SNMP: Domande frequenti sulla teoria e sul funzionamento di MIB

Sommario

[Introduzione](#)
[Quale strumento è possibile utilizzare per acquisire e analizzare pacchetti SNMP e trap SNMP sulla workstation?](#)
[Perché è presente un'interfaccia con ifDescr = Null0 in ifTable?](#)
[Alcune colonne ifTable non vengono visualizzate per determinati tipi di interfaccia. Perché questo accade? Questo è un bug?](#)
[Vedo due trappole coldstart fuori dalla scatola. Questo è un bug?](#)
[Quali sono esattamente le informazioni contenute in una trap SNMP e dove sono documentate?](#)
[Informazioni correlate](#)

Introduzione

Questo documento contiene le risposte alle domande frequenti e guida gli utenti a trovare risorse utili sui problemi SNMP (Simple Network Management Protocol) e SNMP relativi alle apparecchiature Cisco.

D. Quale strumento posso utilizzare per acquisire e analizzare i pacchetti SNMP e le trap SNMP sulla mia workstation?

R. In Solaris, usare il comando **snoop**, che si trova in */usr/sbin/snoop*.

Nota: per acquisire i pacchetti in transito, è necessario essere un utente **root**.

Ad esempio:

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

In questo esempio viene acquisito un pacchetto. Il *router1 del* dispositivo invia un messaggio SNMP-TRAP (porta UDP 162) all'*host1 del* dispositivo.

Èinoltre possibile utilizzare Etheral, un analizzatore di protocolli di rete gratuito per sistemi UNIX e Microsoft Windows. I pacchetti SNMP possono essere analizzati con Etheral versione 0.8.0 e successive. È possibile scaricare Etheral dalla pagina Etheral Download .

D. Perché è disponibile un'interfaccia con ifDescr = Null0 in ifTable?

A partire dal software Cisco IOS® versione 12.0, nella tabella ifTable è visualizzata un'interfaccia con ifDescr Null0.

L'interfaccia null, Null0, è un'interfaccia di rete virtuale (simile all'interfaccia loopback). Il traffico diretto all'interfaccia di loopback viene indirizzato al router stesso, mentre il traffico inviato all'interfaccia null viene scartato.

L'interfaccia Null potrebbe non essere configurata con un indirizzo. Il traffico può essere inviato a questa interfaccia solo configurando una route statica dove l'hop successivo è l'interfaccia Null0. In questo modo, viene creato un percorso a una rete aggregata che può essere successivamente annunciato tramite il Border Gateway Protocol (BGP), o viene garantito che il traffico verso un particolare intervallo di indirizzi non venga propagato attraverso il router, ad esempio per motivi di sicurezza.

Il router ha sempre un'unica interfaccia null, Null0. Per impostazione predefinita, un pacchetto inviato all'interfaccia null fa sì che il router risponda inviando un messaggio ICMP (Internet Control Message Protocol) non raggiungibile all'indirizzo IP di origine del pacchetto. È possibile configurare il router in modo che invii queste risposte o che ignori automaticamente i pacchetti.

Per disabilitare l'invio di messaggi ICMP "destinazione irraggiungibile" in risposta ai pacchetti inviati all'interfaccia null, digitare questo comando in modalità di configurazione interfaccia:

```
no ip unreachables
```

Per abilitare l'invio di messaggi ICMP "destinazione irraggiungibile" in risposta ai pacchetti inviati all'interfaccia null, digitare questo comando in modalità di configurazione interfaccia:

```
ip unreachables
```

D. Alcune colonne ifTable non vengono visualizzate per determinati tipi di interfaccia. Perché questo accade? Questo è un bug?

R: Non è un bug. L'oggetto ifTable, basato sulla RFC 1573, è progettato in modo specifico in modo che non venga creata un'istanza di alcune colonne di una determinata riga in base a ifType. Leggere la dichiarazione di conformità RFC per ulteriori informazioni sulle colonne da prevedere per i diversi gruppi di supporti. Un esempio è dato dall'ATM, un pacchetto a lunghezza fissa. Di conseguenza, le righe in ifTable (e altre) sono basate su ifFixedLengthGroup.

D. Vedo due trappole coldstart fuori dalla scatola. Questo è un bug?

R. Questo comportamento non è un bug. Una trap con avvio a freddo è in genere la prima trap (e il primo pacchetto) da inviare a una destinazione. Il router deve adottare il protocollo ARP (Address Resolution Protocol) per la destinazione della trap. I dispositivi Cisco rilasciano la trap se è necessario inviare un ARP. Pertanto, molti clienti non vedevano la trappola del coldstart prima della correzione, che doveva essere inviata due volte. Questa funzionalità è conforme allo standard RFC, in quanto la rete può anche duplicare le trap coldstart. La stazione del sistema di gestione della rete (NMS) del cliente dovrebbe essere in grado di gestire questa condizione (o in caso contrario si guasta).

Nota: per seguire il collegamento all'ID del bug e visualizzare informazioni dettagliate, è necessario essere un utente registrato (solo utenti registrati) e aver eseguito l'accesso.

D. Quali sono esattamente le informazioni contenute in una trap SNMP e dove sono documentate?

R. Ogni trap è definita in alcuni MIB. Per visualizzare l'esatta definizione della registrazione dei colori con l'elenco degli oggetti in essa contenuti, individuare la registrazione in SNMP Object Navigator. Ad esempio, è possibile vedere la trap cctCallSetupNotification da CISCO-CALL-TRACKER-MIB.

Informazioni correlate

- Suggerimenti tecnici sul protocollo Simple Network Management
- Supporto tecnico – Cisco Systems