SNMP: Frequently Asked Questions About MIB Theory and Operation

Índice

Introdução

Este documento dão respostas às perguntas geralmente feitas e guiam usuários para encontrar recursos úteis no Simple Network Management Protocol (SNMP) e os assuntos do SNMP enquanto se relaciona ao equipamento da Cisco.

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

A. Em Solaris, use o **comando snoop**, que é ficado situado em */usr/sbin/snoop*.

Note: Você precisa de ser um **usuário de raiz** a fim 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 pode igualmente usar etéreo, que é um analisador de protocolo de rede livre para sistemas Unix e Microsoft windows. Os pacotes SNMP podem ser analisados com liberação etéreo 0.8.0 e mais atrasado. Você pode transferir etéreo da página etéreo da transferência.

Q. Por que eu tenho uma relação com ifDescr = Null0 no ifTable?

A. Até à data da Versão 12.0 do Cisco IOS ® Software, há uma relação com o null0 do ifDescr

que aparece no ifTable.

A interface nula, null0, é uma relação de rede virtual (similar 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 não pôde ser 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. Isto é feito para criar uma rota a uma rede agregada que possa então ser anunciada com o Border Gateway Protocol (BGP), ou para assegurar-se de talvez para efeitos de segurança que o tráfego a um intervalo particular dos endereços não esteja propagado através do roteador.

O roteador sempre tem uma única interface nula, Null0. À revelia, um pacote enviado à interface nula faz com que o roteador responda enviando um mensagem inatingível de protocolo de mensagem de controle de Internet (ICMP) ao endereço IP de origem do pacote. É possível configurar o roteador para enviar estas repostas ou para descartar pacotes de modo silencioso.

A fim desabilitar a emissão dos mensagens que não chega a seu destino do ICMP em resposta aos pacotes enviados à interface nula, datilografe este comando no modo de configuração da interface:

```
no ip unreachables
```

A fim permitir a emissão dos mensagens que não chega a seu destino do ICMP em resposta aos pacotes enviados à interface nula, datilografe este comando no modo de configuração da interface:

```
ip unreachables
```

Q. 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 do atendimento às normas do RFC para um esclarecimento mais adicional para que as colunas a esperar para media diferentes agrupam. Um exemplo deste seria o ATM, que é um pacote do comprimento fixo. Como tal, as fileiras no ifTable (e outro) são baseadas no ifFixedLengthGroup.

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

A. Este comportamento não é um erro. Uma armadilha de partida à frio é normalmente a primeira armadilha (e o primeiro pacote) a ser enviados a um destino de armadilha. O roteador precisa o Address Resolution Protocol (ARP) para o destino de 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. Este é em conformidade com RFC, porque a rede pode igualmente duplicar as armadilhas de partida à frio. A estação do

sistema de gerenciamento de rede (NMS) do cliente deve poder segurá-lo isto (ou então é quebrado).

Note: Para seguir este link de Bug ID e ver a informação detalhada de Bug, você deve ser um usuário registrado (do clientes registrados somente) e você deve ser entrado.

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

A. Cada armadilha é definida em algum MIB. A fim ver a definição exata da armadilha com a lista de objetos contidos nela, encontre a armadilha no SNMP Object Navigator. Por exemplo, você pode ver a armadilha do cctCallSetupNotification do CISCO-CALL-TRACKER-MIB.

Informações Relacionadas

- Dicas técnicas simples de protocolo de gerenciamento de rede
- Suporte Técnico - Cisco Systems