

# SNAでのSNMPポーリングおよび不適切なインターフェイスの詳細のトラブルシューティング

## 内容

---

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[コンフィギュレーション](#)

[背景説明](#)

[トラブルシューティング](#)

[誤ったインターフェイス名](#)

[エクスポータまたはインターフェイスが見つからない](#)

[接続性の問題](#)

[エクスポータをポーリングするマネージャ\(SMC\)の機能を検証](#)

[エクスポータのIPアドレスを使用して、SMCでパケットキャプチャを生成します。](#)

[SNMPポーリング設定の検証](#)

[SNMPポーリングのライブトラブルシューティング](#)

[別のデバイスからのSNMPポーリングのテスト](#)

[関連情報](#)

---

## はじめに

このドキュメントでは、Secure Network Analyticsでエクスポータインターフェイス情報が欠落している場合のトラブルシューティング方法について説明します

## 前提条件

- Ciscoでは、基本的なSimple Network Management Protocol(SNMP)のポーリングに関する知識があることを推奨しています
- Secure Network Analytics(SNA/StealthWatch)に関する基本的な知識があることが推奨されます

## 要件

- バージョン7.4.1以降のSNA Manager
- バージョン7.4.1以降のSNA Flow Collector
- SNAにNetFlowをアクティブに送信しているエクスポータ

## 使用するコンポーネント

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。稼働中のネットワークで作業を行う場合は、コマンドの影響について十分に理解したうえで作業してください

- バージョン7.4.1以降のSNA Manager
- バージョン7.4.1以降のSNA Flow Collector
- SNMPwalkソフトウェア
- Wiresharkソフトウェア

## コンフィギュレーション

- デバイス設定：SNMPアクセスを許可するようにエクスポートを設定する必要があります。これには、SNMPコミュニティストリング、アクセスコントロールリスト(ACL)の設定、使用するSNMPバージョンの定義など、各デバイスでのSNMP設定の設定が含まれます
- SNAでのSNMPポーリング設定：エクスポートが正しく設定されると、SMCでは事前に設定されたパラメータを使用してSNMPポーリングがデフォルトで有効になります。ポーリングメカニズムが最適に動作するためには、SNMPコミュニティストリングやSNMPバージョンなど、エクスポートに関する必要な詳細情報を提供することが重要です

## 背景説明

SNAは、インターフェイスステータスレポートを包括的に提供する機能と、NetFlowデータをフローコレクタにアクティブに送信しているエクスポートのインターフェイス名を表示する機能を備えています。このインターフェイスの詳細は、Manager Web UIからInvestigate -> Interfacesメニューに移動して表示できます。

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

## トラブルシューティング

### 誤ったインターフェイス名

生成されたレポートで「ifindex-#」が表示される場合、これはエクスポートインターフェイスに対応していません。これは、SMCまたはエクスポートインターフェイス自体でのSNMPポーリングに関する潜在的な設定の問題を示唆しています。この例では、特定のエクスポートのSNMPポーリングに関する明らかな問題を取り上げています。

Interfaces (152)

Filter by Device

Interface Status (Since Reset Hour)

INTERFACE	EXPORTER	CURRENT UTILIZATION	CURRENT TRAFFIC	MAXIMUM UTILIZATION	MAX TRAFFIC	DIRECTION	SPEED
ifindex-5 ...		90.93%	909.27 Mbps	162.76%	1.63 Gbps	INBOUND	1 Gbps
ifindex-8 ...		85.71%	857.08 Mbps	85.71%	857.08 Mbps	OUTBOUND	1 Gbps
ifindex-26 ...		85.71%	857.08 Mbps	85.71%	857.08 Mbps	INBOUND	1 Gbps
ifindex-3 ...		80.46%	804.6 Mbps	82.07%	820.69 Mbps	INBOUND	1 Gbps
ifindex-25 ...		79.06%	790.63 Mbps	80.29%	802.94 Mbps	OUTBOUND	1 Gbps
ifindex-16 ...		79.06%	790.63 Mbps	80.29%	802.94 Mbps	INBOUND	1 Gbps
ifindex-13 ...		53.29%	532.87 Mbps	94.85%	948.5 Mbps	OUTBOUND	1 Gbps
ifindex-24 ...		53.29%	532.87 Mbps	94.85%	948.5 Mbps	INBOUND	1 Gbps
ifindex-0 ...		0.43%	4.29 Mbps	2.58%	25.84 Mbps	OUTBOUND	1 Gbps
TenGigabitEthernet1/0/38 ...		0.32%	3.17 Mbps	0.98%	9.77 Mbps	INBOUND	1 Gbps
ifindex-0 ...		0.13%	1.28 Mbps	0.37%	3.66 Mbps	OUTBOUND	1 Gbps
ifindex-0 ...		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

## エクスポートまたはインターフェイスが見つからない

テンプレートの検証は、NetFlowデータ処理において非常に重要です。具体的には、エクスポートから受信したNetFlowテンプレートに、フローコレクタによるデコードと処理を正常に行うために必要なすべての必須フィールドが含まれていることを確認します。有効なテンプレートが見つからないと、関連するフローのセットがデコードから除外され、その結果、フローがインターフェイスのリストから欠落します。

インターフェイスリストに必要なエクスポートまたはインターフェイスが表示されない場合は、着信netflow data dnテンプレートを確認する必要があります。NetFlowテンプレートを確認するために、フローコレクタ側でパケットキャプチャを作成し、エクスポートからIPを指定します。「x.x.x.x」を変更して、NetFlowを取得します。

- SSHまたはコンソール経由で、rootクレデンシャルを使用してFlow Collectorにログインします。
- 問題のエクスポートのIPポートとNetFlowポートからパケットキャプチャを実行します。

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

.pcap

- アプライアンスからWiresharkアプリケーションがインストールされているワークステーションにパケットキャプチャをコピーし、任意の方法 ( SCP、SFTPなど ) を使用します。

- Wiresharkでパケットキャプチャを開き、エクスポートがフローコレクタに送信しているテンプレートとデータを確認します

Date	Source	Destination	Protocol	Length	Info	Dest Port
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: Vhware_B4:49:4f (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
  
```

NetFlowテンプレートが9個の必須フィールドを使用していることを確認します。これらのテンプレートフィールドの正確な名前はエクスポートのタイプによって異なる可能性があるため、設定するエクスポートのタイプの詳細については、次のドキュメントを参照してください。

- 送信元 IP アドレス
- 宛先 IP アドレス
- 送信元ポート
- 宛先ポート
- レイヤ4プロトコル
- バイト数
- パケット数
- フロー開始時間
- フロー終了時間

インターフェイスを正しく表示するには、次の項目も追加してください。

- インターフェイス出力
- インターフェイス入力


次に、特定のエクスポータのデバイスからのテンプレートパケットキャプチャの例を示します

- 赤い矢印：必須のNetFlowフィールド
- 緑色の矢印：SNMPフィールド

```
> 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 ←
```

🔗 注：コマンド例に示されているポートは、エクスポートの設定によって異なる場合があります。デフォルトは2055です

🔗 注：パケットキャプチャは5 ~ 10分で実行してください。エクスポートによってはテンプ

 レートをN分ごとに送信できるため、NetFlowが正しくデコードされるようにそのテンプレートをキャッチする必要があります。テンプレートが表示されない場合は、パケットキャプチャをより長い期間繰り返します

## 接続性の問題

接続の確認：SNA Managerアプライアンスとエクスポートが接続されていることを確認します。IPアドレスをpingして、StealthWatch管理コンソールからエクスポートにアクセスできることを確認します。ネットワーク接続の問題がある場合は、トラブルシューティングを行い、状況に応じて問題を解決します。

## エクスポートをポーリングするマネージャ(SMC)の機能を検証

- SSH経由でSNAマネージャに接続し、ルートクレデンシャルでログインします
- `/lancope/var/smc/log/smc-configuration.log` ファイルを分析し、`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
```

- このポーリング例では、エクスポート10.1.0.253に対してエラーは検出されませんでした。しかし、エクスポート10.1.0.254で最初にタイムアウトエラーメッセージが発生し、その後20秒の遅延後にポーリング動作を正常に実行することができました。

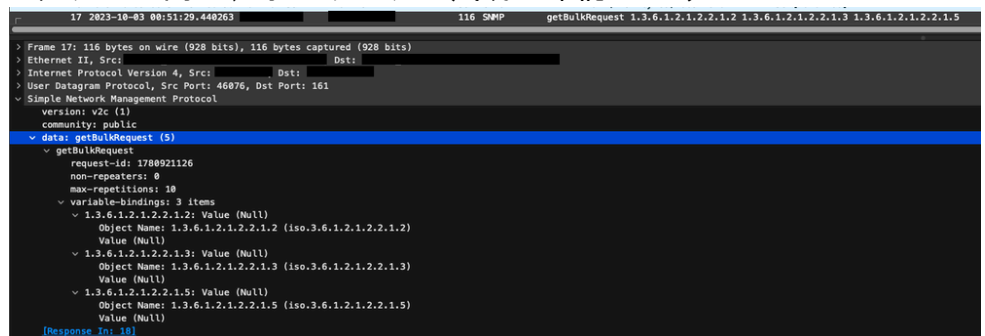
## エクスポートのIPアドレスを使用して、SMCでパケットキャプチャを生成します。

- rootクレデンシャルを使用して、SSHまたはコンソール経由でマネージャノードにログインします
- 次のコマンドを実行します。

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

- 希望する方法 (例：SCP、SFTP) でアプライアンスからパケットキャプチャをエクスポートします。
- Wiresharkでパケットキャプチャを開き、ポーリングの成功を確認します

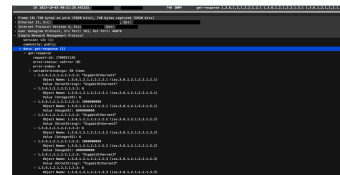
- SMCからの要求：



```
17 2023-10-03 00:51:29.440263 116 SNMP getBulkRequest 1.3.6.1.2.1.2.2.1.2 1.3.6.1.2.1.2.2.1.3 1.3.6.1.2.1.2.2.1.5
> Frame 17: 116 bytes on wire (928 bits), 116 bytes captured (928 bits)
> Ethernet II, Src: [redacted], Dst: [redacted]
> Internet Protocol Version 4, Src: [redacted], Dst: [redacted]
> User Datagram Protocol, Src Port: 46876, Dst Port: 161
> Simple Network Management Protocol
  version: v2c (1)
  community: public
  data: getBulkRequest (5)
    getBulkRequest
      request-id: 1788921126
      non-repeaters: 0
      max-repetitions: 10
      variable-bindings: 3 items
        1.3.6.1.2.1.2.2.1.2: Value (Null)
          Object Name: 1.3.6.1.2.1.2.2.1.2 (iso.3.6.1.2.1.2.2.1.2)
          Value (Null)
        1.3.6.1.2.1.2.2.1.3: Value (Null)
          Object Name: 1.3.6.1.2.1.2.2.1.3 (iso.3.6.1.2.1.2.2.1.3)
          Value (Null)
        1.3.6.1.2.1.2.2.1.5: Value (Null)
          Object Name: 1.3.6.1.2.1.2.2.1.5 (iso.3.6.1.2.1.2.2.1.5)
          Value (Null)
    [Response_Ini_18]
```



- 。 インターフェイス情報を含むエクスポートからのSNMP応答 :

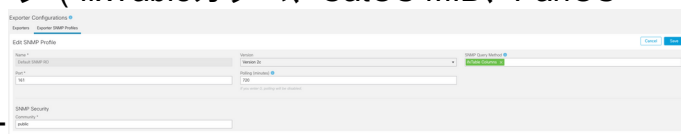


## SNMPポーリング設定の検証


ポーリング間隔が適切であり、必要なメトリックがSNMPクエリに含まれていることを確認します

- Web UIで、Configure -> Exporters -> Exporter SNMP Profilesの順に選択します。
- 正しいSNMPポート ( 通常はUDPポート161 ) と正しいSNMPクエリー方式が選択されていることを確認します。これらは、エクスポート ( ifxTableカラム、CatOS MIB、PanOS

MIB ) と適切に一致している必要があります



 注 : インターフェイスの速度が10 Gbpsの場合は、SNMPクエリー方式にifxTable columnsオプションを選択することをお勧めします。

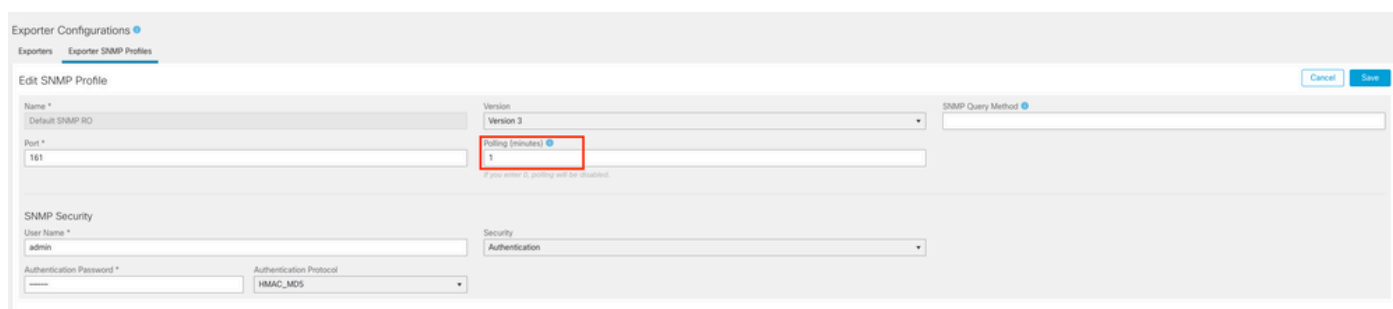
 注 : 最適なシステムパフォーマンスを得るには、SNMPポーリングを12時間間隔に設定します。ポーリングの頻度を上げて、使用率メトリックが最新の状態になるわけではなく、システムの実行速度が低下する可能性があります。

- SNAとエクスポートの両方で設定されているSNMPバージョンに互換性があることを確認します。SNAはSNMPv1、SNMPv2c、およびSNMPv3をサポートします。SNAで設定されているSNMPバージョンと同じバージョンを使用するようにエクスポートが設定されているかどうかを確認します。
  - 。 SNMPv3を使用する場合は、SNMP設定が正しいことを確認します ( ユーザ名、認証パスワード、認証プロトコル、プライバシーパスワード、プライバシープロトコル )

## SNMPポーリングのライブトラブルシューティング

Web UIで、Configure -> Exporters -> Exporter SNMP Profilesの順に選択します。

- ポーリング ( 分 ) を一時的に1 ( 分 ) に設定します。





- SSHまたはコンソール経由で、rootクレデンシャルを使用してSMCにログインします。
- 次のフォルダに移動します。

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

- 次のコマンドを実行します。

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

- SNMPv3の場合、一般的なエラーメッセージは次のようになります。

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

- SNMPプロファイルの認証パスワードが8文字以上に設定されていることを確認します。
- ライブトラブルシューティングが終了したら、エクスポートまたはその設定テンプレートのポーリング (分) 設定を以前の値に戻します。

## 別のデバイスからのSNMPポーリングのテスト

SNMPポーリングのテスト：ローカルマシンから特定のネットワークデバイスへのSNMPポーリングを手動で開始し、応答を受信するかどうかを確認します。これは、SNMPポーリングツールまたはSNMPwalkなどのユーティリティを使用して実行できます。ネットワークデバイスが要求されたSNMPデータで応答することを確認します。応答がない場合は、SNMPの設定または接続に問題があることを示しています。

- SNMPwalkソフトウェアがインストールされているローカルマシンで、エクスポートIPを「x.x.x.x」に置き換えて、CLIで実行します。

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

- -v2c：使用するSNMPバージョンを指定します。
- -c：コミュニティ文字列を設定する

```
% 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)
```

- エクスポートがSNMPデータで応答することを確認します。

## 関連情報

- 詳細については、Technical Assistance Center(TAC)にお問い合わせください。有効なサポート契約が必要です。 [各国のシスコサポートの連絡先](#)。
- また、Cisco Security Analytics [コミュニティ](#) もご覧ください。
- [テクニカルサポートとドキュメント - Cisco Systems](#)

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。