SNMP (Protocolo de administración de red simple): Preguntas frecuentes acerca de la teoría y el funcionamiento de MIB

Contenido

Introducción

Este documento proporciona respuestas a preguntas frecuentes y suministra una guía para que los usuarios puedan encontrar recursos útiles y temas sobre Simple Network Management Protocol (SNMP) asociados al equipo Cisco.

P. ¿Qué herramienta puedo utilizar para capturar y analizar paquetes SNMP y trampas SNMP en mi estación de trabajo?

A. En Solaris, utilice el comando **snoop**, que se encuentra en */usr/sbin/snoop*.

Nota: Debe ser un usuario **raíz** para capturar paquetes en el cable.

Por ejemplo:

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

Este ejemplo capturó un paquete. El dispositivo router1 envía una SNMP-TRAP (puerto UDP 162) al dispositivo host1.

También puede utilizar Ethereal, que es un analizador de protocolo de red gratuito para sistemas UNIX y Microsoft Windows. Los paquetes SNMP se pueden analizar con la versión etérea 0.8.0 y posteriores. Puede descargar Ethereal desde la página de descarga etérea.

P. ¿Por qué tengo una interfaz con ifDescr = Null0 en ifTable?

A. A partir de la versión 12.0 del software Cisco IOS®, hay una interfaz con ifDescr Null0 que aparece en la ifTable.

La interfaz nula, Null0, es una interfaz de red virtual (similar a la interfaz de loopback). Mientras el tráfico a la interfaz de loopback se dirige al router, se descarta el tráfico enviado a la interfaz nula.

Es posible que la interfaz nula no esté configurada con una dirección. Sólo se puede enviar tráfico a esta interfaz al configurar una ruta estática en la que el salto siguiente es la interfaz Null0. Esto se hace para crear una ruta a una red agregada que luego se pueda anunciar a través del protocolo de gateway fronterizo (BGP), o para garantizar que el tráfico a un rango particular de direcciones no se propaga a través del router, tal vez por motivos de seguridad.

El router siempre posee una única interfaz nula, Null0 De forma predeterminada, un paquete enviado a la interfaz nula hace que el router responda enviando un mensaje de protocolo de mensajes de control de Internet (ICMP) inalcanzable a la dirección IP de origen del paquete. Puede configurar el router para que dé estas respuestas o para descartar los paquetes silenciosamente.

Para inhabilitar el envío de mensajes ICMP inalcanzables en respuesta a los paquetes enviados a la interfaz nula, escriba este comando en el modo de configuración de la interfaz:

```
no ip unreachables
```

Para habilitar el envío de mensajes ICMP inalcanzables en respuesta a los paquetes enviados a la interfaz nula, escriba este comando en el modo de configuración de la interfaz:

```
ip unreachables
```

P. Algunas columnas ifTable no aparecen para ciertos tipos de interfaces. ¿Por qué ocurre esto? ¿Es una falla?

A. Esto no es un error. La ifTable, basada en RFC 1573, está diseñada específicamente para que algunas columnas en una fila determinada no se insten sobre la base del ifType. Lea la declaración de conformidad RFC para obtener más información sobre las columnas que se esperan para los distintos grupos de medios. Un ejemplo de esto sería ATM, que es un paquete de longitud fija. Como tal, las filas de ifTable (y otras) se basan en ifFixedLengthGroup.

P. Veo dos procedimientos innovadores de captura de inicio sin presencia de red. ¿Es una falla?

A. Este comportamiento no es un error. Una trampa de inicio en frío es normalmente la primera trampa (y el primer paquete) que se envía a un destino de trampa. El router necesita el protocolo de resolución de direcciones (ARP) para el destino de la trampa. Los dispositivos de Cisco liberan la captura si un ARP debe ser enviado. Por lo tanto, muchos clientes no veían el procedimiento de captura de inicio sin presencia de red antes de la corrección, que era para enviarlo dos veces. Esto es compatible con RFC, ya que la red también puede duplicar las trampas de inicio en frío. La estación del sistema de administración de redes (NMS) del cliente debe poder manejar esto (o si no se rompe).

Nota: Para seguir este enlace de ID de bug y ver información detallada de bug, debe ser un

usuario registrado (sólo clientes registrados) y debe haber iniciado sesión.

P. ¿Cuál es la información exacta contenida en una notificación de trampa SNMP y dónde está documentada?

A. Cada trampa se define en algunos MIB. Para ver la definición exacta de la trampa con la lista de objetos contenidos en ella, busque la trampa en SNMP Object Navigator. Por ejemplo, puede ver la trampa cctCallSetupNotification de CISCO-CALL-TRACKER-MIB.

Información Relacionada

- Consejos técnicos sobre el Protocolo de administración de red simple
- Soporte Técnico - Cisco Systems