

Entendendo os desvios do Protocolo Simples de Gerenciamento de Rede (SNMP)

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Usar interceptações SNMP](#)

[Exemplos de armadilhas enviadas pelo Cisco IOS](#)

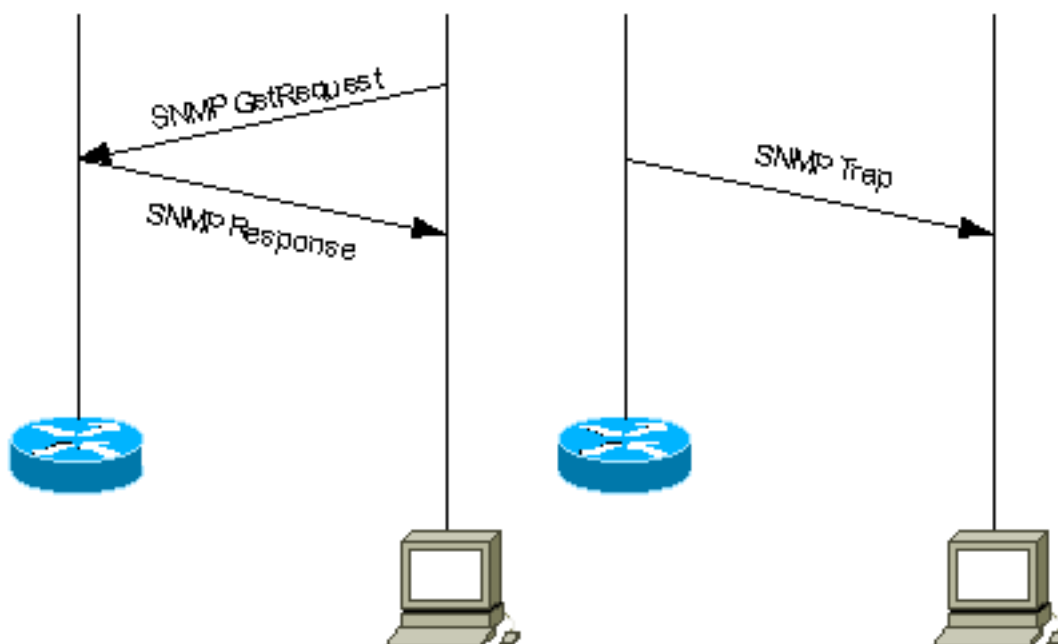
[Informações Relacionadas](#)

Introduction

Este documento fornece uma introdução aos desvios do SNMP. Ele mostra como as traps de SNMP são usadas e a função que desempenham no gerenciamento de uma rede de dados.

As armadilhas de SNMP permitem que um agente notifique a estação de gerenciamento sobre eventos significativos por meio de uma mensagem SNMP não solicitada.

Neste diagrama, a configuração à esquerda mostra um sistema de gerenciamento de rede que pesquisa informações e obtém uma resposta. A configuração à direita mostra um agente que envia uma interceptação não solicitada ou assíncrona para o sistema de gerenciamento de rede (NMS).



Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

Conventions

Consulte as [Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos](#).

Usar interceptações SNMP

Os protocolos SNMPv1 e SNMPv2, junto com o MIB associado, incentivam a notificação direcionada para armadilha.

A ideia por trás da notificação direcionada a armadilhas é que se um gerente é responsável por um grande número de dispositivos, e cada dispositivo tem um grande número de objetos, é impraticável que o gerente faça uma pesquisa ou solicite informações de cada objeto em cada dispositivo. A solução é que cada agente no dispositivo gerenciado notifique o gerenciador sem solicitação. Ele faz isso enviando uma mensagem conhecida como armadilha do evento.

Depois que o gerente receber o evento, ele será exibido e poderá optar por uma ação baseada no evento. Por exemplo, o gerente pode pesquisar o agente diretamente ou pesquisar outros agentes de dispositivos associados para obter uma melhor compreensão do evento.

Uma notificação direcionada ao desvio pode resultar em economia substancial de recursos de rede e de agente, eliminando a necessidade de solicitações desnecessárias de SNMP. Entretanto, não é possível eliminar totalmente a interrogação de SNMP. Solicitações SNMP são necessárias para alterações de detecção e topologia. Além disso, um agente de dispositivo gerenciado não pode enviar uma interceptação (trapping) se o dispositivo tiver sofrido uma interrupção catastrófica.

As interceptações SNMPv1 são definidas no RFC 1157, com estes campos:

- *Enterprise* — Identifica o tipo de objeto gerenciado que gera a interceptação.
- *Endereço do agente* — Fornece o endereço do objeto gerenciado que gera a interceptação.
- *Tipo genérico de interceptação* — Indica um dos vários tipos genéricos de interceptação.
- *Código de armadilha específico* — Indica um dos vários códigos de armadilha específicos.
- *Carimbo de data/hora* — Fornece a quantidade de tempo decorrido entre a última reinicialização da rede e a geração da armadilha.
- *Vinculações variáveis* — O campo de dados da armadilha que contém PDU. Cada enlace de variável associa uma determinada instância de objeto MIB ao seu valor atual.

As armadilhas genéricas padrão são: coldStart, warmStart, linkDown, linkUp, authenticationFailure, egpNeighborLoss. Para interceptações SNMPv1 genéricas, o campo

Enterprise contém o valor de [sysObjectID](#) do dispositivo que envia interceptação. Para armadilhas específicas do fornecedor, o *campo de tipo de armadilha genérica* é definido como `enterpriseSpecific(6)`. A Cisco implementou suas próprias armadilhas específicas de forma não convencional. Em vez de ter o campo *Enterprise* de armadilha ainda o [sysObjectID](#) e ter o *código de armadilha específico* para identificar todas as armadilhas específicas suportadas por todos os dispositivos da Cisco, a Cisco implementou a identificação de interceptações usando vários campos de armadilha *Enterprise* e de código de interceptação Específico. Você pode ver os valores reais do [SNMP Object Navigator](#) . Além disso, a Cisco redefiniu algumas armadilhas genéricas na [MIB CISCO-GENERAL-TRAPS](#) com a adição de variáveis mais vinculadas. Para essas armadilhas, o *tipo de armadilha genérica* é mantido o mesmo e não definido como `enterpriseSpecific(6)`.

No SNMPv2c, a interceptação (trapping) é definida como NOTIFICATION (NOTIFICAÇÃO) e formatada de forma diferente em relação ao SNMPv1. Ele tem estes parâmetros:

- *sysUpTime*—É o mesmo que o Time Stamp na interceptação SNMPv1.
- [snmpTrapOID](#) —Campo de identificação da armadilha. Para armadilhas genéricas, os valores são definidos no RFC 1907, para armadilhas específicas do fornecedor *snmpTrapOID* é essencialmente uma concatenação do parâmetro *Enterprise* SNMPv1 e dois subidentificadores adicionais, '0', e o *parâmetro de código de interceptação específico* SNMPv1.
- *VarBindList* — Esta é uma lista de variáveis-bindings.

Para que um sistema de gerenciamento compreenda uma armadilha enviada a ele por um agente, o sistema de gerenciamento deve saber o que o identificador de objeto (OID) define. Por isso, ele deve ter o MIB para essa armadilha carregado. Fornece as informações OID corretas para que o sistema de gerenciamento de rede possa entender as armadilhas enviadas a ele.

Para armadilhas suportadas por dispositivos Cisco em MIBs específicas, consulte o [Cisco SNMP Object Navigator](#) . Isso lista as armadilhas disponíveis para um MIB específico. Para receber uma dessas armadilhas, o Cisco IOS® Software Release deve suportar a MIB listada. Para saber quais MIBs são suportadas em seu dispositivo Cisco, visite www.cisco.com/go/mibs . O MIB deve estar carregado no seu sistema de gerenciamento de rede. Isso é comumente mencionado como compilação. Consulte o guia do usuário do Network Management System (por exemplo, HP OpenView ou NetView) sobre a compilação de MIB em sua plataforma NMS. Consulte também [SNMP: Perguntas frequentes sobre MIBs](#) e [Compiladores MIB e carregamento de MIBs](#).

Além disso, um dispositivo não envia uma interceptação para um sistema de gerenciamento de rede, a menos que esteja configurado para isso. Um dispositivo deve saber que deve enviar uma armadilha. O destino da armadilha é geralmente definido por um endereço IP, mas pode ser um nome de host, se o dispositivo estiver configurado para consultar um servidor de DNS. Em versões posteriores do software Cisco IOS, os administradores de dispositivos podem escolher quais interceptações desejam enviar. Para obter informações sobre como configurar um dispositivo Cisco para SNMP e como enviar interceptações, consulte os guias de configuração de dispositivos correspondentes e o [Guia de Implementação de NMS de Discagem Básica](#), [Traps SNMP do Cisco IOS suportados e Como Configurar](#) e [Como Suportar e Configurar Armadilhas SNMP do Cisco CatalystOS](#).

Observação: o gerenciador geralmente recebe notificações SNMP (TRAPs e INFORMs) na porta UDP número 162.

[Exemplos de armadilhas enviadas pelo Cisco IOS](#)

Esta seção contém alguns exemplos de armadilhas enviadas pelo Cisco IOS, obtidas com **debug snmp packet**.

trap genérico SNMPv1, redefinido pela Cisco:

```
Nov 21 07:44:17: %LINK-3-UPDOWN: Interface Loopback1, changed state to up
4d23h: SNMP: Queuing packet to 172.17.246.162
4d23h: SNMP: V1 Trap, ent products.45, addr 172.17.246.9, gentrap 3, spectrap 0
  ifEntry.1.23 = 23
  ifEntry.2.23 = Loopback1
  ifEntry.3.23 = 24
  lifEntry.20.23 = up
```

Esta saída mostra a armadilha de linkUp redefinida da [CISCO-GENERAL-TRAPS](#) MIB com quatro variáveis vinculadas. Ele tem estes campos:

- *Enterprise* = products.45 ([sysObjectID](#) do dispositivo enviando trap, neste exemplo, é o roteador c7507)
- *Tipo genérico de armadilha* = 3 (linkUp)
- *Código de armadilha específico* = 0

Desvio específico do SNMPv1 Cisco:

```
4d23h: SNMP: Queuing packet to 172.17.246.162
4d23h: SNMP: V1 Trap, ent ciscoSyslogMIB.2, addr 172.17.246.9, gentrap 6, spectrap 1
  clogHistoryEntry.2.954 = LINK
  clogHistoryEntry.3.954 = 4
  clogHistoryEntry.4.954 = UPDOWN
  clogHistoryEntry.5.954 = Interface Loopback1, changed state to up
  clogHistoryEntry.6.954 = 43021184
```

Esta saída mostra a armadilha específica clogMessageGenerated da [CISCO-SYSLOG-MIB](#) com cinco variáveis de associação. Ele tem estes campos:

- *Empresa* = Valor corporativo da armadilha clogMessageGenerated
- *Tipo genérico de armadilha* = 6 (específico da empresa)
- *Código de armadilha específico* = 1 (*código de armadilha específico de clogMessageGenerated*)

Armadilha específica do SNMPv2c Cisco:

```
4d23h: SNMP: Queuing packet to 172.17.246.162
4d23h: SNMP: V2 Trap, reqid 2, errstat 0, erridx 0
  sysUpTime.0 = 43053404
  snmpTrapOID.0 =
  clogHistoryEntry.2.958 = SYS
  clogHistoryEntry.3.958 = 6
  clogHistoryEntry.4.958 = CONFIG_I
  clogHistoryEntry.5.958 = Configured from console by vty0 (10.10.10.10)
  clogHistoryEntry.6.958 = 43053403
```

Esta saída mostra a notificação específica [ciscoConfigManEvent](#) SNMPv2c da [CISCO-CONFIG-MAN-MIB](#) com três variáveis vinculadas:

- [ccmHistoryEventCommandSource](#)
- [ccmHistoryEventConfigSource](#)
- [ccmHistoryEventConfigDestination](#)

Essa armadilha pode ser usada se tiver sido feita alguma alteração na configuração do dispositivo. Os valores dos dois últimos componentes determinam se um comando **show** foi emitido ou se a configuração foi tocada.

```
6506E#term mon
6506E#debug snmp packet
SNMP packet debugging is on

6506E#sh run
Building configuration...
...
6506E#
19:24:18: SNMP: Queuing packet to 10.198.28.80
19:24:18: SNMP: V2 Trap, reqid 2, errstat 0, erridx 0
sysUpTime.0 = 6981747
snmpTrapOID.0 = ciscoConfigManMIB.2.0.1
ccmHistoryEventEntry.3.100 = 1
!--- 1 -> commandLine. Executed via CLI. ccmHistoryEventEntry.4.100 = 3 !--- 3 -> running
ccmHistoryEventEntry.5.100 = 2 !--- 2 -> commandSource. Show command was executed.
```

```
6506E#term mon
6506E#debug snmp packet
SNMP packet debugging is on
```

```
6506E#conf t
Enter configuration commands, one per line. End with CNTL/Z.
6506E(config)#exit
```

```
22:57:37: SNMP: Queuing packet to 10.198.28.80
22:57:37: SNMP: V2 Trap, reqid 2, errstat 0, erridx 0
sysUpTime.0 = 8261709
snmpTrapOID.0 = ciscoConfigManMIB.2.0.1
ccmHistoryEventEntry.3.108 = 1
!--- 1 -> commandLine. Executed via CLI. ccmHistoryEventEntry.4.108 = 2 !--- 2 -> commandSource
ccmHistoryEventEntry.5.108 = 3 !--- 3 -> running. Change was destined to the running
configuration.
```

[Informações Relacionadas](#)

- [Suporte Técnico e Documentação - Cisco Systems](#)