

# SNMP: Frequently Asked Questions About MIB Theory and Operation

## Contents

### [Introduction](#)

[Que ferramenta posso usar para capturar e analisar pacotes e armadilhas de SNMP em minha estação de trabalho?](#)

[Por que tenho uma interface com ifDescr = Null0 na ifTable?](#)

[Algumas colunas ifTable não são exibidas para determinados tipos de interface. Por que isso acontece? Isto é um bug?](#)

[Vejo duas armadilhas de inicialização a frio fora da caixa. Isto é um bug?](#)

[Quais são as informações exatas contidas em uma armadilha de SNMP e onde elas estão documentadas?](#)

[Informações Relacionadas](#)

## Introduction

Este documento fornece respostas para perguntas frequentes e orienta os usuários a encontrar recursos úteis sobre problemas de SNMP (Simple Network Management Protocol) e SNMP relacionados aos equipamentos da Cisco.

### **P. Que ferramenta posso usar para capturar e analisar pacotes e armadilhas de SNMP em minha estação de trabalho?**

**A.** No Solaris, use o comando **snoop**, localizado em */usr/sbin/snoop*.

**Observação:** você precisa ser um usuário **raiz** para capturar pacotes no fio.

Por exemplo:

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

Este exemplo capturou um pacote. O router1 do dispositivo envia um SNMP-TRAP (UDP porta 162) para o host1 do dispositivo.

Você também pode usar o Ethereal, que é um analisador de protocolo de rede gratuito para sistemas UNIX e Microsoft Windows. Os pacotes SNMP podem ser analisados com Ethereal versão 0.8.0 e posterior. Você pode fazer o download do Ethereal na página [Download Ereal](#).

### **P. Por que tenho uma interface com ifDescr = Null0 na ifTable?**

**A.** A partir do Cisco IOS® Software Release 12.0, há uma interface com ifDescr Null0 aparecendo

na ifTable.

A interface nula, Null0, é uma interface de rede virtual (semelhante à interface de loopback). Embora o tráfego para a interface de loopback seja direcionada ao próprio roteador, o tráfego enviado para a interface nula é descartado.

A interface nula pode não estar configurada com um endereço. O tráfego pode ser enviado para essa interface somente por meio da configuração de uma rota estática, em que o próximo salto seja a interface Null0. Isso é feito para criar uma rota para uma rede agregada que pode ser anunciada através do BGP (Border Gateway Protocol) ou para garantir que o tráfego para um intervalo específico de endereços não seja propagado através do roteador, talvez para fins de segurança.

O roteador sempre tem uma única interface nula, Null0. Por padrão, um pacote enviado à interface nula faz com que o roteador responda enviando uma mensagem inalcançável ICMP (Internet Control Message Protocol) para o endereço IP origem do pacote. É possível configurar o roteador para enviar estas repostas ou para descartar pacotes de modo silencioso.

Para desabilitar o envio de mensagens ICMP inalcançáveis em resposta aos pacotes enviados à interface nula, digite este comando no modo de configuração de interface:

```
no ip unreachablees
```

Para habilitar o envio de mensagens ICMP Inalcançável em resposta aos pacotes enviados à interface nula, digite este comando no modo de configuração de interface:

```
ip unreachablees
```

## **P. Algumas colunas ifTable não são exibidas para determinados tipos de interface. Por que isso acontece? Isto é um bug?**

**A.** Isso não é um erro. O ifTable, baseado no RFC 1573, foi projetado especificamente para que algumas colunas de determinada linha não sejam instanciadas com base no ifType. Leia a declaração de conformidade RFC para obter mais esclarecimentos sobre quais colunas devem esperar para diferentes grupos de mídia. Um exemplo disso seria o ATM, que é um pacote de comprimento fixo. Como tal, as linhas na ifTable (e outras) são baseadas em ifFixedLengthGroup.

## **P. Vejo duas armadilhas de inicialização a frio fora da caixa. Isto é um bug?**

**A.** Este comportamento não é um bug. Uma armadilha de inicialização forçada é normalmente a primeira armadilha (e o primeiro pacote) a ser enviada a um destino de armadilha. O roteador precisa do Address Resolution Protocol (ARP) para o destino da armadilha. Os dispositivos Cisco descartam a armadilha se um ARP precisar ser enviado. Portanto, muitos clientes não estavam vendo o desvio coldstart antes da correção, que foi enviá-la duas vezes. Isso é compatível com RFC, pois a rede também pode duplicar as armadilhas de inicialização forçada. A estação NMS (Network Management System, sistema de gerenciamento de rede) do cliente deve ser capaz de lidar com isso (caso contrário, ele está quebrado).

**Observação:** para seguir este link de ID de bug e ver informações detalhadas de bug, você deve ser um usuário [registrado](#) ([somente](#) clientes registrados) e deve estar conectado.

**P. Quais são as informações exatas contidas em uma armadilha de SNMP e onde elas estão documentadas?**

**A.** Cada armadilha é definida em alguma MIB. Para ver a definição exata da armadilha com a lista de objetos contidos nela, localize a armadilha no [SNMP Object Navigator](#). Por exemplo, você pode ver a armadilha [ctCallSetupNotification](#) de [CISCO-CALL-TRACKER-MIB](#).

## **Informações Relacionadas**

- [Dicas técnicas simples de protocolo de gerenciamento de rede](#)
- [Suporte Técnico - Cisco Systems](#)