

Monitorización Remota - Ejercicios

Gestión de Redes

Ejercicio 1

2

- El operador “Luis” quiere programar una alarma en una sonda RMON (denominada “neon”) con las siguientes características:
 - Monitorizar el número de octetos que recibe el interfaz con ifIndex=12 en la tabla de interfaces, cada 120 segundos.
 - Se debe disparar una alarma de “alta actividad” si en el periodo de observación el valor se incrementa en $14 \cdot 10^7$ octetos (alta actividad) o una alarma de “baja actividad” si los octetos de entrada están por debajo de 1000 (baja actividad).
 - Las alarmas deben guardar un mensaje en el log y enviar un trap con la comunidad public.

Solución: evento

3

```
snmpset -c private neon .1.3.6.1.2.1.16.9.1.1.7.2 integer 4
snmpset -c private neon .1.3.6.1.2.1.16.9.1.1.7.2 integer 2
snmpset -c private neon .1.3.6.1.2.1.16.9.1.1.2.2 string "alta actividad"
snmpset -c private neon .1.3.6.1.2.1.16.9.1.1.3.2 integer 4
snmpset -c private neon .1.3.6.1.2.1.16.9.1.1.4.2 string "public"
snmpset -c private neon .1.3.6.1.2.1.16.9.1.1.6.2 string "Luis"
snmpset -c private neon .1.3.6.1.2.1.16.9.1.1.7.2 integer 1
```

Solución: evento

4

```
snmpset -c private neon .1.3.6.1.2.1.16.9.1.1.7.3 integer 4
snmpset -c private neon .1.3.6.1.2.1.16.9.1.1.7.3 integer 2
snmpset -c private neon .1.3.6.1.2.1.16.9.1.1.2.3 string "baja actividad"
snmpset -c private neon .1.3.6.1.2.1.16.9.1.1.3.3 integer 4
snmpset -c private neon .1.3.6.1.2.1.16.9.1.1.4.3 string "public"
snmpset -c private neon .1.3.6.1.2.1.16.9.1.1.6.3 string "Luis"
snmpset -c private neon .1.3.6.1.2.1.16.9.1.1.7.3 integer 1
```

Solución: alarma

5

```
snmpset -c private neon .1.3.6.1.2.1.16.3.1.1.12.3 integer 2
snmpset -c private neon .1.3.6.1.2.1.16.3.1.1.2.3 integer 120
snmpset -c private neon .1.3.6.1.2.1.16.3.1.1.3.3 objid
    .1.3.6.1.2.1.2.2.1.10.12 – mib no RMON válido en Cisco
snmpset -c private neon .1.3.6.1.2.1.16.3.1.1.4.3 integer 2
snmpset -c private neon .1.3.6.1.2.1.16.3.1.1.6.3 integer 3
snmpset -c private neon .1.3.6.1.2.1.16.3.1.1.7.3 integer 140000000
snmpset -c private neon .1.3.6.1.2.1.16.3.1.1.8.3 integer 1000
snmpset -c private neon .1.3.6.1.2.1.16.3.1.1.9.3 integer 2
snmpset -c private neon .1.3.6.1.2.1.16.3.1.1.10.3 integer 3
snmpset -c private neon .1.3.6.1.2.1.16.3.1.1.11.3 string "Luis"
snmpset -c private neon .1.3.6.1.2.1.16.3.1.1.12.3 integer 1
```

Ejercicio 2

6

- El operador de gestión de una red cuyo nombre de usuario es “user1”, quiere monitorizar cada 10 minutos la evolución temporal del número de paquetes recibidos por el interfaz eth1 (ocupa la tercera fila en la tabla de interfaces) del router “core1” que soporta RMON.
 - Identifique el o los grupos de RMON que hay que programar para activar esta monitorización.
 - Indique detalladamente los comandos snmpset que utilizaría para configurar la sonda RMON, utilizando la comunidad private. Suponga que no hay ninguna monitorización en la sonda, y por lo tanto las tablas de control están vacías. Asigne valores arbitrarios a los parámetros de los que no se indique el valor en el enunciado.

Solución: history

7

- rmon = 1.3.6.1.2.1.16 → historyControlTable
- Configurar rmon.history (rmon.2) para capturar la evolución temporal de dichos contadores

```
snmpset -c private core1 1.3.6.1.2.1.16.2.1.1.7.1 i 2
```

```
snmpset -c private core1 1.3.6.1.2.1.16.2.1.1.2.1 o  
1.3.6.1.2.1.2.2.1.1.3
```

```
snmpset -c private core1 1.3.6.1.2.1.16.2.1.1.3.1 i 100
```

```
snmpset -c private core1 1.3.6.1.2.1.16.2.1.1.5.1 i 600
```

```
snmpset -c private core1 1.3.6.1.2.1.16.2.1.1.6.1 s user1
```

```
snmpset -c private core1 1.3.6.1.2.1.16.2.1.1.7.1 i 1
```

Ejercicio 3

8

- Un operador de gestión (cuyo nombre de usuario es “oper1”) quiere programar una sonda RMONv1 integrada en un router IP Cisco (al que accede mediante la dirección IP 172.14.23.1), para que genere un trap al gestor cuando la tasa de datagramas IP reenviados por el router supera el 80% de la capacidad de reenvío del mismo, que es 6 Mpps (millones de paquetes por segundo).
- Los traps generados llevarán la comunidad “ciscotrap”.
- El sistema tendrá histéresis, es decir no volverá a saltar una alarma hasta que la tasa de reenvío baje del 60 % de la capacidad del router
- Nota: Para configurar el ciclo de histéresis programe los dos umbrales con alarma pero sólo generará evento de alarma cuando se supera el 80%.

Ejercicio 3 (cont)

9

- El agente de gestión del router tiene definida una comunidad de lectura en la vista RMON “rmonpub” y una comunidad de escritura en la vista de RMON “rmonpriv”.
- Escriba la secuencia de comandos setsnmp para programar el router.
- Notas:
 - Supondremos que la implementación de RMON en los routers Cisco tienen capacidad de monitorizar OIDs de las mib-2.
 - Escriba un único comando set por cada OID.
 - Para programar la sonda comience poniendo el status inicial y la final cuando estén introducidas todas las columnas de la fila correspondiente ponga status con valor valid.
 - El operador conoce que la tabla de control de alarmas tiene la fila 3 libre y la de eventos tiene la fila 5 libre.

Solución: eventos

10

```
snmpset -c rmonpriv 172.14.23.1 1.3.6.1.2.1.16.9.1.1.7.5 integer 2
snmpset -c rmonpriv 172.14.23.1 1.3.6.1.2.1.16.9.1.1.2.5 string
    "Alarma: nivel reenvio"
snmpset -c rmonpriv 172.14.23.1 1.3.6.1.2.1.16.9.1.1.3.5 integer 3
snmpset -c rmonpriv 172.14.23.1 1.3.6.1.2.1.16.9.1.1.4.5 string
    "ciscotrap"
snmpset -c rmonpriv 172.14.23.1 1.3.6.1.2.1.16.9.1.1.6.5 string
    "Oper1"
snmpset -c rmonpriv 172.14.23.1 1.3.6.1.2.1.16.9.1.1.7.5 integer 1
```

Solución: alarmas

11

```
snmpset -c rmonpriv 172.14.23.1 1.3.6.1.2.1.16.3.1.1.12.3 integer 2
snmpset -c rmonpriv 172.14.23.1 1.3.6.1.2.1.16.3.1.1.2.3 integer 1
snmpset -c rmonpriv 172.14.23.1 1.3.6.1.2.1.16.3.1.1.3.3 objid
.1.3.6.1.2.1.4.6.0
snmpset -c rmonpriv 172.14.23.1 1.3.6.1.2.1.16.3.1.1.4.3 integer 2
snmpset -c rmonpriv 172.14.23.1 1.3.6.1.2.1.16.3.1.1.6.3 integer 3
snmpset -c rmonpriv 172.14.23.1 1.3.6.1.2.1.16.3.1.1.7.3 integer 4800000
snmpset -c rmonpriv 172.14.23.1 1.3.6.1.2.1.16.3.1.1.8.3 integer 3600000
snmpset -c rmonpriv 172.14.23.1 1.3.6.1.2.1.16.3.1.1.9.3 integer 5
snmpset -c rmonpriv 172.14.23.1 1.3.6.1.2.1.16.3.1.1.10.3 integer 0
snmpset -c rmonpriv 172.14.23.1 1.3.6.1.2.1.16.3.1.1.11.3 string "Oper1"
snmpset -c rmonpriv 172.14.23.1 1.3.6.1.2.1.16.3.1.1.12.3 integer 1
```

Ejercicio 4

12

- Una red consiste en 4 hosts conectados en estrella mediante un conmutador Ethernet con 8 interfaces (eth0..eth7) y con soporte RMONv1.
- La sonda RMONv1 está internamente conectada al bus del conmutador que representa al interfaz (if0).
- Este interfaz es el primero de la tabla de interfaces (por este interfaz se observa el tráfico de todos los interfaces de red del conmutador).
- Se quiere monitorizar el tráfico entre cada pareja de hosts.
- Describa el proceso de configuración de la sonda RMON, detallando los comandos utilizados desde una consola de gestión.
- Considere que el administrador accede al agente de gestión del conmutador mediante la dirección IP 173.28.28.3 y la comunidad admin. El nombre del propietario de las monitorizaciones en la sonda es administrador.

Solución 1

13

- Hay que configurar el grupo matrix 1.3.6.1.2.1.16.6.
- El interface del cual se recolectan los datos es 1.3.6.1.2.1.2.2.1.1.1
- Los objetos de escritura de la tabla de matrixControl toman los valores:
- matrixControlDataSource (1.3.6.1.2.1.16.6.1.2.x) = 1.3.6.1.2.1.2.2.1.1.1
- matrixControlOwner (1.3.6.1.2.1.16.6.1.5.x) = administrator
- matrixControlStatus (1.3.6.1.2.1.16.6.1.6.x) = 2 (createRequest)

Solución 2

14

- Se puede leer la tabla para buscar un valor libre de índice o bien seleccionar uno al azar y comprobar que la sonda no lo anula.
- Seleccionamos por ejemplo el índice $x=3$
- `snmpset 173.28.28.3 admin 1.3.6.1.2.1.16.6.1.6.3 i 2`
- Leemos el estado de la fila 3:
- `status = snmpget 173.28.28.3 admin 1.3.6.1.2.1.16.6.1.6.3`
- Si `status = 3` (underCreation) pasamos a estado valid
- Si no seleccionamos otro índice y repetimos el proceso.

```
snmpset 173.28.28.3 admin 1.3.6.1.2.1.16.6.1.2.3 o 1.3.6.1.2.1.2.2.1.1.1
```

```
snmpset 173.28.28.3 admin 1.3.6.1.2.1.16.6.1.5.3 s administrator
```

```
snmpset 173.28.28.3 admin 1.3.6.1.2.1.16.6.1.6.3 i 1
```

Configuración Eventos en Cisco

15

□ Sintaxis

```
rmon event eventIndex [log] [trap eventCommunity] [description  
eventDescription] [owner eventOwner]
```

□ Ejemplo:

```
rmon event 2 log trap public description "Alta actividad" owner "luis"
```

http://www.cisco.com/en/US/docs/ios/12_2/configfun/command/reference/frf016.html#wp1046781

Configuración Alarmas en Cisco

16

□ Sintaxis

```
rmon alarm alarmIndex alarmVariable alarmInterval {absolute |  
delta} rising-threshold alarmRisingThreshold  
[alarmRisingEventIndex] falling-threshold alarmFallingThreshold  
[alarmFallingEventIndex] [owner alarmOwner]
```

□ Ejemplo:

```
rmon alarm 5 ifEntry.10.4 60 absolute rising-threshold 30000 1  
falling-threshold 5000 2 owner "luis"
```