:
tcpdump vpn 0 interface ge0/4 options "icmp or udp"

Escutando em um número de porta específico (Escutando na porta TLS):
tcpdump vpn 0 interface ge0/4 options "-vvv -nn port 23456"

Escutando em um número de porta específico (Escutando na porta DTLS):
tcpdump vpn 0 interface ge0/4 options "-vvv -nn port 12346"

Escutando um host específico (de/para esse host): -e imprime o cabeçalho no nível do link
tcpdump vpn 0 interface ge0/4 opções "host 64.100.103.2 -vvv -nn -e"

Escutando um host específico somente com ICMP

tcpdump vpn 0 interface ge0/4 options "host 64.100.103.2 && icmp"

Filtragem por origem e/ou destino
tcpdump vpn 0 interface ge0/4 options "src 64.100.103.2 && dst 64.100.100.75"

Filtrar tráfego encapsulado por GRE
tcpdump vpn 0 interface ge0/4 options "-v -n proto 47 "

## Documentos relacionados

- Solucionar problemas de conexões de controle SD-WAN
- SD-WAN da Cisco: Os Suspeitos Usuais
- PÁGINA DO MANUAL TCPDUMP

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.