

SNMP: Häufig gestellte Fragen zu MIB-Theorie und -Betrieb

Inhalt

[Einführung](#)

[Mit welchem Tool kann ich SNMP-Pakete und SNMP-Traps auf meiner Workstation erfassen und analysieren?](#)

[Warum habe ich eine Schnittstelle mit ifDescr = Null0 in der ifTable?](#)

[Einige ifTable-Spalten werden für bestimmte Schnittstellentypen nicht angezeigt. Warum geschieht das? Ist das ein Fehler?](#)

[Ich sehe zwei Coldstart-Traps aus der Box. Ist das ein Fehler?](#)

[Welche genauen Informationen sind in einem SNMP-Trap enthalten, und wo sind diese dokumentiert?](#)

[Zugehörige Informationen](#)

Einführung

Dieses Dokument bietet Antworten auf häufig gestellte Fragen und hilft Benutzern dabei, hilfreiche Ressourcen zu Simple Network Management Protocol (SNMP)- und SNMP-Problemen im Zusammenhang mit Cisco Geräten zu finden.

F. Mit welchem Tool kann ich SNMP-Pakete und SNMP-Traps auf meiner Workstation erfassen und analysieren?

Antwort: Unter Solaris verwenden Sie den Befehl **snoop**, der sich in `/usr/sbin/snoop` befindet.

Hinweis: Sie müssen ein **Root**-Benutzer sein, um Pakete im Kabel zu erfassen.

Beispiel:

```
snoop udp port 162
router1 -> host1 UDP D=162 S=1480 LEN=120
```

In diesem Beispiel wurde ein Paket erfasst. Geräte-*Router1* sendet SNMP-TRAP (UDP-Port 162) an Geräte-*Host1*.

Sie können auch Ethereal verwenden, ein kostenloser Netzwerkprotokollanalytiker für UNIX-Systeme und Microsoft Windows. SNMP-Pakete können mit Ethereal Version 0.8.0 und höher analysiert werden. Sie können Ethereal von der [Ethereal Download](#) Seite herunterladen.

F. Warum habe ich eine Schnittstelle mit ifDescr = Null0 in der ifTable?

Antwort: Ab der Cisco IOS[®] Software-Version 12.0 wird in der ifTable eine Schnittstelle angezeigt,

in der ifDescr Null0 angezeigt wird.

Null-Schnittstelle, Null0, ist eine virtuelle Netzwerkschnittstelle (ähnlich der Loopback-Schnittstelle). Während der an die Loopback-Schnittstelle gerichtete Datenverkehr an den Router selbst weitergeleitet wird, wird der an die Null-Schnittstelle gesendete Datenverkehr verworfen.

Die Nullschnittstelle kann nicht mit einer Adresse konfiguriert werden. Datenverkehr kann nur an diese Schnittstelle gesendet werden, indem eine statische Route konfiguriert wird, bei der der nächste Hop die Null0-Schnittstelle ist. Auf diese Weise wird eine Route zu einem aggregierten Netzwerk erstellt, die dann über das Border Gateway Protocol (BGP) angekündigt werden kann, oder es wird sichergestellt, dass der Datenverkehr zu einem bestimmten Adressbereich nicht über den Router weitergeleitet wird, vielleicht zu Sicherheitszwecken.

Der Router verfügt immer über eine einzige Null-Schnittstelle, Null0. Standardmäßig veranlasst ein an die Null-Schnittstelle gesendetes Paket den Router, eine nicht erreichbare ICMP-Nachricht (Internet Control Message Protocol) an die Quell-IP-Adresse des Pakets zu senden. Sie können den Router so konfigurieren, dass er diese Antworten sendet oder die Pakete leise verwirft.

Um das Senden von nicht erreichbaren ICMP-Nachrichten als Antwort auf Pakete zu deaktivieren, die an die Null-Schnittstelle gesendet wurden, geben Sie diesen Befehl im Schnittstellenkonfigurationsmodus ein:

```
no ip unreachable
```

Um das Senden von nicht erreichbaren ICMP-Nachrichten als Antwort auf Pakete zu aktivieren, die an die Null-Schnittstelle gesendet wurden, geben Sie diesen Befehl im Schnittstellenkonfigurationsmodus ein:

```
ip unreachable
```

F. Einige ifTable-Spalten werden für bestimmte Schnittstellentypen nicht angezeigt. Warum geschieht das? Ist das ein Fehler?

Antwort: Das ist kein Fehler. Die ifTable, die auf RFC 1573 basiert, ist speziell so konzipiert, dass einige Spalten in einer bestimmten Zeile nicht basierend auf ifType instanziiert werden. Lesen Sie die RFC Compliance Statement, um weitere Informationen darüber zu erhalten, welche Spalten für die verschiedenen Mediengruppen zu erwarten sind. Ein Beispiel hierfür wäre ATM, ein Paket mit fester Länge. Daher basieren Zeilen in der ifTable (und andere) auf ifFixedLengthGroup.

F. Ich sehe zwei Coldstart-Traps aus der Box. Ist das ein Fehler?

Antwort: Dieses Verhalten ist kein Fehler. Ein Coldstart-Trap ist normalerweise die erste Trap (und das erste Paket), die an ein Trap-Ziel gesendet wird. Der Router muss für das Trap-Ziel das Address Resolution Protocol (ARP) verwenden. Cisco Geräte lassen das Trap fallen, wenn ein ARP gesendet werden muss. Viele Kunden sahen daher vor dem Fix nicht die "coldstart trap", d. h. die doppelte Versendung. Dies ist RFC-konform, da das Netzwerk auch die Coldstart-Traps duplizieren kann. Die NMS-Station (Network Management System) des Kunden sollte in der Lage sein, dies zu bewältigen (oder es ist defekt).

Hinweis: Um diesem Bug-ID-Link zu folgen und detaillierte Fehlerinformationen zu erhalten,

müssen Sie ein [registrierter](#) (nur registrierte Kunden) Benutzer sein und angemeldet sein.

F. Welche genauen Informationen sind in einem SNMP-Trap enthalten, und wo sind diese dokumentiert?

Antwort: Jede Trap wird in einigen MIB definiert. Um die genaue Definition des Traps mit der Liste der darin enthaltenen Objekte anzuzeigen, suchen Sie das Trap im [SNMP Object Navigator](#). Sie können z. B. das [cctCallSetupNotification](#)-Trap aus [CISCO-CALL-TRACKER-MIB](#) sehen.

Zugehörige Informationen

- [Technische Tipps zum Simple Network Management Protocol](#)
- [Technischer Support - Cisco Systems](#)