Router Teldat

Agente SNMP

Doc. *DM512* Rev. *8.40*

Septiembre, 2000

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.

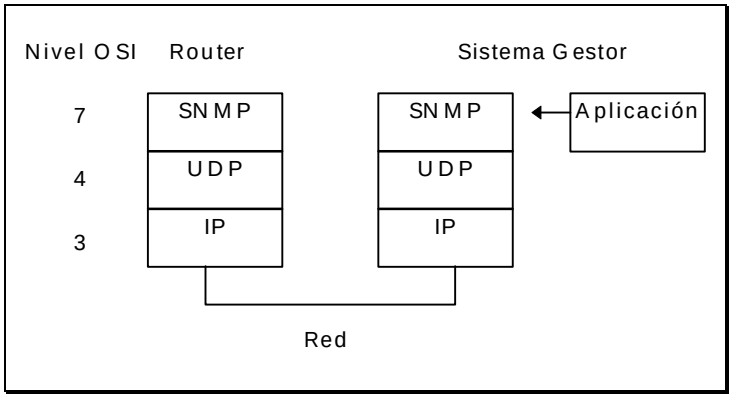

Figura 1: Niveles de protocolo del entorno SNMP

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.
ADD	Añade una comunidad a la lista de las comunidades SNMP, una dirección IP con máscara a una comunidad, o un "subtree" a una vista de MIB.
DELETE	Borra una comunidad de la lista de las comunidades SNMP, una dirección IP con máscara de una comunidad, o un "subtree" de una vista de MIB.
SET	Configura el modo de acceso o la vista de una comunidad. El modo de acceso de una comunidad es uno de los siguientes: • Lectura y generación de traps • Lectura, escritura y generación de traps • Sólo generación de traps También permite la configuración del puerto UDP de destino de traps.
ENABLE	Habilita el protocolo SNMP y traps asociadas con nombres de comunidades.
DISABLE	Deshabilita el protocolo SNMP y traps asociadas con nombres de comunidades.
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, y el puerto UDP de destino de traps.
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> ?
ADD
DELETE
SET
ENABLE
DISABLE
LIST
EXIT
SNMP Config>
```

2.2. ADD

Use el comando **ADD** para añadir un nombre de comunidad a la lista de las comunidades SNMP, añadir una dirección IP a una comunidad o asignar una parte de la MIB ("subtree") a una vista.

Sintaxis:

```
SNMP Config> ADD ?
COMMUNITY
ADDRESS
SUB_TREE
```

a) ADD COMMUNITY

Crea una comunidad con los parámetros por defecto. 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 el comando SET COMMUNITY ACCESS para asignar los tipos de acceso de comunidades SNMP existentes.

Ejemplo:

```
SNMP Config> ADD COMMUNITY
Community name[]? Public
SNMP Config>
```

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

b) ADD ADDRESS

Use el comando **ADD 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> ADD ADDRESS
Community name[]? public
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> ADD ADDRESS
Community name[]? public
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.

c) ADD SUB_TREE

Añade una parte de la MIB a una vista o crea una nueva vista. Si no se agrega ningún “subtree”, la vista es toda la MIB. 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 **SET COMMUNITY VIEW**.

Ejemplo:

```
SNMP Config> ADD SUB_TREE
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.

2.3. DELETE

Use el comando **DELETE** para borrar:

- Una dirección IP específica.
- Una comunidad y todas sus direcciones.
- Un "subtree" de una vista.

Sintaxis:

```
SNMP Config> DELETE ?
COMMUNITY
ADDRESS
SUB_TREE
```

a) DELETE COMMUNITY

Borra una comunidad y sus direcciones IP.

Ejemplo:

```
SNMP Config> DELETE COMMUNITY
Community name[]? public
SNMP Config>
```

b) DELETE ADDRESS

Borra una dirección de una comunidad.

Ejemplo:

```
SNMP Config> DELETE ADDRESS
Community name[]? public
IP Address [0.0.0.0]? 192.6.2.168
SNMP Config>
```

c) DELETE SUB_TREE

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> DELETE SUB_TREE
View name[]? mib2
MIB OID name[]? 1.3.6.1.2.1
SNMP Config>
```

2.4. SET

Use el comando **SET** para asignar una vista o el modo de acceso a una comunidad, o para configurar el número de puerto UDP de envío de traps.

Sintaxis:

```
SNMP Config>  SET ?
COMMUNITY
TRAPS-PORT
TRAP-SENDING-PARAMETERS
```

a) SET COMMUNITY

Sintaxis:

```
SNMP Config> SET COMMUNITY ?
ACCESS
VIEW
```

SET COMMUNITY ACCESS

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

READ_TRAP: Lectura y generación de traps.

WRITE_READ_TRAP: Lectura-escritura y generación de traps.

TRAP_ONLY: Generación de traps.

Ejemplo:

```
SNMP Config> SET COMMUNITY ACCESS WRITE_READ_TRAP
Community name[]? Private
SNMP Config>
```

SET COMMUNITY VIEW

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

Ejemplo:

```
SNMP Config> SET COMMUNITY VIEW
Community name[]? private
View name[]? Teldat
SNMP Config>
```

b) SET TRAPS-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> SET TRAPS-PORT
UDP trap port[162]?
SNMP Config>
```

c) SET TRAP-SENDING-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. Los parámetros de envío de traps que se configuran desde esta opción son:

Max time keeping traps. 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.

Max number traps to keep. Tamaño del buffer de traps a reagrupar: 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.

Max number of trap 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> SET TRAP-SENDING-PARAMETERS
Max time keeping traps (seg)[50]?
Max number traps to keep[32]?
Max number of trap targets[4]?
SNMP Config>
```

2.5. ENABLE

Use el comando **ENABLE** para habilitar el protocolo SNMP o determinadas traps en el router.

Sintaxis:

```
SNMP Config> ENABLE ?
SNMP
TRAP
DEFAULT CONFIGURATION
```

a) ENABLE SNMP

Habilita SNMP.

Ejemplo:

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

b) ENABLE TRAP

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

Tipo de trap	Descripción
ALL	Habilita todas las traps en la comunidad especificada.
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".
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".
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.
AUTH-FAIL	Habilita la trap "authentication failure" en la comunidad especificada. La trap "authentication failure" indica que una petición SNMP no ha sido debidamente autenticada.
ENTERPRISE	Habilita traps específicas de empresa en la comunidad dada. Las traps específicas de empresa indican que algún hecho específico de la empresa ha ocurrido. 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).

Ejemplo:

```
SNMP Config> ENABLE TRAP ALL
Community name[]? private
SNMP Config>
```

c) ENABLE DEFAULT CONFIGURATION

Habilita la configuración por defecto. El comando **ENABLE DEFAULT CONFIGURATION** habilita SNMP y crea una comunidad que se denomina "teldat", con las características siguientes: tiene todos los permisos (lectura, escritura, ...), 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> ENABLE DEFAULT CONFIGURATION
Default configuration is enabled
SNMP Config>
```

2.6. DISABLE

Use el comando **DISABLE** para deshabilitar el protocolo SNMP o determinadas traps en el router.

Sintaxis:

```
SNMP Config> DISABLE ?
SNMP
TRAP
DEFAULT CONFIGURATION
```

a) DISABLE SNMP

Deshabilita SNMP.

Ejemplo:

```
SNMP Config> DISABLE SNMP
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.

b) DISABLE 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.
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".
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".
LINK-DOWN	Deshabilita 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.
AUTH-FAIL	Deshabilita la trap “authentication failure” en la comunidad especificada. La trap “authentication failure” indica que una petición SNMP no ha sido debidamente autenticada.
ENTERPRISE	Deshabilita traps específicas de empresa en la comunidad dada. Las traps específicas de empresa indican que algún hecho específico de la empresa ha ocurrido. 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).

Ejemplo:

```
SNMP Config> DISABLE TRAP ALL
Community name[]? Private
SNMP Config>
```

c) DISABLE DEFAULT CONFIGURATION

Deshabilita la configuración por defecto.

Ejemplo:

```
SNMP Config> DISABLE DEFAULT CONFIGURATION
Default configuration is disabled
SNMP Config>
```

2.7. 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
COMMUNITY
VIEWS
TRAP-SENDING-PARAMETERS
```

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


        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 Restart
                                   Warm Restart
                                   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 habilitada.

b) LIST COMMUNITY

Sintaxis:

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

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 Restart
                                   Warm Restart
                                   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 VIEW

Muestra información de las vistas definidas en el sistema.

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>
```

d) 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
SNMP Config>
```

2.8. 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	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.

Ejemplo:

```
SNMP> LIST ALL
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
SNMP>
```

LIST COMMUNITY ADDRESS

Muestra información las direcciones asociadas a todas las comunidades.

Ejemplo:

```
SNMP> LIST COMMUNITY ADDRESS
SNMP>
```

LIST COMMUNITY TRAPS

Muestra información de las traps asociadas a todas las comunidades.

Ejemplo:

```
SNMP> LIST COMMUNITY TRAPS
SNMP>
```

LIST COMMUNITY VIEW

Muestra información de la vista asociada a cada comunidad.

Ejemplo:

```
SNMP> LIST COMMUNITY VIEW
SNMP>
```

c) LIST VIEW

Muestra información de las vistas definidas en el sistema.

Ejemplo:

```
SNMP> LIST VIEW
SNMP>
```

2.3. EXIT

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

Sintaxis:

```
SNMP> EXIT
```

Ejemplo:

```
SNMP> EXIT
+
```