Router Teldat

Agente SNMP

Doc. *DM712* Rev. *10.00*
Marzo, 2003

ÍNDICE

Capítulo 1
Introducción al protocolo SNMP

1. Introducción

SNMP es un protocolo de nivel 7 (nivel de aplicación) según el modelo OSI (Open Systems Interconnection), para monitorizar características operativas del router.

SNMP permite, a las estaciones de trabajo de la red, leer y modificar algunos de los parámetros del router. Posibilita a un software ejecutándose en una estación remota, contactar a través de la red con el router y obtener información actualizada de dicho router. Por lo tanto, se puede llevar a cabo una gestión centralizada de los routers existentes en la red.

Entre las facilidades básicas de SNMP se incluyen:

- La recogida de información y la modificación de los parámetros operativos del router por parte de los usuarios SNMP remotos.
- El envío y la recepción de paquetes SNMP a través del protocolo IP.

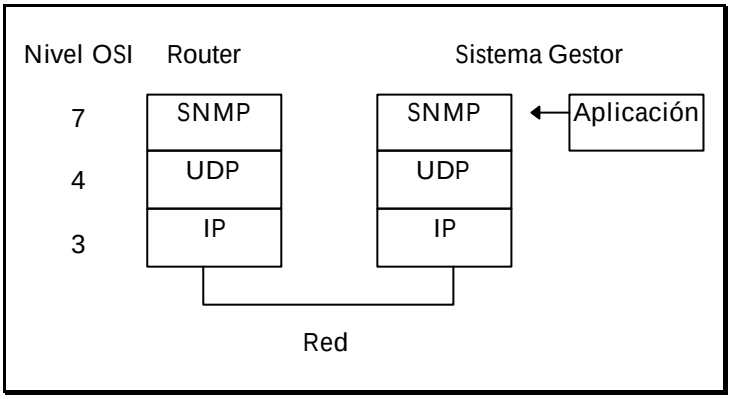

Figura 1: Niveles de protocolo del entorno SNMP

El software que procesa las peticiones SNMP se ejecuta en el router y se llama agente SNMP. El programa de usuario que construye las peticiones SNMP se ejecuta en cualquier estación de usuario de la red, no en el router, y se llama gestor SNMP. El agente SNMP en el router y el gestor en la estación de trabajo usan ambos el protocolo UDP para intercambiar los paquetes.

Para más información sobre SNMP, ver la recomendación RFC 1157, *A Simple Network Management Protocol.* Las recomendaciones RFC 1212 y 1213 contienen una descripción de las variables SNMP, y explican cómo usar el protocolo y los formatos de los paquetes que se emplean.

2. Tipos de paquetes SNMP

Los tipos de paquetes SNMP reflejan las funciones básicas del protocolo, estos son:

- Paquete GET REQUEST. Viaja del usuario al router. Contiene peticiones de información del software de usuario. Espera respuesta de la variable pedida.
- Paquete GET NEXT REQUEST. Viaja del usuario al router. Contiene peticiones de información del software de usuario. Espera respuesta de la siguiente variable a la pedida, según el orden del árbol de información en el agente.
- Paquete SET REQUEST. Viaja del usuario al router. Contiene peticiones del software de usuario para modificar los parámetros operativos del router.
- Paquete GET RESPONSE. Viaja del router al usuario. Contiene las respuestas de las peticiones del software de usuario enviadas en los paquetes GET REQUEST, GET NEXT REQUEST y SET REQUEST.
- Paquete TRAP MESSAGE. Viaja del router al usuario. Contiene información del router no solicitada por el usuario. Se usa para informar de problemas o sucesos importantes en el router, como por ejemplo: "Un interfaz en el router se ha venido abajo".

3. Autenticación

Las entidades que residen en las estaciones de gestión y los elementos de red con los que se comunican usando el protocolo SNMP reciben el nombre de entidades de aplicación SNMP. La pareja formada por un agente SNMP y un conjunto arbitrario de entidades de aplicación SNMP (gestores) recibe el nombre de comunidad SNMP. Cada comunidad SNMP se nombra con una ristra de caracteres, llamada nombre de la comunidad o simplemente comunidad.

Los paquetes SNMP que viajan entre las entidades de aplicación SNMP incluyen el nombre de la comunidad en uno de sus campos. Para determinar si un mensaje entrante representa una petición legítima de un usuario autorizado, o una petición accidental o malintencionada de un usuario no autorizado, SNMP utiliza varios conjuntos de reglas, llamados esquemas de autenticación o simplemente autenticación.

La autenticación evita que usuarios no autorizados obtengan información o modifiquen parámetros operativos del router. En particular, el protocolo de autenticación permite que, tanto el agente como el gestor SNMP, puedan ignorar y descartar peticiones de usuarios no autorizados.

La implementación actual de SNMP ofrece un esquema de autenticación simple por el que en cada elemento de red se definen un conjunto de nombres de comunidad permitidos. Estos nombres de comunidad llevan asociados:

- las direcciones de los gestores de los que aceptarán peticiones y a los que mandarán alarmas (traps)
- las variables a las que el nombre de comunidad tiene acceso
- el tipo de acceso a las mismas

Cada paquete SNMP que llegue al router será validado o descartado según cumpla o no las restricciones impuestas por el esquema de autenticación. En concreto, la variable accedida, su tipo de acceso y la dirección IP origen del paquete SNMP deberán estar incluidas en las asociadas al nombre de comunidad del paquete SNMP.

Este esquema de autenticación es configurable en cada elemento de red, tal y como se explica en el siguiente apartado.

Para más información sobre la creación y uso de esquemas de autenticación con SNMP, ver la recomendación RFC 1157, *A Simple Network Management Protocol.*

Capítulo 2
Configuración del agente SNMP

1. Acceso al entorno de configuración SNMP

En este apartado se describen los pasos requeridos para configurar el protocolo SNMP. Después de configurar las opciones deseadas, se debe guardar la configuración y reiniciar el router para que tenga efecto la nueva configuración. Las siguientes secciones describen el proceso de configuración con más detalle.

Para acceder al entorno de configuración SNMP, desde el prompt *Config>*, se deberá introducir el siguiente comando.

```
Config>PROTOCOL SNMP
SNMP user configuration
SNMP Config>
```

2. Comandos de configuración SNMP

Esta sección resume y explica todos los comandos de configuración SNMP. Estos comandos permiten especificar parámetros de red de los interfaces del router que transmiten paquetes SNMP.

Comando	Función
? (AYUDA)	Lista los comandos disponibles o las opciones asociadas con un comando especifico.
COMMUNITY	Permite añadir una nueva comunidad a la lista de las comunidades SNMP o bien modificar el valor de algún parámetro de una comunidad ya existente: añadir o borrar una dirección IP con máscara asociada a esa comunidad, configurar el modo de acceso, establecer la vista de la comunidad y habilitar o deshabilitar distintos tipos de traps que los miembros de la comunidad envían a los gestores SNMP.
DEFAULT-CONFIG	Habilita la configuración por defecto.
DISABLE	Deshabilita el protocolo SNMP.
ENABLE	Habilita el protocolo SNMP.
LIST	Muestra las comunidades, con sus modos de acceso, traps habilitadas, direcciones IP y vistas asociadas. También muestra todas las vistas y sus "subtrees" de la MIB asociados, así como si el agente SNMP está activo, el puerto UDP de destino de traps y los valores de ciertos parámetros relacionados con el envío de traps.
NO	Borra una comunidad de la lista de las comunidades SNMP y sus direcciones IP asociadas, borra un "subtree" de una vista (y la vista completa si se borra su último "subtree" asociado), deshabilita la configuración por defecto o establece los valores por defecto para el puerto UDP de destino de traps o para los parámetros de envío de traps SNMP.
SUBTREE	Añade una porción de la MIB ("subtree") a una vista o crea una vista nueva.
TRAP	Configura el puerto UDP de destino de traps o ciertos parámetros relacionados con el envío de traps SNMP.
EXIT	Vuelve al prompt *Config*>.

2.1. ? (AYUDA)

Use el comando **? (AYUDA)** para listar los comandos que están disponibles en el nivel donde se está programando el router. También se puede utilizar este comando a continuación de un comando específico para listar sus opciones.

Sintaxis:

```
SNMP Config>?
```

Ejemplo:

```
SNMP Config>?
COMMUNITY           Adds a community or modifies parameters of an existing one
DEFAULT-CONFIG      Enables the default configuration
DISABLE             Disables SNMP
ENABLE              Enables SNMP
LIST                Displays SNMP configuration elements
NO                  Deletes an item, disables an option or sets default values
SUBTREE             Adds a portion of the MIB to a view or creates a view
TRAP                Sets trap UDP port or trap sending parameters
EXIT                Exits SNMP configuration menu
SNMP Config>
```

2.2. COMMUNITY

Use el comando **COMMUNITY** para añadir un nombre de comunidad a la lista de las comunidades SNMP o bien modificar el valor de algún parámetro de una comunidad ya existente: añadir o borrar una dirección IP (con su máscara) asociada a esa comunidad, configurar el modo de acceso, establecer la vista de la comunidad y habilitar o deshabilitar distintos tipos de traps que los miembros de la comunidad envían a los gestores SNMP.

Sintaxis:

```
SNMP config>COMMUNITY
Community name[]? public
default      creates a SNMP community with default values
access       sets community access
address      adds an address to a community
view         sets a view for a community
trap         enables traps of the type specified
no           deletes an address, deletes a view or disables traps
Type an option [default]?
SNMP config>
```

Community name Especifica el nombre de la comunidad (32 caracteres como máximo). Caracteres especiales como espacios, tabuladores, etc., no son válidos.

a) COMMUNITY nombre_comunidad DEFAULT

Crea una comunidad con los parámetros por defecto o establece dichos parámetros para una comunidad ya existente. Estos son: modo de acceso de lectura y generación de traps, vista asociada de toda la MIB, acceso permitido desde todas las direcciones IP y todos los tipos de traps asociados a esa comunidad deshabilitados.

NOTA: Use la opción COMMUNITY nombre_comunidad ACCESS para asignar los tipos de acceso de comunidades SNMP, la opción COMMUNITY nombre_comunidad ADDRESS para fijar una determinada dirección IP desde la que se permite el acceso a una comunidad concreta, la opción COMMUNITY nombre_comunidad VIEW para limitar la vista de una comunidad a ciertos "subtrees" o partes de la MIB y la opción COMMUNITY nombre_comunidad TRAP para habilitar los tipos de traps que se desee que el agente envíe a las direcciones de gestión configuradas para una comunidad.

Ejemplo:

```
SNMP config>COMMUNITY public default
SNMP config>
```

O bien:

```
SNMP config>COMMUNITY
Community name[]? public
default      creates a SNMP community with default values
access       sets community access
address      adds an address to a community
view         sets a view for a community
trap         enables traps of the type specified
no           deletes an address, deletes a view or disables traps
Type an option [default]?
SNMP config>
```

b) COMMUNITY nombre_comunidad ACCESS

Asigna un modo de acceso a una comunidad. Los modos de acceso posibles son:

read-trap: Lectura y generación de traps.

trap-only: Generación de traps.

write-read-trap: Lectura-escritura y generación de traps.

Ejemplo:

```
SNMP config>COMMUNITY public access write-read-trap
SNMP config>
```

O bien:

```
SNMP config>COMMUNITY
Community name[]? public
default      creates a SNMP community with default values
access       sets community access
address      adds an address to a community
view         sets a view for a community
trap         enables traps of the type specified
no           deletes an address, deletes a view or disables traps
Type an option [default]? access
read-trap            read SNMP variables and generate traps
trap-only            only generate traps
write-read-trap      read and write SNMP variables and generate traps
Type an option [read-trap]? write-read-trap
SNMP config>
```

c) COMMUNITY nombre_comunidad ADDRESS

Use la opción **COMMUNITY nombre_comunidad ADDRESS** para añadir una dirección IP a una comunidad. Debe incluir el nombre de la comunidad y la dirección y máscara de red (en la notación estándar *a.b.c.d*).

> ***NOTA: Las peticiones SNMP pueden llegar dirigidas a cualquiera de las direcciones del router.***

Se pueden especificar una o más direcciones para una comunidad. Para ello se debe repetir la operación tantas veces como direcciones IP se quieran añadir.

Las peticiones SNMP serán aceptadas para cada comunidad si el resultado de la función lógica AND entre la dirección IP origen de la trap y la máscara de red de la comunidad coincide con el resultado de la función lógica AND entre la dirección IP de la comunidad y la máscara de la misma, en alguna de las direcciones configuradas en la comunidad. Esto quiere decir que se aceptarán peticiones de cualquier equipo de las subredes definidas por las máscaras. Si no se especifica ninguna dirección para la comunidad, las peticiones son aceptadas desde cualquier host. Las direcciones también especifican los hosts que recibirán las traps. Si no se especifica ninguna dirección no se generará ninguna trap.

Ejemplo 1:

```
SNMP config>COMMUNITY public address 192.6.2.168 255.255.255.0
SNMP config>
```

O bien:

```
SNMP config>COMMUNITY
Community name[]? public
default      creates a SNMP community with default values
access       sets community access
address      adds an address to a community
view         sets a view for a community
trap         enables traps of the type specified
no           deletes an address, deletes a view or disables traps
Type an option [default]? address
IP Address [0.0.0.0]? 192.6.2.168
Mask [255.255.255.0]?
SNMP config>
```

Esta operación ocasiona que las peticiones con la comunidad *public* sean aceptadas si provienen de cualquier host de la red 192.6.2, y que las traps se envíen a la dirección 192.6.2.168.

Ejemplo 2:

```
SNMP config>COMMUNITY public address 192.6.2.168 255.255.255.255
SNMP config>
```

O bien:

```
SNMP config>COMMUNITY
Community name[]? public
default      creates a SNMP community with default values
access       sets community access
address      adds an address to a community
view         sets a view for a community
trap         enables traps of the type specified
no           deletes an address, deletes a view or disables traps
Type an option [default]? address
IP Address [0.0.0.0]? 192.6.2.168
Mask [255.255.255.0]? 255.255.255.255
SNMP config>
```

Esta operación ocasiona que las peticiones con la comunidad *public* sean aceptadas sólo si provienen del host 192.6.2.168, y que las traps se envíen a ese mismo host.

d) COMMUNITY nombre_comunidad VIEW

Asigna una vista de la MIB a una comunidad. La vista debe estar previamente creada con el comando **SUBTREE**. Si *View name* es "ALL", la comunidad tendrá acceso a toda la MIB.

Ejemplo:

```
SNMP config>COMMUNITY private view Teldat
SNMP config>
```

O bien:

```
SNMP config>COMMUNITY
Community name[]? private
default      creates a SNMP community with default values
access       sets community access
address      adds an address to a community
view         sets a view for a community
trap         enables traps of the type specified
no           deletes an address, deletes a view or disables traps
Type an option [default]? view
View name[]? Teldat
SNMP config>
```

e) COMMUNITY nombre_comunidad TRAP

Habilita un determinado tipo de trap o todos los tipos de traps para una comunidad. El tipo de trap es uno de los siguientes:

Tipo de trap	**Descripción**
ALL	Habilita todos los tipos de traps en la comunidad especificada.
AUTHENTICATION-FAILURE	Habilita la trap "authentication failure" en la comunidad especificada. La trap "authentication failure" indica que una petición SNMP no ha sido debidamente autenticada.
COLD-START	Habilita la trap "cold start" en la comunidad especificada. La trap "cold start" indica que el router ha realizado un "arranque en frío".
ENTERPRISE-SPECIFIC	Habilita traps específicas de empresa en la comunidad dada. Las traps específicas de empresa indican que ha ocurrido algún hecho de los que se han definido como destacables y que deben ser notificados. El campo "specific-trap" de la trap identifica la trap particular que ocurrió. En el **Router Teldat**, las traps específicas de empresa son las configuradas como tal en el Sistema de Registro de Eventos (SRE).
LINK-DOWN	Habilita la trap "link down" en la comunidad especificada. La trap "link down" indica un fallo en uno de los interfaces del router. La PDU de trap "link down" contiene el nombre y valor de *ifIndex* del interfaz afectado como primer elemento de su lista de variables.
LINK-UP	Habilita la trap "link up" en la comunidad especificada. La trap "link up" indica que uno de los interfaces del router que estaba caído, ha vuelto a funcionar. La PDU de trap "link up" contiene el nombre y valor de *ifIndex* del interfaz afectado como primer elemento de su lista de variables.
WARM-START	Habilita la trap "warm start" en la comunidad especificada. La trap "warm start" indica que el router ha realizado un "arranque en caliente".

Ejemplo:

```
SNMP config>COMMUNITY private trap all
SNMP config>
```

O bien:

```
SNMP config>COMMUNITY
Community name[]? private
default      creates a SNMP community with default values
access       sets community access
address      adds an address to a community
view         sets a view for a community
trap         enables traps of the type specified
no           deletes an address, deletes a view or disables traps
Type an option [default]? trap
all                          enables all trap types
authentication-failure       enables authentication failure traps
cold-start                   enables cold start traps
enterprise-specific          enables enterprise specific traps
link-down                    enables link down traps
link-up                      enables link up traps
warm-start                   enables warm start traps
Type an option [all]?
SNMP config>
```

f) COMMUNITY nombre_comunidad NO

Este comando permite borrar una dirección IP (con su máscara) asociada a la comunidad especificada, borrar la vista asociada a esa comunidad o deshabilitar un tipo de traps o todas las traps para una comunidad.

Sintaxis:

```
SNMP config>COMMUNITY
Community name[]? public
default      creates a SNMP community with default values
access       sets community access
address      adds an address to a community
view         sets a view for a community
trap         enables traps of the type specified
no           deletes an address, deletes a view or disables traps
Type an option [default]? no
address      deletes a community address
view         deletes the association of a view to a commmunity
trap         disables traps of the type specified
Type an option [address]?
IP Address [0.0.0.0]?
SNMP config>
```

COMMUNITY nombre_comunidad NO ADDRESS

Borra una dirección de una comunidad.

Ejemplo:

```
SNMP Config>COMMUNITY public no address
IP Address [0.0.0.0]? 192.6.2.168
SNMP Config>
```

COMMUNITY nombre_comunidad NO TRAP

Deshabilita una determinada trap o todas las traps para una comunidad. El tipo de trap es uno de los siguientes:

Tipo de trap	**Descripción**
ALL	Deshabilita todas las traps en la comunidad especificada.
AUTHENTICATION-FAILURE	Deshabilita la trap "authentication failure" en la comunidad especificada. La trap "authentication failure" indica que una petición SNMP no ha sido debidamente autenticada.
COLD-START	Deshabilita la trap "cold start" en la comunidad especificada. La trap "cold start" indica que el router ha realizado un "arranque en frío".
ENTERPRISE-SPECIFIC	Deshabilita traps específicas de empresa en la comunidad dada. Las traps específicas de empresa indican que ha ocurrido algún hecho de los que se han definido como destacables y que deben ser notificados. El campo "specific-trap" de la trap identifica la trap particular que ocurrió. En el **Router Teldat**, las traps específicas de empresa son las configuradas como tal en el Sistema de Registro de Eventos (SRE).
LINK-DOWN	Habilita la trap "link down" en la comunidad especificada. La trap "link down" indica un fallo en uno de los interfaces del router. La PDU de trap "link down" contiene el nombre y valor de *ifIndex* del interfaz afectado como primer elemento de su lista de variables.
LINK-UP	Deshabilita la trap "link up" en la comunidad especificada. La trap "link up" indica que uno de los interfaces del router que estaba caído, ha vuelto a funcionar. La PDU de trap "link up" contiene el nombre y valor de *ifIndex* del interfaz afectado como primer elemento de su lista de variables.

WARM-START Deshabilita la trap "warm start" en la comunidad especificada. La trap "warm start" indica que el router ha realizado un "arranque en caliente".

Ejemplo:

```
SNMP config>COMMUNITY private no trap all
```

O bien:

```
SNMP config>COMMUNITY
Community name[]? private
default      creates a SNMP community with default values
access       sets community access
address      adds an address to a community
view         sets a view for a community
trap         enables traps of the type specified
no           deletes an address, deletes a view or disables traps
Type an option [default]? no
address      deletes a community address
view         deletes the association of a view to a commmunity
trap         disables traps of the type specified
Type an option [address]? trap
all                          disables all traps
authentication-failure       disables authentication failure traps
cold-start                   disables cold start traps
enterprise-specific          disables enterprise specific traps
link-down                    disables link down traps
link-up                      disables link up traps
warm-start                   disables warm start traps
Type an option [all]?
SNMP config>
```

COMMUNITY nombre_comunidad NO VIEW

Borra la vista asignada a una comunidad, de manera que ésta tendrá acceso a toda la MIB.

Ejemplo:

```
SNMP Config>COMMUNITY public NO VIEW
SNMP Config>
```

2.3. DEFAULT-CONFIG

Habilita la configuración por defecto. El comando **DEFAULT-CONFIG** habilita SNMP y crea una comunidad que se denomina "teldat", con las características siguientes: tiene todos los permisos (lectura, escritura, etc.), no envía traps, acepta peticiones de cualquier dirección, y ve toda la MIB. El valor por defecto de este comando es habilitado.

Ejemplo:

```
SNMP config>DEFAULT-CONFIG
Default configuration is enabled
SNMP config>
```

2.4. DISABLE

Deshabilita el protocolo SNMP.

Ejemplo:

```
SNMP Config>DISABLE
SNMP disabled
SNMP Config>
```

NOTA: Si se encuentra habilitada la configuración por defecto, SNMP siempre está habilitado, y por tanto no puede ser deshabilitado hasta que no se deshabilite previamente dicha configuración por defecto.

2.5. ENABLE

Habilita el protocolo SNMP.

Ejemplo:

```
SNMP Config>ENABLE
SNMP enabled
SNMP Config>
```

2.6. SUBTREE

Añade una parte de la MIB a una vista o crea una nueva vista. Este comando se usa para configurar las vistas de la MIB. Más de un subtree puede ser agregado a la misma vista. Para crear una nueva vista, se debe usar este comando con un nuevo nombre de vista.

Para asignar una vista a una o más comunidades se debe emplear el comando **COMMUNITY nombre_comunidad VIEW**.

Ejemplo:

```
SNMP config>SUBTREE
View name[]? mib2
MIB OID name[]? 1.3.6.1.2.1
SNMP config>
```

View name Especifica el nombre de la vista (32 caracteres como máximo). Caracteres especiales, como espacios, tabuladores, etc. no son válidos.

MIB OID name Especifica el identificador del objeto de la MIB ("subtree") que provocara que todos los objetos que cuelguen de él, en la MIB implementada, sean visibles para esa vista.

2.7. TRAP

Permite configurar el puerto UDP al que se envían traps o alguno de los parámetros utilizados para determinar las condiciones del envío de dichas traps.

Sintaxis:

```
SNMP config>TRAP ?
PORT                    Allows setting of trap UDP port
SENDING-PARAMETERS      Allows setting of trap sending parameters
SNMP config>
```

a) TRAP PORT

Especifica el número de puerto UDP al que enviar las traps. El valor por defecto es 162, el puerto estándar de envío de traps.

Ejemplo:

```
SNMP Config>TRAP PORT
UDP trap port[162]?
SNMP Config>
```

b) TRAP SENDIG-PARAMETERS

Permite configurar los parámetros del envío de traps. El envío de un trap SNMP puede provocar una llamada X.25 o RDSI si el destinatario de las traps se encuentra situado al otro lado de un interfaz de ese tipo. Por ello puede ser conveniente agrupar las traps a enviar en un buffer y enviarlas todas juntas, para reducir el número de llamadas realizadas. Además, interesaría asegurarse de que la dirección que se ha configurado como destino de las traps es alcanzable (se ha establecido ya la llamada, siguiendo con el ejemplo anterior), de modo que la probabilidad de que las traps se pierdan por el camino disminuya. Sin embargo, en otras ocasiones puede que lo que más interese sea recibir las traps lo más rápido posible, por lo que convendría minimizar el número de traps que se guardarán en el buffer antes de ser enviadas o el tiempo máximo en que una trap puede permanecer esperando ser transmitida. En este caso tampoco sería recomendable comprobar si la estación gestora que recibirá las traps es alcanzable, ya que esto podría introducir un cierto retardo si se tiene que esperar a recibir la respuesta al ECHO UDP o ICMP que desde el equipo se envía a cada destino configurado para averiguar si está accesible.

Los parámetros de envío de traps que se configuran desde esta opción son:

NUMBER	Tamaño del buffer de traps a reagrupar: número de traps que pueden llegar a almacenarse antes de enviarse al destino.
REACHABILITY-CHECKING	Indica si se realizarán las comprobaciones de alcanzabilidad de las estaciones gestoras configuradas como destino de las traps antes de proceder a su envío.
TARGETS	Máximo número de destinatarios de traps (gestores SNMP a los que se envían traps).
TIME	Tiempo que se guarda una trap en el buffer antes de enviarse (si el buffer no se llena antes).

Sintaxis:

```
SNMP config>TRAP SENDING-PARAMETERS ?
NUMBER                    Maximum number of traps to keep before sending
REACHABILITY-CHECKING     Reachability checking before sending traps
TARGETS                   Maximum number of trap targets (managers)
TIME                      Max time keeping traps in buffer before sending
SNMP config>
```

TRAP SENDING-PARAMETERS NUMBER

Configura el tamaño del buffer de traps a reagrupar, es decir, el número de traps que pueden llegar a almacenarse antes de enviarse al destino. En cualquier caso las traps se enviarán individualmente, cada una en un paquete UDP. El valor por defecto es de 32 traps.

Ejemplo:

```
SNMP config>TRAP SENDING-PARAMETERS NUMBER
Max number traps to keep[32]?
SNMP config>
```

TRAP SENDING-PARAMETERS REACHABILITY-CHECKING

Este parámetro indica si se realizarán las comprobaciones de alcanzabilidad de las estaciones gestoras configuradas como destino de las traps antes de proceder a su envío. Si este parámetro se configura a 0 (deshabilitada la comprobación de destino alcanzable), además de transmitir las traps sin preocuparse de si el destino es accesible, deja de tener sentido el envío periódico del ECHO UDP o ICMP que se utiliza para averiguar a qué gestores es posible llegar, que serán aquellos de los que se reciba respuesta, por lo que deshabilitar la comprobación implicará también no transmitir el ECHO. Los valores permitidos para esta variable son:

0- Las traps son emitidas sin comprobar que los destinos sean alcanzables y no se utiliza el ECHO UDP ni ECHO ICMP.

1- Habilitada la comprobación, la cuál se lleva a cabo mediante el envío de ECHO UDP.

2- Habilitada la comprobación, la cuál se lleva a cabo mediante el envío de ECHO ICMP.

Ejemplo:

```
SNMP config>TRAP SENDING-PARAMETERS REACHABILITY-CHECKING
Check if manager is reachable before sending traps:
  0-No
  1-Yes UDP
  2-Yes ICMP[1]?
SNMP config>
```

TRAP SENDING-PARAMETERS TARGETS

Máximo numero de destinatarios de traps. Las comunidades SNMP pueden llevar asociadas una o varias direcciones destino de envío de traps. Este parámetro limita el número de destinos a los que efectivamente se envían traps. El valor por defecto es de 4 direcciones destino.

Ejemplo:

```
SNMP config>TRAP SENDING-PARAMETERS TARGETS
Max number of trap targets[4]?
SNMP config>
```

TRAP SENDING-PARAMETERS TIME

Tiempo que se guarda una trap en el buffer antes de enviarse si el buffer no se llena antes. Las traps se envían cuando el buffer se llena o cuando han pasado los segundos indicados por este parámetro si el buffer no se ha llenado antes. El valor por defecto es de 50 segundos.

Ejemplo:

```
SNMP config>TRAP SENDING-PARAMETERS TIME
Max time keeping traps (sec)[50]?
SNMP config>
```

2.8. NO

Use el comando **NO** para:

- Borrar una comunidad y todas sus direcciones IP asociadas.
- Deshabilitar la configuración por defecto.
- Borrar un "subtree" de una vista.
- Establecer los valores por defecto para el puerto destino de traps o para los parámetros utilizados para determinar las condiciones del envío de dichas traps.

Sintaxis:

```
SNMP config>NO ?
COMMUNITY           Removes a community and its IP addresses
DEFAULT-CONFIG      Disables the default configuration
SUBTREE             Removes a subtree from a view
TRAP                Sets default values to trap port or sending parameters
SNMP config>
```

a) NO COMMUNITY

Borra una comunidad y sus direcciones IP.

Ejemplo:

```
SNMP Config>NO COMMUNITY
Community name[]? public
SNMP Config>
```

b) NO DEFAULT-CONFIG

Deshabilita la configuración por defecto.

Ejemplo:

```
SNMP config>NO DEFAULT-CONFIG
Default configuration is disabled
SNMP config>
```

c) NO SUBTREE

Borra un "subtree" de una vista. Si era el último subtree de la vista, se borrará también dicha vista, así como todas las referencias a ella de cualquier comunidad.

Ejemplo:

```
SNMP Config>NO SUBTREE
View name[]? mib2
MIB OID name[]? 1.3.6.1.2.1
SNMP Config>
```

d) NO TRAP

Este comando permite establecer los valores por defecto para el puerto UDP destino de traps o para los parámetros utilizados para determinar las condiciones del envío de dichas traps.

Sintaxis:

```
SNMP config>NO TRAP ?
PORT                    Sets default value to trap port
SENDING-PARAMETERS      Sets default values to trap sending parameters
SNMP config
```

NO TRAP PORT

Establece como número de puerto UDP al que enviar las traps el valor por defecto: 162, el puerto estándar de envío de traps.

Ejemplo:

```
SNMP config>NO TRAP PORT
SNMP config>
```

NO TRAP SENDING-PARAMETERS

Con este comando se configuran los parámetros relacionados con el envío de traps a sus valores por defecto.

Sintaxis:

```
SNMP config>NO TRAP SENDING-PARAMETERS ?
NUMBER                     Sets default value to max number of traps to keep
REACHABILITY-CHECKING      Sets reachability-checking mechanism to UDP echo
TARGETS                    Sets default value to max number of trap targets
TIME                       Sets default value to max time keeping traps
SNMP config>
```

- *NO TRAP SENDING-PARAMETERS NUMBER*

Configura el tamaño del buffer de traps a reagrupar, es decir, el número de traps que pueden llegar a almacenarse antes de enviarse al destino, dándole su valor por defecto: 32 traps.

Ejemplo:

```
SNMP config>NO TRAP SENDING-PARAMETERS NUMBER
SNMP config>
```

· NO TRAP SENDING-PARAMETERS REACHABILITY-CHECKING

El comando **NO TRAP SENDING-PARAMETERS REACHABILITY-CHECKING** habilita la comprobación de destino alcanzable antes de proceder a enviarle traps, la cuál se lleva a cabo mediante el envío de ECHO UDP.

Ejemplo:

```
SNMP config>NO TRAP SENDING-PARAMETERS REACHABILITY-CHECKING
SNMP config>
```

· NO TRAP SENDING-PARAMETERS TARGETS

Configura el máximo numero de destinatarios de traps a su valor por defecto: como máximo se envían traps a 4 direcciones destino.

Ejemplo:

```
SNMP config>NO TRAP SENDING-PARAMETERS TARGETS
SNMP config>
```

· NO TRAP SENDING-PARAMETERS TIME

Establece el tiempo máximo que se guarda una trap en el buffer antes de enviarse (si el buffer no se llena antes) en su valor por defecto: 50 segundos.

Ejemplo:

```
SNMP config>NO TRAP SENDING-PARAMETERS TIME
SNMP config>
```

2.9. LIST

Use el comando **LIST** para mostrar la configuración de SNMP: comunidades, modos de acceso, traps, direcciones IP, vistas, etc.

Sintaxis:

```
SNMP config>LIST ?
ALL                          Displays all the SNMP configuration information
COMMUNITY                    Displays current communities configuration
TRAP-SENDING-PARAMETERS      Displays the relative information on trap sending
VIEW                         Displays the current views configured
SNMP config>
```

a) LIST ALL

Muestra toda la información de configuración SNMP.

Ejemplo:

```
SNMP Config>LIST ALL
Default configuration is disabled
SNMP is enabled
Trap port: 162
Max time keeping traps (sec):                        50
Max number traps to keep:                            32
Max number of trap targets:                          4
Check if manager is reachable before sending traps: YES – UDP
```

```
        Community Name              IP Address       IP Mask
--------------------------------   -------------------------
public                             ALL
private                            192.6.2.168      255.255.255.255

        Community Name              Access
--------------------------------   -------------------------
public                             Read, Trap
private                            Read, Write, Trap

        Community Name              Enabled traps
--------------------------------   -------------------------
public                             None
private                            Cold Start
                                   Warm Start
                                   Link Down
                                   Link Up
                                   Authentication Failure
                                   Enterprise Specific

        Community name              Views
--------------------------------   -------------------------
public                             mib2
private                            teldat

        View name                   Subtree
--------------------------------   -------------------------
mib2                               1.3.6.1.2.1
teldat                             1.3.6.1.4.1.2007
SNMP Config>
```

NOTA: Si está habilitada la configuración por defecto, SNMP siempre está habilitado.

b) LIST COMMUNITY

Sintaxis:

```
SNMP config>LIST COMMUNITY ?
ACCESS       Displays the access mode information for all communities
ADDRESS      Displays the associated addresses information for all communities
TRAPS        Displays the associated traps information for all communities
VIEW         Displays the view information associated to each community
SNMP config>
```

LIST COMMUNITY ACCESS

Muestra información del modo de acceso de todas las comunidades.

Ejemplo:

```
SNMP Config>LIST COMMUNITY ACCESS
        Community Name              Access
--------------------------------   -------------------------
public                             Read, Trap
private                            Read, Write, Trap
SNMP Config>
```

LIST COMMUNITY ADDRESS

Muestra información las direcciones asociadas a todas las comunidades.

Ejemplo:

```
SNMP Config> LIST COMMUNITY ADDRESS
        Community Name              IP Address       IP Mask
--------------------------------   -------------------------
public                             ALL
private                            192.6.2.168      255.255.255.255
SNMP Config>
```

LIST COMMUNITY TRAPS

Muestra información de las traps asociadas a todas las comunidades.

Ejemplo:

```
SNMP Config>LIST COMMUNITY TRAPS
        Community Name              Enabled traps
--------------------------------   -------------------------
public                              None
private                             Cold Start
                                    Warm Start
                                    Link Down
                                    Link Up
                                    Authentication Failure
                                    Enterprise Specific
SNMP Config>
```

LIST COMMUNITY VIEW

Muestra información de la vista asociada a cada comunidad.

Ejemplo:

```
SNMP Config>LIST COMMUNITY VIEW
        Community name              Views
--------------------------------   -------------------------
public                              mib2
private                             teldat
SNMP Config>
```

c) LIST TRAP-SENDING-PARAMETERS

Muestra la información relativa al envío de traps.

Ejemplo:

```
SNMP Config>LIST TRAP-SENDING-PARAMETERS
Max time keeping traps (sec):                       50
Max number traps to keep:                           32
Max number of trap targets:                         4
Check if manager is reachable before sending traps: YES – UDP

SNMP Config>
```

d) LIST VIEW

Muestra información de las vistas definidas en el sistema, con las partes de la MIB o “subtrees” asociados a cada una.

Ejemplo:

```
SNMP Config>LIST VIEW
        View name                   Subtree
--------------------------------   -------------------------
mib2                                1.3.6.1.2.1
teldat                              1.3.6.1.4.1.2007
SNMP Config>
```

2.10. EJEMPLO DE CONFIGURACIÓN

A continuación se muestra un ejemplo de configuración en modo texto obtenida a partir de un comando **SHOW CONFIG**:

```
SNMP config>LIST ALL
Default configuration is disabled
SNMP is enabled
Trap port: 162
Max time keeping traps (seg):                        40
Max number traps to keep:                            30
Max number of trap targets:                          5
Check if manager is reachable before sending traps: YES - ICMP


        Community Name              IP Address       IP Mask
--------------------------------   -------------------------
public                             ALL
private                            192.6.2.168      255.255.255.255

        Community Name              Access
--------------------------------   -------------------------
public                             Read, Trap
private                            Read, Write, Trap

        Community Name              Enabled traps
--------------------------------   -------------------------
public                             None
private                            Cold Start
                                   Warm Start
                                   Link Down
                                   Link Up
                                   Authentication Failure
                                   Enterprise Specific

        Community name              Views
--------------------------------   -------------------------
public                             mib2
private                            teldat

        View name                   Subtree
--------------------------------   -------------------------
mib2                               1.3.6.1.2.1
teldat                             1.3.6.1.4.1.2007
SNMP config>
```

```
SNMP Config>SHOW CONFIG
; Showing Menu and Submenus Configuration ...
; Router C4i IPSec 1 16 Version 10.0.0CAI

   no default-config
   subtree mib2 1.3.6.1.2.1
   subtree teldat 1.3.6.1.4.1.2007
;
   community public default
   community public view mib2
;
   community private default
   community private access write-read-trap
   community private address 192.6.2.168 255.255.255.255
   community private view teldat
   community private trap all
;
   trap sending-parameters time 40
   trap sending-parameters number 30
   trap sending-parameters targets 5
   trap sending-parameters reachability-checking 2
SNMP config>
```

2.11. EXIT

Use el comando **EXIT** para volver al prompt de configuración.

Sintaxis:

```
SNMP Config>EXIT
```

Ejemplo:

```
SNMP Config>EXIT
Config>
```

Capítulo 3
Monitorización del agente SNMP

1. Acceso al entorno de monitorización SNMP

Para acceder al entorno de monitorización SNMP, desde el prompt de consola (+), se deberá introducir el siguiente comando.

```
+PROTOCOL SNMP
SNMP>
```

2. Comandos de monitorización SNMP

Comando	Función
? (AYUDA)	Lista comandos u opciones.
LIST	Indica si el protocolo SNMP está habilitado o deshabilitado.
	Muestra el puerto UDP destino de traps.
	Muestra las comunidades, con sus modos de acceso, traps habilitadas, direcciones IP y vistas asociadas.
	También muestra todas las vistas y sus "subtrees" de la MIB asociados.
EXIT	Vuelve al prompt +.

2.1. ? (AYUDA)

Use el comando **? (AYUDA)** para listar los comandos válidos en el nivel donde se está programando el router. Se puede también utilizar este comando después de un comando específico para listar sus opciones.

Sintaxis:

```
SNMP>?
```

Ejemplo:

```
SNMP>?
LIST
EXIT
```

2.2. LIST

Use el comando **LIST** para mostrar la configuración actual de SNMP: comunidades, modos de acceso, traps, direcciones IP, vistas, etc.

Sintaxis:

```
SNMP>LIST ?
ALL
COMMUNITY
VIEW
```

a) LIST ALL

Muestra toda la información de configuración SNMP actualmente activa.

Ejemplo:

```
SNMP>LIST ALL
SNMP is enabled
Trap port: 162

        Community Name              IP Address       IP Mask
-------------------------------   -------------------------
public                            ALL
private                           192.6.2.168      255.255.255.255

        Community Name              Access
-------------------------------   -------------------------
public                            Read, Trap
private                           Read, Write, Trap
```

```
        Community Name              Enabled traps
--------------------------------   --------------------------
public                             None
private                            Cold Start
                                   Warm Start
                                   Link Down
                                   Link Up
                                   Authentication Failure
                                   Enterprise Specific

        Community name             Views
--------------------------------   --------------------------
public                             mib2
private                            teldat

        View name                  Subtree
--------------------------------   --------------------------
mib2                               1.3.6.1.2.1
teldat                             1.3.6.1.4.1.2007
SNMP>
```

b) LIST COMMUNITY

Sintaxis:

```
SNMP>LIST COMMUNITY ?
ACCESS
ADDRESS
TRAPS
VIEW
```

LIST COMMUNITY ACCESS

Muestra información del modo de acceso de todas las comunidades.

Ejemplo:

```
SNMP>LIST COMMUNITY ACCESS
        Community Name              Access
--------------------------------   --------------------------
public                             Read, Trap
private                            Read, Write, Trap
SNMP>
```

LIST COMMUNITY ADDRESS

Muestra información de las direcciones asociadas a todas las comunidades.

Ejemplo:

```
SNMP>LIST COMMUNITY ADDRESS
        Community Name              IP Address       IP Mask
--------------------------------   --------------------------
public                             ALL
private                            192.6.2.168      255.255.255.255
SNMP>
```

LIST COMMUNITY TRAPS

Muestra información de las traps asociadas a todas las comunidades.

Ejemplo:

```
SNMP>LIST COMMUNITY TRAPS
        Community Name              Enabled traps
--------------------------------   -------------------------
public                             None
private                            Cold Start
                                   Warm Start
                                   Link Down
                                   Link Up
                                   Authentication Failure
                                   Enterprise Specific
SNMP>
```

LIST COMMUNITY VIEW

Muestra información de la vista asociada a cada comunidad.

Ejemplo:

```
SNMP>LIST COMMUNITY VIEW
        Community name              Views
--------------------------------   -------------------------
public                             mib2
private                            teldat
SNMP>
```

c) LIST VIEW

Muestra información de las vistas definidas en el sistema.

Ejemplo:

```
SNMP>LIST VIEW
        View name                   Subtree
--------------------------------   -------------------------
mib2                               1.3.6.1.2.1
teldat                             1.3.6.1.4.1.2007
SNMP>
```

2.3. EXIT

Use el comando **EXIT** para volver al prompt de consola.

Sintaxis:

```
SNMP>EXIT
```

Ejemplo:

```
SNMP>EXIT
+
```