

# Identificar e solucionar problemas de interrogação SNMP e detalhes de interface incorretos em SNA

## Contents

---

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurações](#)

[Informações de Apoio](#)

[Troubleshooting](#)

[Nomes de interface incorretos](#)

[Exportadores ou interfaces ausentes](#)

[Problemas de conectividade](#)

[Capacidade do Gerenciador de Validação \(SMC\) de sondar exportadores](#)

[Gere uma captura de pacote no SMC usando o endereço IP de um exportador.](#)

[Validar configurações de pesquisa SNMP](#)

[Solução de problemas ao vivo de pesquisa SNMP](#)

[Testando o SNMP Polling a partir de outro dispositivo](#)

[Informações Relacionadas](#)

---

## Introdução

Este documento descreve como solucionar problemas de informações da interface do exportador ausente no Secure Network Analytics

## Pré-requisitos

- A Cisco recomenda que você tenha o conhecimento de pesquisa básico do protocolo de gerenciamento de rede simples (SNMP).
- A Cisco recomenda que você tenha o conhecimento básico do Secure Network Analytics (SNA/StealthWatch)

## Requisitos

- SNA Manager na versão 7.4.1 ou mais recente
- SNA Flow Collector na versão 7.4.1 ou mais recente
- Exportador enviando ativamente o NetFlow para SNA

# Componentes Utilizados

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

- SNA Manager na versão 7.4.1 ou mais recente
- SNA Flow Collector na versão 7.4.1 ou mais recente
- software SNMPwalk
- software Wireshark

# Configurações

- Configuração do dispositivo: os exportadores precisam ser configurados para permitir o acesso SNMP. Isso envolve definir as configurações de SNMP em cada dispositivo, incluindo a configuração de séries de comunidade SNMP, listas de controle de acesso (ACLs) e a definição da versão de SNMP a ser usada
- Configuração de pesquisa SNMP em SNA: após a configuração bem-sucedida dos exportadores, a pesquisa SNMP é habilitada por padrão no SMC usando parâmetros predefinidos. É crucial fornecer os detalhes necessários relativos aos exportadores, como séries de comunidade SNMP e versões SNMP, para garantir que o mecanismo de pesquisa funcione da melhor forma possível

# Informações de Apoio

O SNA tem a capacidade de fornecer relatórios abrangentes de status de interface, juntamente com a capacidade de exibir nomes de interface para exportadores que estão transmitindo ativamente dados do NetFlow para um Flow Collector. Esse detalhe de interface pode ser visto navegando-se para o menu Investigar -> Interfaces a partir da interface de usuário do Manager Web.

Interface Status (Since Reset Hour)

INTERFACE	EXPORTER	CURRENT UTILIZATION	CURRENT TRAFFIC	MAXIMUM UTILIZATION	MAX TRAFFIC	DIRECTION	SPEED
▶ GigabitEthernet1 ...	...	0.01%	66.59 Kbps	0.18%	1.78 Mbps	INBOUND	1 Gbps
▶ GigabitEthernet1 ...	...	0%	27.96 Kbps	0.29%	2.9 Mbps	OUTBOUND	1 Gbps
▶ GigabitEthernet2 ...	...	4.31%	43.13 Mbps	12.22%	122.23 Mbps	INBOUND	1 Gbps
▶ GigabitEthernet2 ...	...	0%	30.51 Kbps	0.02%	154.43 Kbps	OUTBOUND	1 Gbps
▶ GigabitEthernet3 ...	...	0.01%	110.63 Kbps	0.29%	2.93 Mbps	INBOUND	1 Gbps
▶ GigabitEthernet3 ...	...	0.01%	56.49 Kbps	0.04%	396.24 Kbps	OUTBOUND	1 Gbps
▶ GigabitEthernet4 ...	...	0%	3.52 Kbps	0.06%	594.94 Kbps	INBOUND	1 Gbps
▶ GigabitEthernet4 ...	...	0.01%	70.79 Kbps	0.18%	1.8 Mbps	OUTBOUND	1 Gbps
▶ GigabitEthernet5 ...	...	0%	346 bps	0%	2.82 Kbps	INBOUND	1 Gbps

# Troubleshooting

Nomes de interface incorretos

Caso o relatório gerado exiba um "ifindex-#" que não corresponda às interfaces do seu exportador, ele sugere um possível problema de configuração com a pesquisa de SNMP no SMC ou no próprio exportador. Neste exemplo, eu destaquei um problema aparente com a interrogação SNMP de um determinado exportador.

Interfaces (152)

Filter by Device

Interface Status (Since Reset Hour)

INTERFACE	EXPORTER	CURRENT UTILIZATION	CURRENT TRAFFIC	MAXIMUM UTILIZATION	MAX TRAFFIC	DIRECTION	SPEED
ifindex-5 ...	192.168.99.2 ...	90.93%	909.27 Mbps	162.76%	1.63 Gbps	INBOUND	1 Gbps
ifindex-8 ...	192.168.99.2 ...	85.71%	857.08 Mbps	85.71%	857.08 Mbps	OUTBOUND	1 Gbps
ifindex-26 ...	192.168.99.2 ...	85.71%	857.08 Mbps	85.71%	857.08 Mbps	INBOUND	1 Gbps
ifindex-3 ...	192.168.99.2 ...	80.46%	804.6 Mbps	82.07%	820.69 Mbps	INBOUND	1 Gbps
ifindex-25 ...	192.168.99.2 ...	79.06%	790.63 Mbps	80.29%	802.94 Mbps	OUTBOUND	1 Gbps
ifindex-16 ...	192.168.99.2 ...	79.06%	790.63 Mbps	80.29%	802.94 Mbps	INBOUND	1 Gbps
ifindex-13 ...	192.168.99.2 ...	53.29%	532.87 Mbps	94.85%	948.5 Mbps	OUTBOUND	1 Gbps
ifindex-24 ...	192.168.99.2 ...	53.29%	532.87 Mbps	94.85%	948.5 Mbps	INBOUND	1 Gbps
ifindex-0 ...	192.168.99.2 ...	0.43%	4.29 Mbps	2.58%	25.84 Mbps	OUTBOUND	1 Gbps
TenGigabitEthernet1/0/38 ...	192.168.99.2 ...	0.32%	3.17 Mbps	0.98%	9.77 Mbps	INBOUND	1 Gbps
ifindex-0 ...	192.168.99.2 ...	0.13%	1.28 Mbps	0.37%	3.66 Mbps	OUTBOUND	1 Gbps
ifindex-0 ...	192.168.99.2 ...	0.12%	1.18 Mbps	2.77%	27.74 Mbps	OUTBOUND	1 Gbps
GigabitEthernet1/0/1 ...	192.168.99.4 ...	0.1%	1 Mbps	0.32%	3.19 Mbps	INBOUND	1 Gbps
ifindex-0 ...	192.168.99.2 ...	0.06%	573.21 Kbps	1.29%	12.92 Mbps	OUTBOUND	1 Gbps
TenGigabitEthernet1/0/1 ...	192.168.99.5 ...	0.05%	531.31 Kbps	0.29%	2.86 Mbps	INBOUND	1 Gbps
TenGigabitEthernet1/0/37 ...	192.168.99.1 ...	0.05%	503.01 Kbps	2.02%	20.15 Mbps	INBOUND	1 Gbps
TenGigabitEthernet1/0/1 ...	192.168.99.2 ...	0.04%	354.1 Kbps	1.25%	12.5 Mbps	INBOUND	1 Gbps

## Exportadores ou interfaces ausentes

A verificação de modelo tem importância significativa no contexto do processamento de dados do NetFlow. Especificamente, ele garante que o modelo do NetFlow recebido do exportador contenha todos os campos necessários para a decodificação e o processamento bem-sucedidos pelo Flow Collector. A falha em encontrar um modelo válido leva à exclusão do conjunto associado de fluxos da decodificação, resultando, portanto, em sua ausência da lista de interfaces.

Se você não vir o exportador/as interfaces esperados na lista de interfaces, verifique o modelo de dados do netflow de entrada. Para verificar o modelo do NetFlow, uma captura de pacote pode ser criada no lado do Flow Collector, especificando o IP do exportador do qual estamos obtendo o NetFlow alterando "x.x.x.x":

- Faça login no Flow Collector via SSH ou console com credenciais de raiz.
- Execute uma captura de pacote a partir do IP do exportador e da porta de netflow em questão:

```
tcpdump -s0 -v -nnn -i eth0 host x.x.x.x and port 2055 -w /lancope/var/admin/tmp/
```

- Copie a captura de pacotes do dispositivo para uma estação de trabalho com o aplicativo Wireshark instalado, use seu método preferido (por exemplo: SCP, SFTP).
- Abra a captura de pacotes com o Wireshark e verifique o modelo e os dados que o exportador está enviando ao coletor de fluxo

Date	Source	Destination	Protocol	Length	Info
19:35:07.222163	...	...	CFLOW	182	total: 3 (v9) records Obs-Domain-ID= 257 [Data-Template:2856] [Option...
19:35:07.222299	...	...	CFLOW	1416	total: 27 (v9) records Obs-Domain-ID= 257 [Data:2856]
19:35:07.222377	...	...	CFLOW	1416	total: 27 (v9) records Obs-Domain-ID= 257 [Data:2856]
19:35:07.222385	...	...	CFLOW	1416	total: 27 (v9) records Obs-Domain-ID= 257 [Data:2856]
19:35:07.222388	...	...	CFLOW	1416	total: 27 (v9) records Obs-Domain-ID= 257 [Data:2856]
19:35:07.222462	...	...	CFLOW	1416	total: 27 (v9) records Obs-Domain-ID= 257 [Data:2856]

```

Frame 1: 182 bytes on wire (1456 bits), 182 bytes captured (1456 bits)
  Ethernet II, Src: Cisco_94:b4:fc (8c:60:4f:94:b4:fc), Dst: VMware_84:49:4f (00:50:56:b4:49:4f)
  Internet Protocol Version 4, Src: ..., Dst: ...
  User Datagram Protocol, Src Port: 23384, Dst Port: 2055
  Cisco NetFlow/IPFIX
    Version: 9
    Count: 3
    SysUptime: 6981.205000000 seconds
    Timestamp: Jul 20, 2021 15:23:50.000000000 Eastern Daylight Time
    FlowSequence: 226153525
    SourceId: 257
    FlowSet 1 [id=0] (Data Template): 2856
      FlowSet Id: Data Template (v9) (0)
      FlowSet Length: 68
      Template (Id = 2856, Count = 15)
        Template Id: 2856
        Field Count: 15
        Field (1/15): BYTES
        Field (2/15): PKTS
        Field (3/15): OUTPUT_SNMP
        Field (4/15): IP_DST_ADDR
        Field (5/15): SRC_VLAN
        Field (6/15): IP_TOS
        Field (7/15): IPv4 ID
        Field (8/15): FRAGMENT_OFFSET
        Field (9/15): IP_SRC_ADDR
        Field (10/15): L4_DST_PORT
        Field (11/15): L4_SRC_PORT
        Field (12/15): PROTOCOL
        Field (13/15): FIRST_SWITCHED
  
```

Verifique se o modelo do NetFlow está usando os 9 campos obrigatórios, o nome exato desses campos de modelo pode variar dependendo do tipo de exportador. Portanto, consulte a documentação do tipo de exportador específico que você está configurando:

- Endereço IP origem
- Endereço IP de destino
- Porta de origem
- Porta de Destino
- Protocolo de Camada 4

- Contagem de bytes
- Contagem de pacotes
- Hora de início do fluxo
- Hora de término do fluxo


Para exibir as interfaces corretamente, adicione também:


- saída de interface
- entrada de interface

Aqui está um exemplo de captura de pacote de modelo de um determinado dispositivo exportador


- Setas vermelhas: campos obrigatórios do NetFlow
- Setas verdes: campos SNMP

```
> User Datagram Protocol, Src Port: 51431, Dst Port: 2055
v Cisco NetFlow/IPFIX
  Version: 10
  Length: 120
  > Timestamp: Jun 20, 2023 00:24:38.000000000 CST
  FlowSequence: 41662155
  Observation Domain Id: 256
  v Set 1 [id=2] (Data Template): 260
    FlowSet Id: Data Template (V10 [IPFIX]) (2)
    FlowSet Length: 104
    v Template (Id = 260, Count = 24)
      Template Id: 260
      Field Count: 24
      > Field (1/24): IPv4 ID
      > Field (2/24): IP_SRC_ADDR ←
      > Field (3/24): IP_DST_ADDR ←
      > Field (4/24): IP_TOS
      > Field (5/24): IP_DSCP
      > Field (6/24): PROTOCOL ←
      > Field (7/24): IP TTL MINIMUM
      > Field (8/24): IP TTL MAXIMUM
      > Field (9/24): L4_SRC_PORT ←
      > Field (10/24): L4_DST_PORT ←
      > Field (11/24): TCP_FLAGS
      > Field (12/24): SRC_AS
      > Field (13/24): IP_SRC_PREFIX
      > Field (14/24): SRC_MASK
      > Field (15/24): INPUT_SNMP ←
      > Field (16/24): DST_AS
      > Field (17/24): IP_NEXT_HOP
      > Field (18/24): DST_MASK
      > Field (19/24): OUTPUT_SNMP ←
      > Field (20/24): DIRECTION
      > Field (21/24): BYTES ←
      > Field (22/24): PKTS ←
      > Field (23/24): FIRST_SWITCHED ←
      > Field (24/24): LAST_SWITCHED ←
```

 Observação: a porta listada no comando de exemplo pode variar dependendo da configuração do seu exportador, o padrão é 2055

 Observação: mantenha a captura de pacotes em execução de 5 a 10 minutos, dependendo

---

 do exportador, o modelo pode ser enviado a cada N minutos e você precisa capturar esse modelo para que o NetFlow seja decodificado corretamente; se o modelo não for exibido, repita a captura de pacotes por um período de tempo maior

---

## Problemas de conectividade

Verificar a conectividade: Certifique-se de que haja conectividade entre o dispositivo do SNA Manager e os exportadores. Verifique se os exportadores podem ser alcançados no console de gerenciamento do Stealthwatch, fazendo ping em seus endereços IP. Se houver algum problema de conectividade de rede, solucione-o adequadamente.

## Capacidade do Gerenciador de Validação (SMC) de sondar exportadores

- Conecte-se ao gerenciador SNA via SSH e faça login com as credenciais raiz
- Analise o arquivo `/lancope/var/smc/log/smc-configuration.log` e procure os logs do tipo `ExporterSnmpSession`:

```
INFO [ExporterSnmpSession] SNMP polling for 10.1.0.253 took 0s
INFO [ExporterSnmpSession] SNMP polling for 10.1.0.253 took 0s
WARN [ExporterSnmpSession] SNMP polling for 10.10.0.254 failed: java.lang.Exception: timeout
INFO [ExporterSnmpSession] SNMP polling for 10.10.0.254 took 20s
WARN [ExporterSnmpSession] SNMP polling for 10.10.0.254 failed: java.lang.Exception: timeout
INFO [ExporterSnmpSession] SNMP polling for 10.10.0.254 took 20s
```

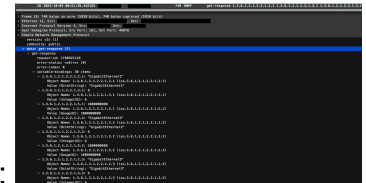
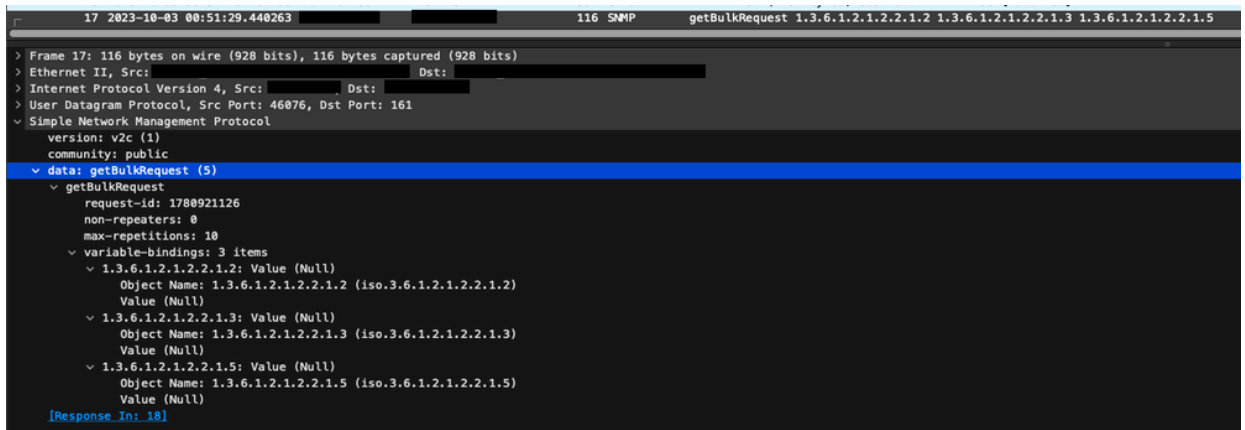
- Neste exemplo de pesquisa, não foram detectados erros para o exportador 10.1.0.253. No entanto, o exportador 10.1.0.254 recebeu inicialmente uma mensagem de erro de timeout, mas subsequentemente conseguiu executar com êxito a operação de polling após um atraso de 20 segundos.

Gere uma captura de pacote no SMC usando o endereço IP de um exportador.

- Faça login no nó Gerenciador através do SSH ou console com as credenciais raiz
- Executar:

```
tcpdump -s0 -v -nnn -i [Interface] host [Exporter_IP_address] -w /lancope/var/admin/tmp/[file_name]
```

- Exporte a captura de pacotes do equipamento com seu método preferido (Exemplo: SCP, SFTP)
- Abra a captura de pacotes com o Wireshark para ver as tentativas de pesquisa bem-sucedidas
  - Solicitação feita no SMC:



- Resposta SNMP do exportador com informações de interface:

## Validar configurações de pesquisa SNMP

Certifique-se de que os intervalos de polling sejam apropriados e que as métricas desejadas sejam incluídas nas consultas SNMP

- Na interface do usuário da Web, navegue para: Configure -> Exporters -> Exporter SNMP Profiles:
- Valide se a porta SNMP correta (geralmente a porta UDP 161) e o método de consulta SNMP correto foram selecionados, eles devem corresponder de acordo com seu exportador

(ifxTable Columns, CatOS MIB, PanOS MIB)



Observação: se você tiver interfaces de 10 Gbps, recomendamos que escolha a opção de colunas ifxTable para o método de consulta SNMP.

Observação: para obter o desempenho ideal do sistema, defina a pesquisa de SNMP para um intervalo de 12 horas. A sondagem mais frequente não torna suas métricas de utilização mais atualizadas e pode fazer com que seu sistema seja executado mais lentamente.

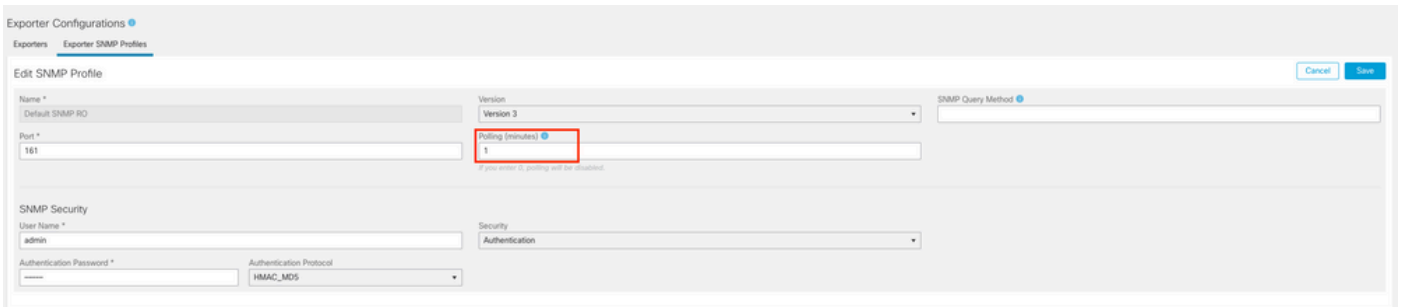
- Valide se as versões do SNMP configuradas no SNA e nos exportadores são compatíveis. SNA suporta SNMPv1, SNMPv2c e SNMPv3. Verifique se os exportadores estão configurados para usar a mesma versão de SNMP configurada em SNA.
  - Em caso de uso do SNMPv3, verifique se a configuração do SNMP está correta (Nome de usuário, Senha de autenticação, Protocolo de autenticação, Senha de privacidade, Protocolo de privacidade)

## Solução de problemas ao vivo de pesquisa SNMP



Na interface do usuário da Web, navegue para Configure -> Exporters -> Exporter SNMP Profiles (Configurar -> Exportadores -> Perfis SNMP do exportador)

- Defina Polling (minutos) como 1 (minuto) temporariamente.



The screenshot shows the 'Edit SNMP Profile' configuration page. The 'Polling (minutes)' field is highlighted with a red box and contains the value '1'. Other fields include Name, Version (Version 3), Port (161), User Name (admin), and Authentication Protocol (HMAC\_MD5).

- Faça login no SMC via SSH ou console com credenciais de raiz.
- Navegue até esta pasta:

```
cd /lancope/var/smc/log
```

- Executar:

```
tail -f smc-configuration.log
```

- Para SNMPv3, uma mensagem de erro comum seria:

```
failed: java.lang.IllegalArgumentException: USM passphrases must be at least 8 bytes long (RFC3414)
```

- Verifique se a senha de autenticação no Perfil SNMP está definida para 8 caracteres ou mais.
- Quando a solução de problemas ao vivo for concluída, retorne a configuração de Pesquisa (minutos) para o exportador ou seu modelo de configuração ao seu valor anterior.

## Testando o SNMP Polling a partir de outro dispositivo

Testar pesquisa SNMP: inicie manualmente uma pesquisa SNMP de uma máquina local para um dispositivo de rede específico e verifique se ele recebe uma resposta. Isso pode ser feito usando ferramentas de pesquisa SNMP ou utilitários como SNMPwalk. Verifique se o dispositivo de rede responde com os dados SNMP solicitados. Se não houver resposta, isso indica um problema com a configuração ou a conectividade SNMP.

- Na sua máquina local com o software SNMPwalk, substitua "x.x.x.x" pelo IP exportador e execute no CLI:

```
snmpwalk -v2c -c public x.x.x.x
```

- -v2c: especifica a versão do SNMP a ser usada
- -c: define a sequência de caracteres da comunidade

```
% snmpwalk -v2c -c public 1
SNMPv2-MIB::sysDescr.0 = STRING: Cisco IOS Software [Amsterdam], Virtual XE Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 17.3.4a, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2021 by Cisco Systems, Inc.
Compiled Tue 20-Jul-21 04:
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.9.1.1537
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (373833542) 43 days, 6:25:35.42
SNMPv2-MIB::sysContact.0 =
SNMPv2-MIB::sysName.0 = STRING:
SNMPv2-MIB::sysLocation.0 = STRING: cxlabs
SNMPv2-MIB::sysServices.0 = INTEGER: 78
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (0) 0:00:00.00
IF-MIB::ifNumber.0 = INTEGER: 10
IF-MIB::ifIndex.1 = INTEGER: 1
IF-MIB::ifIndex.2 = INTEGER: 2
IF-MIB::ifIndex.3 = INTEGER: 3
IF-MIB::ifIndex.4 = INTEGER: 4
IF-MIB::ifIndex.5 = INTEGER: 5
IF-MIB::ifIndex.6 = INTEGER: 6
IF-MIB::ifIndex.7 = INTEGER: 7
IF-MIB::ifIndex.8 = INTEGER: 8
IF-MIB::ifIndex.9 = INTEGER: 9
IF-MIB::ifIndex.10 = INTEGER: 10
IF-MIB::ifDescr.1 = STRING: GigabitEthernet1
IF-MIB::ifDescr.2 = STRING: GigabitEthernet2
IF-MIB::ifDescr.3 = STRING: GigabitEthernet3
IF-MIB::ifDescr.4 = STRING: GigabitEthernet4
IF-MIB::ifDescr.5 = STRING: GigabitEthernet5
IF-MIB::ifDescr.6 = STRING: VoIP-Null0
IF-MIB::ifDescr.7 = STRING: Null0
IF-MIB::ifDescr.8 = STRING: GigabitEthernet6
IF-MIB::ifDescr.9 = STRING: GigabitEthernet7
IF-MIB::ifDescr.10 = STRING: Tunnel1
IF-MIB::ifType.1 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.2 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.3 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.4 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.5 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.6 = INTEGER: other(1)
```

- Verifique se o exportador responde com dados SNMP

## Informações Relacionadas

- Para obter assistência adicional, entre em contato com o Technical Assistance Center (TAC). É necessário um contrato de suporte válido: [Contatos de suporte da Cisco no mundo inteiro](#).
- Você também pode visitar a [comunidade](#) de análise de segurança da Cisco [aqui](#).
- [Suporte Técnico e Documentação - Cisco Systems](#)

## 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.