

# SNMP

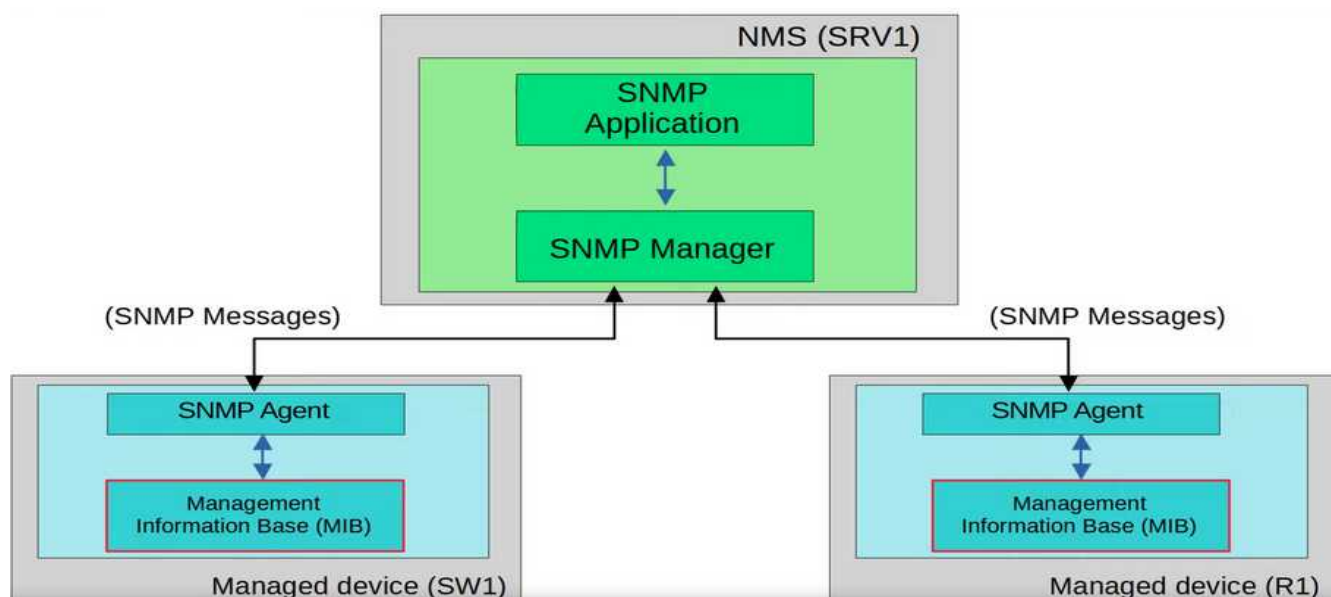
## Índice

Introducción.....	2
OID.....	2
Componentes SNMP:.....	3
Administrador de SNMP (NMS).....	3
Agente SNMP.....	3
Base de información de gestión (MIB).....	3
Notificaciones/traps SNMP:.....	3
Comandos SNMP básicos:.....	4
Puertos.....	5
SNMPv1 y 2.....	5
Configuración SNMPv2c.....	6
SNMPv3.....	7
Configuración de SNMPv3.....	7
Configurador del administrador de SNMP.....	10
Seguridad.....	11
SYSLOG.....	12
Localizaciones.....	12
Ejemplo de configuración.....	13

# Introducción

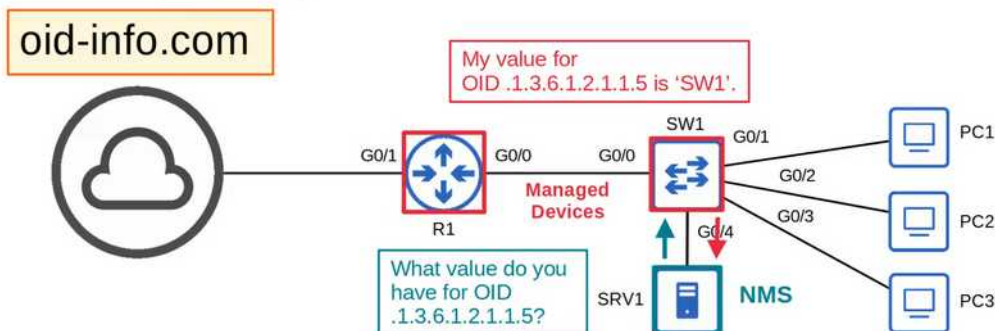
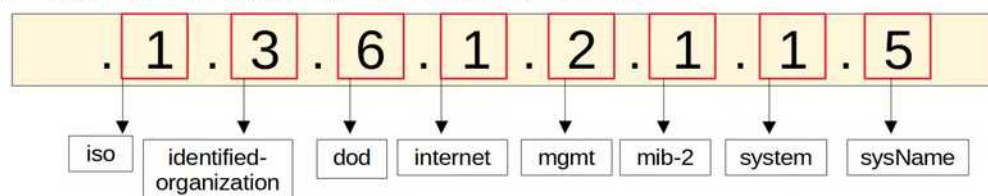
**SNMP** (Simple Network Management Protocol) es un protocolo de gestión de red que se utiliza para administrar (controlar y monitorear) los dispositivos de infraestructura de red (routers, switches, firewall, balanceadores de carga, servidores, cámaras CCTV y dispositivos inalámbricos).

Permite que un dispositivo de red comparta información sobre sí mismo y sus actividades.



## OID

- SNMP Object IDs are organized in a hierarchical structure.



## Componentes SNMP:

Un sistema SNMP completo consta de las siguientes tres partes:

- Administrador de SNMP
- Agente SNMP
- Base de Información de Gestión (MIB)

### Administrador de SNMP (NMS)

El administrador SNMP normalmente es una aplicación que se ejecuta en una ubicación central. Puede solicitar (sondear) información de dispositivos o agentes administrados por SNMP (enrutadores, conmutadores, servidores de red, etc.). El administrador SNMP también puede recibir información no solicitada, conocida como "trampa", desde un dispositivo administrado por SNMP



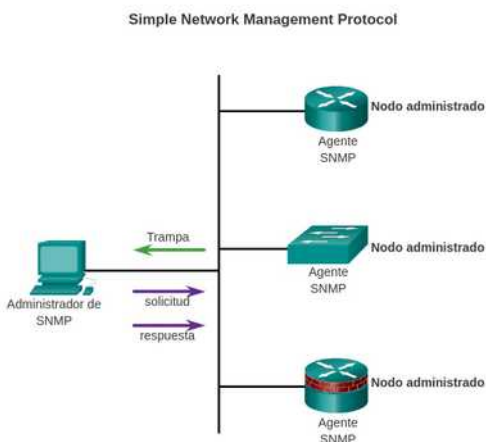
### Agente SNMP

El agente SNMP es el software cliente SNMP que se ejecuta en un dispositivo administrado por SNMP, como un enrutador, un conmutador o un servidor. Todos los tipos de datos son recopilados por el propio dispositivo y sus actividades se almacenan en una base de datos local denominada Base de Información de Gestión (MIB).

El agente puede entonces responder a sondeos (solicitudes) y consultas SNMP con información de la base de datos y puede enviar alertas no solicitadas o "traps" a un administrador SNMP.

### Base de información de gestión (MIB)

Es una base de datos que contiene una colección de información organizada jerárquicamente (estructura de árbol). Todo el MIB es en realidad una colección de variables (OID) que se almacenan en MIB individuales y más granulares que forman las ramas del árbol.



## Notificaciones/traps SNMP:

Una característica clave de SNMP es la capacidad de generar notificaciones desde un agente SNMP. Estas notificaciones no requieren que se envíen solicitudes (sondeos) desde el administrador SNMP.

Las notificaciones no solicitadas (asíncronas) se pueden generar como trampas (traps) o solicitudes de información. Las trampas son mensajes que alertan al administrador de SNMP sobre una condición en la red.

Las solicitudes de informe (informes) son trampas que incluyen una solicitud de confirmación de recepción del administrador SNMP.

## Comandos SNMP básicos:

Message Class	Description	Messages
Read	Messages sent by the <b>NMS</b> to read information from the <b>managed devices</b> . (ie. What's your current CPU usage %?)	<i>Get</i> <i>GetNext</i> <i>GetBulk</i>
Write	Messages sent by the <b>NMS</b> to change information on the <b>managed devices</b> . (ie. change an IP address)	<i>Set</i>
Notification	Messages sent by the <b>managed devices</b> to alert the <b>NMS</b> of a particular event. (ie. interface going down)	<i>Trap</i> <i>Inform</i>
Response	Messages sent in response to a previous message/request.	<i>Response</i>

**GET:** - La operación GET es una solicitud que envía el administrador al dispositivo administrado. Se realiza para recuperar uno o más valores del dispositivo administrado.

**GET NEXT:** - Esta operación es similar a GET. La diferencia significativa es que la operación GET NEXT recupera el valor del siguiente OID en el árbol MIB.

**GET BULK:** - La operación GETBULK se utiliza para recuperar datos voluminosos de una tabla MIB

**SET:** - Esta operación es utilizada por los administradores para modificar o asignar el valor del dispositivo administrado.

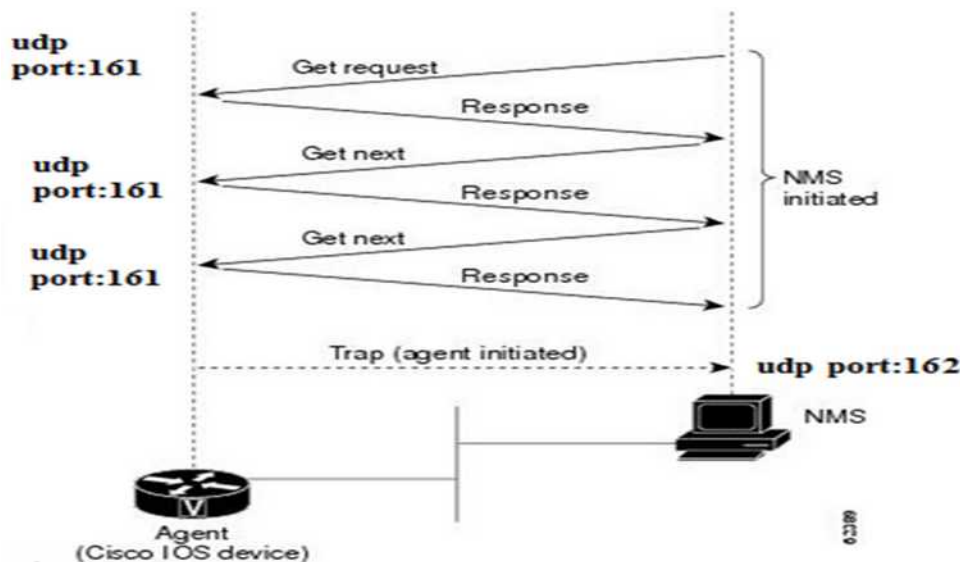
**TRAPS:** a diferencia de los comandos anteriores que se inician desde el Administrador SNMP, los TRAPS son iniciados por los Agentes. Es una señal que el Agente envía al Administrador SNMP cuando ocurre un evento. (El Administrador no envía ACK)

**INFORM:** - Este comando es similar al TRAP iniciado por el Agente, adicionalmente INFORM incluye confirmación del administrador SNMP al recibir el mensaje. (un ACK)

**RESPONSE:** - Es el comando utilizado para devolver el valor(es) o señal de las acciones dirigidas por el Administrador SNMP.

## Puertos

SNMP utiliza UDP como transporte y utiliza los números de puerto: 161 y 162. NMS (SNMP Manager) utiliza el puerto UDP 161 para solicitar (sondear) MIB del agente SNMP. El agente SNMP utiliza el puerto UDP 162 para enviar trampas o informar solicitudes al administrador SNMP.



## SNMPv1 y 2

Para que SNMP funcione, NMS debe tener acceso a la MIB. Para asegurar que las solicitudes de acceso sean válidas, debe haber cierta forma de autenticación.

SNMPv1 y SNMPv2c usan **cadenas de comunidad** que controlan el acceso a la MIB. Las cadenas de comunidad son contraseñas de texto no cifrado. Las cadenas de la comunidad de SNMP autentican el acceso a los objetos MIB.

Existen dos tipos de cadenas de comunidad:

- Solo lectura (ro):** proporciona acceso a las variables de MIB, pero no permite realizar cambios a estas variables, solo leerlas. Debido a que la seguridad es mínima en la versión 2c, muchas organizaciones usan SNMPv2c en modo de solo lectura.

- Lectura y escritura (rw):** proporciona acceso de lectura y escritura a todos los objetos de la MIB.

Para ver o establecer variables de MIB, el usuario debe especificar la cadena de comunidad correspondiente para el acceso de lectura o escritura.

**Nota:** las contraseñas de texto no cifrado no se consideran un mecanismo de seguridad. Esto se debe a que las contraseñas de texto no cifrado son sumamente vulnerables a los ataques man-in-the-middle (intermediario), en los que se ven comprometidas a través de la captura de paquetes.

## Configuración SNMPv2c

Paso 1. (Obligatorio) Configure la cadena de comunidad y el nivel de acceso (solo lectura o lectura y escritura), basicamente son como passwords, mediante el comando

```
R1(config)# snmp-server community cadena ro | rw [nombreACL]
```

```
R1(config)# snmp-server community rodeira1 ro SNMP_ACL
```

```
R1(config)# snmp-server community rodeira2 rw SNMP_ACL
```

Si no especificamos community strings se usará public y private.

Paso 2. (Optativo) Registre la ubicación del dispositivo mediante el comando snmp-server location

Paso 3. (Optativo) Registre el contacto del sistema mediante el comando snmp-server contact texto.

```
R1(config)# snmp-server contact email
```

```
R1(config)# snmp-server location localización
```

```
R1(config)# snmp-server location IES de Rodeira
```

```
R1(config)# snmp-server contact manuel.sanchez@iesrodeira.gal
```

Paso 4. (Optativo) Restrinja el acceso de SNMP a los hosts NMS (administradores de SNMP) que autoriza una ACL: defina la ACL y, a continuación, nombre la ACL con el comando snmp-server community *cadena* número-o-nombre-lista-acceso. Si no hacemos ACL en el paso 1 no la ponemos

```
R1(config)# ip access-list standard nombreACL
```

```
R1(config-std-nacl)# permit IP
```

```
R1(config)# ip access-list standard SNMP_ACL
```

```
R1(config-std-nacl)# permit 192.168.1.3
```

Paso 5. (Optativo) Especifique el destinatario de las operaciones de trap de SNMP con el comando

```
R1(config)# snmp-server host id-host [version 1 | 2c | 3 [auth | noauth | priv]] cade na
```

```
R1(config)# snmp-server host 192.168.1.3 version 2c rodeira1
```

De manera predeterminada, no se define ningún administrador de traps.

Paso 6. (Optativo) Habilite las traps en un agente SNMP con el comando

```
R1(config)# snmp-server enable traps tipos-notificación
```

```
R1(config)# snmp-server enable traps
```

Si no se especifica ningún tipo de notificación de traps en este comando, entonces se envían todos los tipos de trap. Es necesario el uso reiterado de este comando si se desea un subconjunto determinado de tipos de trap.

Ejemplos

```
R1(config)# snmp-server enable traps config -- cambios de configuracion
```

```
R1(config)# snmp-server enable traps snmp linkdown linkup -- cambios interfaces
```

# SNMPv3

SNMPv1 y SNMPv2 son versiones antiguas y ya no las utilizan las organizaciones. Por lo tanto, no hablaremos de las configuraciones de esas versiones. Sólo hablaremos de SNMPv3. SNMPv3 proporciona mejoras significativas para abordar las debilidades de seguridad existentes en las versiones anteriores.

**Integridad** del mensaje: garantizar que un paquete no haya sido modificado durante el tránsito.

**Autenticación**: garantizar que el mensaje proviene de una fuente válida en la red.

**Privacidad** (cifrado): mediante el uso de cifrado para cifrar el contenido de un paquete.

Niveles de seguridad de SNMPv3: el agente SNMPv3 admite los siguientes tres niveles de seguridad

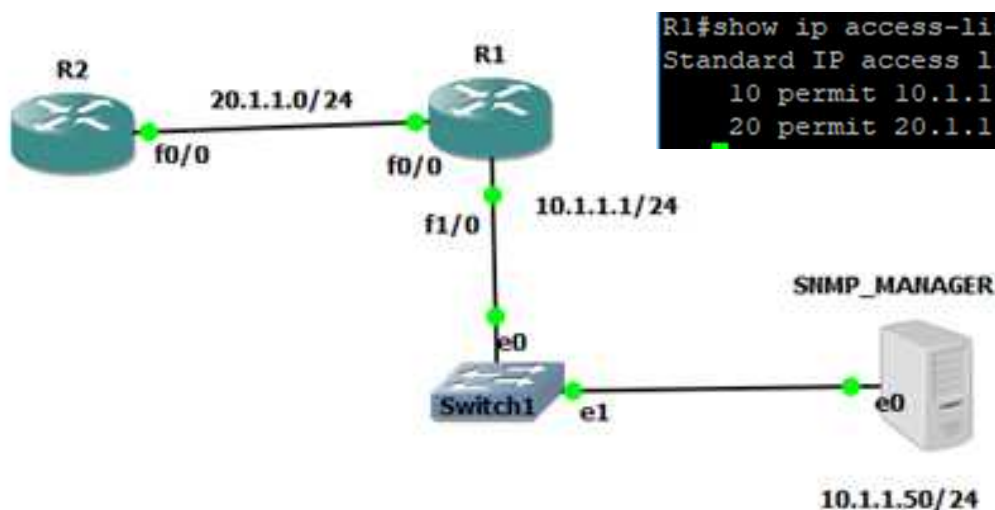
noAuthnoPriv - Comunicación sin autenticación ni privacidad.

authNoPriv - Comunicación con autenticación y sin privacidad.

authPriv - Comunicación con autenticación y privacidad.

Los protocolos utilizados para la autenticación son MD5 y SHA; y para la privacidad, se pueden utilizar los protocolos DES (Data Encryption Standard) y AES (Advanced Encryption Standard).

## Configuración de SNMPv3



Aquí, 10.1.1.1(R1) y 20.1.1.1(R2) son los agentes SNMP, y tenemos nuestro administrador SNMP en 10.1.1.50.

Lo primero que queremos hacer es definir un grupo de servidores SNMP. Esto creará algunas políticas de seguridad específicas que podemos aplicar a varios usuarios. Y cualquier usuario que asignemos a un grupo de servidores en particular tendrá la política de seguridad asociada.



### R1# show snmp mib

Este comando nos proporciona una lista muy larga de las bases de información de administración de esas MIB. Estos son ejemplos de OID. Tengamos en cuenta el OID ifInErrors; vamos a utilizar este OID en nuestra configuración de SNMPv3. Es sensible a mayúsculas y minúsculas. Este OID ifInErrors es para proporcionar errores de entrada de interfaz.

```
R1#show snmp mib
system.1
system.2
sysUpTime
system.4
system.5
system.6
system.7
system.8
sysOREntry.2
sysOREntry.3
sysOREntry.4
ifNumber
ifIndex
ifDescr
ifType
ifMtu
ifSpeed
ifPhysAddress
ifAdminStatus
ifOperStatus
ifLastChange
ifInOctets
ifInUcastPkts
ifInNUcastPkts
ifInDiscards
ifInErrors
ifInUnknownProtos
ifOutOctets
ifOutUcastPkts
ifOutNUcastPkts
ifOutDiscards
ifOutErrors
--More--
```



Ahora, configuremos una vista específica para los usuarios. Esto nos permitirá especificar solo ciertas cosas que se pueden recopilar mediante la vista SNMP.

**R1(config)# snmp-server view helpdesk ifInErrors include**

Aquí, helpdesk es el nombre de la vista y ifInErrors es el OID que desea incluir. Puedes repetir este comando una y otra vez con los diferentes OID que desees agregar. Si no configuras una vista, todas estas variables MIB serán visibles para los usuarios.

**R1(config)# snmp-server group admin v3 priv read helpdesk access 1**

Aquí, admin es el nombre del grupo, helpdesk es el nombre de la vista y 1 es el número de ACL.

Ahora, necesitamos configurar un nombre de usuario que un administrador SNMP usará para comunicarse con nosotros.

**R1(config)# snmp-server user manuel admin v3 auth sha abc123 priv aes 256 cba321 access 1**

Aquí, manuel es el nombre de usuario, admin es el nombre del grupo, abc123 es la contraseña de autenticación, cba321 es la contraseña de privacidad y 1 es el número de ACL. Es un solo comando de una sola longitud.

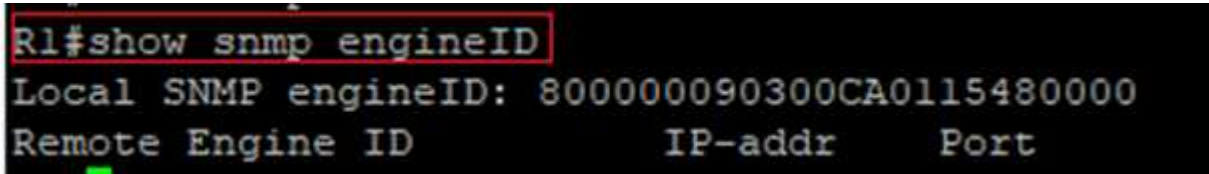
Hay un comando más a tener en cuenta para identificar el administrador SNMP por dirección IP.

**1(config)# snmp-server host 10.1.1.50 informs version 3 priv robert**

Esto completará nuestra configuración SNMPv3.

Ahora, veamos algunos comandos de visualización:

**R1# show namp engineID**



```
R1#show snmp engineID
Local SNMP engineID: 800000090300CA0115480000
Remote Engine ID      IP-addr      Port
```

El engineID es algo específico de SNMPv3 que identifica cada dispositivo SNMPv3 único en la red y que es generado por el enrutador.

**R1# show snmp user**

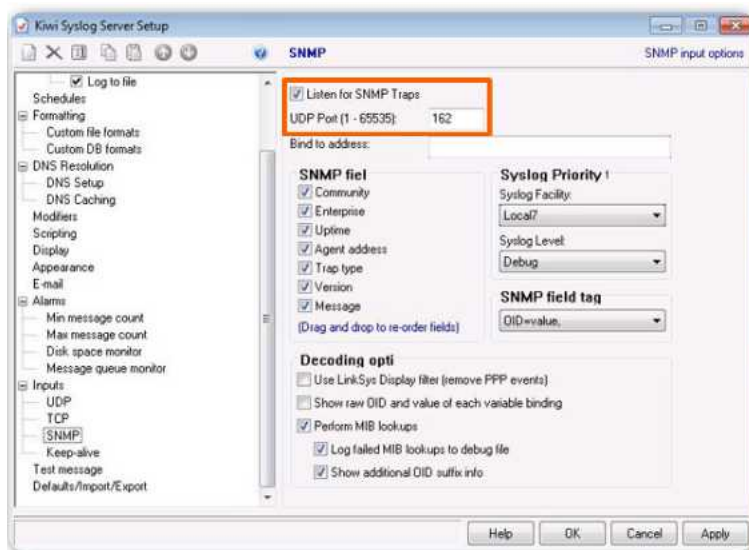
**R1# show snmp group**

# Configurador del administrador de SNMP

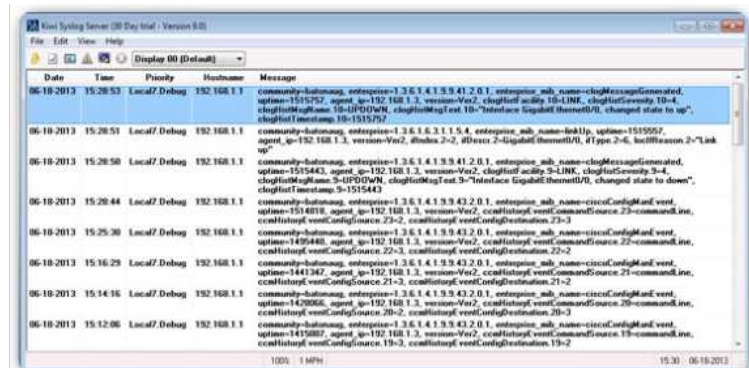
Existen varias soluciones de software para ver el resultado de SNMP. Para nuestros fines, el servidor de syslog Kiwi muestra los mensajes de SNMP asociados a las traps de SNMP.

El PC1 y el R1 están configurados para demostrar el resultado en un administrador de SNMP en relación con las traps de SNMP. Se asignó la dirección IP 192.168.1.3/24 al PC1. El servidor de syslog Kiwi está instalado en PC1.

Después de que se configura el R1, cada vez que ocurre un evento que califique como trap, se envían traps de SNMP al administrador de SNMP. Por ejemplo, si se activa una interfaz, se envía una trap al servidor. Los cambios de configuración en el router también activan el envío de traps de SNMP al administrador de SNMP. Se puede ver una lista de más de 60 tipos de notificación de traps con el comando **snmp-server enable traps ?**.



En la figura izquierda se activó una casilla de verificación en el menú Setup (Configuración) para indicar que el administrador de red desea que el software del administrador de SNMP escuche para detectar las traps de SNMP en el puerto UDP 162.



En la figura, la fila superior del resultado de trap de SNMP que se muestra indica que el estado de la interfaz GigabitEthernet0/0 cambió a up (activo). Además, cada vez que se pasa del modo EXEC privilegiado al modo de configuración global, el administrador de SNMP recibe una trap, como se muestra en la fila resaltada.

Para verificar la configuración SNMP el comando más útil es simplemente el comando **show snmp**, ya que muestra la información que suele ser de interés al examinar la configuración SNMP. A menos que haya una configuración SNMPv3 involucrada, la mayoría de las otras opciones de comandos solo muestran partes seleccionadas del resultado del comando show snmp.

El resultado del comando show snmp no muestra información relacionada con la cadena de comunidad SNMP o, si corresponde, con la ACL asociada. Use el comando **show snmp community**.

# Seguridad

Si bien SNMP es muy útil para el monitoreo y la resolución de problemas, también puede crear vulnerabilidades de seguridad. Por este motivo, antes de implementar SNMP, tenga en cuenta las prácticas recomendadas de seguridad.

SNMPv1 y SNMPv2c dependen de las cadenas de comunidad SNMP en texto no cifrado para autenticar el acceso a los objetos de la MIB. Estas cadenas de comunidad, al igual que todas las contraseñas, se deben elegir cuidadosamente para asegurar que no sean demasiado fáciles de descifrar. Además, las cadenas de comunidad se deben cambiar a intervalos regulares y de acuerdo con las políticas de seguridad de la red. Por ejemplo, se deben cambiar las cadenas cuando un administrador de red cambia de función o deja la empresa. Si SNMP se utiliza solo para monitorear los dispositivos, use comunidades de solo lectura. No deje las cadenas por defecto que son public para ro y private para rw

Asegúrese de que los mensajes de SNMP no se propaguen más allá de las consolas de administración. Se deben usar ACL para evitar que los mensajes de SNMP se envíen más allá de los dispositivos requeridos. También se deben usar ACL en los dispositivos monitoreados para limitar el acceso solamente a los sistemas de administración.

Se recomienda SNMPv3 porque proporciona autenticación y cifrado de seguridad. Existen otros comandos del modo de configuración global que puede implementar un administrador de red para aprovechar la autenticación y el cifrado en SNMPv3:

El comando `snmp-server group nombre-grupo {v1 | v2c | v3 {auth | noauth | priv}}` crea un nuevo grupo SNMP en el dispositivo.

El comando `snmp-server user nombre-usuario nombre-grupo v3 [encrypted] [auth {md5 | sha} contraseña-aut] [priv {des | 3des | aes {128 | 192 | 256}} contraseña-priv]` se usa para agregar un nuevo usuario al grupo SNMP especificado en el comando `snmp-server group nombre-grupo`.

# SYSLOG

syslog es un protocolo estándar de la industria que guarda los acontecimientos que han sucedido en un dispositivo en un log. Por ejemplo interfaces up/down, cambios en OSPF, restarts. Estos eventos pueden verse en la consola a medida que suceden pero también pueden guardarse en la RAM del dispositivo o en un servidor externo. Estos logs son muy importantes.

```
R1(config)#int g0/0
R1(config-if)#no shutdown
R1(config-if)#
*Feb 11 03:02:55.304: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up
*Feb 11 03:02:56.305: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
```

Syslog y SNMP son usados para monitorizar problemas en los dispositivos, son complementarios pero sus funcionalidades son diferentes.

Formato del mensaje

**seq:time stamp: %facility-severity-MNEMONIC:description**

**seq** : numero de secuencia

**time stamp** : timestamp indicando cuando se ha generado el mensaje. Tanto este como el anterior puede que no se muestren dependiendo de la configuración del dispositivo

**facility**: que proceso ha lanzado el mensaje

**severity** : numero que indica la severidad del problema

**MNEMONIC**: codigo corto del mensaje que indica qué ha pasado

**description** : descripción del evento.

Level	Keyword	Description
0	Emergency	System is unusable
1	Alert	Action must be taken immediately
2	Critical	Critical conditions
3	Error	Error conditions
4	Warning	Warning conditions
5	Notice	Normal but significant condition ( <b>Notification</b> )
6	Informational	Informational messages
7	Debugging	Debug-level messages

## Localizaciones

**Consola**: Todos los mensajes se muestran en la consola por defecto

**VTY lines**: Los mensajes serán mostrados en las conexiones telnet/ssh. Deshabilitado por defecto

**Buffer**: Se colocarán en la RAM. Deshabilitado por defecto. Pueden verse con **show logging**

**Servidores externos**: Podemos configurar el dispositivo para enviar los mensajes de log a un servidor externo que escuchará en el puerto **UDP 514**

## Ejemplo de configuración

```
!configure logging to the console line
R1(config)#logging console 6

!configure logging to the vty lines
R1(config)#logging monitor informational

!configure logging to the buffer
R1(config)#logging buffered 8192 6

!configure logging to an external server
R1(config)#logging 192.168.1.100

R1(config)#logging host 192.168.1.100

R1(config)#logging trap debugging
```

El nivel podemos ponerlo como el número o el nombre, como en este caso 6 o informational.

El nivel indicado asume que se mostrarán los niveles menores o iguales a ese.

En el buffer podemos poner el tamaño del buffer o quedará el que tenga por defecto

logging server-ip o logging host es el mismo comando. Para indicar el nivel necesitamos otro comando distinto. Logging trap

Aunque hayamos configurado el logging monitor, los mensajes de syslog no se mostrarán en un telnet/ssh .

Tenemos que poner el siguiente comando cada vez que nos loguemos en el dispositivo.

```
R1#terminal monitor
```

Recordemos poner el logging synchronous para que los mensajes mostrados en el CLI en el medio de un comando resulte en una nueva linea en la que podamos seguir tecleando el comando.

```
R1(config)#line console 0
R1(config-line)#logging synchronous
```

R1(config)#service timestamps log datetime msec habilita el logging con timestamps