

SNMP: Frequently Asked Questions About MIB Theory and Operation

Document ID: 26012

Contents

Introduction

What tool can I use to capture and analyze SNMP packets and SNMP traps on my workstation?

Why do I have an interface with ifDescr = Null0 in the ifTable?

Some ifTable columns do not show up for certain interface types. Why does this happen? Is this a bug?

I see two coldstart traps out of the box. Is this a bug?

What is the exact information contained in an SNMP trap, and where is it documented?

Related Information

Introduction

This document provides answers to commonly asked questions and guides users to find helpful resources on Simple Network Management Protocol (SNMP) and SNMP issues as they relate to Cisco equipment.

Q. What tool can I use to capture and analyze SNMP packets and SNMP traps on my workstation?

A. On Solaris, use the **snoop** command, which is located in */usr/sbin/snoop*.

Note: You need to be a **root** user in order to capture packets on the wire.

For example:

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

This example captured one packet. Device *router1* sends a SNMP-TRAP (UDP port 162) to device *host1*.

You can also use Ethereal, which is a free network protocol analyzer for UNIX systems and Microsoft Windows. SNMP packets can be analyzed with Ethereal release 0.8.0 and later. You can download Ethereal from the [Ethereal Download page](#).

Q. Why do I have an interface with ifDescr = Null0 in the ifTable?

A. As of Cisco IOS[®] Software release 12.0, there is an interface with ifDescr Null0 showing up in the ifTable.

The null interface, Null0, is a virtual network interface (similar to the loopback interface). While traffic to the loopback interface is directed to the router itself, traffic sent to the null interface is discarded.

The null interface might not be configured with an address. Traffic can only be sent to this interface by configuring a static route where the next hop is the Null0 interface. This is done

to create a route to an aggregate network that can then be announced through the Border Gateway Protocol (BGP), or to ensure that traffic to a particular range of addresses is not propagated through the router, perhaps for security purposes.

The router always has a single null interface, Null0. By default, a packet sent to the null interface causes the router to respond by sending an Internet Control Message Protocol (ICMP) unreachable message to the packet's source IP address. You can configure the router either to send these responses or to silently drop the packets.

In order to disable the sending of ICMP unreachable messages in response to packets sent to the null interface, type this command in interface configuration mode:

```
no ip unreachable
```

In order to enable the sending of ICMP Unreachable messages in response to packets sent to the null interface, type this command in interface configuration mode:

```
ip unreachable
```

Q. Some ifTable columns do not show up for certain interface types. Why does this happen? Is this a bug?

A. This is not a bug. The ifTable, based on RFC 1573, is designed specifically so that some columns in a given row are not instantiated based on ifType. Read the RFC compliance statement for further clarification for which columns to expect for different media groups. An example of this would be ATM, which is a fixed-length packet. As such, rows in the ifTable (and others) are based on ifFixedLengthGroup.

Q. I see two coldstart traps out of the box. Is this a bug?

A. This behavior is not a bug. A coldstart trap is normally the first trap (and the first packet) to be sent to a trap destination. The router needs to Address Resolution Protocol (ARP) for the trap destination. Cisco devices drop the trap if an ARP has to be sent out. Therefore, many customers were not seeing the coldstart trap before the fix, which was to send it twice. This is RFC compliant, as the network can also duplicate the coldstart traps. The customer's network management system (NMS) station should be able to handle this (or else it is broken).

Note: To follow this bug ID link and see detailed bug information, you must be a registered (registered customers only) user and you must be logged in.

Q. What is the exact information contained in an SNMP trap, and where is it documented?

A. Each trap is defined in some MIB. In order to see the exact definition of the trap with the list of objects contained in it, find the trap in SNMP Object Navigator. For example, you can see the cctCallSetupNotification trap from CISCO-CALL-TRACKER-MIB.

Related Information

- **Simple Network Management Protocol Technical Tips**
 - **Technical Support – Cisco Systems**
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2014 – 2015 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Jul 16, 2009

Document ID: 26012
