Modicon

Switch MCSESM, MCSESP con administración
Manual de usuario Configuración

QGH59081.02

www.schneider-electric.com

Schneider Electric

La información que se ofrece en esta documentación contiene descripciones de carácter general y/o características técnicas sobre el rendimiento de los productos incluidos en ella. La presente documentación no tiene como objeto sustituir dichos productos para aplicaciones de usuario específicas, ni debe emplearse para determinar su idoneidad o fiabilidad. Los usuarios o integradores tienen la responsabilidad de llevar a cabo un análisis de riesgos adecuado y completo, así como la evaluación y las pruebas de los productos en relación con la aplicación o el uso de dichos productos en cuestión. Ni Schneider Electric ni ninguna de sus filiales o asociados asumirán responsabilidad alguna por el uso inapropiado de la información contenida en este documento. Si tiene sugerencias de mejoras o modificaciones o ha hallado errores en esta publicación, le rogamos que nos lo notifique.

Al instalar y utilizar este producto es necesario tener en cuenta todas las regulaciones sobre seguridad correspondientes, ya sean regionales, locales o estatales. Por razones de seguridad y para garantizar que se siguen los consejos de la documentación del sistema, las reparaciones solo podrá realizarlas el fabricante.

Cuando se utilicen dispositivos para aplicaciones con requisitos técnicos de seguridad, siga las instrucciones pertinentes.

Si con nuestros productos de hardware no se utiliza el software de Schneider Electric u otro software aprobado, pueden producirse lesiones, daños o un funcionamiento incorrecto del equipo.

Si no se tiene en cuenta esta información, se pueden causar daños personales o en el equipo.

Como parte de un grupo de empresas responsables e inclusivas, estamos actualizando nuestras comunicaciones que contienen terminología no inclusiva. Sin embargo, hasta que completemos este proceso, es posible que nuestro contenido todavía incluya términos estandarizados del sector que nuestros clientes puedan considerar inapropiados.

Contenido

Indicaciones de seguridad

Tenga en cuenta lo siguiente: Lea detenidamente estas instrucciones y familiarícese con el dispositivo, antes de instalarlo, ponerlo en marcha o efectuar tareas de mantenimiento. Las siguientes indicaciones pueden figurar en distintos apartados de esta documentación o estar escritas en el dispositivo. Éstas alertan de posibles peligros o llaman la atención sobre información que aclara o simplifica los procesos del dispositivo.

La inclusión de este icono en una etiqueta "Peligro" o "Advertencia" indica que existe un riesgo de descarga eléctrica, que puede provocar lesiones si no se siguen las instrucciones.

Este es un símbolo de advertencia general. Llama su atención acerca de posibles riesgos de sufrir lesiones. Tenga en cuenta todas las indicaciones bajo este símbolo para evitar lesiones o accidentes mortales.

⚠ PELIGRO

PELIGRO indica una situación inminente de peligro que, si no se evita, **provocará** lesiones graves o incluso la muerte.

⚠ ADVERTENCIA

ADVERTENCIA indica una situación peligrosa que, si no se evita, **puede provocar** la muerte o lesiones graves.

⚠ ATENCIÓN

ATENCIÓN indica una situación potencialmente peligrosa que, si no se evita, **puede provocar** lesiones leves o moderadas.

AVISO

AVISO indica una situación potencialmente peligrosa que, si no se evita, puede provocar daños en el equipo.

Tenga en cuenta lo siguiente: La instalación, el manejo, las revisiones y el mantenimiento de equipos eléctricos deberán ser realizados sólo por personal cualificado. Schneider Electric no se hace responsable de ninguna de las consecuencias del uso de este material.

Una persona cualificada es aquella que cuenta con capacidad y conocimientos relativos a la construcción, el funcionamiento y la instalación de equipos eléctricos, y que ha sido formada en materia de seguridad para reconocer y evitar los riesgos que conllevan tales equipos.

Acerca de este manual

Campo de aplicación

Los datos y las ilustraciones que contiene este manual no son vinculantes. Nosotros nos reservamos el derecho a modificar cualquiera de nuestros productos en serie, según nuestra política de desarrollo continuo de productos. La información incluida en este documento está sujeta a cambios sin previo aviso y no debe interpretarse como un compromiso de Schneider Electric.

Comentarios del usuario

Agradecemos sus comentarios sobre este documento. Envíe sus comentarios a la dirección electrónica techpub@schneider-electric.com

Documentos relacionados

El manual de usuario "Configuración" contiene la información necesaria para la puesta en servicio del dispositivo. Éste le guiará paso a paso desde la primera puesta en marcha hasta la configuración básica para un funcionamiento apropiado a su entorno.

El manual de usuario "Instalación" contiene una descripción del dispositivo, instrucciones de seguridad, una descripción de la pantalla y el resto de información que necesitará para instalar el dispositivo.

El manual de referencia "Interfaz gráfica de usuario" contiene información detallada sobre cómo utilizar la interfaz gráfica de usuario para controlar las funciones individuales del dispositivo.

El manual de referencia "Interfaz de línea de comando" contiene información detallada sobre cómo utilizar la interfaz de línea de comando para controlar las funciones individuales del dispositivo.

El software Network Management de ConneXium Network Manager le ofrece opciones adicionales para una configuración y supervisión fluida:
- Detección de topología automática
- Interfaz del navegador
- Estructura cliente/servidor
- Gestión de eventos
- Registro de eventos
- Configuración simultánea de varios dispositivos
- Interfaz gráfica de usuario con diseño de red
- Pasarela SNMP/OPC

Leyenda

Las designaciones utilizadas en este manual tienen los siguientes significados:

▶	Lista
☐	Paso de trabajo
Enlace	Referencia cruzada con acceso directo
Nota:	Una nota enfatiza un hecho importante o llama su atención sobre una dependencia.
`Courier`	Representación de un comando de la CLI o de contenido de un campo en la interfaz gráfica de usuario

Ejecución en la interfaz gráfica de usuario

Ejecución en la interfaz de línea de comando

Sustituir un dispositivo

El dispositivo ofrece las siguientes soluciones plug-and-play para sustituir un dispositivo por un dispositivo del mismo tipo:

- El dispositivo nuevo carga el perfil de configuración del dispositivo sustituido desde la memoria externa.
  Ver “Carga del perfil de configuración desde la memoria externa” en página 106.
- El dispositivo nuevo recibe su dirección IP usando DHCP *Option 82*.
  Ver “DHCP L2 Relay ‹Retransmisión DHCP L2›” en página 322.
  Ver “Ajuste de un servidor DHCP con la Opción 82” en página 369.

Con cada solución, tras el reinicio, el dispositivo nuevo recibe la misma configuración de IP que tenía el dispositivo sustituido.

- Para acceder a la gestión del dispositivo utilizando HTTPS, el dispositivo utiliza un certificado digital. Tiene la opción de importar su propio certificado al dispositivo.
  Ver “Administración de certificados HTTPS” en página 375.
- Para acceder a la gestión del dispositivo utilizando SSH, el dispositivo utiliza una clave de host RSA. Tiene la opción de importar su propia clave de host en formato PEM al dispositivo.
  Ver “Carga de una clave propia en el dispositivo” en página 372.

1 Interfaces de usuario

El dispositivo le permite especificar la configuración del dispositivo mediante las siguientes interfaces de usuario.

Tabla 1: Interfaces de usuario para acceder a la gestión del dispositivo

Interfaz de usuario	Se puede acceder a través de…	Requisito previo
Interfaz gráfica de usuario	Ethernet (In-Band)	Navegador web
Command Line Interface ‹Interfaz de línea de comando›	Ethernet (In-Band) Interfaz serie (Out-of-Band)	Software de emulación de terminal
Supervisión del sistema	Interfaz serie (Out-of-Band)	Software de emulación de terminal

1.1 Interfaz gráfica de usuario

Requisitos del sistema

Para abrir la interfaz gráfica de usuario, debe tener la versión de escritorio de un navegador web con soporte HTML5.

Nota: Los softwares de terceros, como los navegadores web, validan los certificados basados en criterios como la fecha de caducidad y las recomendaciones actuales de parámetros criptográficos. Los certificados obsoletos pueden ocasionar problemas por información no válida o no actualizada. Ejemplo: Un certificado caducado o un cambio de recomendaciones criptográficas. Para resolver los conflictos de validación con un software de terceros, transfiera su propio certificado al día al dispositivo o vuelva a generar el certificado con el firmware más reciente.

Inicio de la interfaz gráfica de usuario

El requisito previo para iniciar la interfaz gráfica de usuario es que los parámetros IP estén configurados en el dispositivo. Ver “Especificación de los parámetros IP” en página 43.

Lleve a cabo los siguientes pasos:

- ☐ Inicie el navegador web.
- ☐ En el campo de dirección del navegador web, escriba la dirección IP del dispositivo.
  Utilice el siguiente formato: `https://xxx.xxx.xxx.xxx`
  El navegador web establece la conexión con el dispositivo y muestra el cuadro de diálogo de Inicio de sesión.
- ☐ Si desea cambiar el idioma de la interfaz gráfica de usuario, haga clic en el enlace adecuado en la esquina superior derecha del cuadro de diálogo de inicio de sesión.
- ☐ Escriba el nombre de usuario.
- ☐ Escriba la contraseña.
- ☐ Haga clic en el botón *Login*.
  El navegador web muestra la interfaz gráfica de usuario.

1.2 Command Line Interface ‹Interfaz de línea de comando›

La interfaz de línea de comando le permite utilizar las funciones del dispositivo a través de una conexión local o remota.

La interfaz de línea de comando proporciona a los especialistas de TI un entorno familiar para la configuración de dispositivos de TI. Como usuario o administrador experto, dispone del conocimiento básico sobre el uso de los dispositivos Schneider Electric.

1.2.1 Preparación de la conexión de datos

Puede encontrar más información sobre la instalación y puesta en funcionamiento de su dispositivo en el Manual de usuario "Instalación".

- ☐ Conecte el dispositivo a la red. El requisito previo para lograr una conexión de datos correcta es el ajuste adecuado de los parámetros de la red.

Puede acceder a la interfaz de usuario de la interfaz de línea de comando, por ejemplo, con el programa de software gratuito *PuTTY*.

- ☐ Instale el programa *PuTTY* en su ordenador.

1.2.2 Acceso a la interfaz de línea de comando mediante Telnet

Conexión Telnet con Windows

Telnet solo se instala de serie en las versiones de Windows anteriores a Windows Vista.

Lleve a cabo los siguientes pasos:

- ☐ Inicie el programa *Command Prompt* en su ordenador.
- ☐ Introduzca el comando `telnet <IP_address>`.

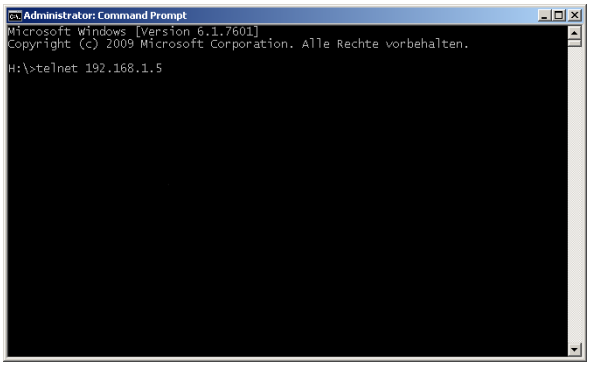


Figura 1: Command Prompt: establecimiento de la conexión Telnet con el dispositivo

Conexión Telnet con PuTTY

Lleve a cabo los siguientes pasos:
- ☐ Inicie el programa *PuTTY* en su ordenador.

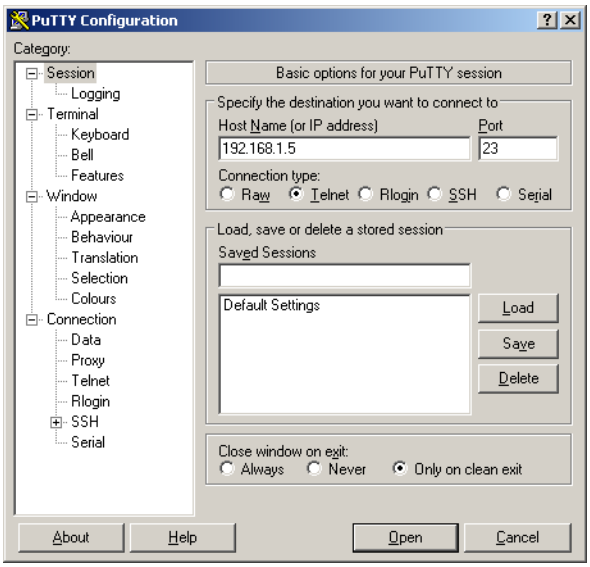


Figura 2: Pantalla de entrada de PuTTY

- ☐ En el campo *Host Name (or IP address)*, introduzca la dirección IP de su dispositivo.
  La dirección IP se compone de 4 números decimales con valores de entre `0` y `255`. Los 4 números decimales están separados por puntos.
- ☐ Para seleccionar el tipo de conexión, seleccione el botón de opción *Telnet* en la lista de opciones *Connection type*.
- ☐ Haga clic en el botón *Open* para establecer la conexión de datos con su dispositivo.
  La interfaz de línea de comando aparecerá en la pantalla con una ventana para introducir el nombre de usuario. El dispositivo admite que hasta 5 usuarios accedan a la interfaz de línea de comando al mismo tiempo.

Nota: Este dispositivo es un producto importante para la seguridad. Cambie la contraseña durante el primer procedimiento de arranque.

Lleve a cabo los siguientes pasos:
- ☐ Escriba el nombre de usuario.
  El nombre de usuario por defecto es `admin`.
- ☐ Pulse la tecla <Intro>.

- ☐ Escriba la contraseña.
  La contraseña por defecto es `private`.
- ☐ Pulse la tecla <Intro>.

```
                    Copyright (c) 2011-2022 Schneider Electric

                                All rights reserved

                             MCSESM-E Release 08.7.00

                            (Build date 2022-07-11 16:29)


                    System Name    :  MCSESM-646038d5e846
                    Management IP  :  192.168.1.5
                    Subnet Mask    :  255.255.255.0
                    Base MAC       :  64:60:38:01:02:03
                    USB IP         :  91.0.0.100
                    USB Mask       :  255.255.255.0
                    System Time    :  2022-07-13 19:40:28


NOTE: Enter '?' for Command Help.  Command help displays all options
      that are valid for the particular mode.
      For the syntax of a particular command form, please
      consult the documentation.

MCSESM-E>
```

Figura 3: Iniciar la pantalla de la interfaz de línea de comando

1.2.3 Acceso a la interfaz de línea de comando mediante SSH (Secure Shell)

En el siguiente ejemplo, se utiliza el programa *PuTTY*. Otra opción para acceder a su dispositivo mediante SSH es la suite OpenSSH.

Lleve a cabo los siguientes pasos:

- ☐ Inicie el programa *PuTTY* en su ordenador.

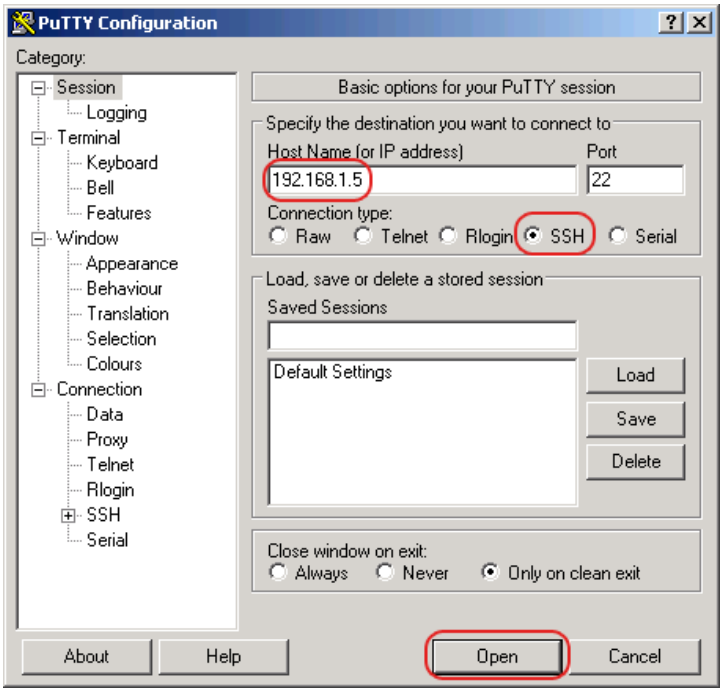


Figura 4: Pantalla de entrada de PuTTY

- ☐ En el campo *Host Name (or IP address)*, introduzca la dirección IP de su dispositivo.
  La dirección IP se compone de 4 números decimales con valores de entre `0` y `255`. Los 4 números decimales están separados por puntos.
- ☐ Para especificar el tipo de conexión, seleccione el botón de opción *SSH* en la lista de opciones *Connection type*.
  Tras seleccionar y configurar los parámetros necesarios, el dispositivo le permite establecer la conexión de datos mediante SSH.

- Haga clic en el botón *Open* para establecer la conexión de datos con su dispositivo.
  En función del dispositivo y del momento de la configuración de SSH, puede transcurrir hasta un minuto para que se establezca la conexión.
  Cuando inicie sesión por primera vez, en la última fase de la configuración de la conexión, el programa *PuTTY* muestra un mensaje de alarma de seguridad y le permite comprobar la huella digital de la clave.

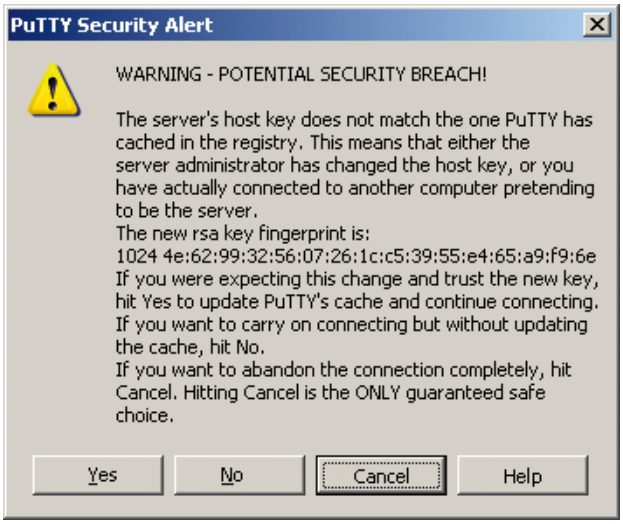


Figura 5: Pregunta de seguridad sobre la huella digital

- Compruebe la huella digital.
  De este modo, podrá protegerse de visitas no deseadas.
- Si la huella digital coincide con la huella digital de la clave del dispositivo, haga clic en el botón *Yes*.
  El dispositivo le permite mostrar las huellas digitales de las claves del dispositivo mediante el comando `show ssh` o en el cuadro de diálogo *Device Security > Management Access > Server*, pestaña *SSH*.
  La interfaz de línea de comando aparecerá en la pantalla con una ventana para introducir el nombre de usuario. El dispositivo admite que hasta 5 usuarios accedan a la interfaz de línea de comando al mismo tiempo.
- Escriba el nombre de usuario.
  El nombre de usuario por defecto es `admin`.
- Pulse la tecla <Intro>.
- Escriba la contraseña.
  La contraseña por defecto es `private`.
- Pulse la tecla <Intro>.

Nota: Este dispositivo es un producto importante para la seguridad. Cambie la contraseña durante el primer procedimiento de arranque.

```
login as: admin
admin@192.168.1.5's password:


                        Copyright (c) 2011-2022 Schneider Electric

                                   All rights reserved

                                MCSESM-E Release 08.7.00

                               (Build date 2022-07-11 16:29)


                    System Name    :  MCSESM-646038d5e846
                    Management IP  :  192.168.1.5
                    Subnet Mask    :  255.255.255.0
                    Base MAC       :  64:60:38:01:02:03
                    USB IP         :  91.0.0.100
                    USB Mask       :  255.255.255.0
                    System Time    :  2022-07-13 19:40:28


NOTE: Enter '?' for Command Help.  Command help displays all options
      that are valid for the particular mode.
      For the syntax of a particular command form, please
      consult the documentation.

MCSESM-E>
```

Figura 6: Iniciar la pantalla de la interfaz de línea de comando

1.2.4 Acceso a la interfaz de línea de comando mediante una interfaz serie

La interfaz serie se utiliza para la conexión local de una estación de administración de red externa (terminal VT100 o PC con emulación de terminal). La interfaz le permite establecer una conexión de datos con la interfaz de línea de comando y la supervisión del sistema.

Lleve a cabo los siguientes pasos:

- ☐ Conecte el dispositivo a un dispositivo final con la interfaz serie. También puede conectar el dispositivo a un puerto COM de su PC a través de la emulación de terminal basada en el VT100 y pulsando cualquier tecla.
- ☐ También puede establecer la conexión de datos en serie entre el dispositivo y la interfaz serie con el programa *PuTTY*. Pulse la tecla <Intro>.

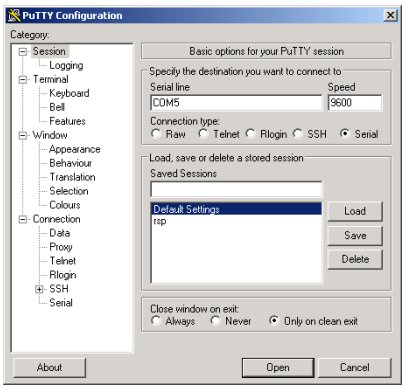


Figura 7: Conexión de datos en serie con la interfaz serie mediante el programa PuTTY.

- ☐ Pulse cualquier tecla del teclado del terminal varias veces hasta que la pantalla de inicio de sesión indique el modo CLI.
- ☐ Escriba el nombre de usuario.
  El nombre de usuario por defecto es `admin`.
- ☐ Pulse la tecla <Intro>.
- ☐ Escriba la contraseña.
  La contraseña por defecto es `private`.
- ☐ Pulse la tecla <Intro>.

Nota: Este dispositivo es un producto importante para la seguridad. Cambie la contraseña durante el primer procedimiento de arranque.

```
                    Copyright (c) 2011-2022 Schneider Electric

                                All rights reserved

                             MCSESM-E Release 08.7.00

                            (Build date 2022-07-11 16:29)


                  System Name   :  MCSESM-646038d5e846
                  Management IP :  192.168.1.5
                  Subnet Mask   :  255.255.255.0
                  Base MAC      :  64:60:38:01:02:03
                  USB IP        :  91.0.0.100
                  USB Mask      :  255.255.255.0
                  System Time   :  2022-07-13 19:40:28


NOTE: Enter '?' for Command Help.  Command help displays all options
      that are valid for the particular mode.
      For the syntax of a particular command form, please
      consult the documentation.

MCSESM-E>
```

Figura 8: Iniciar la pantalla de la interfaz de línea de comando

1.2.5 Jerarquía de comandos en función del modo

En la interfaz de línea de comando, los comandos se agrupan según los modos relacionados en función del tipo de comando. Cada modo de comando admite comandos específicos de software de Schneider Electric.

Los comandos estarán disponibles para usted como usuario en función de su nivel de privilegio (administrador, operador, invitado, auditor). También dependen del modo en el que esté trabajando. Si cambia a un modo específico, los comandos de ese modo estarán disponibles para usted.

Los comandos del modo User Exec son una excepción. La interfaz de línea de comando también le permite ejecutar estos comandos en el modo Privileged Exec.

La siguiente ilustración muestra los modos de la interfaz de línea de comando.

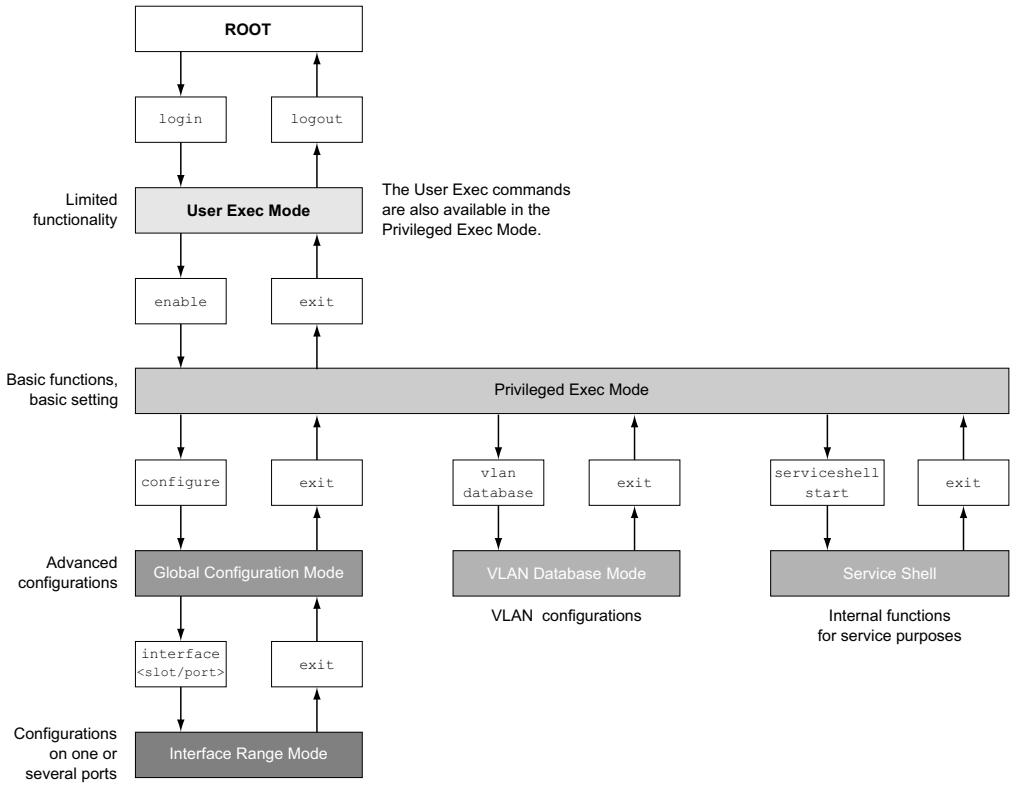


Figura 9: Estructura de la interfaz de línea de comando

En función del nivel de usuario, la interfaz de línea de comando admite los siguientes modos:

- Modo User Exec
  Al iniciar sesión en la interfaz de línea de comando, entra en el modo User Exec. El modo User Exec contiene un número limitado de comandos.
  Símbolo del sistema: `(MCSESM-E) >`
- Modo Privileged Exec
  Para acceder a todos los comandos, debe entrar en el modo Privileged Exec. Si inicia sesión como usuario privilegiado, podrá entrar en el modo Privileged Exec. En el modo Privileged Exec, también podrá ejecutar los comandos del modo User Exec.
  Símbolo del sistema: `(MCSESM-E) #`
- Modo VLAN
  El modo VLAN contiene comandos relativos a la VLAN.
  Símbolo del sistema: `(MCSESM-E) (VLAN)#`
- Service Shell
  Service Shell se utiliza únicamente para fines de asistencia.
  Símbolo del sistema: `/mnt/fastpath #`

- Modo Global Config
  El modo Global Config le permite realizar modificaciones en la configuración actual. Este modo agrupa los comandos de configuración generales.
  Símbolo del sistema: `(MCSESM-E) (config)#`
- Modo Interface Range
  Los comandos del modo Interface Range afectan a un puerto específico, un grupo seleccionado de varios puertos o todos los puertos del dispositivo. Los comandos modifican un valor o conectan/desconectan una función de uno o varios puertos específicos.
  - Todos los puertos físicos del dispositivo
    Símbolo del sistema: `(MCSESM-E) ((interface) all)#`
    Ejemplo: al cambiar del modo Global Config al modo Interface Range, el símbolo del sistema cambia de la siguiente manera:
    ```
    (MCSESM-E) (config)#interface all
    (MCSESM-E) ((Interface)all)#
    ```
  - Un solo puerto en una interfaz
    Símbolo del sistema: `(MCSESM-E) (interface <slot/port>)#`
    Ejemplo: al cambiar del modo Global Config al modo Interface Range, el símbolo del sistema cambia de la siguiente manera:
    ```
    (MCSESM-E) (config)#interface 2/1
    (MCSESM-E) (interface 2/1)#
    ```
  - Una serie de puertos en una interfaz
    Símbolo del sistema: `(MCSESM-E) (interface <interface range> )#`
    Ejemplo: al cambiar del modo Global Config al modo Interface Range, el símbolo del sistema cambia de la siguiente manera:
    ```
    (MCSESM-E) (config)#interface 1/2-1/4
    (MCSESM-E) ((Interface)1/2-1/4)#
    ```
  - Un listado de puertos individuales
    Símbolo del sistema: `(MCSESM-E) (interface <interface list>)#`
    Ejemplo: al cambiar del modo Global Config al modo Interface Range, el símbolo del sistema cambia de la siguiente manera:
    ```
    (MCSESM-E) (config)#interface 1/2,1/4,1/5
    (MCSESM-E) ((Interface)1/2,1/4,1/5)#
    ```
  - Un listado de rangos de puertos y puertos individuales
    Símbolo del sistema: `(MCSESM-E) (interface <complex range>)#`
    Ejemplo: al cambiar del modo Global Config al modo Interface Range, el símbolo del sistema cambia de la siguiente manera:
    ```
    (MCSESM-E) (config)#interface 1/2-1/4,1/6-1/9
    (MCSESM-E) ((Interface)1/2-1/4,1/6-1/9)
    ```

La siguiente tabla muestra los modos de comando, los símbolos del sistema (caracteres de solicitud de entrada) visibles en el modo correspondiente y la opción con la que puede salir del modo.

Tabla 2: Modos de comando

Modo de comando	Método de acceso	Salir o iniciar el siguiente modo

Modo User Exec	Primer nivel de acceso. Realizar tareas básicas y mostrar información del sistema.	Para salir, introduzca `logout`:
		`(MCSESM-E) >logout`
		`Are you sure (Y/N) ?y`

Modo Privileged Exec	Desde el modo User Exec, introduzca el comando `enable`:
	`(MCSESM-E) >enable`
	`(MCSESM-E) #`
		Para salir del modo Privileged Exec y volver al modo User Exec, introduzca `exit`:
		`(MCSESM-E) #exit`
		`(MCSESM-E) >`

Modo VLAN	Desde el modo Privileged Exec, introduzca el comando `vlan database`:
	`(MCSESM-E) #vlan database`
	`(MCSESM-E) (Vlan)#`
		Para finalizar el modo VLAN y volver al modo Privileged Exec, introduzca `exit` o pulse Ctrl Z.
		`(MCSESM-E) (Vlan)#exit`
		`(MCSESM-E) #`

Modo Global Config	Desde el modo Privileged Exec, introduzca el comando `configure`:
	`(MCSESM-E) #configure`
	`(MCSESM-E) (config)#`
	Desde el modo User Exec, introduzca el comando `enable` y, en el modo Privileged Exec, introduzca el comando `Configure`:
	`(MCSESM-E) >enable`
	`(MCSESM-E) #configure`
	`(MCSESM-E) (config)#`
		Para salir del modo Global Config y volver al modo Privileged Exec, introduzca `exit`:
		`(MCSESM-E) (config)#exit`
		`(MCSESM-E) #`
		Para salir otra vez del modo Privileged Exec y volver al modo User Exec, introduzca `exit` de nuevo:
		`(MCSESM-E) #exit`
		`(MCSESM-E) >`

Modo Interface Range	Desde el modo Global Config, introduzca el comando `interface {all|<slot/port>|<interface range>|<interface list>|<complex range>}`.
	`(MCSESM-E) (config)#interface <slot/port>`
	`(MCSESM-E) (interface slot/port)#`
		Para salir del modo Interface Range y volver al modo Global Config, introduzca `exit`. Para volver al modo Privileged Exec, pulse Ctrl Z.
		`(MCSESM-E) (interface slot/port)#exit`
		`(MCSESM-E) #`

Si escribe un signo de interrogación (?) después de que aparezca el símbolo, la interfaz de línea de comando muestra un listado con los comandos disponibles y una breve descripción de los mismos.

```
(MCSESM-E)>
  cli              Set the CLI preferences.
  enable           Turn on privileged commands.
  help             Display help for various special keys.
  history          Show a list of previously run commands.
  logout           Exit this session.
  ping             Send ICMP echo packets to a specified IP address.
  show             Display device options and settings.
  telnet           Establish a telnet connection to a remote host.

(MCSESM-E)>
```

Figura 10: Comandos del modo User Exec

1.2.6 Ejecución de comandos

Análisis de sintaxis

Al iniciar sesión en la interfaz de línea de comando, entra en el modo User Exec. La interfaz de línea de comando muestra el símbolo `(MCSESM-E)>` en pantalla.

Cuando introduzca un comando y pulse la tecla <Intro>, la interfaz de línea de comando iniciará el análisis de sintaxis. La interfaz de línea de comando busca el árbol de comandos para el comando deseado.

Si el comando está fuera del rango de comandos de la interfaz de línea de comando, un mensaje le informará del error detectado.

Por ejemplo:

Desea ejecutar el comando `show system info`, pero introduce `info` sin `f` y pulsa la tecla <Intro>.

A continuación, la interfaz de línea de comando muestra un mensaje:

```
(MCSESM-E)>show system ino

Error: Invalid command 'ino'
```

Árbol de comandos

Los comandos de la interfaz de línea de comando están organizados en una estructura de árbol. Los comandos y, en los casos aplicables, los parámetros relacionados se bifurcan hasta que el comando queda completamente definido y se puede ejecutar. La interfaz de línea de comando verifica la entrada. Si ha introducido el comando y los parámetros íntegra y correctamente, podrá ejecutar el comando con la tecla <Intro>.

Tras introducir el comando y los parámetros requeridos, el resto de parámetros introducidos se tratarán como parámetros opcionales. Si uno de los parámetros es desconocido, la interfaz de línea de comando muestra un mensaje de sintaxis.

El árbol de comandos se ramifica para los parámetros requeridos hasta que hayan alcanzado la última rama de la estructura.

Con los parámetros opcionales, el árbol de comandos se ramifica hasta que los parámetros requeridos y los parámetros opcionales hayan alcanzado la última rama de la estructura.

1.2.7 Estructura de un comando

Esta sección describe la sintaxis, las convenciones y la terminología, y utiliza ejemplos para representarlos.

Formato de los comandos

La mayoría de los comandos incluyen parámetros.

Si falta el parámetro del comando, la interfaz de línea de comando le informará sobre la detección de una sintaxis de comandos incorrecta.

Este manual muestra los comandos y parámetros con el tipo de letra `Courier`.

Parámetros

La secuencia de parámetros es importante para que la sintaxis de un comando sea correcta.

Los parámetros son valores requeridos, valores opcionales, selecciones o una combinación de estos elementos. La representación indica el tipo de parámetro.

Tabla 3: Sintaxis de parámetros y comandos

`<command>`	Los comandos que aparecen entre cuñas (<>) son obligatorios.
`[command]`	Los comandos que aparecen entre corchetes ([]) son opcionales.
`<parameter>`	Los parámetros que aparecen entre cuñas (<>) son obligatorios.
`[parameter]`	Los parámetros que aparecen entre corchetes ([]) son opcionales.
`...`	Los puntos suspensivos (3 puntos en una secuencia, sin espacios) que aparecen detrás de un elemento indican que puede repetir dicho elemento.

Tabla 3: Sintaxis de parámetros y comandos

`[Choice1 | Choice2]`	Una línea vertical entre paréntesis indica una opción de selección. Seleccione un valor. Los elementos separados por una línea vertical y entre corchetes indican una selección opcional (opción 1, opción 2 o ninguna selección).
`{list}`	Las llaves (`{}`) indican que debe seleccionarse un parámetro de una lista de opciones.
`{Choice1 | Choice2}`	Los elementos separados por una línea vertical y entre llaves (`{}`) indican una opción de selección obligatoria (opción 1 u opción 2).
`[param1 {Choice1 | Choice2}]`	Muestra un parámetro opcional que contiene una selección obligatoria.
`<a.b.c.d>`	Las letras en minúsculas son comodines. Introduzca los parámetros con la notación a.b.c.d con puntos decimales (por ejemplo, direcciones IP)
`<cr>`	Pulse la tecla <Intro> para introducir un salto de línea (retorno de carro).

La siguiente lista muestra los valores de parámetros posibles en la interfaz de línea de comando:

Tabla 4: Valores de parámetros en la interfaz de línea de comando

Valor	Descripción
IP address ‹Dirección IP›	Este parámetro representa una dirección IPv4 válida. La dirección se compone de 4 números decimales con valores de entre 0 y 255. Los 4 números decimales están separados por puntos decimales. La dirección IP `0.0.0.0` es una entrada válida.
Dirección MAC	Este parámetro representa una dirección MAC válida. La dirección se compone de 6 números decimales con valores de entre 00 y FFF. Los números están separados por dos puntos, por ejemplo, `00:F6:29:B2:81:40`.
cadena	Texto definido por el usuario con una longitud dentro del rango especificado, por ejemplo, un máximo de 32 caracteres.
cadena de caracteres	Utilice las comillas dobles para indicar una cadena de caracteres, por ejemplo, `"System name with space character"`.
número	Número entero dentro del rango especificado, por ejemplo, `0..999999`.
fecha	Fecha en formato `YYYY-MM-DD`.
hora	Hora en formato `HH:MM:SS`.

Direcciones de red

Las direcciones de red son un requisito para establecer una conexión de datos con una estación de trabajo remota, un servidor u otra red. Se dividen entre direcciones IP y direcciones MAC.

La dirección IP es una dirección asignada por el administrador de red. La dirección IP es única en un área de red.

Las direcciones MAC son asignadas por el fabricante del hardware. Las direcciones MAC son únicas a nivel mundial.

La siguiente tabla muestra la representación y el rango de los tipos de direcciones:

Tabla 5: Formato y rango de direcciones de red

Tipo de dirección	Formato	Rango	Ejemplo
Dirección IP	nnn.nnn.nnn.nnn	nnn: de 0 a 255 (decimal)	192.168.11.110
Dirección MAC	mm:mm:mm:mm:mm:mm	mm: de 00 a ff (pares numéricos hexadecimales)	A7:C9:89:DD:A9:B3

Cadenas

Una cadena está indicada por comillas dobles. Por ejemplo, `"System name with space character"`. Los caracteres de espacio no son cadenas válidas definidas por el usuario. Introduzca un carácter de espacio en un parámetro entre comillas dobles.

Por ejemplo:

```
*(MCSESM-E)#cli prompt Device name
Error: Invalid command 'name'

*(MCSESM-E)#cli prompt 'Device name'

*(Device name)#
```

1.2.8 Ejemplos de comandos

Ejemplo 1: clear arp-table-switch

Comando para eliminar la tabla ARP del agente de administración (caché).

`clear arp-table-switch` es el nombre del comando. El comando se puede ejecutar sin otros parámetros pulsando la tecla <Intro>.

Ejemplo 2: radius server timeout

Comando para la configuración del valor de tiempo de retardo del servidor RADIUS.

```
(MCSESM-E) (config)#radius server timeout
 <1..30>              Timeout in seconds (default: 5).
```

`radius server timeout` es el nombre del comando.

Este parámetro es necesario. El rango del valor es `1..30`.

Ejemplo 3: radius server auth modify <1..8>

Comando para establecer los parámetros del servidor de autenticación RADIUS 1.

```
(MCSESM-E) (config)#radius server auth modify 1
 [name]               RADIUS authentication server name.
 [port]               RADIUS authentication server port.
```

```
                      (default: 1812).
 [msgauth]            Enable or disable the message authenticator
                      attribute for this server.
 [primary]            Configure the primary RADIUS server.
 [status]             Enable or disable a RADIUS authentication
                      server entry.
 [secret]             Configure the shared secret for the RADIUS
                      authentication server.
 [encrypted]          Configure the encrypted shared secret.
  <cr>                Press Enter to execute the command.
```

`radius server auth modify` es el nombre del comando.

El parámetro `<1..8>` (índice del servidor RADIUS) es necesario. El rango del valor es `1..8` (número entero).

Los parámetros `[name]`, `[port]`, `[msgauth]`, `[primary]`, `[status]`, `[secret]` y `[encrypted]` son opcionales.

1.2.9 Símbolo de entrada

Modo de comando

Con el símbolo de entrada, la interfaz de línea de comando muestra en cuál de los tres modos se encuentra:

- `(MCSESM-E) >`
  Modo User Exec
- `(MCSESM-E) #`
  Modo Privileged Exec
- `(MCSESM-E) (config)#`
  Modo Global Config
- `(MCSESM-E) (Vlan)#`
  VLAN Database mode
- `(MCSESM-E) ((Interface)all)#`
  Modo Interface Range/todos los puertos del dispositivo
- `(MCSESM-E) ((Interface)2/1)#`
  Modo Interface Range/un solo puerto en una interfaz
- `(MCSESM-E) ((Interface)1/2-1/4)#`
  Modo Interface Range/un rango de puertos en una interfaz
- `(MCSESM-E) ((Interface)1/2,1/4,1/5)#`
  Modo Interface Range/un listado de puertos individuales
- `(MCSESM-E) ((Interface)1/1-1/2,1/4-1/6)#`
  Modo Interface Range/un listado de rangos de puertos y puertos individuales

Asterisco, símbolo de almohadilla y signo de exclamación

- Asterisco `*`
  Un asterisco `*` en la primera o segunda posición del símbolo de entrada le muestra que los ajustes de la memoria volátil y los ajustes de la memoria no volátil son diferentes. En su configuración, el dispositivo ha detectado modificaciones que no se han guardado.
  `*(MCSESM-E)>`

- Símbolo de almohadilla `#`
  Un símbolo de almohadilla `#` al principio del símbolo de entrada le muestra que los parámetros de inicio y los parámetros durante la fase de inicio son diferentes.
  `*#(MCSESM-E)>`
- Signo de exclamación `!`
  Un signo de exclamación `!` al principio del símbolo de entrada muestra que la contraseña de la cuenta de usuario `user` o `admin` se corresponde con la configuración por defecto.
  `!(MCSESM-E)>`

Comodines

El dispositivo le permite cambiar el símbolo de la línea de comando.

La Interfaz de línea de comando admite los siguientes comodines:

Tabla 6: Uso de comodines en el símbolo de entrada de la interfaz de línea de comando

Comodín	Descripción
`%d`	Fecha del sistema
`%t`	Hora del sistema
`%i`	Dirección IP del dispositivo
`%m`	Dirección MAC del dispositivo
`%p`	Nombre de producto del dispositivo

```
!(MCSESM-E)>enable

!(MCSESM-E)#cli prompt %i

!192.168.1.5#cli prompt (MCSESM-E)%d

!*(MCSESM-E)2022-07-13#cli prompt (MCSESM-E)%d%t

!*(MCSESM-E)2022-07-13 19:40:28#cli prompt %m

!*AA:BB:CC:DD:EE:FF#
```

1.2.10 Combinaciones de teclas

Las siguientes combinaciones de teclas facilitan trabajar con la interfaz de línea de comando:

Tabla 7: Combinaciones de teclas de la interfaz de línea de comando

Combinación de teclas	Descripción
<CTRL> + <H>, <tecla de retroceso>	Borrar el carácter anterior
<CTRL> + <A>	Ir al principio de la línea
<CTRL> + <E>	Ir al final de la línea
<CTRL> + <F>	Adelantar un carácter

Tabla 7: Combinaciones de teclas de la interfaz de línea de comando

Combinación de teclas	Descripción
<CTRL> + <B>	Retroceder un carácter
<CTRL> + <D>	Borrar el carácter actual
<CTRL> + <U>, <X>	Borrar hasta el principio de la línea
<CTRL> + <K>	Borrar hasta el final de la línea
<CTRL> + <W>	Borrar la palabra anterior
<CTRL> + <P>	Ir a la línea anterior en el búfer de historial
<CTRL> + <R>	Reescribir o pegar la línea
<CTRL> + <N>	Ir a la línea siguiente en el búfer de historial
<CTRL> + <Z>	Volver al símbolo de comando raíz
<CTRL> + <G>	Abortar la sesión tcpdump en ejecución
<Tabulador>, <ESPACIO>	Completar la línea de comando
`Exit`	Ir al símbolo de comando inferior
<?>	Opciones de lista

El comando Ayuda muestra en la pantalla las posibles combinaciones de teclas de la interfaz de línea de comando

```
(MCSESM-E) #help

HELP:
Special keys:

  Ctrl-H, BkSp delete previous character
  Ctrl-A  .... go to beginning of line
  Ctrl-E  .... go to end of line
  Ctrl-F  .... go forward one character
  Ctrl-B  .... go backward one character
  Ctrl-D  .... delete current character
  Ctrl-U, X .. delete to beginning of line
  Ctrl-K  .... delete to end of line
  Ctrl-W  .... delete previous word
  Ctrl-P  .... go to previous line in history buffer
  Ctrl-R  .... rewrites or pastes the line
  Ctrl-N  .... go to next line in history buffer
  Ctrl-Z  .... return to root command prompt
  Ctrl-G  .... aborts running tcpdump session
  Tab, <SPACE> command-line completion
  Exit    .... go to next lower command prompt
  ?       .... list choices

(MCSESM-E) #
```

Figura 11: Listado de las combinaciones de teclas con el comando Ayuda

1.2.11 Elementos de entrada de datos

Completar el comando

Para simplificar la escritura de comandos, la interfaz de línea de comando le permite completar los comandos (completar con el tabulador). De este modo, podrá abreviar las palabras clave.

- Escriba el principio de una palabra clave. Si los caracteres introducidos identifican una palabra clave, la interfaz de línea de comando completa la palabra clave si presiona el tabulador o la barra de espacio. Si hay más de una opción para completar la palabra, escriba la letra o letras necesarias para la identificación única de la palabra clave. Pulse el tabulador o la barra de espacio de nuevo. A continuación, el sistema completará el comando o el parámetro.
- Si especifica una entrada que no sea única y pulsa la tecla <Tabulador> o <Espacio> dos veces, la interfaz de línea de comando le proporcionará una lista de opciones.
- Si introduce una entrada que no sea única y pulsa <Tabulador> o <Espacio>, la interfaz de línea de comando completará el comando hasta finalizar la unicidad. Si existen varios comandos y pulsa la tecla <Tabulador> o <Espacio> de nuevo, la interfaz de línea de comando le proporcionará una lista de opciones.
  Por ejemplo:

```
(MCSESM-E) (Config)#lo
(MCSESM-E) (Config)#log
logging logout
```

  Si introduce `lo` y pulsa <Tabulador> o <Espacio>, la interfaz de línea de comando completará el comando hasta finalizar la unicidad y mostrar `log`.
  Si pulsa la tecla <Tabulador> o <Espacio> de nuevo, la interfaz de línea de comando le proporcionará una lista de opciones (`logging logout`).

Comandos/parámetros posibles

Puede obtener una lista de comandos o parámetros posibles escribiendo `help` o `?`; por ejemplo,

```
(MCSESM-E) >show ?
```

Si introduce el comando mostrado, obtendrá una lista de los parámetros disponibles para el comando `show`.

Si introduce el comando sin carácter de espacio delante de un signo de interrogación, el dispositivo le mostrará el texto de ayuda para el propio comando:

```
!*#(MCSESM-E)(Config)#show?

   show          Display device options and settings.
```

1.2.12 Casos prácticos

Grabación de la configuración

Para garantizar que los ajustes de la contraseña y otros cambios de configuración se conserven tras un reinicio del dispositivo o tras la interrupción de la alimentación eléctrica, guarde la configuración. Para ello, siga los siguientes pasos:

- ☐ Introduzca `enable` para cambiar al modo Privileged Exec.
- ☐ Introduzca el siguiente comando:
  `save [profile]`
- ☐ Ejecute el comando pulsando la tecla <Intro>.

Sintaxis del comando "radius server auth add"

Utilice este comando para añadir un servidor de autenticación RADIUS.

- Modo: modo `Global Config`
- Nivel de privilegio: Administrator
- Formato: `radius server auth add <1..8> ip <a.b.c.d> [name <string>] [port <1..65535>]`
  - `[name]`: nombre del servidor de autenticación RADIUS.
  - `[port]`: puerto del servidor de autenticación RADIUS (por defecto: `1813`).

Parámetro	Significado	Valores posibles
`<1..8>`	Índice del servidor RADIUS	`1..8`
`<a.b.c.d>`	Dirección IP del servidor de administración RADIUS.	IP address ‹Dirección IP›
`<string>`	Introduzca un texto definido por el usuario, con un máximo de 32 caracteres.	
`<1..65535>`	Introduzca un número de puerto de entre 1 y 65535.	`1..65535`

Modo y nivel de privilegio:

- Requisito previo para ejecutar el comando: encontrarse en el modo Global Config.
  Ver “Jerarquía de comandos en función del modo” en página 25.
- Requisito previo para ejecutar el comando: disponer del rol de acceso Administrator.

Sintaxis de comandos y parámetros: Ver “Estructura de un comando” en página 30.

Ejemplos para los comandos ejecutables:

- `radius server auth add 1 ip 192.168.30.40`
- `radius server auth add 2 ip 192.168.40.50 name radiusserver2`
- `radius server auth add 3 ip 192.168.50.60 port 1813`
- `radius server auth add 4 ip 192.168.60.70 name radiusserver4 port 1814`

1.2.13 Service Shell

Service Shell se utiliza únicamente para fines de asistencia.

Service Shell permite a los usuarios acceder a funciones internas del dispositivo. Cuando necesite ayuda con su dispositivo, el personal de servicio utilizará Service Shell para supervisar las condiciones internas, por ejemplo, los registros de la CPU o el switch.

AVISO
RIESGO DE QUE NO FUNCIONE EL DISPOSITO No ejecute ninguna función interna, como eliminar la memoria no volátil (*NVM*) sin seguir las instrucciones del servicio técnico. **El incumplimiento de estas instrucciones puede provocar que no funcione el dispositivo.**

Cómo iniciar Service Shell

Como requisito previo, debe encontrarse en el modo User Exec: `(MCSESM-E) >`

Lleve a cabo los siguientes pasos:

- ☐ Introduzca `enable` y pulse la tecla <Intro>.
  Para reducir el esfuerzo al escribir:
  - Introduzca `e` y pulse la tecla <Tabulador>.
- ☐ Introduzca `serviceshell start` y pulse la tecla <Intro>.
  Para reducir el esfuerzo al escribir:
  - Introduzca `ser` y pulse la tecla <Tabulador>.
  - Introduzca `s` y pulse la tecla <Tabulador>.

```
!MCSESM-E >enable

!*MCSESM-E #serviceshell start
 WARNING! The service shell offers advanced diagnostics and functions.
 Proceed only when instructed by a service technician.

 You can return to the previous mode using the 'exit' command.

 BusyBox v1.31.0 (2022-07-13 19:40:28 UTC) built-in shell (ash)
 Enter 'help' for a list of built-in commands.

!/mnt/fastpath #
```

Trabajo con Service Shell

Cuando Service Shell esté activo, el tiempo de espera de la interfaz de línea de comando estará inactivo. Para ayudar a evitar las incoherencias de configuración, finalice Service Shell antes de que otro usuario empiece a transferir una nueva configuración al dispositivo.

Visualización de los comandos de Service Shell

Como requisito previo, debe haber iniciado Service Shell.

Lleve a cabo los siguientes pasos:
☐ Introduzca `help` y pulse la tecla <Intro>.

```
/mnt/fastpath # help
Built-in commands:
------------------
        . : [ [[ alias bg break cd chdir command continue echo eval exec
        exit export false fg getopts hash help history jobs kill let
        local pwd read readonly return set shift source test times trap
        true type ulimit umask unalias unset wait
/mnt/fastpath #
```

Finalización de Service Shell

Lleve a cabo los siguientes pasos:
☐ Introduzca `exit` y pulse la tecla <Intro>.

Cómo desactivar Service Shell de forma permanente en el dispositivo

Si desactiva Service Shell, todavía podrá configurar el dispositivo. No obstante, limitará las posibilidades del personal de servicio de realizar el diagnóstico del sistema. El técnico de servicio dejará de tener acceso a las funciones internas de su dispositivo.

La desactivación es irreversible. Service Shell permanecerá desactivado permanentemente. **Para poder activar de nuevo Service Shell, el dispositivo requiere el desmontaje por parte del fabricante.**

Requisitos previos:
- Service Shell no se ha iniciado.
- Se encuentra en modo User Exec: `(MCSESM-E) >`

Lleve a cabo los siguientes pasos:
☐ Introduzca `enable` y pulse la tecla <Intro>.
  Para reducir el esfuerzo al escribir:
  – Introduzca `e` y pulse la tecla <Tabulador>.

- ☐ Introduzca `serviceshell deactivate` y pulse la tecla <Intro>.
  Para reducir el esfuerzo al escribir:
  - Introduzca `ser` y pulse la tecla <Tabulador>.
  - Introduzca `dea` y pulse la tecla <Tabulador>.
- ☐ **¡Este paso es irreversible!**
  Pulse la tecla <Y>.

```
!MCSESM-E >enable

!*MCSESM-E #serviceshell deactivate
Notice: If you continue, then the Service Shell is permanently deactivated.
This step is irreversible!
For details, refer to the Configuration Manual.
Are you sure (Y/N) ?
```

1.3 Supervisión del sistema

La supervisión del sistema le permite establecer parámetros de funcionamiento básicos antes de iniciar el sistema operativo.

1.3.1 Alcance funcional

En la supervisión del sistema, puede realizar las siguientes tareas, por ejemplo:
- Administrar el sistema operativo y verificar la imagen del software
- Actualizar el sistema operativo
- Iniciar el sistema operativo
- Eliminar perfiles de configuración, restablecer la configuración de fábrica del dispositivo
- Comprobar la información del código de inicio

1.3.2 Inicio de la supervisión del sistema

Establece una conexión en serie con el dispositivo mediante la interfaz USB-C. Durante el proceso de arranque, la interfaz en serie del dispositivo no está disponible. Por esta razón, el inicio de la supervisión del sistema funciona de forma distinta a otros dispositivos Schneider Electric. Para iniciar la supervisión del sistema, ajuste el dispositivo al modo recuperación.

Ajuste el dispositivo al modo recuperación

Accesorios necesarios:
- Memoria externa (recomendada: ACA22-USB-C)
- Adaptador USB-C a USB-A (solo si utiliza una memoria externa distinta a la recomendada)
- Cable USB para conectar el puerto USB-C del dispositivo al ordenador
- Ordenador con emulación de terminal VT100 (por ejemplo, PuTTY) o terminal serie

Lleve a cabo los siguientes pasos:
- ☐ Conecte la memoria externa a su ordenador.
- ☐ En el directorio raíz de la memoria externa, cree un archivo vacío denominado `recovery.txt`.
- ☐ Conecte la memoria externa al dispositivo.
- ☐ Reinicie el dispositivo.
- ☐ Observe los LED mientras está arrancando el dispositivo. Cuando el *Status* LED parpadea alternativamente en rojo y verde, el dispositivo ha arrancado correctamente en el modo recuperación.

Nota: Encontrará la descripción de los elementos de la pantalla en el manual de usuario “Instalación”.

Acceso a la supervisión del sistema

Lleve a cabo los siguientes pasos:
- ☐ Desconecte la memoria externa del dispositivo.
- ☐ Conecte su ordenador al dispositivo mediante el cable USB.
- ☐ Abra la emulación de terminal VT100 del ordenador para visualizar la supervisión del sistema.
- ☐ Seleccione el puerto COM adecuado.

Cuando el ordenador y el dispositivo están conectados correctamente, verá una pantalla negra.

Lleve a cabo los siguientes pasos:
- ☐ Pulse la tecla <Intro> para visualizar la supervisión del sistema.
  Tendrá la siguiente vista en su ordenador:

```
System Monitor 1
(Selected OS: ...-8.7 (2022-07-11 16:29))

1  Manage operating system
3  Start selected operating system
4  Manage configurations
5  Show boot code information
q  End (reset and reboot)




sysMon1>
```

Figura 12: System Monitor vista

- ☐ Para seleccionar un elemento del menú, introduzca el número correspondiente.
- ☐ Para salir de un submenú y volver al menú principal, pulse la tecla <ESC>.

Nota: Para iniciar de forma normal el dispositivo la próxima vez, solamente añada la memoria externa sin el archivo `recovery.txt`.

2 Especificación de los parámetros IP

Al instalar por primera vez el dispositivo, debe introducir parámetros IP.

El dispositivo ofrece las siguientes opciones para especificar los parámetros IP durante la primera instalación:

- Introducción mediante la interfaz de línea de comando.
  Al configurar previamente el dispositivo fuera de su entorno de uso o restaurar el acceso a la red ("In-Band") del dispositivo, seleccione este método "Out-of-Band".
- Introducción con el protocolo Ethernet Switch Configurator.
  Si ha instalado previamente un dispositivo de red o dispone de otra conexión de datos entre su PC y el dispositivo, seleccione el método "In-Band".
- Configuración mediante la memoria externa.
  Cuando sustituya un dispositivo por otro del mismo tipo y ya haya guardado la configuración en la memoria externa, seleccione este método.
- Uso de BOOTP.
  Para configurar el dispositivo instalado mediante BOOTP, seleccione el método "In-Band". Para ello, se requiere un servidor BOOTP. El servidor BOOTP asigna los datos de configuración al dispositivo mediante su dirección MAC. El modo DHCP es el modo por defecto para la referencia de los datos de configuración.
- Configuración mediante DHCP.
  Para configurar el dispositivo instalado mediante DHCP, seleccione el método "In-Band". Para ello, se requiere un servidor DHCP. El servidor DHCP asigna los datos de configuración al dispositivo mediante su dirección MAC o el nombre del sistema.
- Configuración mediante la interfaz gráfica de usuario.
  Si el dispositivo ya tiene una dirección IP y se puede acceder a él a través de la red, la interfaz gráfica de usuario le proporcionará otra opción para configurar los parámetros IP.

2.1 Principios básicos de los parámetros IP

2.1.1 IPv4

IP address ‹Dirección IP›

Las direcciones IP están compuestas de 4 bytes. Escriba estos 4 bytes en notación decimal, separados por un punto decimal.

RFC 1340, escrito en 1992, define 5 clases de direcciones IP.

Tabla 8: Clases de direcciones IP

Clase	Dirección de red	Host address ‹Dirección de host›	Rango de direcciones
A	1 Byte	3 Bytes	0.0.0.0 a 127.255.255.255
B	2 Bytes	2 Bytes	128.0.0.0 a 191.255.255.255
C	3 Bytes	1 Byte	192.0.0.0 a 223.255.255.255
D			224.0.0.0 a 239.255.255.255
E			240.0.0.0 a 255.255.255.255

El primer byte de una dirección IP es la dirección de la red. El primer organismo mundial para conceder direcciones de red es la IANA ("Internet Assigned Numbers Authority"). Si requiere un bloque de direcciones IP, póngase en contacto con su Internet Service Provider (ISP). Su ISP se pondrá en contacto con su organización de nivel superior para reservar un bloque de direcciones IP:

- APNIC (Asia Pacific Network Information Center)
  Región de Asia/Pacífico
- ARIN (American Registry for Internet Numbers)
  América y África subsahariana
- LACNIC (Regional Latin-American and Caribbean IP Address Registry)
  Latinoamérica y algunas islas del Caribe
- RIPE NCC (Réseaux IP Européens)
  Europa y las regiones colindantes

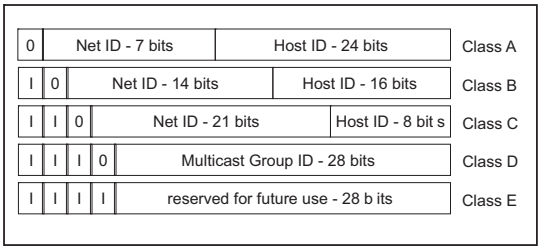


Figura 13: representación de bits de direcciones IP

Cuando el primer bit de una dirección IP es cero, significa que pertenece a la clase A, por ejemplo, el primer octeto es inferior a 128.

Cuando el primer bit de una dirección IP es un uno y el segundo es un cero, significa que pertenece a la clase B, por ejemplo, el primer octeto se encuentra entre 128 y 191.

Cuando los primeros 2 bits de una dirección IP son un uno, significa que pertenece a la clase C, por ejemplo, el primer octeto es superior a 191.

El operador de red es responsable de asignar la dirección de host (host ID). Solo el operador de red es responsable de la unicidad de las direcciones IP asignadas.

Netmask ‹Máscara de red›

Los enrutadores y Gateways subdividen las redes grandes en subredes. La máscara de red asigna las direcciones IP de los dispositivos individuales a una subred particular.

Puede realizar la división en subredes con la máscara de red de manera muy similar a la división de direcciones de red (ID de red) entre las clases A y C.

Configure los bits de la dirección de host (ID de host) que correspondan a la máscara en uno. Configure el resto de los bits de la dirección de host en cero (consulte los siguientes ejemplos).

Ejemplo de una máscara de subred:

Decimal notation
255.255.192.0

Binary notation
11111111.11111111.11000000.00000000

Subnetwork mask bits
Class B

Ejemplo de aplicación de la máscara de subred a las direcciones IP para la asignación de subredes:

Decimal notation
129.218.65.17
128 < 129 191 › Class B

Binary notation
10000001.11011010.01000001.00010001
Subnetwork 1
Network address

Decimal notation
129.218.129.17
128 < 129 191 › Class B

Binary notation
10000001.11011010.10000001.00010001
Subnetwork 2
Network address

Ejemplo de utilización de la máscara de red

En una red grande, es posible que las Gateways y los enrutadores separen al agente de administración de su estación de administración de red. ¿Cómo se asignan direcciones en tal caso?

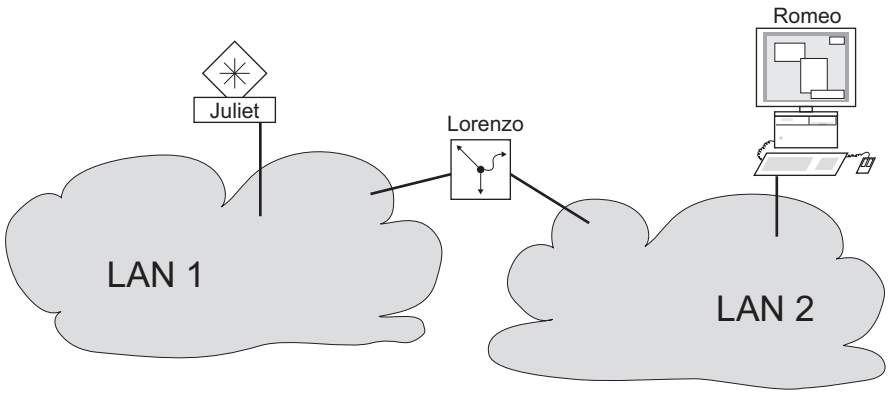


Figura 14: El agente de administración es separado por el enrutador de la estación de administración de red

La estación de administración de red "Romeo" desea enviar datos a la agente de administración "Julieta". Romeo conoce la dirección IP de Julieta y que el enrutador "Lorenzo" conoce la ruta hasta Julieta.

Romeo mete su mensaje en un sobre y escribe como dirección de destino la dirección IP de Julieta y la suya como dirección de origen.

A continuación, Romeo mete ese sobre en otro con la dirección MAC de Lorenzo como dirección de destino y la suya como dirección de origen. Este proceso es similar a la transición de la Capa 3 a la Capa 2 del modelo de referencia básico ISO/OSI.

Finalmente, Romeo pone el paquete de datos completo en el buzón, que es como ir de la Capa 2 a la Capa 1, lo que significa que envía el paquete de datos a través de Ethernet.

Lorenzo recibe la carta, retira el sobre exterior y se da cuenta, por el sobre interior, de que la carta era para Julieta. Coloca el sobre interior en un nuevo sobre exterior y busca su lista de direcciones (la tabla ARP) para encontrar la dirección MAC de Julieta; escribe su dirección MAC en el sobre exterior como dirección de destino y su propia dirección MAC como dirección de origen. A continuación, pone el paquete de datos completo en el buzón.

Julieta recibe la carta y quita el sobre exterior. Encuentra el sobre interior con la dirección IP de Romeo. Abrir el sobre interior y leer su contenido corresponde a transferir el mensaje a las capas más altas del protocolo del modelo de capas ISO/OSI.

Julieta desea enviar una respuesta a Romeo. Mete la respuesta en un sobre con la dirección de Romeo como dirección de destino y la suya como dirección de origen. Pero ¿adónde debe enviar ella la respuesta? No ha recibido la dirección MAC de Romeo. La dirección MAC de Romeo se ha perdido porque Lorenzo ha cambiado el sobre exterior.

En la MIB, Julieta encuentra a Lorenzo en la variable `NetGatewayIPAddr` como intermediario de Romeo. Por lo tanto, mete el sobre con las direcciones de IP en otro sobre con la dirección de destino MAC de Lorenzo.

A continuación, la carta sigue el mismo camino hasta Romeo pasando por Lorenzo, igual que lo hizo entre Romeo y Julia.

Classless Inter-Domain Routing

La clase C, con un máximo de 254 direcciones, era demasiado pequeña, y la clase B, con un máximo de 65534 direcciones, era, para la mayoría de los usuarios, demasiado grande. Esto da como resultado un uso no efectivo de las direcciones de clase B disponibles.

La clase D contiene direcciones Multicast reservadas. La clase E está reservada a fines de ensayo. Una Gateway no participante ignora los datagramas experimentales con estas direcciones de destino.

Desde 1993, RFC 1519 ha utilizado Classless Inter-Domain Routing (CIDR) para proporcionar una solución. CIDR supera los límites de clase y es compatible con rangos de direcciones IP sin clase.

Con CIDR, puede especificar el número de bits que caracterizan al rango de direcciones IP. Representa el rango de direcciones IP en formato binario y hace el recuento de los bits de la máscara que designan la máscara de red. Los bits de la máscara equivalen al número de bits utilizados para la subred en un rango de direcciones IP.

Por ejemplo:

IP address, decimal	Network mask, decimal	IP address, binary
192.168.112.1	255.255.255.128	11000000 10101000 01110000 00000001
192.168.112.127		11000000 10101000 01110000 01111111

25 mask bits

CIDR notation: 192.168.112.0/25

Mask bits

El término "creación de subredes" se refiere al rastreo de una serie de rangos de direcciones de clase C. Con la creación de subredes, los rangos de direcciones de la clase B se pueden subdividir muy bien.

2.1.2 IPv6

Principios básicos de los parámetros IP

El protocolo de Internet versión 6 (IPv6) es la nueva versión del protocolo de Internet versión 4 (IPv4). La necesidad de implementar IPv6 se debía al hecho de que las direcciones IPv4 no son suficientes en el contexto del Internet actual en continuo crecimiento. El protocolo IPv6 se describe en RFC 8200.

Algunas de las diferencias entre IPv6 e IPv4 son las siguientes:
- Representación y longitud de las direcciones
- Ausencia del tipo de dirección de difusión
- Estructura de encabezado simplificada
- Fragmentación realizada únicamente por el host de origen
- Capacidades añadidas para la identificación del flujo de paquetes en la red

Los protocolos IPv4 y IPv6 pueden funcionar a la vez en el dispositivo. Esto es posible gracias al uso de la técnica capa IP dual, también denominada pila dual.

Nota: Si desea que el dispositivo funcione solo utilizando la función IPv4, desactive la función IPv6 en el dispositivo.

En el dispositivo, el protocolo IPv6 tiene las siguientes restricciones:
- Puede especificar un número máximo de 8 direcciones unicast IPv6 del modo siguiente:
  - 4 direcciones IPv6 utilizando la configuración manual
  - 2 direcciones IPv6 cuando se selecciona el botón de opción *Auto*
  - 1 dirección IPv6 utilizando el servidor DHCPv6
  - 1 dirección de enlace-local
- La función IPv6 solo puede activarse en la interfaz de gestión. Puede utilizarse el número total de direcciones IPv6 configurables a la vez en la interfaz.
- Las direcciones IPv6 pueden utilizarse para establecer la dirección IP de gestión del dispositivo. Entre otros servicios en los que se pueden utilizar direcciones IPv6 se incluyen por ejemplo SNTP, SYSLOG, DNS y LDAP.

Representación de direcciones

La dirección IPv6 está compuesta por 128 bytes. Está representada como 8 grupos de 4 dígitos hexadecimales, y cada uno representa 16 bits, denominados además hextets. Los hextets están separados por dos puntos (:). Las direcciones IPv6 no distinguen entre mayúsculas y minúsculas y puede escribirlos de ambas maneras.

De acuerdo con RFC 4291, el formato preferido de una dirección IPv6 es x:x:x:x:x:x:x:x. Cada “x” consta de 4 valores hexadecimales y representa un hextet. En la ilustración siguiente se muestra un ejemplo de un formato preferido de una dirección IPv6.

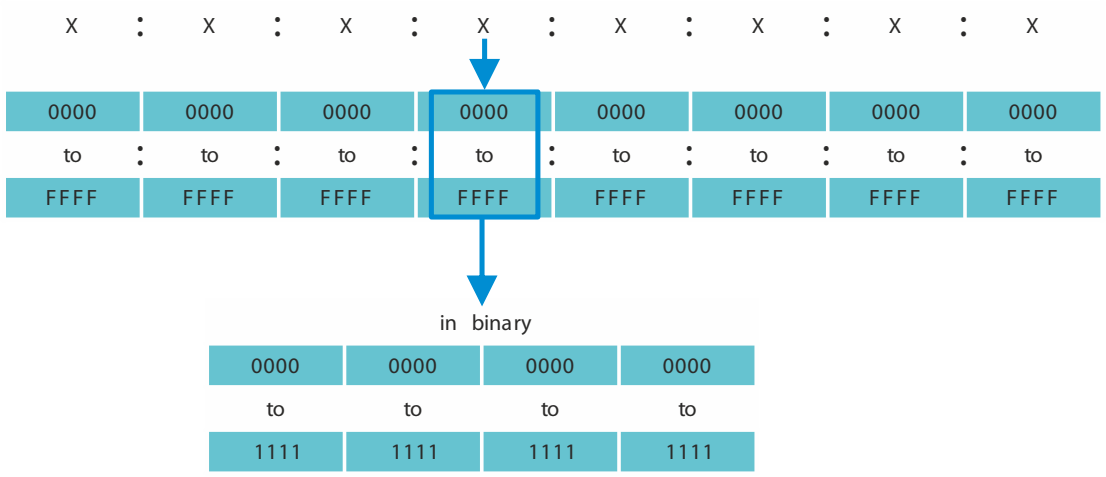


Figura 15: Representación de la dirección IPv6

Como puede ver en la ilustración anterior, normalmente las direcciones IPv6 contienen muchos ceros. Para acortar las direcciones IPv6 que contienen 0 bits, es necesario seguir 2 reglas de escritura:

- La primera regla consiste en descartar los ceros iniciales en cada hextet. Esta regla solamente se aplica a los ceros iniciales y no a los finales de un hextet. Si también se descartan los ceros finales, la dirección resultante será ambigua.
- La segunda regla utiliza una sintaxis especial para comprimir los ceros. Puede utilizar 2 dos puntos adyacentes “::” para sustituir una cadena de hextets adyacentes que solo contienen ceros. El signo “::” solamente puede utilizarse una vez en las direcciones. Si se utiliza el signo “::” más de una vez en la representación de una dirección, puede que se expanda más de una posible dirección de esa notación.

Cuando se aplican las dos reglas, el resultado se conoce comúnmente como formato comprimido.

En la tabla siguiente puede encontrar 2 ejemplos de cómo se aplican estas reglas:

Tabla 9: Compresión de la dirección IPv6

Preferida	CC03:0000:0000:0000:0001:AB30:0400:FF02
Sin ceros iniciales	CC03: 0: 0: 0: 1:AB30: 400:FF02
Comprimida	CC03::1:AB30:400:FF02

Preferida	2008:00B7:0000:DEF0:DDDD:0000:E604:0001
Sin ceros iniciales	2008: B7: 0:DEF0:DDDD: 0:E604: 1
Comprimida	2008:B7::DEF0:DDDD:0:E604:1

Longitud del prefijo

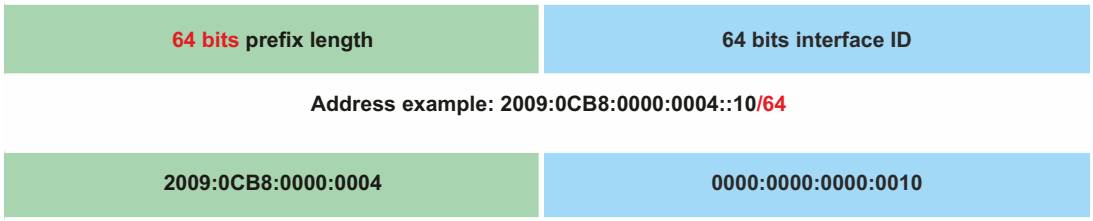
Al contrario que una dirección IPv4, la dirección IPv6 no utiliza una máscara de subred para identificar la parte de red de una dirección. En su lugar, el protocolo IPv6 utiliza la longitud del prefijo.

La representación del texto de los prefijos de las direcciones IPv6 es similar al modo en que se escriben los prefijos de las direcciones IPv4 en Classless Inter-Domain Routing (CIDR):

```
<ipv6-address>/<prefix-length>
```

El rango de longitud del prefijo está comprendido entre `0..128`. La longitud habitual del prefijo de IPv6 para las LAN y otros tipos de redes es de /64. Esto significa que la parte de la red de la dirección ocupa 64 bits de longitud. Los 64 bits restantes representan la ID de la interfaz, de modo similar a la parte del host de la dirección IPv4.

En la ilustración siguiente puede encontrar un ejemplo de asignación de bits de longitud de prefijo.



Tipos de direcciones

Los tipos de direcciones IPv6 se describen en RFC 4291.

Los tipos de direcciones IPv6 se identifican mediante los bits de orden superior de la dirección, tal y como se muestra en la tabla siguiente:

Tabla 10: Tipos de direcciones IPv6

Tipo de dirección	Prefijo binario	Notación IPv6
Sin especificar	00...0 (128 bits)	::/128
De bucle de retorno	00...1 (128 bits)	::1/128
Multicast	11111111	FF00::/8
Unicast de enlace-local	1111111010	FE80::/10
Unicast global	(everything else)	

La dirección sin especificar

La dirección IPv6 con cada bit establecido en 0 se denomina dirección sin especificar, y se corresponde con 0.0.0.0 en IPv4. La dirección sin especificar solo se utiliza para indicar la ausencia de una dirección. Normalmente se utiliza como dirección de origen si todavía no se ha determinado una dirección única.

Nota: La dirección sin especificar no se puede asignar a una interfaz como dirección de destino.

Dirección de bucle de retorno

La dirección unicast 0:0:0:0:0:0:0:1 se denomina dirección de bucle de retorno. Puede ser utilizada por un dispositivo para enviarse un paquete IPv6 a sí mismo. No se puede asignar a una interfaz física.

La dirección Multicast

IPv6 no dispone de una dirección broadcast como IPv4. Pero existe una dirección Multicast para todos los nodos IPv6, que esencialmente ofrece el mismo resultado.

Se utiliza una dirección Multicast IPv6 para enviar un paquete IPv6 a varios destinos. La estructura de una dirección Multicast es la siguiente: Los siguientes 4 bits identifican el alcance de la dirección Multicast (hasta dónde se transmite el paquete):

- Los primeros 8 bits están establecidos en `FF`.
- Los 4 bits siguientes equivalen a la vida útil de la dirección: El valor 0 equivale a una duración permanente y 1, a una temporal.
- Los siguientes 4 bits identifican el alcance de la dirección Multicast (hasta dónde se transmiten los paquetes a través de la red).

La dirección de enlace-local

La dirección de enlace local se utiliza para comunicarse con otros dispositivos del mismo enlace. El término "enlace" hace referencia a una subred. Los enrutadores no reenvían paquetes con direcciones de origen o destino de enlace-local a otros enlaces.

Las direcciones de enlace-local se utilizan para transmitir paquetes de un único enlace para ámbitos como la configuración automática de direcciones, descubrimiento de elementos cercanos o cuando no hay ningún enrutador presente. Tienen el formato siguiente:

Tabla 11: Formato de dirección de enlace-local

10 bits	54 bits	64 bits
1111111010	0	ID de interfaz

La dirección de enlace-local está siempre configurada y no se puede cambiar.

La dirección unicast global

Las direcciones unicast globales son únicas globalmente y se pueden dirigir a través de Internet. Este tipo de direcciones son equivalentes a las direcciones IPv4 públicas. Actualmente, solo se asignan las direcciones unicast globales con los primeros tres bits de 001 o 2000::/3.

Las direcciones unicast globales están compuestas por 3 partes:

- Prefijo de enrutamiento global
- ID de subred
- ID de interfaz.

El prefijo de enrutamiento global es la parte correspondiente a la red de la dirección.

La ID de la subred es utilizado por una organización para identificar sus subredes y tiene una longitud de hasta 16 bits. La longitud de la ID de subred la proporciona la longitud del prefijo de enrutamiento global.

La ID de interfaz identifica una interfaz de un nodo en particular. El término ID de interfaz se utiliza debido a que un host puede tener varias interfaces, cada una con una o más direcciones IPv6.

El formato general de las direcciones unicast globales IPv6 se representa en la ilustración siguiente.

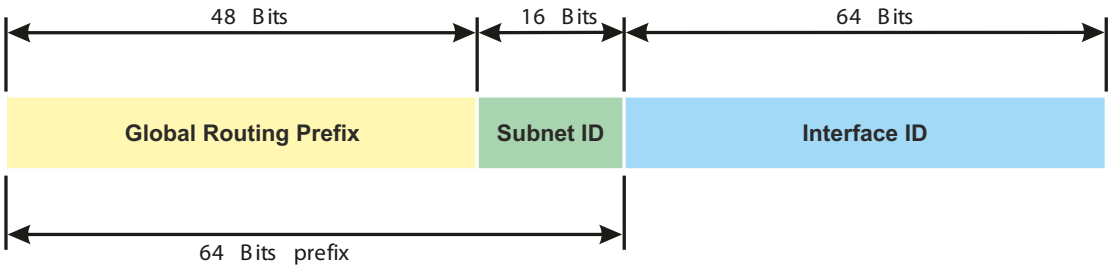


Figura 16: Formato general de direcciones unicast globales IPv6

2.2 Especificación de los parámetros IP con la interfaz de línea de comando

2.2.1 IPv4

Se ofrecen los siguientes métodos para introducir los parámetros IP:
- Protocolo BOOTP/
- Ethernet Switch Configurator
- External memory ‹Memoria externa›
- Interfaz de línea de comandos que utiliza la conexión serie

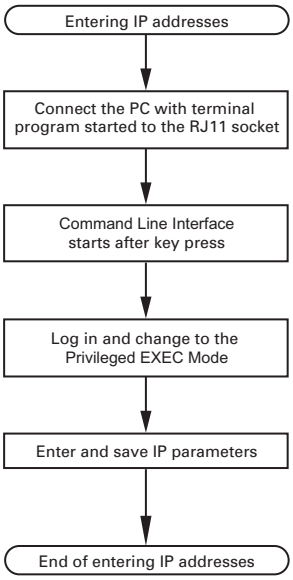
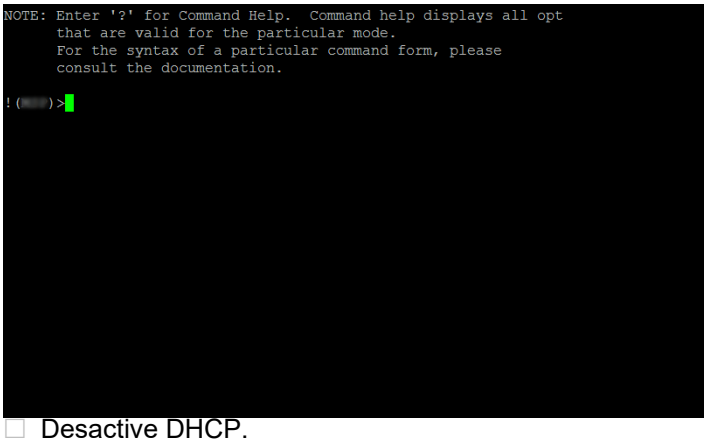


Figura 17: Diagrama del proceso para introducir direcciones IP

Nota: Si no hay disponible ningún terminal o PC con una emulación de terminal en las proximidades de la ubicación de la instalación, puede configurar el dispositivo en su propia estación de trabajo y llevarlo a la ubicación final de instalación.

Lleve a cabo los siguientes pasos:
- ☐ Establezca una conexión con el dispositivo.
  Aparecerá la pantalla de inicio.



- ☐ Desactive DHCP.

- ☐ Escriba los parámetros IP.
  - ▶ Dirección IP local
    Con la configuración por defecto, la dirección IP local es `0.0.0.0`.
  - ▶ Netmask ‹Máscara de red›
    Tras haber dividido la red en subredes e identificar estas con una máscara de red, introduzca la máscara de red aquí. Con la configuración por defecto, la máscara de red local es `0.0.0.0`.
  - ▶ Dirección IP de la Gateway.
    Esta entrada solo se requiere cuando el dispositivo y la estación de administración de red o el servidor TFTP estén ubicados en subredes diferentes (ver en página 45 “Ejemplo de utilización de la máscara de red”).
    Especifique la dirección IP de la Gateway entre la subred con el dispositivo y la ruta a la estación de administración de red.
    Con la configuración por defecto, la dirección IP es `0.0.0.0`.
- ☐ Guarde la configuración especificada mediante `copy config running-config nvm`.

`enable`	Cambiar al modo Privileged EXEC.
`network protocol none`	Desactivar DHCP.
`network parms 10.0.1.23 255.255.255.0`	Asignar al dispositivo la dirección IP `10.0.1.23` y la máscara de red `255.255.255.0`. También puede asignar una dirección de Gateway.
`copy config running-config nvm`	Guardar la configuración actual en la memoria no volátil (`nvm`) del perfil de configuración "seleccionado".

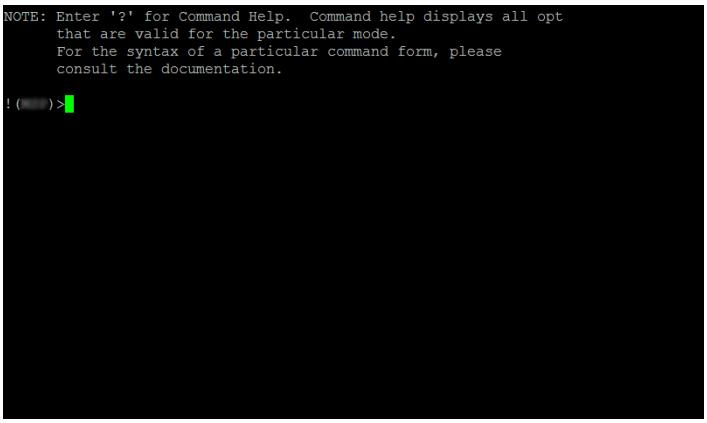
Tras especificar los parámetros IP, puede configurar fácilmente el dispositivo con la interfaz gráfica de usuario.

2.2.2 IPv6

El dispositivo le permite especificar los parámetros de IPv6 mediante la interfaz de línea de comandos a través de la interfaz serie. Otra opción para acceder a la interfaz de línea de comandos consiste en utilizar una conexión SSH mediante el uso de la dirección de gestión IPv4.

Lleve a cabo los siguientes pasos:

- ☐ Establezca una conexión con el dispositivo.
  Aparecerá la pantalla de inicio.



- ☐ Active el protocolo IPv6 si está desactivado.
- ☐ Introduzca los parámetros de IPv6.
  - ▶ Dirección IPv6
    Dirección IPv6 válida. La dirección IPv6 se muestra en formato comprimido.
  - ▶ Longitud del prefijo
    Al contrario que una dirección IPv4, la dirección IPv6 no utiliza una máscara de subred para identificar la parte de red de una dirección. Esta función se lleva a cabo en IPv6 mediante la longitud del prefijo (ver en página 49 “Longitud del prefijo”).
  - ▶ Función *EUI option*
    Puede utilizar la función *EUI option* para configurar automáticamente la ID de la interfaz de la dirección IPv6. El dispositivo utiliza la dirección MAC de su interfaz con los valores `ff` y `fe` añadidos entre el byte 3 y el byte 4 para generar un ID de interfaz de 64 bits.
    Solamente puede seleccionar esta opción para direcciones IPv6 que tengan una longitud de prefijo equivalente a `64`.
  - ▶ Dirección de puerta de enlace IPv6
    La dirección de puerta de enlace IPv6 es la dirección de un enrutador a través del cual el dispositivo accede a otros dispositivos de fuera de su propia red.
    Puede especificar cualquier dirección IPv6 excepto direcciones de bucle de retorno y *Multicast*.
    Con la configuración por defecto, la dirección de puerta de enlace IPv6 es `::`.

`enable`	Cambiar al modo Privileged EXEC.
`network ipv6 operation`	Active el protocolo IPv6 si está desactivado. Con la configuración por defecto, el protocolo IPv6 está activado.
`network ipv6 address add 2001::1 64 eui-64`	Asigne la dirección IPv6`2001::1` y la longitud del prefijo `64`. El parámetro `eui-64` es opcional. Se puede asignar de forma opcional una dirección de puerta de enlace.
`copy config running-config nvm`	Guardar la configuración actual en la memoria no volátil (`nvm`) del perfil de configuración "seleccionado".

Tras especificar los parámetros de IPv6, puede configurar fácilmente el dispositivo con la interfaz gráfica de usuario. Para utilizar una dirección IPv6 en una URL, utilice la siguiente sintaxis de URL:`https://[<ipv6_address>]`.

2.3 Especificación de los parámetros IP mediante Ethernet Switch Configurator

El protocolo Ethernet Switch Configurator le permite asignar parámetros IP al dispositivo mediante Ethernet.

Puede configurar fácilmente otros parámetros con la interfaz gráfica de usuario.

Instale el software Ethernet Switch Configurator en su PC.

Lleve a cabo los siguientes pasos:
- Inicie el programa Ethernet Switch Configurator.

Cuando Ethernet Switch Configurator se haya iniciado, Ethernet Switch Configurator buscará automáticamente la red para aquellos dispositivos compatibles con el protocolo Ethernet Switch Configurator.

Ethernet Switch Configurator utiliza la primera interfaz de red detectada para el PC. Si su ordenador tiene varias tarjetas de red, puede seleccionar la que desee en la barra de herramientas Ethernet Switch Configurator.

Ethernet Switch Configurator muestra una línea para cada dispositivo que responde a una consulta del protocolo Ethernet Switch Configurator.

Ethernet Switch Configurator le permite identificar los dispositivos mostrados.
- Seleccione una línea de dispositivo.
- Para configurar los LED de forman que parpadeen con el dispositivo seleccionado, haga clic en el botón *Signal* de la barra de herramientas. Para detener el parpadeo, haga clic en el botón *Signal* otra vez.
- Haciendo doble clic en una línea, se abre la ventana en la que puede especificar el nombre del dispositivo y los parámetros IP.

Nota: Desactivar la función Ethernet Switch Configurator en el dispositivo después de asignarle los parámetros de IP.

Nota: Guarde los ajustes para conservar las entradas tras un reinicio.

2.4 Especificación de los parámetros IP con la interfaz gráfica de usuario

2.4.1 IPv4

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Basic Settings > Network > Global*.

En este cuadro de diálogo, especifique la VLAN en la que se puede acceder a la administración del dispositivo y configure el acceso Ethernet Switch Configurator.

- ☐ En la columna *VLAN ID*, especifique la VLAN en la que se puede acceder a la administración del dispositivo a través de la red.

Tenga en cuenta que aquí solo puede acceder a la administración del dispositivo mediante puertos que sean miembros de la VLAN correspondiente.

El campo *MAC address* muestra la dirección MAC del dispositivo con el que se accede al dispositivo a través de la red.

- ☐ En el cuadro *Ethernet Switch Configurator protocol v1/v2*, especifique los ajustes para acceder al dispositivo mediante el software Ethernet Switch Configurator.
- ☐ El protocolo Ethernet Switch Configurator le permite asignar al dispositivo una dirección IP a partir de la dirección MAC. Activar el protocolo Ethernet Switch Configurator si desea asignar al dispositivo una dirección IP desde su PC con el software Ethernet Switch Configurator.
- ☐ Abra el cuadro de diálogo *Basic Settings > Network > IPv4*.

En este cuadro de diálogo, especifique la fuente desde la que el dispositivo obtiene sus parámetros IP tras el inicio.

- ☐ En el cuadro *Management interface*, especifique de dónde recibe el dispositivo sus parámetros IP:

▶ En el modo `BOOTP`, la configuración utiliza un servidor BOOTP o DHCP a partir de la dirección MAC del dispositivo.
▶ En el modo `DHCP`, la configuración utiliza un servidor DHCP a partir de la dirección MAC o el nombre del dispositivo.
▶ En el modo `Local`, el dispositivo utiliza parámetros de red de la memoria interna del dispositivo.

Nota: Si se cambia el modo de asignación de la dirección IP, el dispositivo activa el nuevo modo inmediatamente después de pulsar el botón ☑.

- ☐ Si es necesario, introduzca la dirección IP, la máscara de red y la Gateway en el cuadro *IP parameter*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ☑.

2.4.2 IPv6

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Basic Settings > Network > IPv6*.
- ☐ El protocolo IPv6 está activado por defecto. Compruebe que el botón de opción `On` esté seleccionado en el cuadro *Operation*.
- ☐ En el cuadro *Configuration*, especifique de dónde recibe el dispositivo sus parámetros IPv6:
  - ▶ Si se selecciona el botón de opción *None*, el dispositivo recibe sus parámetros IPv6 manualmente.
    Puede especificar manualmente un número máximo de 4 direcciones IPv6. No puede especificar las direcciones de loopback, enlace-local y *Multicast* como direcciones IPv6 estáticas.
  - ▶ Si se selecciona el botón de opción *Auto*, el dispositivo recibe sus parámetros de IPv6 dinámicamente, por ejemplo, mediante el uso de un Router Advertisement Daemon (radvd).
    El dispositivo recibe un máximo de 2 direcciones IPv6.
  - ▶ Si se selecciona el botón de opción *DHCPv6*, el dispositivo recibe sus parámetros de IPv6 de un servidor DHCPv6.
    El dispositivo solo puede recibir una dirección IPv6 del servidor DHCPv6.
  - ▶ Si se selecciona el botón de opción *All*, el dispositivo recibirá sus parámetros IPv6 utilizando cada alternativa para asignaciones dinámicas y manuales.

Nota: Si se cambia el modo de asignación de la dirección IPv6, el dispositivo activa el nuevo modo inmediatamente después de pulsar el botón .

- ☐ Si es necesario, introduzca el *Gateway address* en el cuadro *IP parameter*.

Nota: Si se selecciona el botón de opción *Auto* y utiliza un Router Advertisement Daemon (radvd), el dispositivo recibirá automáticamente una *Gateway address* de tipo enlace-local con una métrica superior a la *Gateway address* establecida manualmente.

- ☐ En el cuadro *Duplicate Address Detection* puede especificar el número de mensajes *Neighbor Solicitation* consecutivos que el dispositivo envía para la función *Duplicate Address Detection*(ver en página 63 “Duplicate Address Detection”).

Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón .

Especifique manualmente una dirección IPv6. Para ello, siga los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Basic Settings > Network > IPv6*.
- ☐ Haga clic en el botón .
  El cuadro de diálogo muestra la ventana *Create*.
- ☐ Introduzca la dirección IPv6 en el campo *IP address*.
- ☐ Introduzca la longitud del prefijo de la dirección IPv6 en el campo *PrefixLength*.
- ☐ Haga clic en el botón *Ok*.
  El dispositivo añade una nueva entrada a la tabla.

2.5 Especificación de los parámetros IP con BOOTP

Con la función *BOOTP* activada, el dispositivo envía un mensaje de solicitud de arranque al servidor BOOTP. El mensaje de solicitud de arranque contiene el ID del cliente configurado en el cuadro de diálogo *Basic Settings > Network > IPv4*. El servidor BOOTP introduce el ID del cliente en una base de datos y asigna una dirección IP. El servidor responde con un mensaje de respuesta de arranque. El mensaje de respuesta de arranque contiene la dirección IP asignada.

2.6 Especificación de los parámetros IP con DHCP

2.6.1 IPv4

El protocolo DHCP (Dynamic Host Configuration Protocol, Protocolo de configuración dinámica de host) se ha desarrollado a partir del BOOTP y lo ha sustituido. El protocolo DHCP permite además configurar un cliente DHCP utilizando un nombre en lugar de una dirección MAC.

Para el DHCP, este nombre se conoce como "Client Identifier" de acuerdo con RFC 2131.

El dispositivo utiliza el nombre introducido en sysName en el grupo del sistema de la MIB II como Client Identifier. Puede cambiar el nombre del sistema mediante la interfaz gráfica de usuario (consulte el cuadro de diálogo *Basic Settings > System*), la interfaz de línea de comandos o SNMP.

El dispositivo transfiere su nombre del sistema al servidor DHCP. El servidor DHCP asigna entonces una dirección IP de forma alternativa a la dirección MAC a partir del nombre del sistema.

Además de la dirección IP, el servidor DHCP transfiere
- la máscara de red
- la Gateway por defecto (si existe)
- la URL del archivo de configuración en el TFTP (si existe)

El dispositivo aplica los datos de configuración a los parámetros adecuados. Cuando el servidor DHCP asigna la dirección IP, el dispositivo guarda permanentemente los datos de configuración en una memoria no volátil.

Tabla 12: Opciones DHCP que solicita el dispositivo

Opciones	Significado
1	Subnet Mask
2	Time Offset
3	Router
4	Time server
12	Host Name
42	NTP server
61	Client Identifier
66	TFTP Server Name
67	Bootfile Name

La ventaja de utilizar DHCP frente a BOOTP es que el servidor DHCP puede limitar la validez de los parámetros de configuración ("Lease") a un período determinado de tiempo (la llamada asignación dinámica de la dirección). Antes de que termine este período de tiempo ("Lease Duration"), el cliente DHCP puede tratar de renovar esta asignación o "Lease". Como alternativa, el cliente puede negociar una nueva asignación. El servidor asigna entonces una dirección cualquiera que no se esté utilizando.

Para evitar esto, la mayoría de los servidores DHCP ofrecen la opción explícita de configuración que permite asignar la misma dirección IP a un cliente determinado a partir de un ID de hardware inequívoco (la llamada asignación estática de la dirección).

En la configuración por defecto, DHCP está activado. Mientras DHCP esté activado, el dispositivo intenta obtener una dirección IP. Si después de un reinicio el dispositivo no encuentra ningún servidor DHCP, no obtendrá una dirección IP. El cuadro de diálogo *Basic Settings > Network > IPv4* le permite activar o desactivar DHCP.

Nota: Cuando utilice la administración ConneXium Network Manager de red, verifique que el DHCP asigna la dirección IP original a cada dispositivo.

El apéndice incluye una configuración de ejemplo del servidor BOOTP/DHCP.

Ejemplo de archivo de configuración DHCP:

```
# /etc/dhcpd.conf for DHCP Daemon
#
subnet 10.1.112.0 netmask 255.255.240.0 {
option subnet-mask 255.255.240.0;
option routers 10.1.112.96;
}
#
# Host berta requests IP configuration
# with her MAC address
#
host berta {
hardware ethernet 00:80:63:08:65:42;
fixed-address 10.1.112.82;
}
#
# Host hugo requests IP configuration
# with his client identifier.
#
host hugo {
#
option dhcp-client-identifier "hugo";
option dhcp-client-identifier 00:68:75:67:6f;
fixed-address 10.1.112.83;
server-name "10.1.112.11";
filename "/agent/config.dat";
}
```

Las líneas que empiezan por el carácter `#` contienen comentarios.

Las líneas que preceden a los dispositivos enumerados individualmente se refieren a los ajustes que se aplican al dispositivo siguiente.

La línea de dirección fija asigna una dirección IP permanente al dispositivo.

Para obtener más información, consulte el manual del servidor DHCP.

2.6.2 IPv6

El Protocolo de configuración dinámica de host (DHCPv6) versión 6 es un protocolo de red utilizado para especificar dinámicamente direcciones IPv6. Este protocolo es el equivalente en IPv6 del protocolo DHCP de IPv4. El protocolo DHCPv6 se describe en RFC 8415.

El dispositivo utiliza un Identificador único de DHCP (DUID) para enviar una solicitud al servidor DHCPv6. En el dispositivo, el DUID representa el *Client ID* que el servidor DHCPv6 utiliza para identificar el dispositivo que ha solicitado una dirección IPv6.

El *Client ID* se muestra en el cuadro de diálogo *Basic Settings > Network > IPv6*, en el cuadro *DHCP*.

El dispositivo solo puede recibir una dirección IPv6 del servidor DHCPv6 con un *PrefixLength* de `128`. No se facilita información de *Gateway address*. Si es necesario, puede especificar información de *Gateway address* manualmente.

Con la configuración por defecto, el protocolo DHCPv6 está desactivado. Puede activar o desactivar el protocolo en el cuadro de diálogo *Basic Settings > Network > IPv6*. Compruebe que el botón de opción *DHCPv6* esté seleccionado en el cuadro *Configuration*.

Si desea obtener una dirección IPv6 dinámicamente con un *PrefixLength* distinto de `128`, seleccione el botón de opción *Auto*. Como ejemplo, aquí tenemos el uso de un Router Advertisement Daemon (radvd). El radvd utiliza mensajes *Router Solicitation* y *Router Advertisement* para configurar automáticamente una dirección IPv6.

Con la configuración por defecto, el botón de opción *Auto* está seleccionado. Puede seleccionar o deseleccionar el botón de opción *Auto* en el cuadro de diálogo *Basic Settings > Network > IPv6*, en el cuadro *Configuration*.

Si se selecciona el botón de opción *All*, el dispositivo recibirá sus parámetros IPv6 utilizando cada alternativa para asignaciones dinámicas y manuales.

2.7 Detección de conflictos de direcciones de administración

Puede asignar una dirección IP al dispositivo a través de distintos métodos. Esta función permite al dispositivo detectar conflictos de direcciones IP en una red tras el arranque y hacer comprobaciones periódicamente durante el funcionamiento. Esta función se describe en RFC 5227.

Si está activada, el dispositivo envía una trampa SNMP que le informa de que ha detectado un conflicto de direcciones IP.

La siguiente lista contiene la configuración por defecto para esta función:
- *Operation*: `On`
- *Detection mode*: `active and passive`
- *Send periodic ARP probes*: `marcado`
- *Detection delay [ms]*: `200`
- *Release delay [s]*: `15`
- *Address protections*: `3`
- *Protection interval [ms]*: `200`
- *Send trap*: `marcado`

2.7.1 Detección activa y pasiva

Comprobar activamente la red ayuda a prevenir que el dispositivo se conecte a la red con una dirección IP duplicada. Tras conectar el dispositivo a una red o configurar la dirección IP, el dispositivo comprueba inmediatamente si la dirección IP existe en la red. Para comprobar la red ante conflictos de direcciones, el dispositivo envía 4 sondas ARP con un retardo de detección de 200 ms a la red. Si la dirección IP existe, el dispositivo intenta devolver la configuración anterior y realizar otra comprobación una vez transcurrido el tiempo de retardo de liberación configurado.

Si desactiva la detección activa, el dispositivo envía 2 avisos ARP gratuitos en intervalos de 2 segundos. Mediante los avisos ARP con detección pasiva activada, el dispositivo sondea la red para determinar si hay algún conflicto de direcciones. Tras resolver un conflicto de direcciones o una vez transcurrido el tiempo de retardo de liberación, el dispositivo se vuelve a conectar a la red. Tras 10 conflictos detectados, y si el intervalo de retardo de liberación configurado es inferior a 60 segundos, el dispositivo establece el intervalo de retardo de liberación en 60 segundos.

Una vez que el dispositivo lleva a cabo la detección activa o si desactiva la función de detección activa y la detección pasiva es activada, el dispositivo escucha a la red en busca de otros dispositivos que utilicen la misma dirección IP. Si el dispositivo detecta una dirección IP duplicada, defiende primero su dirección con el mecanismo ACD en el modo de detección pasiva y envía ARP gratuitos. Es posible configurar el número de protecciones que el dispositivo envía y el intervalo de protección. Para resolver los conflictos, si el dispositivo remoto permanece conectado a la red, la interfaz de red del dispositivo local se desconecta de la red.

Si un servidor DHCP asigna una dirección IP al dispositivo y se produce un conflicto de direcciones, el dispositivo responde con un mensaje de rechazo de DHCP.

El dispositivo utiliza el método de sonda ARP. Este método tiene las siguientes ventajas:
- Las memorias caché ARP de los otros dispositivos no se modifican
- El método es sólido a través de varias transmisiones de sondas ARP

2.8 Duplicate Address Detection

La función *Duplicate Address Detection* determina la singularidad de una dirección unicast IPv6 en una interfaz. La función se lleva a cabo cuando se configura una dirección IPv6 mediante métodos manuales, *DHCPv6* o *Auto*. La función también se desencadena mediante un cambio en el estado de un enlace, por ejemplo, el cambio del estado de un enlace de inactivo a activo.

La función *Duplicate Address Detection* utiliza mensajes *Neighbor Solicitation* y *Neighbor Advertisement*. Tiene la opción de establecer el número de mensajes *Neighbor Solicitation* consecutivos que envía el dispositivo. Para ello, siga los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Basic Settings > Network > IPv6*.
- ☐ En el cuadro *Duplicate Address Detection*, establezca el valor necesario en el campo *Number of neighbor solicitants*.
  Valores posibles:
  - `0`
    La función está desactivada.
  - `1..5` (configuración por defecto: `1`)
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✔.

`enable`	Cambiar al modo Privileged EXEC.
`network ipv6 dad-transmits <0..5>`	Establezca el número de mensajes *Neighbor Solicitation* enviados por el dispositivo. El valor `0` desactiva la función.

Nota: Si la función *Duplicate Address Detection* descubre que una dirección IPv6 no es única en un enlace, el dispositivo no registra este evento en el archivo de registro (registro del sistema).

3 Acceso al dispositivo

3.1 Access roles ‹Roles de acceso›

El dispositivo estará operativamente disponible para usted como usuario en función de su rol de acceso. Si ha iniciado sesión con un rol de acceso específico, las funciones del rol de acceso estarán disponibles para usted.

Los comandos disponibles como usuario también dependen del modo de interfaz de línea de comando en el que esté trabajando. Ver “Jerarquía de comandos en función del modo” en página 25.

El dispositivo ofrece los siguientes roles de acceso:

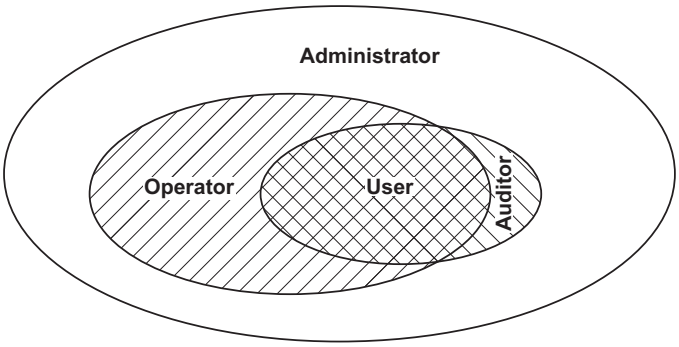


Tabla 13: Alcance y roles de acceso de las autorizaciones de usuario

Rol de acceso	Autorizaciones de usuario
`User`	Los usuarios que hayan iniciado sesión con el rol de acceso `User` están autorizados a supervisar el dispositivo.
`Auditor`	Los usuarios que hayan iniciado sesión con el rol de acceso `Auditor` están autorizados a supervisar el dispositivo y guardar un archivo de registro en el cuadro de diálogo *Diagnostics > Report > Audit Trail*.
`Operator`	Los usuarios que hayan iniciado sesión con el rol de acceso `Operator` están autorizados a supervisar el dispositivo y cambiar la configuración, a excepción de los ajustes de seguridad para el acceso al dispositivo.
`Administrator`	Los usuarios que hayan iniciado sesión con el rol de acceso `Administrator` están autorizados a supervisar el dispositivo y cambiar la configuración.
`Unauthorized`	Lo usuarios no autorizados están bloqueados y el dispositivo rechaza su inicio de sesión. Asigne este valor para bloquear temporalmente la cuenta de usuario. Si se detecta un error durante un cambio de rol de acceso, el dispositivo asigna este rol de acceso a la cuenta de usuario.

3.2 Primer inicio de sesión (cambio de contraseña)

Para ayudar a evitar un acceso no deseado al dispositivo, es obligatorio cambiar la contraseña predeterminada durante la configuración inicial.

Lleve a cabo los siguientes pasos:

- ☐ Abra la interfaz gráfica de usuario, la aplicación SE View o la interfaz de línea de comando la primera vez que inicie sesión.
- ☐ Inicie sesión con la contraseña predeterminada.
  El dispositivo le indicará que escriba una nueva contraseña.
- ☐ Escriba su nueva contraseña.
  Para aumentar la seguridad, elija una contraseña que contenga al menos 8 caracteres formados por mayúsculas, minúsculas, dígitos numéricos y caracteres especiales.
- ☐ Cuando inicie sesión con la Interfaz de línea de comando, el dispositivo le indicará que confirme su nueva contraseña.
- ☐ Vuelva a iniciar sesión con su nueva contraseña.

Nota: Si perdió su contraseña, contacte con su equipo de asistencia local.

3.3 Listas de autenticación

Cuando un usuario accede al dispositivo utilizando una conexión específica, este verifica las credenciales de inicio de sesión del usuario en una lista de autenticación que contiene las políticas que el dispositivo aplica para la autenticación.

El requisito previo para el acceso de un usuario a la gestión del dispositivo es que se asigne al menos una política a la lista de autenticación de la aplicación a través de la cual se lleva a cabo el acceso.

3.3.1 Aplicaciones

El dispositivo ofrece una aplicación para cada tipo de conexión a través de la cual alguien accede al dispositivo:
- Acceso a la interfaz de línea de comando mediante una conexión serie: `Console(V.24)`
- Acceso a la interfaz de línea de comando mediante SSH: `SSH`
- Acceso a la interfaz de línea de comando mediante Telnet: `Telnet`
- Acceso a la interfaz gráfica de usuario: `WebInterface`

El dispositivo también proporciona una aplicación para controlar el acceso a la red desde dispositivos terminales conectados mediante el control de acceso basado en puerto: `8021x`

3.3.2 Políticas

Cuando un usuario inicia sesión con datos de acceso válidos, el dispositivo permite al usuario acceder a la gestión del dispositivo. El dispositivo autentica a los usuarios mediante las siguientes políticas:
- Gestión del dispositivo por parte del usuario
- LDAP
- RADIUS

Cuando el dispositivo terminal inicia sesión con datos de acceso válidos, el dispositivo permite a los dispositivos terminales conectados disponer de acceso a la red mediante el control de acceso basado en puerto conforme al estándar IEEE 802.1X. El dispositivo autentica los dispositivos finales mediante las siguientes políticas:
- RADIUS
- IAS (Integrated Authentication Server)

El dispositivo le brinda la posibilidad de recurrir a una solución alternativa. Para esto, puede especificar más de una política en la lista de autenticación. Cuando la autenticación no es correcta utilizando la política actual, el dispositivo aplica la siguiente política especificada.

3.3.3 Gestión de listas de autenticación

Las listas de autenticación se gestionan en la interfaz gráfica de usuario o en la interfaz de línea de comando. Para ello, siga los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Device Security > Authentication List*.

  En el cuadro de diálogo se mostrarán las listas de autenticación que están configuradas.

`show authlists`	Mostrar las listas de autenticación que están configuradas.

☐ Desactive la lista de autenticación correspondiente a estas aplicaciones mediante la cual no se puede llevar a cabo el acceso al dispositivo, por ejemplo `8021x`.

- ☐ Desmarque la casilla de la columna *Active* de la lista de autenticación `defaultDot1x8021AuthList`.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón  .

`authlists disable defaultDot1x8021AuthList`	Desactiva la lista de autenticación `defaultDot1x8021AuthList`.

3.3.4 Ajuste de la configuración

Ejemplo: Configure una lista de autenticación independiente para la aplicación `WebInterface` que se incluye de manera predeterminada en la lista de autenticación `defaultLoginAuthList`.

El dispositivo reenvía solicitudes de autenticación a un servidor RADIUS en la red. Como solución alternativa, el dispositivo autentica a los usuarios mediante la gestión local de usuarios. Para ello, siga los siguientes pasos:

☐ Cree una lista de autenticación `loginGUI`.

- ☐ Abra el cuadro de diálogo *Device Security > Authentication List*.
- ☐ Haga clic en el botón  .
  El cuadro de diálogo muestra la ventana *Create*.
- ☐ Introduzca un nombre significativo en el campo *Name*.
  En este ejemplo, introduzca el nombre `loginGUI`.
- ☐ Haga clic en el botón *Ok*.
  El dispositivo añade una nueva entrada a la tabla.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`authlists add loginGUI`	Crear la lista de autenticación `loginGUI`.

☐ Seleccione las políticas de la lista de autenticación `loginGUI`.

- ☐ En la columna *Policy 1*, seleccione el valor *`radius`*.
- ☐ En la columna *Policy 2*, seleccione el valor *`local`*.
- ☐ En las columnas *Policy 3* a *Policy 5*, seleccione el valor *`reject`* para ayudar a evitar retrocesos adicionales.
- ☐ Marque la casilla en la columna *Active*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón  .

`authlists set-policy loginGUI radius local reject reject reject`	Asigne las políticas `radius`, `local` y `reject` a la lista de autenticación `loginGUI`.
`show authlists`	Mostrar las listas de autenticación que están configuradas.
`authlists enable loginGUI`	Activar la lista de autenticación `loginGUI`.

☐ Asigne una aplicación a la lista de autenticación `loginGUI`.

- ☐ En el cuadro de diálogo *Device Security > Authentication List*, marque la lista de autenticación `loginGUI`.
- ☐ Haga clic en el botón  y, a continuación, en el elemento *Allocate applications*.
  El cuadro de diálogo muestra la ventana *Allocate applications*.
- ☐ En la columna izquierda, destaque la aplicación `WebInterface`.
- ☐ Haga clic en el botón  .
  En la columna derecha se muestra ahora la aplicación `WebInterface`.
- ☐ Haga clic en el botón *Ok*.
  El cuadro de diálogo muestra la configuración actualizada:
  - La columna *Dedicated applications* de la lista de autenticación `loginGUI` muestra la aplicación `WebInterface`.
  - La columna *Dedicated applications* de la lista de autenticación `defaultLoginAuthList` ya no muestra la aplicación `WebInterface`.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón  .

`show applists`	Muestre las aplicaciones y las listas asignadas.
`applists set-authlist WebInterface loginGUI`	Asignar la aplicación `loginGUI` a la lista de autenticación `WebInterface`.

3.4 Gestión de usuarios

Cuando un usuario inicia sesión con datos de acceso válidos, el dispositivo permite al usuario acceder a la gestión del dispositivo. El dispositivo autentica a los usuarios mediante la gestión local de usuarios o mediante un servidor RADIUS en la red. Para que el dispositivo utilice la gestión de usuarios, asigne la política `local` a una lista de autenticación y consulte el cuadro de diálogo *Device Security > Authentication List*.

En la gestión local de usuarios, puede gestionar las cuentas de usuario. Normalmente se asigna una cuenta de usuario a cada usuario.

3.4.1 Access roles ‹Roles de acceso›

El dispositivo le permite utilizar un modelo de autorización basado en roles para controlar de manera específica el acceso a la gestión del dispositivo. Los usuarios a los que se les asigne un perfil de autorización específico podrán utilizar comandos y funciones del mismo perfil de autorización o de uno inferior.

El dispositivo utiliza los perfiles de autorización en cada aplicación con la que se puede acceder a la gestión del dispositivo.

Cada cuenta de usuario está vinculada a un rol de acceso que regula el acceso a las funciones individuales del dispositivo. En función de la actividad planeada para el usuario correspondiente, podrá asignar un rol de acceso predefinido al usuario. El dispositivo distingue entre los siguientes roles de acceso.

Tabla 14: Roles de acceso para cuentas de usuario

Role	Descripción	Autorizado para las siguientes actividades
Administrator	El usuario tiene autorización para supervisar y administrar el dispositivo.	Todas las actividades con acceso de lectura/escritura, incluidas las siguientes actividades, están reservadas para un administrador: ▶ Añadir, modificar o eliminar cuentas de usuario ▶ Activar, desactivar o desbloquear cuentas de usuario ▶ Cambiar todas las contraseñas ▶ Configurar la gestión de contraseñas ▶ Establecer o cambiar la hora del sistema ▶ Cargar archivos en el dispositivo, por ejemplo, configuraciones del dispositivo, certificados o imágenes de software ▶ Restablecer las configuraciones y los ajustes relacionados con la seguridad a los valores de fábrica ▶ Configurar el servidor RADIUS y las listas de autenticación ▶ Aplicar scripts mediante la interfaz de línea de comando. ▶ Activar/desactivar CLI Logging y SNMP Logging ▶ Activación y desactivación de la memoria externa ▶ Activación y desactivación de la supervisión del sistema ▶ Activar/desactivar los servicios para acceder a la gestión del dispositivo (por ejemplo, SNMP). ▶ Configurar restricciones de acceso a la interfaz gráfica de usuario o a la interfaz de línea de comando según las direcciones IP
Operator	El usuario tiene autorización para supervisar y configurar el dispositivo, a excepción de la configuración relacionada con la seguridad.	Todas las actividades con acceso de lectura/escritura, a excepción de las actividades nombradas anteriormente, que están reservadas para un administrador:

Tabla 14: Roles de acceso para cuentas de usuario (cont

Role	Descripción	Autorizado para las siguientes actividades
Auditor	El usuario tiene autorización para supervisar el dispositivo y para guardar el archivo de registro en el cuadro de diálogo *Diagnostics > Report* > Audit Trail.	Supervisión de actividades con acceso de lectura.
Guest	El usuario tiene autorización para supervisar el dispositivo, a excepción de la configuración relacionada con la seguridad.	Supervisión de actividades con acceso de lectura.
Unauthorized	No es posible acceder al dispositivo. ▶ Como administrador, puede asignar este rol de acceso para bloquear una cuenta de usuario temporalmente. ▶ Si un administrador asigna un rol de acceso diferente a la cuenta de usuario y se detecta un error, el dispositivo asigna este rol de acceso a la cuenta de usuario.	No se permiten actividades.

3.4.2 Gestión de cuentas de usuario

Administra las cuentas de usuario en la interfaz gráfica de usuario o en la interfaz de línea de comando. Para ello, siga los siguientes pasos:

☐ Abra el cuadro de diálogo *Device Security > User Management*.

El cuadro de diálogo muestra las cuentas de usuario que están configuradas.

`show users`	Muestra las cuentas de usuario que están configuradas.

3.4.3 Configuración por defecto

En la configuración por defecto, las cuentas de usuario `admin` y `user` se encuentran configuradas en el dispositivo.

Tabla 15: Configuración por defecto de las cuentas de usuario configuradas de fábrica

Parámetro	Configuración por defecto	
User name	`admin`	`user`
Password	`private`	`public`
Role	`administrator`	`guest`
User locked	`sin marcar`	`sin marcar`
Policy check	`sin marcar`	`sin marcar`
SNMP auth type	`hmacmd5`	`hmacmd5`
SNMP encryption type	`des`	`des`

Cambie la contraseña de la cuenta de usuario `admin` antes de que el dispositivo esté disponible en la red.

3.4.4 Cambio de las contraseñas predeterminadas

Para ayudar a evitar un acceso no deseado, cambie la contraseña de las cuentas de usuario predeterminadas. Para ello, siga los siguientes pasos:

☐ Cambie las contraseñas de las cuentas de usuario `admin` y `user`.

☐ Abra el cuadro de diálogo *Device Security > User Management*.

El cuadro de diálogo muestra las cuentas de usuario que están configuradas.

☐ Para obtener un nivel superior de complejidad para la contraseña, marque la casilla de la columna *Policy check*.
Antes de guardarla, el dispositivo comprueba la contraseña conforme a la política especificada en el cuadro *Password policy*.

Nota: La comprobación de la contraseña puede provocar la aparición de un mensaje en el cuadro *Security status* del cuadro de diálogo *Basic Settings > System*. Puede especificar los ajustes que provocan la aparición de este mensaje en el cuadro de diálogo *Basic Settings > System*.

☐ Haga clic en la fila de la cuenta de usuario correspondiente en el campo *Password*. Introduzca una contraseña de al menos 6 caracteres.
Se permiten hasta 64 caracteres alfanuméricos.
- ▶ El dispositivo distingue entre mayúsculas y minúsculas.
- ▶ La longitud mínima de la contraseña se especifica en el cuadro *Configuration*. El dispositivo comprueba constantemente la longitud mínima de la contraseña.

☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón .

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`users password-policy-check <user> enable`	Activa la comprobación de la contraseña en la cuenta de usuario `<user>` según la política especificada. De esta manera, obtendrá un nivel superior de complejidad para la contraseña.

Nota: Cuando muestra el estado de la seguridad, la comprobación de la contraseña puede provocar la aparición de un mensaje (`show security-status all`). Puede especificar los ajustes que provocan la aparición de este mensaje con el comando `security-status monitor pwd-policy-inactive`.

`users password <user> SECRET`	Especifica la contraseña `SECRET` de la cuenta de usuario `<user>`. Introduzca al menos 6 caracteres.
`save`	Guardar los ajustes en el perfil de configuración "seleccionado" de la memoria no volátil (`nvm`).

3.4.5 Configuración de una nueva cuenta de usuario

Asigne una cuenta de usuario independiente a cada usuario que acceda a la gestión de dispositivos. De esta manera puede controlar de manera específica las autorizaciones de acceso.

En el ejemplo siguiente, configuraremos la cuenta de un usuario `USER` con el rol `operator`. Los usuarios con el rol `operator` tienen autorización para supervisar y configurar el dispositivo, a excepción de la configuración relacionada con la seguridad. Para ello, siga los siguientes pasos:

☐ Cree una nueva cuenta de usuario.

- ☐ Abra el cuadro de diálogo *Device Security > User Management*.
- ☐ Haga clic en el botón .
  El cuadro de diálogo muestra la ventana *Create*.
- ☐ Introduzca el nombre en el campo *User name*.
  En este ejemplo, asignamos el nombre `USER` a la cuenta de usuario.
- ☐ Haga clic en el botón *Ok*.
- ☐ Para obtener un nivel superior de complejidad para la contraseña, marque la casilla de la columna *Policy check*.
  Antes de guardarla, el dispositivo comprueba la contraseña conforme a la política especificada en el cuadro *Password policy*.
- ☐ Introduzca una contraseña de al menos 6 caracteres en el campo *Password*.
  Se permiten hasta 64 caracteres alfanuméricos.
  - ▶ El dispositivo distingue entre mayúsculas y minúsculas.
  - ▶ La longitud mínima de la contraseña se especifica en el cuadro *Configuration*. El dispositivo comprueba constantemente la longitud mínima de la contraseña.
- ☐ En la columna *Role*, seleccione el rol de usuario.
  En este ejemplo, seleccionamos el valor `operator`.
- ☐ Para activar la cuenta de usuario, marque la casilla de la columna *Active*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón .
  El cuadro de diálogo muestra las cuentas de usuario que están configuradas.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`users add USER`	Crea la cuenta de usuario `USER`.
`users password-policy-check USER enable`	Activa la comprobación de la contraseña en la cuenta de usuario `USER` según la política especificada. De esta manera, obtendrá un nivel superior de complejidad para la contraseña.

`users password USER SECRET`	Especifica la contraseña `SECRET` de la cuenta de usuario `USER`. Introduzca al menos 6 caracteres.
`users access-role USER  operator`	Asignar el rol de usuario `operator` a la cuenta de usuario `USER`.
`users enable USER`	Activa la cuenta de usuario `USER`.
`show users`	Muestra las cuentas de usuario que están configuradas.
`save`	Guardar los ajustes en el perfil de configuración "seleccionado" de la memoria no volátil (`nvm`).

Nota: Cuando esté configurando una nueva cuenta de usuario en la interfaz de línea de comando, no olvide asignar la contraseña.

3.4.6 Desactivación de la cuenta de usuario

Una vez desactivada una cuenta de usuario, el dispositivo deniega el acceso del usuario correspondiente a la gestión del dispositivo. En comparación con su eliminación completa, la desactivación de una cuenta de usuario le permite conservar la configuración y utilizarla de nuevo en el futuro. Para ello, siga los siguientes pasos:

☐ Para conservar la configuración de la cuenta del usuario y utilizarla de nuevo en el futuro, puede desactivar la cuenta de usuario temporalmente.

☐ Abra el cuadro de diálogo *Device Security > User Management*.
El cuadro de diálogo muestra las cuentas de usuario que están configuradas.

☐ En la fila de la cuenta de usuario correspondiente, desmarque la casilla de la columna *Active*.

☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón  .

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`users disable <user>`	Desactivar la cuenta de usuario.
`show users`	Muestra las cuentas de usuario que están configuradas.
`save`	Guardar los ajustes en el perfil de configuración "seleccionado" de la memoria no volátil (`nvm`).

☐ Para desactivar la configuración de la cuenta del usuario permanentemente, elimine la cuenta de usuario.

☐ Destaque la fila de la cuenta de usuario correspondiente.

☐ Haga clic en el botón  .

`users delete <user>`	Elimina la cuenta de usuario `<user>`.
`show users`	Muestra las cuentas de usuario que están configuradas.
`save`	Guardar los ajustes en el perfil de configuración "seleccionado" de la memoria no volátil (`nvm`).

3.4.7 Ajuste de las políticas de contraseñas

El dispositivo le permite comprobar si las contraseñas de las cuentas de usuario cumplen con la política especificada. Cuando las contraseñas cumplen con la política, se obtiene un nivel superior de complejidad en estas.

La gestión del dispositivo por parte del usuario le permite activar o desactivar la comprobación por separado en cada cuenta de usuario. Si marca la casilla y la contraseña nueva cumple los requisitos de la política, el dispositivo acepta el cambio de contraseña.

En la configuración por defecto, los valores prácticos de la política se configuran en el dispositivo. Puede ajustar la política para cumplir con sus requisitos. Para ello, siga los siguientes pasos:

☐ Ajuste la política para que las contraseñas cumplan con sus requisitos.

☐ Abra el cuadro de diálogo *Device Security > User Management*.

En el cuadro *Configuration*, puede especificar el número de intentos de inicio de sesión que desea permitir antes de que el dispositivo bloquee el acceso del usuario. También puede especificar el número mínimo de caracteres que desea que tengan las contraseñas.

Nota: El dispositivo solo permite eliminar el bloqueo a usuarios con autorización de *`administrator`*.

El número de intentos de inicio de sesión y el bloqueo posible del usuario solo aplican si accede a la gestión del dispositivo a través de:

- la interfaz gráfica de usuario
- el protocolo SSH
- el protocolo Telnet

Nota: Si accede a la gestión del dispositivo utilizando la interfaz de línea de comando a través de la interfaz serie, el número de intentos de inicio de sesión es ilimitado.

☐ Especifique los valores necesarios para cumplir con sus requisitos.

- En el campo *Login attempts*, especifique el número de veces que desea que un usuario intente iniciar sesión. El campo le permite definir este valor en el rango `0..5`.
  En el ejemplo de arriba, el valor `0` desactiva la función.
- El campo *Min. password length* le permite introducir valores dentro del rango `1..64`.

El cuadro de diálogo muestra la política configurada en el cuadro *Password policy*.

☐ Ajuste los valores necesarios para cumplir con sus requisitos.

- Se permiten valores dentro del rango de `1` a `16`.
  El valor `0` desactiva la política correspondiente.

Para aplicar las entradas especificadas en los cuadros *Configuration* y *Password policy*, marque la casilla de la columna *Policy check* para un usuario en particular.

☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✔.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`passwords min-length 6`	Especifica la política correspondiente a la longitud mínima de la contraseña.
`passwords  min-lowercase-chars 1`	Especifica la política correspondiente al número mínimo de letras minúsculas de la contraseña.
`passwords  min-numeric-chars 1`	Especifica la política correspondiente al número mínimo de dígitos de la contraseña.
`passwords  min-special-chars 1`	Especifica la política correspondiente al número mínimo de caracteres especiales de la contraseña.
`passwords  min-uppercase-chars 1`	Especifica la política correspondiente al número mínimo de letras mayúsculas de la contraseña.
`show passwords`	Muestra las políticas que están configuradas.
`save`	Guardar los ajustes en el perfil de configuración "seleccionado" de la memoria no volátil (`nvm`).

3.5 LDAP

Los administradores del servidor gestionan Active Directory, que contienen credenciales de inicio de sesión del usuario para aplicaciones utilizadas en el entorno de la oficina. El Active Directory es jerárquico por naturaleza, contiene nombres de usuario, contraseñas y los niveles de permisos de lectura/escritura autorizados para cada usuario.

Este dispositivo utiliza el Protocolo Ligero de Acceso a Directorios (LDAP) para recuperar la información de inicio de sesión del usuario y los niveles de permiso de un Active Directory. Esto proporciona un “inicio de sesión único“ para los dispositivos de red. Recuperar credenciales de inicio de sesión de un Active Directory permite al usuario iniciar sesión con las mismas credenciales de inicio de sesión utilizadas en el entorno de oficina.

Una sesión LDAP se inicia con el contacto del dispositivo con el agente del sistema de directorios (DSA) para buscar el Active Directory de un servidor LDAP. Si el servidor encuentra varias entradas en el Active Directory de un usuario, el servidor envía el nivel de permisos más elevado encontrado. El DSA escucha solicitudes de información y envía respuestas en el puerto TCP `389` para LDAP, o en el puerto TCP `636` para LDAP a través de SSL (LDAPS). Los clientes y los servidores codifican solicitudes y respuestas de LDAPS mediante las Reglas de codificación básicas (BER). El dispositivo abre una nueva conexión por cada solicitud y cierra la conexión tras recibir una respuesta del servidor.

El dispositivo le permite cargar un certificado de CA para validar el servidor para sesiones de Nivel de capa de conexión (SSL) y Seguridad de capa de transporte (TLS). Esto hace que el certificado sea opcional para sesiones TLS.

El dispositivo es capaz de almacenar en la memoria caché credenciales de inicio de sesión para hasta 1024 usuarios en la memoria. Si no se puede acceder a los servidores de Active Directory, los usuarios podrán seguir iniciando sesión mediante sus credenciales de inicio de sesión de oficina.

3.5.1 Coordinación con el administrador del servidor

Configurar la función *LDAP* requiere que el administrador de red solicite la siguiente información del administrador del servidor:

- El nombre o la dirección IP del servidor
- La ubicación del Active Directory en el servidor
- El tipo de conexión utilizado
- El puerto de escucha TCP
- Cuando sea necesario, la ubicación del certificado de CA
- El nombre del atributo que contiene el nombre de inicio de sesión del usuario
- Los nombres del atributo que contienen los niveles de permiso de usuario

El administrador del servidor puede asignar niveles de permiso individualmente utilizando un atributo como `description` o a un grupo utilizando el atributo `memberOf`. En el cuadro de diálogo *Device Security > LDAP > Role Mapping*, especifique qué atributos reciben los distintos niveles de permiso.

También tiene la opción de recuperar el nombre de los atributos que contienen el nombre de inicio de sesión del usuario y los niveles de permiso utilizando un navegador LDAP como JXplorer o Softerra.

3.5.2 Configuración de ejemplo

El dispositivo es capaz de establecer un enlace cifrado a un servidor local utilizando tan solo el nombre del servidor o a un servidor de una red diferente mediante una dirección IP. El administrador del servidor utiliza atributos para identificar credenciales de inicio de sesión de un usuario y asignar niveles de permisos individuales y de grupo.

Utilizando información recibida del administrador del servidor, especifique qué atributos de Active Directory contienen las credenciales de inicio de sesión del usuario y el nivel del permiso. A continuación, el dispositivo compara las credenciales de inicio de sesión del usuario con los niveles de permisos especificados en el dispositivo y permite al usuario iniciar sesión en el nivel de permiso asignado.

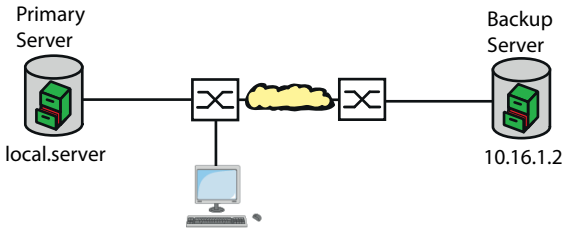


Figura 18: Configuración de ejemplo de LDAP

Para este ejemplo, el administrador del servidor envió la siguiente información:

Information	Primary Server	Backup Server
El nombre o la dirección IP del servidor	`local.server`	`10.16.1.2`
La ubicación del Active Directory en el servidor	`País/Ciudad/Usuario`	`País/Empresa/Usuario`
El tipo de conexión utilizado	`TLS`(con certificado)	`SSL`
El administrador del servidor envió el certificado de CA en un correo electrónico.	Certificado de CA para el servidor principal guardado localmente	Certificado de CA para el servidor de respaldo guardado localmente
El puerto de escucha TCP	`389 (tls)`	`636 (ssl)`
Nombre del atributo que contiene el nombre de usuario	`userPrincipalName`	`userPrincipalName`
Los nombres del atributo que contienen los niveles de permiso de usuario	`OPERATOR` `ADMINISTRATOR`	`OPERATOR` `ADMINISTRATOR`

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Device Security > Authentication List*.
- ☐ Para configurar el dispositivo para recuperar las credenciales de inicio de sesión del usuario, durante el inicio de sesión y mediante la interfaz gráfica de usuario, desde Active Directory en primer lugar, especifique para la lista `defaultLoginAuthList` el valor `ldap` en la columna *Policy 1*.
- ☐ Abra el cuadro de diálogo *Device Security > LDAP > Configuration*.

- El dispositivo le permite especificar el tiempo que guarda las credenciales de inicio de sesión del usuario en la memoria caché. Para guardar las credenciales de inicio de sesión del usuario en la memoria caché, en el cuadro *Configuration*, campo *Client cache timeout [min]*, introduzca el valor `1440`.
- La entrada *Bind user* es opcional. Cuando se especifica, los usuarios solo tienen que introducir su nombre de usuario para iniciar sesión. El usuario del servicio puede acceder con las credenciales de inicio de sesión enumeradas en el Active Directory en el atributo especificado en la columna *User name attribute*. Introduzca el nombre de usuario y el dominio en la columna *Bind user*.
- El *Base DN* es una combinación del componente del dominio (cd) y la unidad organizativa (uo). El *Base DN* permite al dispositivo localizar un servidor en un dominio (cd) y encontrar el Active Directory (uo). Especifique la ubicación del Active Directory. En la columna *Base DN*, especifique el valor `ou=Users,ou=City,ou=Country,dc=server,dc=local`.
- En la columna *User name attribute*, introduzca el valor `userPrincipalName` para especificar el atributo en el que el administrador del servidor enumera los usuarios.

El dispositivo utiliza un certificado de CA para verificar el servidor.

- Si el certificado se encuentra en su PC o en una unidad de red, arrastre y suelte el certificado en el área  . También puede hacer clic en el área para seleccionar el certificado.
- Para transferir el certificado de CA al dispositivo, haga clic en el botón *Start*.
- Para añadir una entrada de tabla, haga clic en el botón  .
- Para especificar una descripción, introduzca el valor `Primary AD Server` en la columna *Description*.
- Para especificar el nombre del servidor y el dominio del servidor primario, en la columna *Address*, introduzca el valor `local.server`.
- El servidor primario utiliza el puerto TCP `389` para establecer comunicación, que es el valor predeterminado de *Destination TCP port*.
- El servidor primario utiliza TLS para cifrar la comunicación y un certificado de CA para la validación del servidor. En la columna *Connection security*, especifique el valor `startTLS`.
- Para activar la entrada, marque la casilla de la columna *Active*.
- Utilizando información recibida del administrador del servidor para el servidor de respaldo, añada, configure y active otra fila.

- Abra el cuadro de diálogo *Device Security > LDAP > Role Mapping*.
- Para añadir una entrada de tabla, haga clic en el botón  .

Cuando un usuario inicia sesión, con LDAP configurado y activado, el dispositivo busca el Active Directory para las credenciales de inicio de sesión del usuario. Si el dispositivo encuentra que el nombre de usuario y la contraseña son correctos, el dispositivo busca el valor especificado en la columna *Type*. Si el dispositivo encuentra el atributo y el texto de la columna *Parameter* coincide con el texto de Active Directory, el dispositivo permite al usuario iniciar sesión con el nivel de permiso asignado. Si se especifica el valor `attribute` en la columna *Type*, especifique el valor de la columna *Parameter* de la siguiente manera: `attributeName=attributeValue`

- En la columna *Role*, introduzca el valor `operator` para especificar el rol de usuario.
- Para activar la entrada, marque la casilla de la columna *Active*.

- ☐ Haga clic en el botón  .
  El cuadro de diálogo muestra la ventana *Create*.
  Introduzca los valores recibidos del administrador del servidor para el rol `administrator`.
  Para activar la entrada, marque la casilla de la columna *Active*.
- ☐ Abra el cuadro de diálogo *Device Security > LDAP > Configuration*.
- ☐ Para activar la función, seleccione el botón de opción `On` en el cuadro *Operation*.

En la tabla siguiente se describe cómo configurar la función *LDAP* en el dispositivo utilizando la interfaz de línea de comandos. La tabla muestra los comandos de `Index 1`. Para configurar `Index 2`, utilice los mismos comandos y sustituya la información correspondiente.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`ldap cache-timeout 1440`	Especifique el dispositivo para vaciar la memoria no volátil tras transcurrir un día.
`ldap client server add 1 local.server port 389`	Añada una conexión al servidor cliente de autenticación remota con el nombre de host `local.server` y el puerto UDP `389`.
`ldap client server modify 1 security startTLS`	Especifique el tipo de seguridad utilizado para la conexión.
`ldap client server modify 1 description Primary_AD_Server`	Especifique el nombre de la configuración de la entrada.
`ldap basedn ou=Users,ou=City,ou=Country,dc=server, dc=local`	Especifique el nombre del dominio base utilizado para encontrar el Active Directory en el servidor.
`ldap search-attr userPrincipalName`	Especifique el atributo que desea buscar en el Active Directory que contiene la credencial de inicio de sesión de los usuarios.
`ldap bind-user user@company.com`	Especifique el nombre y el dominio del usuario del servicio.
`ldap bind-passwd Ur-123456`	Especifique la contraseña del usuario del servicio.
`ldap client server enable 1`	Active la conexión del servidor de cliente de autenticación remota.
`ldap mapping add 1 access-role operator mapping-type attribute mapping-parameter OPERATOR`	Añada una entrada de asignación de roles de autenticación remota para el rol `Operator`. Asigne el rol `operator` al atributo que contiene la palabra `OPERATOR`.
`ldap mapping enable 1`	Active la entrada de asignación de roles de autenticación remota.
`ldap operation`	Active la función de autenticación remota.

3.6 Acceso con SNMP

El protocolo SNMP le permite trabajar con un sistema de gestión de red para supervisar el dispositivo a través de la red y cambiar su configuración.

3.6.1 Acceso con SNMPv1/v2

Cuando se utiliza SNMPv1 o SNMPv2, el sistema de gestión de red y el dispositivo se comunican de manera encriptada. Cada paquete SNMP contiene el nombre de la comunidad en texto no cifrado y la dirección IP del remitente.

Los nombres de la comunidad `user` para accesos de lectura y `admin` para accesos de escritura están presentes en el dispositivo. Si SNMPv1/v2 se encuentra activado, el dispositivo permitirá a cualquier usuario que conozca el nombre de la comunidad acceder al dispositivo.

Haga que el acceso no deseado al dispositivo resulte más difícil. Para ello, siga los siguientes pasos:

- Cambie los nombres de comunidad predeterminados en el dispositivo.
  Trate los nombres de la comunidad con discreción.
  Todos los usuarios que conozcan el nombre de la comunidad para disponer de acceso de escritura tendrán la capacidad de cambiar la configuración del dispositivo.
- Especifique un nombre de comunidad diferente para el acceso de lectura/escritura que el correspondiente al acceso de lectura.
- Utilice SNMPv1 o SNMPv2 únicamente en entornos protegidos contra intercepciones. Los protocolos no utilizan ninguna encriptación.
- Es recomendable utilizar SNMPv3 y desactivar el acceso con SNMPv1 y SNMPv2 en el dispositivo.

3.6.2 Acceso con SNMPv3

Cuando se utiliza SNMPv3, el sistema de gestión de red y el dispositivo se comunican de manera encriptada. El sistema de gestión de red se autentica a sí mismo con el dispositivo utilizando las credenciales de inicio de sesión de un usuario. El requisito previo del acceso con SNMPv3 consiste en que el sistema de gestión de red utiliza la misma configuración que la definida en el dispositivo.

El dispositivo le permite especificar los parámetros *SNMP auth type* y *SNMP encryption type* individualmente en cada cuenta de usuario.

Cuando configure una nueva cuenta de usuario en el dispositivo, los parámetros quedarán predefinidos de forma que el sistema de gestión de red ConneXium Network Manager llegue al dispositivo inmediatamente.

Las cuentas de usuario configuradas en el dispositivo utilizan las mismas contraseñas en la interfaz gráfica de usuario, en la interfaz de línea de comando y para SNMPv3.

Para adaptar los parámetros de SNMPv3 de la configuración de la cuenta de usuario a la configuración del sistema de gestión de red, lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Device Security > User Management*.

El cuadro de diálogo muestra las cuentas de usuario que están configuradas.

- ☐ Haga clic en la fila de la cuenta de usuario correspondiente en el campo *SNMP auth type*. Seleccione la configuración que desee.
- ☐ Haga clic en la fila de la cuenta de usuario correspondiente en el campo *SNMP encryption type*. Seleccione la configuración que desee.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✔.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`users snmpv3 authentication <user> md5 | sha1`	Asigne el protocolo HMAC-MD5 o HMACSHA para solicitudes de autenticación a la cuenta de usuario de `<user>`.
`users snmpv3 encryption <user> des | aescfb128 | none`	Asigna el algoritmo DES o AES-128 a la cuenta de usuario de `<user>`. Con este algoritmo, el dispositivo encripta las solicitudes de autenticación. El valor `none` elimina la encriptación.
`show users`	Mostrar las cuentas de usuario que se han configurado.
`save`	Guardar los ajustes en el perfil de configuración "seleccionado" de la memoria no volátil (`nvm`).

3.7 Acceso a Out of Band

El dispositivo cuenta con un puerto independiente que le permite acceder a la gestión del dispositivo out-of-band. Cuando exista una carga in-band elevada en los puertos de conmutación, puede usar este puerto independiente para acceder a la gestión del dispositivo.

Como requisito previo, debe conectar la estación de administración directamente al puerto USB. Si utiliza Microsoft Windows, instale el controlador RNDIS en caso necesario. Cuando haya conectado la estación de administración, puede comunicarse con la gestión del dispositivo a través de una conexión de red virtual.

En la configuración por defecto, puede acceder a la gestión del dispositivo a través de este puerto utilizando los siguientes parámetros IP.

- *IP address* `91.0.0.100`
- *Netmask* `255.255.255.0`

El dispositivo le permite acceder a la gestión del dispositivo mediante los siguientes protocolos:

- SNMP
- Telnet
- SSH
- HTTP
- HTTPS
- FTP
- SCP
- TFTP
- SFTP

3.7.1 Especificación de los parámetros IP

Si conecta la estación de administración a través del puerto USB, el dispositivo asignará la dirección IP de la interfaz de red USB, más 1, a la estación de administración (`91.0.0.101` en la configuración por defecto). El dispositivo le permite cambiar los parámetros IP para adaptar el dispositivo a los requisitos de su entorno.

Compruebe que la subred IP de esta interfaz de red no se solapa con ninguna otra subred conectada a otra interfaz del dispositivo:

- Interfaz de administración

Si la estación de administración accede a la gestión del dispositivo a través del puerto USB, el dispositivo desconecta la interfaz gráfica de usuario y la interfaz de línea de comando inmediatamente después de que haya realizado los cambios.

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Basic Settings > Out of Band over USB*.
- ☐ Sobrescriba la dirección IP en el cuadro *IP parameter*, campo *IP address*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✓.

```
enable
```
Cambiar al modo Privileged EXEC.

```
network usb parms 192.168.1.1
255.255.255.0
```
Especificar la dirección IP `192.168.1.1` y la máscara de red `255.255.255.0` para la interfaz de red USB.

```
show network usb
```
Mostrar la configuración de la interfaz de red USB.

```
Out-of-band USB management settings
-----------------------------------
Management operation.....................enabled
IP address..............................192.168.1.1
Subnet mask.............................255.255.255.0
Host MAC address........................64:60:38:1f:85:85
Device MAC address......................64:60:38:1f:85:86
```

```
save
```
Guardar los ajustes en el perfil de configuración "seleccionado" de la memoria no volátil (`nvm`).

3.7.2 Desactivación de la interfaz de red USB

Con la configuración por defecto, se activa la interfaz de red USB. Si desea que alguien no acceda a la gestión del dispositivo a través del puerto USB, el dispositivo le permite desactivar la interfaz de red USB.

Si la estación de administración accede a la gestión del dispositivo a través del puerto USB, el dispositivo desconecta la interfaz gráfica de usuario y la interfaz de línea de comando inmediatamente después de que haya realizado los cambios.

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Basic Settings > Out of Band over USB*.
- ☐ Para desactivar la interfaz de red USB, seleccione el botón de opción *Off* en el cuadro *Operation*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✓.

```
enable
```
Cambiar al modo Privileged EXEC.

```
no network usb operation
```
Desactivar la interfaz de red USB.

```
Out-of-band USB management settings
-----------------------------------
Management operation.....................disabled
IP address..............................192.168.1.1
Subnet mask.............................255.255.255.0
Host MAC address........................64:60:38:1f:85:85
Device MAC address......................64:60:38:1f:85:86
```

```
save
```
Guardar los ajustes en el perfil de configuración "seleccionado" de la memoria no volátil (`nvm`).

4 Sincronización de la hora del sistema en la red

Muchas aplicaciones confían en un ajuste horario lo más preciso posible. La precisión necesaria y, por tanto, la desviación admisible con respecto a la hora real, depende del área de aplicación.

Las áreas de aplicación son, a modo de ejemplo:
- Entradas de registro
- Asignación de marcas de hora en datos de producción
- Control de procesos

El dispositivo le permite sincronizar la hora de la red utilizando las siguientes opciones:
- El Protocolo simple de tiempo de red (SNTP, Simple Network Time Protocol) es una solución sencilla para requisitos de baja precisión. En las mejores condiciones, el SNTP logra una precisión en la franja de los milisegundos. La precisión depende del retraso de la señal.
- IEEE 1588 con el Precision Time Protocol (PTP) logra una exactitud en el rango de submicrosegundos. Este método es adecuado incluso para aplicaciones exigentes, incluido el control de procesos.

La mejor opción es que los dispositivos involucrados sean compatibles con el protocolo PTP. PTP es más preciso, tiene métodos avanzados para corrección de errores y causa una carga de red baja. La implementación de PTP es comparativamente fácil.

Nota: Según los estándares PTP y SNTP, ambos protocolos funcionan en paralelo en la misma red. Sin embargo, como ambos protocolos influyen en la hora del sistema, pueden ocurrir situaciones en las que los dos protocolos estén en conflicto.

4.1 Configuración básica

En el cuadro de diálogo *Time > Basic Settings*, especifique la configuración general de la hora.

4.1.1 Setting the time ‹Ajuste horario›

Si no hay fuente de referencia horaria disponible, tiene la opción de ajustar la hora en el dispositivo.

Tras un arranque en frío o un reinicio, si no dispone de un reloj en tiempo real o este indica una hora no válida, el dispositivo inicializa su reloj a 1 de enero, 00:00 h. Tras desconectar la alimentación de corriente, el dispositivo almacena en búfer los ajustes del reloj en tiempo real hasta 24 horas.

De manera alternativa, puede configurar los ajustes en el dispositivo de forma que obtenga automáticamente la hora actual desde un reloj PTP o un servidor SNTP.

De manera alternativa, puede configurar los ajustes en el dispositivo de forma que obtenga automáticamente la hora actual desde un servidor SNTP.

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Time > Basic Settings*.
- ▶ El campo *System time (UTC)* muestra el UTC (tiempo universal coordinado) actual del dispositivo. El UTC es la hora correspondiente a la medición mundial coordinada. El UTC es el mismo a nivel mundial y no tiene en cuenta los cambios de hora locales.
- ▶ La hora del campo *System time* se obtiene de *System time (UTC)* más el valor *Local offset [min]* y la posible modificación por el horario de verano.

Nota: El PTP envía el Tiempo Atómico Internacional (TAI). Desde el 1 de julio de 2020, la hora TAI se encuentra 37 segundos por delante de la hora UTC. Cuando se configura correctamente el origen de tiempo de referencia PTP de la compensación UTC, el dispositivo corrige automáticamente esta diferencia en el campo *System time (UTC)*.

- ☐ Para que el dispositivo aplique la hora de su PC al campo *System time*, haga clic en el botón *Set time from PC*.
  Según el valor del campo *Local offset [min]*, el dispositivo calcula la hora en el campo *System time (UTC)*: la *System time (UTC)* se obtiene de la *System time* menos el valor *Local offset [min]* y la posible modificación por el horario de verano.
- ▶ El campo *Time source* muestra el origen de los datos de tiempo. El dispositivo selecciona automáticamente la fuente de mayor precisión.
  Inicialmente, la fuente es `local`.
  Si el SNTP está activo y el dispositivo recibe un paquete SNTP válido, el dispositivo ajusta la fuente horaria a `sntp`.
  Si el PTP está activo y el dispositivo recibe un mensaje PTP válido, el dispositivo ajusta la fuente horaria a `ptp`. El dispositivo prioriza PTP sobre SNTP.
- ▶ El valor *Local offset [min]* especifica la diferencia horaria entre la hora local y la *System time (UTC)*.
- ☐ Para que el dispositivo determine la zona horaria de su PC, haga clic en el botón *Set time from PC*. El dispositivo calcula la diferencia horaria local con respecto al UTC y la introduce en el campo *Local offset [min]*.

Nota: El dispositivo también puede proporcionar la variación local a partir de un servidor DHCP.

- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ☑.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`clock set <YYYY-MM-DD> <HH:MM:SS>`	Ajustar la hora del sistema del dispositivo.
`clock timezone offset <-780..840>`	Especificar la diferencia horaria entre la hora local y la hora UTC obtenida en minutos.
`save`	Guardar los ajustes en el perfil de configuración "seleccionado" de la memoria no volátil (`nvm`).

4.1.2 Cambio automático por horario de verano

Si el dispositivo se utiliza en una zona horaria en la que existe un cambio por horario de verano, ajuste el cambio automático en la pestaña *Daylight saving time*.

Cuando el horario de verano está activado, el dispositivo adelanta la hora local del sistema 1 hora al inicio del horario de verano. Al finalizar el horario de verano, el dispositivo retrasa la hora local del sistema 1 hora. Para ello, siga los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Time > Basic Settings*, pestaña *Daylight saving time*.
- ☐ Para seleccionar un perfil preconfigurado para el inicio y el final del horario de verano, haga clic en el botón *Profile...* en el cuadro *Operation*.
- ☐ Si no hay ningún perfil compatible disponible, especifique las horas de cambio en los campos *Summertime begin* y *Summertime end*.
  Para ambos momentos, debe especificar el mes, la semana del mes, el día de la semana y la hora del día.
- ☐ Para activar la función, seleccione el botón de opción `On` en el cuadro *Operation*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✔.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`clock summer-time mode <disable|recurring|eu|usa>`	Configurar el cambio automático por horario de verano: activar/desactivar o activar con un perfil.
`clock summer-time recurring start`	Introducir la hora de inicio del cambio por horario de verano.
`clock summer-time recurring end`	Introducir la hora de finalización del cambio por horario de verano.
`save`	Guardar los ajustes en el perfil de configuración "seleccionado" de la memoria no volátil (`nvm`).

4.2 SNTP

El Protocolo simple de tiempo de red (SNTP, Simple Network Time Protocol) le permite sincronizar la hora del sistema en su red. El dispositivo es compatible con el cliente SNTP y la función del servidor SNTP.

El servidor SNTP pone a disposición el UTC (tiempo universal coordinado). El UTC es la hora correspondiente a la medición mundial coordinada. El UTC es el mismo a nivel mundial e ignora los cambios de hora locales.

El SNTP es una versión simplificada del NTP (Network Time Protocol, Protocolo de tiempo de red). Los paquetes de datos son idénticos con el SNTP y NTP. De igual manera, tanto los servidores NTP como SNTP sirven como fuente horaria para los clientes SNTP.

Nota: La información recogida en este capítulo con respecto a los servidores SNTP externos también es válida para los servidores NTP.

El SNTP conoce los siguientes modos de funcionamiento para la transmisión de la hora:
- *Unicast*
  En el modo de funcionamiento *Unicast*, un cliente SNTP envía solicitudes a un servidor SNTP y espera una respuesta de dicho servidor.
- *Broadcast*
  En el modo de funcionamiento *Broadcast*, un servidor SNTP envía mensajes SNTP a la red en intervalos especificados. Los clientes SNTP reciben estos mensajes SNTP y los evalúan.

En un entorno IPv6, el modo de funcionamiento *Broadcast* funciona de la siguiente forma:
- El cliente SNTP escucha solamente los mensajes del servidor SNTP que tienen la dirección IPv6 *Multicast* establecida en `ff05::101` como la dirección de destino IPv6.
- El servidor SNTP solamente envía mensajes SNTP a la dirección *Multicast*`ff05::101`. El servidor SNTP no envía mensajes SNTP con la dirección de enlace-local como dirección de origen IPv6.

Tabla 16: Clases de dirección IPv4 de destino para el modo de funcionamiento Broadcast

Dirección IPv4 de destino	Enviar paquetes SNTP a
`0.0.0.0`	Nadie
`224.0.1.1`	Dirección *Multicast* para los mensajes SNTP
`255.255.255.255`	Dirección *Broadcast*

Nota: Un servidor SNTP en el modo de funcionamiento *Broadcast* también responde a solicitudes directas mediante *Unicast* de los clientes SNTP. Por el contrario, los clientes SNTP trabajan en el modo de funcionamiento *Unicast* o *Broadcast*.

4.2.1 Preparación

Lleve a cabo los siguientes pasos:

- Dibuje un plano de la red con todos los dispositivos que usan SNTP para obtener una vista de conjunto de la transmisión de la hora.
  Durante la planificación, tenga en cuenta que la precisión de la hora depende de los retrasos de los mensajes SNTP. Para minimizar los retrasos y su variación, asigne un servidor SNTP a cada segmento de la red. Cada uno de estos servidores SNTP sincroniza su propia hora del sistema como un cliente SNTP con su servidor SNTP principal (cascada de SNTP). El servidor SNTP más alto de la cascada de SNTP dispone del acceso más directo a una fuente de referencia horaria.

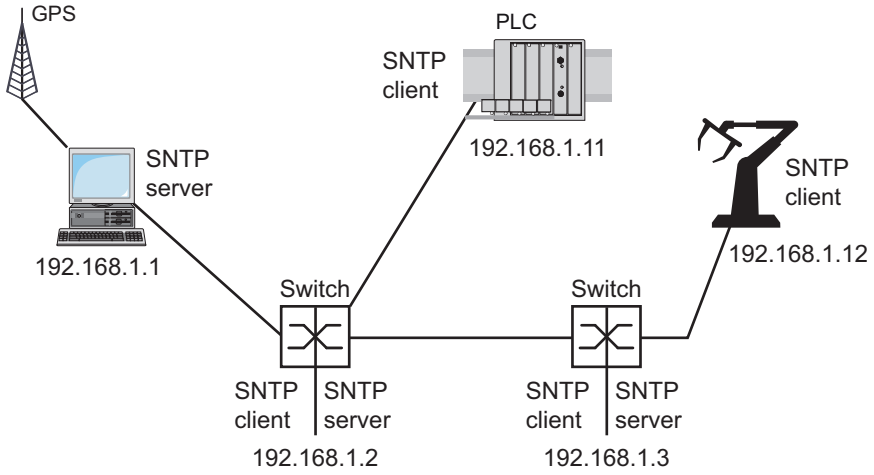


Figura 19: Ejemplo de cascada de SNTP

Nota: Para una distribución horaria precisa, es preferible utilizar componentes de red (enrutadores y switches) entre los servidores SNTP y los clientes SNTP para que reenvíen los paquetes SNTP con un horario de transmisión bajo y uniforme (latencia).

▶ Un cliente SNTP envía sus solicitudes a un máximo de 4 servidores SNTP configurados. Si no hay respuesta del primer servidor SNTP, el cliente SNTP envía sus solicitudes al segundo servidor SNTP. Si esta solicitud tampoco es satisfactoria, envía la solicitud al tercero y, por último, al cuarto servidor. Si ninguno de estos servidores SNTP responde, el cliente SNTP pierde la sincronización. El cliente SNTP envía solicitudes cíclicamente a cada servidor SNTP hasta que uno envía una hora válida.

Nota: El dispositivo ofrece también la opción de obtener una lista de direcciones IP de servidores SNTP a partir de un servidor DHCP.

☐ Si no hay una fuente de referencia horaria disponible, determine un dispositivo con un servidor SNTP como fuente de referencia horaria. Ajuste la hora del sistema en intervalos regulares.

4.2.2 Definición de ajustes del cliente SNTP

Como cliente SNTP, el dispositivo obtiene la información de la hora de los servidores SNTP y NTP, y sincroniza el reloj del sistema de manera correspondiente. Para ello, siga los siguientes pasos:

☐ Abra el cuadro de diálogo *Time > SNTP > Client*.

☐ Configure el modo de funcionamiento SNTP.
En el cuadro *Configuration*, seleccione uno de los siguientes valores en el campo *Mode*:

▶ `unicast`
El dispositivo envía solicitudes a un servidor SNTP y espera una respuesta de dicho servidor.

▶ `broadcast`
El dispositivo espera los mensajes *Broadcast* o *Multicast* de los servidores SNTP de la red.

☐ Para sincronizar la hora solo una vez, marque la casilla *Disable client after successful sync*. Tras la sincronización, el dispositivo desactiva la función *SNTP Client*.

▶ La tabla muestra el servidor SNTP al que el cliente SNTP envía una solicitud en el modo de funcionamiento *Unicast*. La tabla contiene hasta 4 definiciones de servidores SNTP.

☐ Para añadir una entrada de tabla, haga clic en el botón .

☐ Especifique los datos de conexión del servidor SNTP.

☐ Para activar la función, seleccione el botón de opción `On` en el cuadro *Operation*.

☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón .

▶ El campo *State* muestra el estado actual de la función *SNTP Client*.

Tabla 17: Configuración del cliente SNTP para el ejemplo

Dispositivo	192.168.1.1	192.168.1.2	192.168.1.3	192.168.1.11	192.168.1.12
Función *SNTP Client*	`Off`	`On`	`On`	`On`	`On`

Tabla 17: Configuración del cliente SNTP para el ejemplo (cont

Dispositivo	192.168.1.1	192.168.1.2	192.168.1.3	192.168.1.11	192.168.1.12
Configuration: *Mode*	unicast	unicast	unicast	unicast	unicast
Request interval [s]	30	30	30	30	30
Direcciones *SNTP Server* –		192.168.1.1	192.168.1.2 192.168.1.1	192.168.1.2 192.168.1.1	192.168.1.3 192.168.1.2 192.168.1.1

4.2.3 Especificación de la configuración del servidor SNTP

Si un dispositivo funciona como servidor SNTP, proporciona la hora del sistema como tiempo universal coordinado (UTC) en la red. Para ello, siga los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Time > SNTP > Server*.
- ☐ Para activar la función, seleccione el botón de opción On en el cuadro *Operation*.
- ☐ Para activar el modo de funcionamiento *Broadcast*, seleccione el botón de opción *Broadcast admin mode* en el cuadro *Configuration*.
  En el modo de funcionamiento *Broadcast*, el servidor SNTP envía mensajes SNTP a la red en intervalos especificados. El servidor SNTP también responde a las solicitudes de los clientes SNTP en el modo de funcionamiento *Unicast*.
  - ☐ En el campo *Broadcast destination address*, establezca la dirección IPv4 a la que el servidor SNTP envía los paquetes SNTP. Establezca una dirección *Broadcast* o una dirección *Multicast*.
    En un entorno IPv6, no puede establecer la dirección IPv6 a la que el servidor SNTP envía los paquetes SNTP. El servidor SNTP utiliza la dirección *Multicast*ff05::101 como dirección de destino IPv6.
  - ☐ En el campo *Broadcast UDP port*, establezca el número de puertos UDP a los que el servidor SNTP envía los paquetes SNTP en el modo de funcionamiento *Broadcast*.
  - ☐ En el campo *Broadcast VLAN ID*, establezca el ID de la VLAN a la que el servidor SNTP envía los paquetes SNTP en el modo de funcionamiento *Broadcast*.
  - ☐ En el campo *Broadcast send interval [s]*, introduzca los intervalos de tiempo con los que el servidor SNTP del dispositivo envía paquetes *Broadcast* SNTP.

Nota: A excepción del campo *Broadcast destination address*, el resto de los ajustes son aplicables para los servidores SNTP IPv4 e IPv6.

- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ☑.
- ▶ El campo *State* muestra el estado actual de la función *SNTP Server*.

Tabla 18: Configuración para el ejemplo

Dispositivo	192.168.1.1	192.168.1.2	192.168.1.3	192.168.1.11	192.168.1.12
Función *SNTP Server*	On	On	On	Off	Off
UDP port	123	123	123	123	123
Broadcast admin mode	sin marcar	sin marcar	sin marcar	sin marcar	sin marcar
Broadcast destination address	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Broadcast UDP port	123	123	123	123	123

Tabla 18: Configuración para el ejemplo (cont

Dispositivo	192.168.1.1	192.168.1.2	192.168.1.3	192.168.1.11	192.168.1.12
Broadcast VLAN ID	1	1	1	1	1
Broadcast send interval [s]	128	128	128	128	128
Disable server at local time source	sin marcar	sin marcar	sin marcar	sin marcar	sin marcar

4.3 PTP

Para que las aplicaciones controladas mediante LAN funcionen sin latencia, es necesario realizar una gestión precisa del tiempo. Con el PTP (Precision Time Protocol), IEEE 1588 describe un método que permite una sincronización precisa de los relojes de la red.

PTP permite la sincronización con una precisión de 100 ns. PTP utiliza Multicasts para los mensajes de sincronización, lo cual permite reducir la carga de la red.

4.3.1 Tipos de relojes

PTP define los roles “maestro” y “esclavo” para los relojes de la red:
- Un reloj maestro (fuente de hora de referencia) distribuye su hora.
- Un reloj esclavo se sincroniza con la señal de hora recibida del reloj maestro.

Boundary clock ‹Reloj delimitador›

La hora de transmisión (latencia) de los enrutadores y switches tiene un efecto que se puede medir en la precisión de la transmisión de la hora. Para corregir estas imprecisiones, PTP define qué es lo que se conoce como boundary clocks.

En un segmento de red, un boundary clock es la fuente de la hora de referencia (reloj maestro) con la que se sincronizan los relojes esclavos subordinados. Normalmente los enrutadores y switches asumen el rol de boundary clock.

El boundary clock obtiene posteriormente la hora de una fuente de hora de referencia de nivel superior (gran maestro).

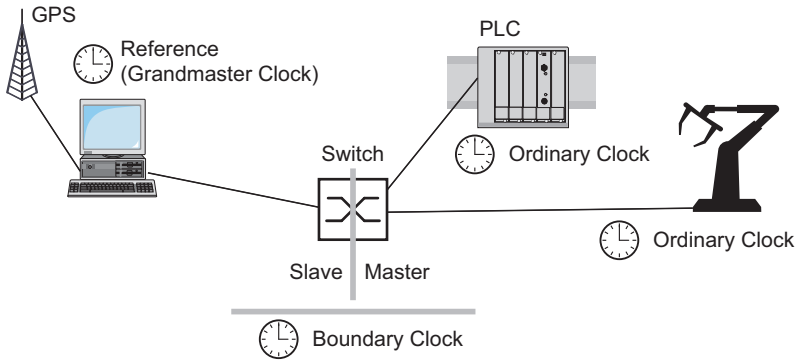


Figura 20: Posición del boundary clock en una red

Transparent Clock

Normalmente los switches asumen el rol de Transparent Clock para permitir una precisión elevada en las cascadas. El Transparent Clock es un reloj Slave que corrige su propia hora de transmisión cuando reenvía los mensajes de sincronización recibidos.

Ordinary Clock

PTP designa el reloj en un dispositivo final como un “Ordinary Clock”. Los Ordinary Clock funcionan como un reloj maestro o esclavo.

4.3.2 Mejor algoritmo de reloj maestro

Los dispositivos que participan en PTP designan un dispositivo de la red como fuente de hora de referencia (gran maestro). Aquí se utiliza el algoritmo “Best Master Clock”, que determina la precisión de los relojes disponibles en la red.

El algoritmo “Best Master Clock” evalúa los siguientes criterios:
- *Priority 1*
- *Clock class*
- *Clock accuracy*
- *Clock variance*
- *Priority 2*

En primer lugar, el algoritmo evalúa el valor del campo *Priority 1* de los dispositivos participantes. El dispositivo con el valor más pequeño del campo *Priority 1* se convierte en la fuente de hora de referencia (Grandmaster). Si el valor es el mismo para varios dispositivos, el algoritmo toma el siguiente criterio. Si este también coincide, toma el siguiente. Si estos valores coinciden para varios dispositivos, el valor más bajo del campo *Clock identity* decide qué dispositivo se convierte en el origen de hora de referencia (Grandmaster).

En la configuración del boundary clock, el dispositivo le permite especificar individualmente los valores de *Priority 1* y *Priority 2*. Esto le permite influir sobre qué dispositivo será el origen de hora de referencia (Grandmaster) en la red.

4.3.3 Medición del retardo

El retardo de los mensajes de sincronización entre los dispositivos afecta a la precisión. La medición del retardo permite a los dispositivos tener en cuenta la media de retardo.

PTP versión 2 ofrece los siguientes métodos para la medición del retardo:
- `e2e` (End to End)
  El reloj esclavo mide el retardo de los mensajes de sincronización hasta el reloj maestro.
- `e2e-optimized`
  El reloj esclavo mide el retardo de los mensajes de sincronización hasta el reloj maestro. Este método está disponible tan solo para transparent clocks. El dispositivo reenvía los mensajes de sincronización enviados mediante Multicast solamente al reloj maestro, manteniendo baja la carga de la red. Si el dispositivo recibe un mensaje de sincronización de otro reloj maestro, reenvía los mensajes de sincronización solamente a este puerto nuevo.
  Si el dispositivo no conoce ningún reloj maestro, reenvía los mensajes de sincronización a cada puerto.
- `p2p` (Peer to Peer)
  El reloj esclavo mide el retardo de los mensajes de sincronización hasta el reloj maestro. Además, el reloj maestro mide el retardo hasta cada reloj esclavo, incluso a través de puertos bloqueados. Para ello, se requiere que el reloj maestro y esclavo admitan el retardo Peer-to-Peer (`p2p`).
  En caso de interrupción del acoplamiento redundante entre anillos, por ejemplo, el reloj esclavo se convierte en el reloj maestro y el reloj maestro se convierte en el esclavo. Este cambio se produce sin pérdida alguna de precisión, ya que los relojes ya conocen el retardo en la otra dirección.

4.3.4 Dominios PTP

El dispositivo transmite mensajes de sincronización solamente de y a dispositivos del mismo dominio PTP. El dispositivo le permite establecer el dominio para el boundary clock y para el transparent clock de manera individual.

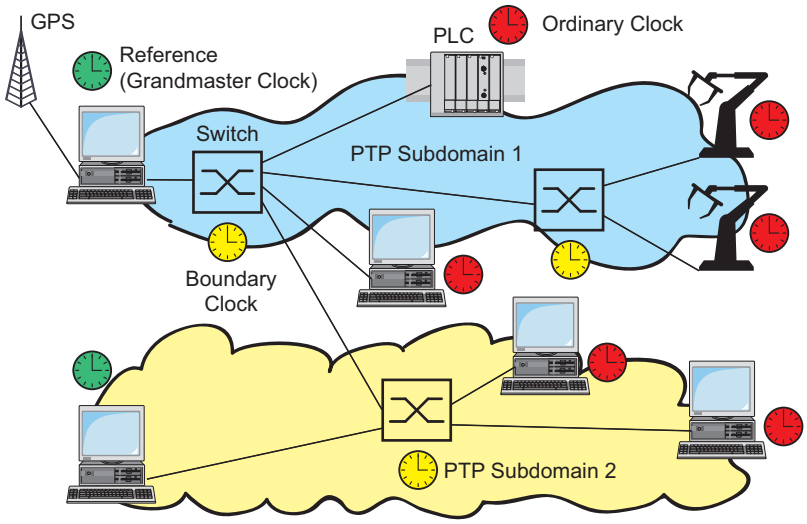


Figura 21: Ejemplo de dominios PTP

4.3.5 Uso de PTP

Para poder sincronizar los relojes de manera precisa con PTP, utilice solamente switches con un boundary clock o un transparent clock como nodos.

Lleve a cabo los siguientes pasos:

- ☐ Dibuje un plano de la red con los dispositivos implicados en PTP para tener una vista de conjunto de la distribución de los relojes.
- ☐ Especifique el rol de cada switch participante (boundary clock o transparent clock). En el dispositivo, esta configuración se denomina *PTP mode*.

Tabla 19: Posibles ajustes para el modo PTP

Modo PTP	Application
`v2-boundary-clock`	Como boundary clock, el dispositivo distribuye mensajes de sincronización a los relojes esclavos en el segmento de la red subordinada. El boundary clock obtiene posteriormente la hora de una fuente de hora de referencia de nivel superior (gran maestro).
`v2-transparent-clock`	Como transparent clock, el dispositivo reenvía los mensajes de sincronización recibidos una vez corregidos por el retardo del transparent clock.

- ☐ Active PTP en cada switch participante.
  PTP se configura a continuación de manera predominantemente automática.
- ☐ Active PTP en los dispositivos finales.
- ☐ El dispositivo le permite influir sobre qué dispositivo de la red se convierte en el reloj de referencia (gran maestro). Por lo tanto, cambie el valor predeterminado en los campos *Priority 1* y *Priority 2* para el *Boundary Clock*.

5 Administración de perfiles de configuración

Si cambia la configuración del dispositivo durante el funcionamiento, este almacenará los cambios en su memoria (*RAM*). Tras reiniciar el dispositivo, se pierde la configuración.

Para mantener los cambios después de reiniciar el dispositivo, este le permite guardar los ajustes en un perfil de configuración en la memoria no volátil (*NVM*). Para poder cambiar rápidamente a otros ajustes, la memoria no volátil ofrece espacio de almacenamiento para varios perfiles de configuración.

Si se conecta una memoria externa, el dispositivo guarda automáticamente una copia del perfil de configuración en la memoria externa (*ENVM*). Puede desactivar esta función.

5.1 Detección de los ajustes modificados

El dispositivo almacena los cambios efectuados en la configuración durante el funcionamiento en su memoria volátil (*RAM*). El perfil de configuración de la memoria no volátil (*NVM*) permanece invariable hasta que guarda los ajustes cambiados de manera explícita. Hasta entonces, los perfiles de configuración de la memoria y de la memoria no volátil son diferentes. El dispositivo le ayuda a reconocer los ajustes cambiados.

5.1.1 Memoria volátil (RAM) y memoria no volátil (NVM)

Puede reconocer si el perfil de configuración de la memoria volátil (*RAM*) es diferente del perfil de configuración «seleccionado» en la memoria no volátil (*NVM*). Para ello, siga los siguientes pasos:

- ☐ Compruebe la barra de estado situada en la parte superior del menú:
  - – Si aparece un icono parpadeante, los perfiles de configuración varían.
  - – Si no hay ningún icono visible, los perfiles de configuración coinciden.

O:

- ☐ Abra el cuadro de diálogo *Basic Settings > Load/Save*.
- ☐ Compruebe el estado de la casilla de verificación en el cuadro *Information*:
  - – Si la casilla de verificación está desmarcada, los perfiles de configuración varían.
  - – Si la casilla de verificación está marcada, los perfiles de configuración coinciden.

```
show config status

Configuration Storage sync State
--------------------------------
running-config to NV.....................out of sync
...
```

5.1.2 Memoria externa (EAM) y memoria no volátil (NVM)

También puede reconocer cuándo la copia de la memoria externa (EAM) es diferente del perfil de configuración de la memoria no volátil (*NVM*). Para ello, siga los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Basic Settings > Load/Save*.
- ☐ Compruebe el estado de la casilla de verificación en el cuadro *Information*:
  - Si la casilla de verificación está desmarcada, los perfiles de configuración varían.
  - Si la casilla de verificación está marcada, los perfiles de configuración coinciden.

```
show config status

Configuration Storage sync State
--------------------------------
...
NV to EAM.................................out of sync
...
```

5.2 Cómo guardar la configuración

5.2.1 Grabación del perfil de configuración en el dispositivo

Si cambia la configuración del dispositivo durante el funcionamiento, este almacenará los cambios en su memoria (RAM). Para mantener los cambios después de reiniciar el dispositivo, guarde el perfil de configuración en la memoria no volátil (*NVM*).

Grabación de un perfil de configuración

El dispositivo almacena los ajustes en el perfil de configuración "seleccionado" de la memoria no volátil (*NVM*).

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Basic Settings > Load/Save*.
- ☐ Compruebe que el perfil de configuración necesario esté "Seleccionado".
  Puede reconocer el perfil de configuración "seleccionado" por la casilla de la columna *Selected* marcada.
- ☐ Haga clic en el botón  .

`show config profiles nvm`	Muestra los perfiles de configuración contenidos en la memoria no volátil (nvm).
`enable`	Cambiar al modo Privileged EXEC.
`save`	Guardar los ajustes en el perfil de configuración "seleccionado" de la memoria no volátil (nvm).

Copiado de los ajustes en un perfil de configuración

El dispositivo le permite almacenar los ajustes guardados en la memoria (RAM) en un perfil de configuración distinto del "seleccionado". De esta manera, puede crear un perfil de configuración nuevo en la memoria no volátil (*NVM*) o sobrescribir uno existente.

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Basic Settings > Load/Save*.
- ☐ Haga clic en el botón  y, a continuación, en el elemento *Save as...*.
  El cuadro de diálogo muestra la ventana *Save as...*.
- ☐ En el campo *Name*, cambie el nombre del perfil de configuración. Si mantiene el nombre propuesto, el dispositivo sobrescribirá un perfil de configuración existente del mismo nombre.
- ☐ Haga clic en el botón *Ok*.

El perfil de configuración nuevo se designa con el nombre "Seleccionado".

`show config profiles nvm`	Muestra los perfiles de configuración contenidos en la memoria no volátil (`nvm`).
`enable`	Cambiar al modo Privileged EXEC.
`copy config running-config nvm profile <string>`	Guardar los ajustes actuales en el perfil de configuración denominado `<string>` en la memoria no volátil (`nvm`). Si está presente, el dispositivo sobrescribirá un perfil de configuración del mismo nombre. El perfil de configuración nuevo se designa con el nombre "Seleccionado".

Selección de un perfil de configuración

Si la memoria no volátil (*NVM*) contiene varios perfiles de configuración, tiene la opción de seleccionar cualquier perfil de configuración que contenga. El dispositivo almacena los ajustes en el perfil de configuración "seleccionado". Tras reiniciarlo, el dispositivo carga los ajustes del perfil de configuración "seleccionado" en la memoria (`RAM`).

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Basic Settings > Load/Save*.

La tabla muestra los perfiles de configuración presentes en el dispositivo. Puede reconocer el perfil de configuración "seleccionado" por la casilla de la columna *Selected* marcada.

- ☐ En la tabla, seleccione la entrada del perfil de configuración requerido almacenada en la memoria no volátil (*NVM*).
- ☐ Haga clic en el botón y, a continuación, en el elemento *Select*.

En la columna *Selected*, la casilla del perfil de configuración aparecerá ahora como `marked`.

`enable`	Cambiar al modo Privileged EXEC.
`show config profiles nvm`	Muestra los perfiles de configuración contenidos en la memoria no volátil (`nvm`).
`configure`	Cambiar al modo de configuración.
`config profile select nvm 1`	Identificador del perfil de configuración. Anote el nombre adyacente del perfil de configuración.
`save`	Guardar los ajustes en el perfil de configuración "seleccionado" de la memoria no volátil (`nvm`).

5.2.2 Grabación del perfil de configuración en la memoria externa

Si hay conectada una memoria externa y guarda un perfil de configuración, el dispositivo guardará automáticamente una copia en la *Selected external memory*. Con la configuración por defecto, la función estará activada. Puede desactivar esta función.

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Basic Settings > External Memory*.
- ☐ Marque la casilla de la columna *Backup config when saving* para permitir al dispositivo guardar automáticamente una copia en la memoria externa durante el proceso de almacenamiento.
- ☐ Para desactivar la función, desmarque la casilla de la columna *Backup config when saving*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✓.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`config envm config-save usb`	Active la función. Cuando guarda un perfil de configuración, el dispositivo almacena una copia en la memoria externa. `usb` = Memoria USB externa
`save`	Guardar los ajustes en el perfil de configuración "seleccionado" de la memoria no volátil (`nvm`).

5.2.3 Copia de seguridad del perfil de configuración en un servidor remoto

El dispositivo le permite realizar automáticamente una copia de seguridad del perfil de configuración en un servidor remoto. Como requisito previo, debe activar la función antes de guardar el perfil de configuración.

Después de guardar el perfil de configuración en la memoria no volátil (*NVM*), el dispositivo le enviará una copia a la URL especificada.

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Basic Settings > Load/Save*.
  En el cuadro *Backup config on a remote server when saving*, lleve a cabo los pasos siguientes:
- ☐ En el campo *URL*, especifique el servidor, la ruta y el nombre del archivo del perfil de configuración del que ha hecho una copia de seguridad.
- ☐ Haga clic en el botón *Set credentials*.
  El cuadro de diálogo muestra la ventana *Credentials*.
- ☐ Introduzca las credenciales de inicio de sesión necesarias para autenticarse en el servidor remoto.
- ☐ En la lista de opciones *Operation*, active la función.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✓.

`enable`	Cambiar al modo Privileged EXEC.
`show config remote-backup`	Comprobar el estado de la función.
`configure`	Cambiar al modo de configuración.
`config remote-backup destination`	Introducir la URL de destino de la copia de seguridad del perfil de configuración.
`config remote-backup username`	Introducir el nombre de usuario para autenticarse en el servidor remoto.
`config remote-backup password`	Introducir la contraseña para autenticarse en el servidor remoto.
`config remote-backup operation`	Active la función.

Si la transferencia al servidor remoto no es correcta, el dispositivo registra este evento en el archivo de registro (System Log).

5.2.4 Exportación de un perfil de configuración

El dispositivo le permite guardar un perfil de configuración en un servidor como un archivo XML. Si utiliza la interfaz gráfica de usuario, tiene la opción de guardar el archivo XML directamente en su PC.

Requisitos previos:
- Para guardar el archivo en un servidor, necesita un servidor configurado en la red.
- Para guardar el archivo en un servidor SCP o SFTP, también necesita el nombre de usuario y la contraseña a fin de acceder a este servidor.

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Basic Settings > Load/Save*.
- ☐ En la tabla, seleccione la entrada del perfil de configuración requerido.

Exporte el perfil de configuración a su PC. Para ello, siga los siguientes pasos:

- ☐ Haga clic en el enlace de la columna *Profile name*.
- ☐ Seleccione la ubicación de almacenamiento y especifique el nombre del archivo.
- ☐ Haga clic en el botón *Ok*.

El perfil de configuración se guardará ahora como un archivo XML en la ubicación especificada.

Exporte el perfil de configuración a un servidor remoto. Para ello, siga los siguientes pasos:

- Haga clic en el botón ☰ y, a continuación, en el elemento *Export...*.
  El cuadro de diálogo muestra la ventana *Export...*.
- En el campo *URL*, especifique la URL del archivo en el servidor remoto:
  - Para guardar el archivo en un servidor FTP, especifique la URL correspondiente al archivo en el formato siguiente:
    `ftp://<usuario>:<contraseña>@<dirección IP>:<puerto>/<nombre archivo>`
  - Para guardar el archivo en un servidor TFTP, especifique la URL correspondiente al archivo en el formato siguiente:
    `tftp://<dirección IP>/<ruta>/<nombre archivo>`
  - Para guardar el archivo en un servidor SCP o SFTP, especifique la URL correspondiente al archivo en uno de los siguientes formatos:
    `scp://` o `sftp://<usuario>:<contraseña>@<dirección IP>/<ruta>/<nombre archivo>`
    `scp://` o `sftp://<IP address>/<path>/<file name>`
    Si hace clic en el botón *Ok*, el dispositivo mostrará la ventana *Credentials*. Ahí podrá introducir el *User name* y la *Password* para iniciar sesión en el servidor.
- Haga clic en el botón *Ok*.
  El perfil de configuración se guardará ahora como un archivo XML en la ubicación especificada.

`show config profiles nvm`	Muestra los perfiles de configuración contenidos en la memoria no volátil (`nvm`).
`enable`	Cambiar al modo Privileged EXEC.
`copy config running-config remote tftp://<IP_address>/ <path>/<file_name>`	Guardar la configuración actual en un servidor TFTP.
`copy config nvm remote sftp://<user_name>:<password>@<IP_address>/<path>/<file_name>`	Guardar el perfil de configuración seleccionado de la memoria no volátil (`nvm`) en un servidor SFTP.
`copy config nvm profile config3 remote tftp://<IP_address>/ <path>/<file_name>`	Guardar el perfil de configuración `config3` de la memoria no volátil (`nvm`) en un servidor TFTP.
`copy config nvm profile config3 remote ftp://<IP_address>:<port>/<path>/<file_name>`	Guardar el perfil de configuración `config3` de la memoria no volátil (`nvm`) en un servidor FTP.

5.3 Carga de la configuración

Si guarda varios perfiles de configuración en la memoria, tendrá la opción de cargar un perfil de configuración diferente.

5.3.1 Activación de un perfil de configuración

La memoria no volátil del dispositivo puede contener varios perfiles de configuración. Si activa un perfil de configuración almacenado en la memoria no volátil (*NVM*), podrá cambiar inmediatamente los ajustes del dispositivo. El dispositivo no necesita reiniciarse.

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Basic Settings > Load/Save*.
- ☐ En la tabla, seleccione la entrada del perfil de configuración requerido.
- ☐ Haga clic en el botón ☰ y, a continuación, en el elemento *Activate*.

El dispositivo copia la configuración en la memoria (RAM) y se desconecta de la interfaz gráfica de usuario. El dispositivo utiliza inmediatamente los ajustes del perfil de configuración.

- ☐ Vuelva a cargar la interfaz gráfica de usuario.
- ☐ Inicie sesión de nuevo.

En la columna *Selected*, la casilla del perfil de configuración activada anteriormente aparecerá como `marked`.

`show config profiles nvm`	Muestra los perfiles de configuración contenidos en la memoria no volátil (`nvm`).
`enable`	Cambiar al modo Privileged EXEC.
`copy config nvm profile config3 running-config`	Activar los ajustes del perfil de configuración `config3` en la memoria no volátil (`nvm`). El dispositivo copia los ajustes en la memoria volátil y desconecta la conexión a la interfaz de línea de comando. El dispositivo utiliza inmediatamente los ajustes del perfil de configuración `config3`.

5.3.2 Carga del perfil de configuración desde la memoria externa

Si se conecta una memoria externa, el dispositivo carga un perfil de configuración desde la memoria externa tras el reinicio automático. El dispositivo le permite guardar estos ajustes adicionales en un perfil de configuración en la memoria no volátil.

Si la memoria externa contiene el perfil de configuración de un dispositivo idéntico, tiene la posibilidad de transferir la configuración de un dispositivo a otro.

Lleve a cabo los siguientes pasos:

- ☐ Compruebe que el dispositivo cargue un perfil de configuración desde la memoria externa tras el reinicio.
  Con la configuración por defecto, la función estará activada. Si la función está desactivada, actívela de nuevo del siguiente modo:

- ☐ Abra el cuadro de diálogo *Basic Settings > External Memory*.
- ☐ En la columna *Config priority*, seleccione el valor `first`.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✔.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`config envm load-priority usb first`	Active la función. Tras el reinicio, el dispositivo carga un perfil de configuración desde la memoria externa. `usb` = Memoria USB externa
`show config envm settings`	Muestra los ajustes de la memoria externa (`envm`).

```
Type   Status      Auto Update Save Config Config Load Prio
------ ----------- ----------- ----------- ----------------
usb    ok          [x]         [x]           first
```

`save`	Guardar los ajustes en un perfil de configuración en la memoria no volátil (*NVM*) del dispositivo.

Si utiliza la interfaz de línea de comando, el dispositivo le permite copiar los ajustes de la memoria externa directamente en la memoria no volátil (*NVM*).

`show config profiles nvm`	Muestra los perfiles de configuración contenidos en la memoria no volátil (`nvm`).
`enable`	Cambiar al modo Privileged EXEC.
`copy config envm profile config3 nvm`	Copiar el perfil de configuración `config3` de la memoria externa (`envm`) a la memoria no volátil (`nvm`).

El dispositivo también pude cargar un perfil de configuración de un archivo de script durante el proceso de arranque.

Requisitos previos:

- ▶ Compruebe que la memoria externa esté conectada antes de iniciar el dispositivo.
- ▶ El directorio raíz de la memoria externa contiene un archivo de texto `startup.txt` con el contenido `script=<file_name>`. El carácter comodín `<file_name>` representa el archivo de script que el dispositivo ejecuta durante el proceso de arranque.
- ▶ El directorio raíz de la memoria externa contiene el archivo de script. Tiene la opción de guardar el script con un nombre especificado por el usuario. Guarde el archivo con la extensión `.cli`.

Nota: Compruebe que el script guardado en la memoria externa no esté vacío. Si el script está vacío, el dispositivo carga el siguiente perfil de configuración en función de los ajustes de prioridad de la configuración.

Una vez aplicado el script, el dispositivo guarda automáticamente el perfil de configuración del archivo de script como un archivo XML en la memoria externa. Cuando escriba el comando correspondiente en el archivo de script, tendrá la opción de desactivar esta función:

- `no config envm config-save usb`
  El dispositivo no creará una copia en la memoria USB externa.

Si el archivo del script contiene un comando incorrecto, el dispositivo no aplica este comando durante el proceso de arranque. El dispositivo registra el evento en el archivo de registro (System Log).

5.3.3 Importación de un perfil de configuración

El dispositivo le permite importar desde un servidor un perfil de configuración guardado como un archivo XML. Si utiliza la interfaz gráfica de usuario, puede importar el archivo XML directamente desde su PC.

Requisitos previos:

- Para guardar el archivo en un servidor, necesita un servidor configurado en la red.
- Para guardar el archivo en un servidor SCP o SFTP, también necesita el nombre de usuario y la contraseña a fin de acceder a este servidor.

Lleve a cabo los siguientes pasos:

- Abra el cuadro de diálogo *Basic Settings > Load/Save*.
- Haga clic en el botón ☰ y, a continuación, en el elemento *Import...*.
  El cuadro de diálogo muestra la ventana *Import...*.
- En la lista desplegable *Select source*, seleccione la ubicación desde la que el dispositivo importa el archivo de configuración.
  - *PC/URL*
    El dispositivo importa el perfil de configuración desde el PC local o desde un servidor remoto.
  - *External memory*
    El dispositivo importa el perfil de configuración desde la memoria externa.

Importe el perfil de configuración desde el PC local o desde un servidor remoto. Para ello, siga los siguientes pasos:

- ☐ Importe el perfil de configuración:
  - ☐ Cuando el archivo se encuentre en un servidor FTP, especifique la URL correspondiente al archivo en el formato siguiente:
    `ftp://<usuario>:<contraseña>@<dirección IP>:<puerto>/<nombre archivo>`
  - ☐ Cuando el archivo se encuentre en un servidor TFTP, especifique la URL correspondiente al archivo en el formato siguiente:
    `tftp://<dirección IP>/<ruta>/<nombre archivo>`
  - ☐ Cuando el archivo se encuentre en un servidor SCP o SFTP, especifique la URL correspondiente al archivo en uno de los siguientes formatos:
    `scp://` o `sftp://<IP address>/<path>/<file name>`
    Si hace clic en el botón *Start*, el dispositivo mostrará la ventana *Credentials*. Ahí podrá introducir el *User name* y la *Password* para iniciar sesión en el servidor.
    `scp://` o `sftp://<usuario>:<contraseña>@<dirección IP>/<ruta>/<nombre archivo>`
- ☐ En el cuadro *Destination*, especifique dónde desea que el dispositivo guarde el perfil de configuración importado:
  - ☐ En el campo *Profile name*, especifique el nombre con el que desea que el dispositivo guarde el perfil de configuración.
  - ☐ En el campo *Storage type*, especifique la ubicación de almacenamiento del perfil de configuración.
- ☐ Haga clic en el botón *Ok*.

El dispositivo copia el perfil de configuración en la memoria especificada.

Si ha especificado el valor `ram` en el cuadro *Destination*, el dispositivo desconecta la interfaz gráfica de usuario y utiliza los ajustes inmediatamente.

Importe el perfil de configuración desde la memoria externa. Para ello, siga los siguientes pasos:

- ☐ En el cuadro *Import profile from external memory*, lista desplegable *Profile name*, seleccione el nombre del perfil de configuración que desee importar.
  El requisito previo es que la memoria externa contenga un perfil de configuración exportado.
- ☐ En el cuadro *Destination*, especifique dónde desea que el dispositivo guarde el perfil de configuración importado:
  - ☐ En el campo *Profile name*, especifique el nombre con el que desea que el dispositivo guarde el perfil de configuración.
- ☐ Haga clic en el botón *Ok*.

El dispositivo copia el perfil de configuración en la memoria no volátil (*NVM*) del dispositivo.

Si ha especificado el valor `ram` en el cuadro *Destination*, el dispositivo desconecta la interfaz gráfica de usuario y utiliza los ajustes inmediatamente.

`enable`	Cambiar al modo Privileged EXEC.
`copy config remote ftp://<IP_address>:<port>/<path>/<file_name> running-config`	Importar y activar los ajustes de un perfil de configuración guardado en un servidor FTP. El dispositivo copia los ajustes en la memoria volátil y desconecta la conexión a la interfaz de línea de comando. El dispositivo utiliza inmediatamente los ajustes del perfil de configuración importado.
`copy config remote tftp://<IP_address>/ <path>/<file_name> running-config`	Importar y activar los ajustes de un perfil de configuración guardado en un servidor TFTP. El dispositivo copia los ajustes en la memoria volátil y desconecta la conexión a la interfaz de línea de comando. El dispositivo utiliza inmediatamente los ajustes del perfil de configuración importado.
`copy config remote sftp://<user name>:<password>@<IP_address>/<path>/<file_name> running-config`	Importar y activar los ajustes de un perfil de configuración guardado en un servidor SFTP. El dispositivo copia los ajustes en la memoria volátil y desconecta la conexión a la interfaz de línea de comando. El dispositivo utiliza inmediatamente los ajustes del perfil de configuración importado.
`copy config remote ftp://<IP_address>:<port>/<path>/<file_name> nvm profile config3`	Importar los ajustes de un perfil de configuración guardado en un servidor FTP y guardar los ajustes en el perfil de configuración `config3` de la memoria no volátil (`nvm`).
`copy config remote tftp://<IP_address>/<path>/<file_name> nvm profile config3`	Importar los ajustes de un perfil de configuración guardado en un servidor TFTP y guardar los ajustes en el perfil de configuración `config3` de la memoria no volátil (`nvm`).

5.4 Restablecimiento del dispositivo a la configuración de fábrica

Si restablece la configuración por defecto del dispositivo, este eliminará los perfiles de configuración de la memoria volátil y la no volátil.

Si se conecta una memoria externa, el dispositivo también eliminará los perfiles de configuración guardados en la memoria externa.

El dispositivo se reiniciará y cargará la configuración de fábrica.

5.4.1 Uso de la Interfaz gráfica de usuario o la Interfaz de línea de comando

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Basic Settings > Load/Save*.
- ☐ Haga clic en el botón y, a continuación, en *Back to factory...*.
  El cuadro de diálogo mostrará un mensaje.
- ☐ Haga clic en el botón *Ok*.

El dispositivo elimina los perfiles de configuración de la memoria (`RAM`) y de la memoria no volátil (`NVM`).

Si se conecta una memoria externa, el dispositivo también eliminará los perfiles de configuración guardados en la memoria externa.

Tras un breve período, el dispositivo se reinicia y carga la configuración por defecto.

`enable`	Cambiar al modo Privileged EXEC.
`clear factory`	Elimina los perfiles de configuración de la memoria no volátil y de la memoria externa. Si se conecta una memoria externa, el dispositivo también eliminará los perfiles de configuración guardados en la memoria externa. Tras un breve período, el dispositivo se reinicia y carga la configuración por defecto.

5.4.2 Uso de la supervisión del sistema

Requisito previo:

- Su PC está conectado con la conexión serie del dispositivo mediante un cable de terminal.

Lleve a cabo los siguientes pasos:

- ☐ Reinicie el dispositivo.
- ☐ Para cambiar a la supervisión del sistema, pulse la tecla <1> antes de que transcurran 3 segundos cuando se le solicite durante el reinicio.
  El dispositivo cargará la supervisión del sistema.
- ☐ Para cambiar del menú principal al menú `Manage configurations`, pulse la tecla <4>.
- ☐ Para ejecutar el comando `Clear configs and boot params`, pulse la tecla <1>.

- Para cargar los ajustes de fábrica, pulse la tecla <Intro>.
  El dispositivo elimina los perfiles de configuración de la memoria (RAM) y de la memoria no volátil (NVM).
  Si se conecta una memoria externa, el dispositivo también eliminará los perfiles de configuración guardados en la memoria externa.
- Para cambiar al menú principal, pulse la tecla <q>.
- Para reiniciar el dispositivo con los ajustes de fábrica, pulse la tecla <q>.

6 Carga de actualizaciones de software

Schneider Electric está trabajando de manera continua para mejorar y desarrollar su software. Compruebe con frecuencia si existe una versión actualizada del software que le proporcionará ventajas adicionales. Puede encontrar información y descargas de software en las páginas del producto Schneider Electric de Internet, en la dirección www.schneider-electric.com.

El dispositivo le ofrece las siguientes opciones para actualizar el software del dispositivo:
- Actualización del software desde el PC
- Actualización del software desde un servidor
- Actualización del software desde la memoria externa
- Carga de una versión anterior del software

Nota: La configuración del dispositivo se mantiene tras actualizar el software.

Podrá ver la versión del software del dispositivo instalada en el cuadro de diálogo de inicio de sesión de la interfaz gráfica de usuario.

Para visualizar la versión del software instalado cuando ya tiene la sesión iniciada, lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Basic Settings > Software*.
  El campo *Running version* muestra el número de versión y la fecha de creación del software del dispositivo cargado durante el último reinicio y que se está ejecutando actualmente.

`enable`	Cambiar al modo Privileged EXEC.
`show system info`	Muestra información del sistema, como el número de versión y la fecha de creación del software del dispositivo cargado durante el último reinicio y que se está ejecutando actualmente.

6.1 Actualización del software desde el PC

El requisito previo es que el archivo de imagen del software del dispositivo se guarde en un soporte de datos al que se pueda acceder desde su PC.

Lleve a cabo los siguientes pasos:

- ☐ Desplácese hasta la carpeta en la que se encuentre guardado el archivo de imagen del software del dispositivo.
- ☐ Abra el cuadro de diálogo *Basic Settings > Software*.
- ☐ Arrastre y suelte el archivo de imagen en el área  . También puede hacer clic en el área para seleccionar el archivo.
- ☐ Para iniciar el procedimiento de actualización, haga clic en el botón *Start*.
  En cuanto se complete el procedimiento de actualización correctamente, el dispositivo mostrará una información indicando que el software se ha actualizado correctamente. Tras reiniciar el dispositivo, este cargará el software instalado.

6.2 Actualización del software desde un servidor

Para actualizar el software mediante SFTP o SCP, se necesita un servidor en el que guardar el archivo de imagen del software del dispositivo.

Para actualizar el software mediante TFTP, SFTP o SCP, se necesita un servidor en el que guardar el archivo de imagen del software del dispositivo.

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Basic Settings > Software*.
- ☐ En el cuadro *Software update*, campo *URL*, introduzca la URL correspondiente al archivo de imagen en el formato siguiente:
  - ▶ Cuando se guarde el archivo de imagen en un servidor FTP:
    `ftp://<dirección_IP>:<puerto>/<ruta>/<nombre_archivo_imagen>.bin`
  - ▶ Cuando se guarde el archivo de imagen en un servidor TFTP:
    `tftp://<dirección_IP>/<ruta>/<nombre_archivo_imagen>.bin`
  - ▶ Cuando se guarde el archivo de imagen en un servidor SCP o SFTP:
    `scp://` o `sftp://<dirección_IP>/<ruta>/<nombre_archivo_imagen>.bin`
    `scp://` o `sftp://<nombre_de_usuario>:<contraseña>@<dirección_IP>/<ruta>/<nombre_archivo_imagen>.bin`
    Cuando introduzca la URL sin el nombre de usuario y la contraseña, el dispositivo mostrará la ventana *Credentials*. Ahí podrá introducir las credenciales de inicio de sesión necesarias para iniciar sesión en el servidor.
- ☐ Para iniciar el procedimiento de actualización, haga clic en el botón *Start*.
  El dispositivo copia el software del dispositivo que se está ejecutando actualmente en la memoria de la copia de seguridad.
  En cuanto se complete el procedimiento de actualización correctamente, el dispositivo mostrará una información indicando que el software se ha actualizado correctamente.
  Tras reiniciar el dispositivo, este cargará el software instalado.

`enable`	Cambiar al modo Privileged EXEC.
`copy firmware remote tftp://10.0.1.159/product.bin system`	Transferir el archivo `product.bin` del servidor TFTP con la dirección IP `10.0.1.159` al dispositivo.

6.3 Actualización del software desde la memoria externa

6.3.1 Manualmente (iniciada por el administrador)

El dispositivo le permite actualizar el software del dispositivo con unos cuantos clics del ratón. El requisito previo es que el archivo de imagen del software del dispositivo se encuentre en la memoria externa.

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Basic Settings > Software*.
- ☐ En la tabla, marque la fila en la que se muestre el nombre del archivo de imagen deseado de la memoria externa.
- ☐ Haga clic con el botón derecho del ratón para visualizar el menú contextual.
- ☐ Para iniciar el procedimiento de actualización, haga clic en el elemento *Update* del menú contextual.
  El dispositivo copia el software del dispositivo que se está ejecutando actualmente en la memoria de la copia de seguridad.
  En cuanto se complete el procedimiento de actualización correctamente, el dispositivo mostrará una información indicando que el software se ha actualizado correctamente.
  Tras reiniciar el dispositivo, este cargará el software instalado.

6.3.2 Automáticamente (iniciada por el dispositivo)

Cuando los siguientes archivos se encuentran en la memoria externa durante un reinicio, el dispositivo actualizará el software del dispositivo automáticamente:

- el archivo de imagen del software del dispositivo
- un archivo de texto `startup.txt` con el contenido `autoUpdate=<Image_file_name>.bin`

El requisito previo es que marque la casilla de la columna *Software auto update* del cuadro de diálogo *Basic Settings > External Memory*. Este es el ajuste por defecto en el dispositivo.

Lleve a cabo los siguientes pasos:

- ☐ Copie el archivo de imagen del software del dispositivo nuevo en el directorio principal de la memoria externa. Utilice solamente un archivo de imagen adecuado para el dispositivo.
- ☐ Cree un archivo de texto `startup.txt` en el directorio principal de la memoria externa.
- ☐ Abra el archivo `startup.txt` en el editor de texto y añada la línea siguiente: `autoUpdate=<Image_file_name>.bin`
- ☐ Instale la memoria externa en el dispositivo.

- ☐ Reinicie el dispositivo.
  Durante el proceso de arranque, el dispositivo comprueba los siguientes criterios automáticamente:
  - ¿Hay conectada una memoria externa?
  - ¿Hay un archivo `startup.txt` en el directorio principal de la memoria externa?
  - ¿Existe el archivo de imagen especificado en el archivo `startup.txt`?
  - ¿Es la versión del software del archivo de imagen más reciente que el software que se está ejecutando actualmente en el dispositivo?

  Cuando se cumplan los criterios, el dispositivo iniciará el procedimiento de actualización.
  El dispositivo copia el software del dispositivo que se está ejecutando actualmente en la memoria de la copia de seguridad.
  En cuanto se complete el procedimiento de actualización correctamente, el dispositivo se reiniciará automáticamente y cargará la nueva versión del software.
- ☐ Compruebe el resultado del procedimiento de actualización. El archivo de registro del cuadro de diálogo *Diagnostics > Report > System Log* contiene uno de los siguientes mensajes:
  - `S_watson_AUTOMATIC_SWUPDATE_SUCCESS`
    Actualización del software completada correctamente
  - `S_watson_AUTOMATIC_SWUPDATE_ABORTED`
    Actualización del software cancelada
  - `S_watson_AUTOMATIC_SWUPDATE_ABORTED_WRONG_FILE`
    Actualización del software cancelada debido al uso de un archivo de imagen incorrecto
  - `S_watson_AUTOMATIC_SWUPDATE_ABORTED_SAVING_FILE`
    Actualización de software cancelada debido a que el dispositivo no guardó el archivo de imagen.

6.4 Carga de una versión anterior del software

El dispositivo le permite sustituir el software por una versión anterior. La configuración básica del dispositivo se mantiene tras sustituir el software del dispositivo.

Nota: Solamente se perderán las configuraciones de las funciones que estén disponibles en el software del dispositivo nuevo.

7 Configuración de los puertos

Están disponibles las siguientes funciones de configuración de puertos.

- Activación/desactivación del puerto
- Selección del modo de funcionamiento
- Modo Gigabit Ethernet para puertos

7.1 Activación/desactivación del puerto

Con la configuración por defecto, todos los puertos están activados. Para disponer de un nivel superior de seguridad de acceso, desactive los puertos no conectados. Para ello, siga los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Basic Settings > Port*, pestaña *Configuration*.
- ☐ Para activar un puerto, marque la casilla de la columna *Port on*.
- ☐ Para desactivar un puerto, desmarque la casilla de la columna *Port on*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón  .

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`interface 1/1`	Cambiar al modo de configuración de la interfaz `1/1`.
`no shutdown`	Activar la interfaz.

7.2 Selección del modo de funcionamiento

En la configuración por defecto, los puertos están ajustados en el modo de funcionamiento *Automatic configuration*.

Nota: la configuración automática activa tiene preferencia ante la configuración manual.

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Basic Settings > Port*, pestaña *Configuration*.
- ☐ Si el dispositivo conectado a este puerto requiere un ajuste fijo, lleve a cabo los siguientes pasos:
  - ☐ Desactive la función. Desmarque la casilla de la columna *Automatic configuration*.
  - ☐ En la columna *Manual configuration*, acceda al modo de funcionamiento deseado (velocidad de transmisión, modo dúplex).
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ☑.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`interface 1/1`	Cambiar al modo de configuración de la interfaz `1/1`.
`no auto-negotiate`	Desactivar el modo de configuración automática.
`speed 100 full`	Velocidad del puerto de 100 MBits/s, Full-Dúplex

7.3 Modo Gigabit Ethernet para puertos

El dispositivo admite 2.5 Gbits/s en varias interfaces con uno de los siguientes transceptores SFP:
- M-SFP-2.5-MM/LC EEC
- M-SFP-2.5-SM-/LC EEC
- M-SFP-2.5-SM/LC EEC
- M-SFP-2.5-SM+/LC EEC

El tipo de transceptor conectado a la ranura determinará la velocidad del puerto. El dispositivo no dispone de ninguna opción para ajustar la velocidad manualmente. Los puertos con una velocidad de 2,5 Gbits/s no admiten velocidades de transferencia de 100 Mbits/s.

Nota: Puede obtener más información sobre los números de pedido de los transceptores en el capítulo "Accesorios" del manual de usuario "Instalación".

7.3.1 Ejemplo

Utilice el modo Gigabit Ethernet a fin de obtener un ancho de banda superior para los puertos Uplink. Para utilizar esta función, introduzca un transceptor adecuado en la ranura correspondiente.

Lleve a cabo los siguientes pasos:

☐ Abra el cuadro de diálogo *Basic Settings > Port*, pestaña *Configuration*.

En la columna *Manual configuration* se muestra el valor `2.5 Gbit/s FDX` para los puertos que disponen de un transceptor 2.5 de SFP Gbits/s insertado.

No se puede cambiar la velocidad.

```
show port 1/1
```

Muestra los parámetros del puerto `1` de la ranura `1`. La entrada de la lista `Physical Mode` muestra el valor `2500 full` de los puertos que disponen de un transceptor 2.5 de SFP Gbits/s insertado.

```
Interface.....................1/1
Name..........................My interface
--
Cable-crossing Setting........-
Physical Mode.................2500 full
Physical Status...............-
```

8 Asistencia en la protección ante accesos no autorizados

El dispositivo ofrece funciones que le ayudan a proteger el dispositivo frente a accesos no autorizados.

Una vez configurado el dispositivo, lleve a cabo los siguientes pasos para reducir los posibles accesos no autorizados.

- Cambio de la comunidad SNMPv1/v2
- Desactivación de SNMPv1/v2
- Desactivación de HTTP
- Uso de su propio certificado HTTPS
- Uso de su propia clave SSH
- Desactivación de Telnet
- Desactivación de Ethernet Switch Configurator
- Activación de la restricción de acceso a IP
- Ajuste de los tiempos de espera de sesión

8.1 Cambio de la comunidad SNMPv1/v2

El protocolo SNMPv1/v2 funciona sin encriptación. Cada paquete SNMP contiene la dirección IP del remitente y el nombre de la comunidad en texto no cifrado con el que el remitente accede al dispositivo. Si SNMPv1/v2 se encuentra activado, el dispositivo permitirá a cualquier usuario que conozca el nombre de la comunidad acceder al dispositivo.

Los nombres de la comunidad `user` para accesos de lectura y `admin` para accesos de escritura están presentes. Si utiliza SNMPv1 o SNMPv2, cambie el nombre de la comunidad predeterminado. Trate los nombres de la comunidad con discreción. Para ello, siga los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Device Security > Management Access > SNMPv1/v2 Community*.

Este mostrará las comunidades que están configuradas.

- ☐ Para la comunidad `Write`, especifique su nombre en la columna *Name*.
  - Se permiten hasta 32 caracteres alfanuméricos en los nombres.
  - El dispositivo distingue entre mayúsculas y minúsculas.
  - Especifique un nombre de comunidad diferente que el correspondiente al acceso de lectura.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✓.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`snmp community rw <community name>`	Especificar la comunidad correspondiente al acceso de lectura/escritura.
`show snmp community`	Mostrar las comunidades que se han configurado.
`save`	Guardar los ajustes en el perfil de configuración "seleccionado" de la memoria no volátil (`nvm`).

8.2 Desactivación de SNMPv1/v2

Si necesita SNMPv1 o SNMPv2, utilice estos protocolos únicamente en entornos protegidos contra intercepciones. SNMPv1 y SNMPv2 no utilizan ninguna encriptación. Los paquetes SNMP contienen la comunidad en texto no cifrado. Es recomendable utilizar SNMPv3 en el dispositivo y desactivar el acceso con SNMPv1 y SNMPv2. Para ello, siga los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Device Security > Management Access > Server*, pestaña *SNMP*.

El cuadro muestra la configuración del servidor SNMP.

- ☐ Para desactivar el protocolo SNMPv1, desmarque la casilla *SNMPv1*.
- ☐ Para desactivar el protocolo SNMPv2, desmarque la casilla *SNMPv2*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón  .

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`no snmp access version v1`	Desactivar el protocolo SNMPv1.
`no snmp access version v2`	Desactivar el protocolo SNMPv2.
`show snmp access`	Mostrar la configuración del servidor SNMP.
`save`	Guardar los ajustes en el perfil de configuración "seleccionado" de la memoria no volátil (`nvm`).

8.3 Desactivación de HTTP

El servidor web proporciona una interfaz gráfica de usuario con el protocolo HTTP o HTTPS. Las conexiones HTTPS están encriptadas, mientras que las HTTP están sin encriptar.

El protocolo HTTP está activado por defecto. Si desactiva HTTP, no dispondrá de acceso sin encriptar a la interfaz gráfica de usuario. Para ello, siga los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Device Security > Management Access > Server*, pestaña *HTTP*.
- ☐ Para desactivar el protocolo HTTP, seleccione el botón de opción `Off` en el cuadro *Operation*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✓.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`no http server`	Desactivar el protocolo HTTP.

Si el protocolo HTTP está desactivado, solamente podrá acceder a la interfaz gráfica de usuario del dispositivo mediante HTTPS. En la barra de dirección del navegador web, introduzca la cadena `https://` antes de la dirección IP del dispositivo.

Si el protocolo HTTPS está desactivado y también desactiva HTTP, no podrá acceder a la interfaz gráfica de usuario. Para trabajar con la interfaz gráfica de usuario, active el servidor HTTPS con la interfaz de línea de comando. Para ello, siga los siguientes pasos:

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`https server`	Activar el protocolo HTTP.

8.4 Desactivación de Telnet

El dispositivo le permite acceder de forma remota a la gestión del dispositivo mediante Telnet o SSH. Las conexiones Telnet no están encriptadas, mientras que las SSH sí lo están.

El servidor Telnet está activado en el dispositivo por defecto. Si desactiva Telnet, no podrá volver a acceder de forma remota y sin encriptación a la interfaz de línea de comando. Para ello, siga los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Device Security > Management Access > Server*, pestaña *Telnet*.
- ☐ Para desactivar el servidor Telnet, seleccione el botón de opción `Off` en el cuadro *Operation*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✓.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`no telnet server`	Desactivar el servidor Telnet.

Si se desactiva el servidor SSH y también Telnet, el acceso a la interfaz de la línea de comando solo será posible con la interfaz serie del dispositivo. Para trabajar de forma remota con la interfaz de la línea de comando, active SSH. Para ello, siga los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Device Security > Management Access > Server*, pestaña *SSH*.
- ☐ Para activar el servidor *SSH*, seleccione el botón de opción `On` en el cuadro *Operation*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✓.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`ssh server`	Active el servidor SSH.

8.5 Desactivación del acceso a Ethernet Switch Configurator

Ethernet Switch Configurator le permite asignar parámetros IP al dispositivo a través de la red durante la puesta en marcha. Ethernet Switch Configurator establece comunicación en la VLAN de gestión del dispositivo sin encriptación ni autenticación.

Una vez puesto en marcha el dispositivo, es recomendable ajustar Ethernet Switch Configurator en modo de solo lectura o desactivar el acceso a Ethernet Switch Configurator por completo. Para ello, siga los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Basic Settings > Network*.
- ☐ Para retirar el permiso de escritura del software Ethernet Switch Configurator, en el cuadro *Ethernet Switch Configurator protocol v1/v2*, especifique el valor `readOnly` en el campo *Access*.
- ☐ Para desactivar el acceso a Ethernet Switch Configurator por completo, seleccione el botón de opción `Off` en el cuadro *Ethernet Switch Configurator protocol v1/v2*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón .

`enable`	Cambiar al modo Privileged EXEC.
`network ethernet-switch-conf mode read-only`	Desactivar el permiso de escritura del software Ethernet Switch Configurator.
`no network ethernet-switch-conf operation`	Desactive el acceso a Ethernet Switch Configurator.

8.6 Activación de la restricción de acceso a IP

En la configuración predeterminada, podrá acceder a la gestión del dispositivo desde cualquier dirección IP y con los protocolos compatibles.

La restricción de acceso a IP le permite restringir el acceso a la gestión del dispositivo a rangos de direcciones IP y protocolos basados en IP específicos.

Por ejemplo:

Solo se puede acceder al dispositivo desde la red de la empresa a través de la interfaz gráfica de usuario. El administrador dispone de un acceso remoto adicional mediante SSH. La red de la empresa posee el rango de direcciones `192.168.1.0/24` y un acceso remoto desde una red móvil con el rango de direcciones IP `109.237.176.0/24`. El programa de aplicación de SSH conoce la huella digital de la clave RSA.

Tabla 20: Parámetros de la restricción de acceso a IP

Parámetro	Red de la empresa	Red de telefonía móvil
Dirección de red	`192.168.1.0`	`109.237.176.0`
Netmask ‹Máscara de red›	`24`	`24`
Protocolos deseados	https, snmp	ssh

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Device Security* > *Management Access* > *IP Access Restriction*.
- ☐ Desmarque la casilla de la columna *Active* para la entrada.
  Esta entrada permite a los usuarios disponer de acceso al dispositivo desde cualquier dirección IP y los protocolos compatibles.

Rango de direcciones de la red de la empresa:

- ☐ Para añadir una entrada de tabla, haga clic en el botón .
- ☐ Especifique el rango de direcciones de la red de la empresa en la columna *IP address range*: `192.168.1.0/24`
- ☐ Para obtener el rango de direcciones de la red de la empresa, desactive los protocolos no deseados. Las casillas *HTTPS*, *SNMP* y *Active* permanecerán marcadas.

Rango de direcciones de la red de telefonía móvil:

- ☐ Para añadir una entrada de tabla, haga clic en el botón .
- ☐ Especifique el rango de direcciones de la red móvil en la columna *IP address range*: `109.237.176.0/24`
- ☐ Para obtener el rango de direcciones de la red móvil, desactive los protocolos no deseados. Las casillas *SSH* y *Active* permanecerán marcadas.

Antes de activar la función, compruebe que al menos una entrada activa de la tabla le permite disponer de acceso. De lo contrario, si cambia la configuración, la conexión con el dispositivo finalizará. El acceso a la gestión del dispositivo solo es posible utilizando la interfaz de línea de comando a través de la interfaz serie del dispositivo.

- ☐ Para activar la restricción de acceso a IP, seleccione el botón de opción `On` en el cuadro *Operation*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón .

`enable`	Cambiar al modo Privileged EXEC.
`show network management access global`	Muestra si la restricción de acceso a IP está activada o desactivada.
`show network management access rules`	Mostrar las entradas que se han configurado.
`no network management access operation`	Desactivar la restricción de acceso a IP.
`network management access add 2`	Crear la entrada para el rango de direcciones de la red de la empresa. Número del siguiente índice disponible en este ejemplo: `2`.
`network management access modify 2 ip 192.168.1.0`	Especificar la dirección IP de la red de la empresa.
`network management access modify 2 mask 24`	Especificar la máscara de red de la red de la empresa.
`network management access modify 2 ssh disable`	Desactivar SSH del rango de direcciones de la red de la empresa. Repetir la operación para cada protocolo no deseado.
`network management access add 3`	Crear una entrada para el rango de direcciones de la red de telefonía móvil. Número del siguiente índice disponible en este ejemplo: `3`.
`network management access modify 3 ip 109.237.176.0`	Especificar la dirección IP de la red de telefonía móvil.
`network management access modify 3 mask 24`	Especificar la máscara de red de la red de telefonía móvil.
`network management access modify 3 snmp disable`	Desactivar SNMP para el rango de direcciones de la red de telefonía móvil. Repetir la operación para cada protocolo no deseado.
`no network management access status 1`	Desactivar la entrada predeterminada. Esta entrada permite a los usuarios disponer de acceso al dispositivo desde cualquier dirección IP y los protocolos compatibles.
`network management access status 2`	Activar una entrada para el rango de direcciones de la red de la empresa.
`network management access status 3`	Activar una entrada para el rango de direcciones de la red de telefonía móvil.
`show network management access rules`	Mostrar las entradas que se han configurado.
`network management access operation`	Activar la restricción de acceso a IP.

8.7 Ajuste de los tiempos de espera de sesión

El dispositivo le permite terminar automáticamente la sesión tras un período de inactividad del usuario conectado. El tiempo de espera de sesión es el período de inactividad transcurrido después de la última acción realizada por el usuario.

Puede especificar un tiempo de espera de sesión para las siguientes aplicaciones:
- Sesiones de la interfaz de línea de comando que utilizan una conexión SSH
- Sesiones de la interfaz de línea de comando que utilizan una conexión Telnet
- Sesiones de la interfaz de línea de comando que utilizan una conexión serie
- Interfaz gráfica de usuario

Tiempo de espera de las sesiones de la interfaz de línea de comando que utilizan una conexión SSH

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Device Security > Management Access > Server*, pestaña *SSH*.
- ☐ Especifique el tiempo de espera en minutos en el cuadro *Configuration*, campo *Session timeout [min]*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ☑.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`ssh timeout <0..160>`	Especificar el período de tiempo de espera en minutos para sesiones de la interfaz de línea de comando que utilizan una conexión SSH.

Tiempo de espera de las sesiones de la interfaz de línea de comando que utilizan una conexión Telnet

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Device Security > Management Access > Server*, pestaña *Telnet*.
- ☐ Especifique el tiempo de espera en minutos en el cuadro *Configuration*, campo *Session timeout [min]*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ☑.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`telnet timeout <0..160>`	Especificar el período de tiempo de espera en minutos para sesiones de la interfaz de línea de comando que utilizan una conexión Telnet.

Tiempo de espera de las sesiones de la interfaz de línea de comando que utilizan una conexión serie

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Device Security > Management Access > CLI*, pestaña *Global*.
- ☐ Especifique el tiempo de espera en minutos en el cuadro *Configuration*, campo *Serial interface timeout [min]*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ☑.

`enable`	Cambiar al modo Privileged EXEC.
`cli serial-timeout <0..160>`	Especificar el período de tiempo de espera en minutos para sesiones de la interfaz de línea de comando que utilizan una conexión serie.

Tiempo de espera de sesión de la interfaz gráfica de usuario

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Device Security > Management Access > Web*.
- ☐ Especifique el tiempo de espera en minutos en el cuadro *Configuration*, campo *Web interface session timeout [min]*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ☑.

`enable`	Cambiar al modo Privileged EXEC.
`network management access web timeout <0..160>`	Especificar el período de tiempo de espera en minutos para sesiones de interfaz gráfica de usuario

9 Control del tráfico de datos

El dispositivo comprueba los paquetes de datos que desea reenviar conforme a las reglas definidas. Los paquetes de datos a los que se aplican las reglas son reenviados por el dispositivo o bloqueados. Si los paquetes de datos no se corresponden con ninguna de las reglas, el dispositivo bloquea los paquetes.

Los puertos de enrutamiento que no tienen asignada ninguna regla permiten el paso de los paquetes. En cuanto se asigna una regla, las reglas asignadas se procesan en primer lugar. Posteriormente, se lleva a cabo la acción estándar especificada del dispositivo.

El dispositivo le ofrece las siguientes funciones para controlar el flujo de datos:
- Control de la solicitud de servicio (Denial of Service, DoS)
- Denegación del acceso a los dispositivos según su dirección IP o MAC (lista de control de acceso)

El servicio observa y supervisa el flujo de datos. El dispositivo toma los resultados de la observación y la supervisión y los combina con las reglas de seguridad de red para crear lo que se conoce como una tabla de estado. En función de la tabla de estado, el dispositivo decida si aceptar, anular o rechazar datos.

Los paquetes de datos atraviesan las funciones de filtrado del dispositivo en la siguiente secuencia:
- DoS … si `permit` o `accept`, entonces diríjase a la siguiente regla
- ACL … si `permit` o `accept`, entonces diríjase a la siguiente regla

9.1 ¿Cómo ayudar a proteger contra el acceso no autorizado?

Con esta función, el dispositivo le ayuda a protegerse frente a paquetes de datos no válidos o falsificados destinados a determinados servicios o dispositivos. Tiene la opción de especificar filtros para restringir el flujo de datos a fin de protegerlos contra ataques de denegación de servicio. Los filtros activados comprueban los paquetes de datos entrantes y los descartan en cuanto se detecta una coincidencia con los criterios de filtración.

El cuadro de diálogo *Network Security > DoS > Global* contiene 2 cuadros en los que se pueden activar diferentes filtros. Para activarlos, marque las casillas correspondientes.

En el cuadro *TCP/UDP*, puede activar hasta 4 filtros que solo afectan a los paquetes TCP y UDP. Al utilizar este filtro, se desactivan las búsquedas de puertos, que los atacantes utilizan para intentar reconocer dispositivos y servicios ofrecidos. Los filtros funcionan de la siguiente manera:

Tabla 21: Filtros DoS para paquetes TCP

Filtro	Acción
Activar el filtro Null Scan	El dispositivo acepta y descarta paquetes TCP entrantes con las siguientes propiedades: ▶ No hay establecida ninguna marca TCP. ▶ El número de la secuencia TCP es 0.
Activar el filtro Xmas	El dispositivo acepta y descarta paquetes TCP entrantes con las siguientes propiedades: ▶ Las marcas TCP *FIN*, *URG* y *PSH* se establecen de manera simultánea. ▶ El número de la secuencia TCP es 0.
Activar el filtro SYN/FIN	El dispositivo detecta y descarta paquetes TCP entrantes en los que están ajustadas de manera simultánea las marcas TCP *SYN* y *FIN*.
Activar el filtro Minimal Header	El dispositivo detecta y descarta paquetes TCP entrantes en los que el encabezado TCP es demasiado corto.

El cuadro *ICMP* le ofrece 2 opciones de filtro para los paquetes ICMP. La fragmentación de paquetes ICMP entrantes es un síntoma de un ataque. Si activa este filtro, el dispositivo detectará paquetes ICMP fragmentados y los descartará. Mediante el parámetro *Allowed payload size [byte]*, también podrá especificar el tamaño máximo permitido de la carga útil de los paquetes ICMP. El dispositivo descarta paquetes de datos que superan esta especificación de bytes.

Nota: Puede combinar los filtros de cualquier manera en el cuadro de diálogo *Network Security* > DoS > *Global*. Cuando se seleccionan varios filtros o se aplica un Or lógico: si se aplica el primer o segundo filtro (o el tercero, etc.) a un paquete de datos, el dispositivo lo descarta.

9.2 ACL

En este menú, puede introducir los parámetros de las Listas de control de acceso (ACL).

El dispositivo utiliza las ACL para filtrar paquetes de datos recibidos en VLAN o en puertos individuales o múltiples. En una ACL, especifica reglas que el dispositivo utiliza para filtrar paquetes de datos. Cuando se aplica una regla de este tipo a un paquete, el dispositivo aplica las acciones especificadas en la regla al paquete. Las acciones disponibles son las siguientes:
- permitir (`permit`)
- descartar (`deny`)
- redireccionar a un puerto determinado (consulte el campo *Redirection port*)
- reflejar (consulte el campo *Mirror port*)

La lista siguiente contiene criterios que puede aplicar para filtrar los paquetes de datos:
- Dirección de origen o destino de un paquete (MAC)
- Dirección de origen o destino de un paquete de datos (IPv4)
- Puerto de origen o destino de un paquete de datos (IPv4)

Puede especificar los siguientes tipos de ACL:
- ACL de IP para VLAN
- ACL de IP para puertos
- ACL de MAC para VLAN
- ACL de MAC para puertos

Cuando asigna una ACL de IP y una de MAC a la misma interfaz, el dispositivo utiliza primero la ACL de IP para filtrar el flujo de datos. El dispositivo aplica las reglas ACL de MAC solamente después de que se filtren los paquetes a través de la ACL de IP. La prioridad de una ACL es independiente del índice de una regla.

Dentro de una ACL, el dispositivo procesa las reglas en orden. El índice de la regla correspondiente determina el orden en el que el dispositivo filtra el flujo de datos. Cuando asigna una ACL a un puerto o VLAN, puede especificar su prioridad con el índice. Cuanto menor sea el número, mayor será la prioridad. El dispositivo procesa la regla con la máxima prioridad en primer lugar.

Si no se aplica ninguna de las reglas de una ACL a un paquete de datos, se aplicará la regla `deny` implícita. Como resultado, el dispositivo anulará los paquetes de datos recibidos.

Tenga en cuenta que el dispositivo implementa la regla `deny` implícita directamente.

Nota: El número de ACL disponibles depende del dispositivo. Puede obtener más información acerca de los valores de ACL en el capítulo “Datos técnicos” en página 384.

Nota: Puede asignar una única ACL al número de puertos o VLAN que desee.

El menú *ACL* contiene los siguientes cuadros de diálogo:
- *ACL IPv4 Rule*
- *ACL MAC Rule*
- *ACL Assignment*

Estos cuadros de diálogo proporcionan las siguientes opciones:
- Especificar las reglas de los distintos tipos de ACL.
- Proporcionar las reglas con las propiedades requeridas.
- Asignar las ACL a puertos o VLAN.

9.2.1 Creación y edición de reglas IPv4

Al filtrar paquetes de datos IPv4, el dispositivo le permite:
- crear reglas y grupos nuevos
- añadir reglas nuevas a grupos existentes
- editar una regla existente
- activar y desactivar grupos y reglas
- eliminar grupos y reglas existentes
- cambiar el orden de las reglas existentes

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Network Security > ACL > IPv4 Rule*.
- ☐ Haga clic en el botón  .
  El cuadro de diálogo muestra la ventana *Create*.
- ☐ Para crear un grupo, especifique un nombre significativo en el campo *Group name*. Puede combinar varias reglas en un grupo.
- ☐ Para añadir una regla a un grupo existente, seleccione el nombre del grupo en el campo *Group name*.
- ☐ En el campo *Index*, especifique el número de la regla dentro de la ACL.
  Este número define la prioridad de la regla.
- ☐ Haga clic en el botón *Ok*.
  El dispositivo añade la regla a la tabla.
  El grupo y el rol estarán activos inmediatamente.
  Para desactivar un grupo o reglas, desmarque la casilla de la columna *Active*.
  Para eliminar una regla, resalte la entrada de tabla afectada y haga clic en el botón  .
- ☐ Edite los parámetros de la regla en la tabla.
  Para cambiar un valor, haga doble clic en el campo correspondiente.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón  .

Nota: El dispositivo le permite utilizar comodines con los parámetros *Source IP address* y *Destination IP address*. Si introduce, por ejemplo, `192.168.?.?`, el dispositivo permitirá direcciones que empiecen por `192.168`.

Nota: El requisito previo para cambiar los valores de la columna *Source TCP/UDP port* y *Destination TCP/UDP port* es que especifique el valor `tcp` o `udp` en la columna *Protocol*.

Nota: El requisito previo para cambiar el valor de la columna *Redirection port* y *Mirror port* es que especifique el valor `permit` en la columna *Action*.

9.2.2 Creación y configuración de una ACL de IP mediante la interfaz de línea de comando

En el ejemplo siguiente, configure las ACL para bloquear comunicaciones entre los ordenadores B y C y el ordenador A a través de IP (TCP, UDP, etc.).

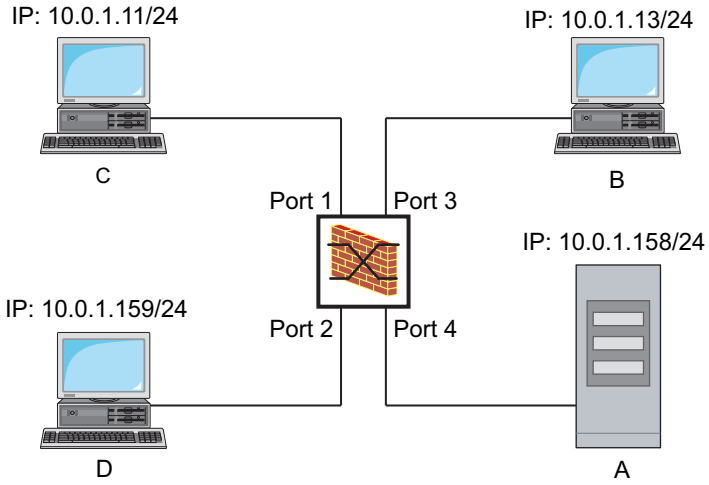


Figura 22: Ejemplo de una ACL de IP

Lleve a cabo los siguientes pasos:

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`ip access-list extended name filter1 deny src 10.0.1.11-0.0.0.0 dst 10.0.1.158-0.0.0.0 assign-queue 1`	Añada una ACL de IP con el nombre `filter1`. Añada una regla que rechace paquetes de datos de IP de `10.0.1.11` a `10.0.1.158`. Prioridad `1` (prioridad máxima).
`ip access-list extended name filter1 permit src any dst any`	Añada una regla a la ACL de IP que admita paquetes de datos de IP.
`show access-list ip filter1`	Muestre las reglas de la ACL de IP `filter1`.
`ip access-list extended name filter2 deny src 10.0.1.13-0.0.0.0 dst 10.0.1.158-0.0.0.0 assign-queue 1`	Añada una ACL de IP con el nombre `filter2`. Añada una regla que rechace paquetes de datos de IP de `10.0.1.13` a `10.0.1.158`. Prioridad `1` (prioridad máxima).
`show access-list ip filter2`	Muestre las reglas de la ACL de IP `filter2`.

9.2.3 Creación y edición de reglas MAC

Al filtrar paquetes de datos MAC, el dispositivo le permite:

- crear reglas y grupos nuevos
- añadir reglas nuevas a grupos existentes
- editar una regla existente
- activar y desactivar grupos y reglas
- eliminar grupos y reglas existentes
- cambiar el orden de las reglas existentes

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Network Security > ACL > MAC Rule*.
- ☐ Haga clic en el botón  .
  El cuadro de diálogo muestra la ventana *Create*.
- ☐ Para crear un grupo, especifique un nombre significativo en el campo *Group name*. Puede combinar varias reglas en un grupo.
- ☐ Para añadir una regla a un grupo existente, seleccione el nombre del grupo en el campo *Group name*.
- ☐ En el campo *Index*, especifique el número de la regla dentro de la ACL.
  Este número define la prioridad de la regla.
- ☐ Haga clic en el botón *Ok*.
  El dispositivo añade la regla a la tabla.
  El grupo y el rol estarán activos inmediatamente.
  Para desactivar un grupo o reglas, desmarque la casilla de la columna *Active*.
  Para eliminar una regla, resalte la entrada de tabla afectada y haga clic en el botón  .
- ☐ Edite los parámetros de la regla en la tabla.
  Para cambiar un valor, haga doble clic en el campo correspondiente.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón  .

Nota: En los campos *Source MAC address* y *Destination MAC address*, puede utilizar comodines en formato `FF:??:??:??:??:??` o `??:??:??:??:00:01`. Aquí debe utilizar mayúsculas.

9.2.4 Creación y configuración de una ACL de MAC mediante la interfaz de línea de comando

En el ejemplo siguiente, AppleTalk e IPX se filtrarán de toda la red. Para ello, siga los siguientes pasos:

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`mac acl add 1 macfilter`	Añade una ACL de MAC con el ID `1` y el nombre `macfilter`.
`mac acl rule add 1 1 deny src any any dst any any etype appletalk`	Añade una regla a la posición `1` de la ACL de MAC con el ID `1` rechazando paquetes con EtherType `0x809B (AppleTalk)`.
`mac acl rule add 1 2 deny src any any dst any any etype ipx-old`	Añade una regla a la posición `2` de la ACL de MAC con el ID `1` rechazando paquetes con EtherType `0x8137 (IPX alt)`.
`mac acl rule add 1 3 deny src any any dst any any etype ipx-new`	Añade una regla a la posición `3` de la ACL de MAC con el ID `1` rechazando paquetes con EtherType `0x8138 (IPX)`.
`mac acl rule add 1 4 permit src any any dst any any`	Añade una regla a la posición `4` de la ACL de MAC con el ID `1` reenviando paquetes.
`show acl mac rules 1`	Muestra las reglas de la ACL de MAC con el ID `1`.
`interface 1/1,1/2,1/3,1/4,1/5,1/6`	Cambiar al modo de configuración de la interfaz de las interfaces `1/1` a `1/6`.

`acl mac assign 1 in 1`	Asigna la ACL de MAC con el ID `1` a paquetes de datos entrantes (`1/1`) en las interfaces `1/6` a `in`.
`exit`	Abandona el modo de interfaz.
`show acl mac assignment 1`	Muestra la asignación de la ACL de MAC con el ID `1` a interfaces o VLAN.

9.2.5 Asignación de ACL a un puerto o VLAN

Cuando asigna ACL a un puerto o VLAN, el dispositivo le ofrece las siguientes opciones:
- Seleccionar el puerto o la VLAN.
- Especificar la prioridad de la ACL.
- Seleccionar la ACL mediante el nombre del grupo.

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Network Security > ACL > Assignment*.
- ☐ Haga clic en el botón  .
  El cuadro de diálogo muestra la ventana *Create*.
  - ☐ En el campo *Port/VLAN*, especifique el puerto o la VLAN deseados.
  - ☐ En el campo *Priority*, especifique la prioridad.
  - ☐ En el campo *Direction*, especifique los paquetes de datos a los que el dispositivo aplica la regla.
  - ☐ En el campo *Group name*, especifique la regla que el dispositivo asigna al puerto o a la VLAN.
- ☐ Haga clic en el botón *Ok*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón  .

9.3 Omisión de autenticación con MAC

La función *MAC authorized bypass* permite a los clientes sin compatibilidad con el estándar 802.1X, como impresoras y faxes, autenticarse en la red con su dirección MAC. El dispositivo le permite especificar el formato de la dirección MAC que se utiliza para autenticar a los clientes en el servidor RADIUS.

Por ejemplo:

Divida la dirección MAC en 6 grupos de 2 caracteres. Escriba en mayúsculas y utilice los dos puntos para separar los caracteres: `AA:BB:CC:DD:EE:FF`

Utilice la contraseña `xY-45uM_e`. Para ello, siga los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Network Security > 802.1X Port Authentication > Global*.
  En el cuadro *MAC authentication bypass format options*, lleve a cabo los pasos siguientes:
- ☐ En la lista desplegable *Group size*, seleccione el valor `2`.
  El dispositivo divide la dirección MAC en 6 grupos de 2 caracteres.
- ☐ En la lista desplegable *Group separator*, seleccione el carácter `:`.
- ☐ En la lista desplegable *Upper or lower case*, seleccione el elemento `upper-case`.
- ☐ Introduzca la contraseña `xY-45uM_e` en el campo *Password*.
  El dispositivo utiliza esta contraseña para todos los clientes que se autentican en el servidor RADIUS. Si deja el campo en blanco, el dispositivo utilizará también la dirección MAC formateada como contraseña.
- ☐ Para guardar temporalmente la configuración, haga clic en el botón ☑.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`dot1x mac-authentication-bypass format group-size 2`	Especifique el tamaño del grupo `2`.
`dot1x mac-authentication-bypass format group-separator :`	Especifique el separador del grupo `:`.
`dot1x mac-authentication-bypass format letter-case upper-case`	Especifique que el dispositivo formatea los datos de autenticación en mayúsculas.
`dot1x mac-authentication-bypass password xY-45uM_e`	Especifique la contraseña `xY-45uM_e`. El dispositivo utiliza esta contraseña para autenticar a todos los clientes en el servidor RADIUS.

10 Control de la carga de red

El dispositivo incluye varias funciones que pueden ayudarle a reducir la carga de la red:
- Tráfico de paquetes filtrado
- Multicasts
- Rate limiter ‹Limitador de carga›
- Priorización - QoS
- Flow control ‹Control de flujo›

10.1 Tráfico de paquetes filtrado

El dispositivo reduce la carga de la red con el tráfico de paquetes filtrado.

En cada uno de sus puertos, el dispositivo aprende la dirección MAC del remitente de los paquetes de datos recibidos. El dispositivo almacena la combinación "puerto y dirección MAC" en su tabla de direcciones MAC (FDB).

Mediante la aplicación del método "Store and Forward", el dispositivo almacena los datos recibidos en el búfer y comprueba si son válidos antes de reenviarlos. El dispositivo rechaza paquetes de datos no válidos y defectuosos.

10.1.1 Aprendizaje de direcciones MAC

Cuando el dispositivo recibe un paquete de datos, comprueba si la dirección MAC del remitente ya está almacenada en la tabla de direcciones MAC (FDB). Cuando la dirección MAC del remitente es desconocida, el dispositivo genera una entrada nueva. A continuación, el dispositivo compara la dirección MAC de destino del paquete de datos con las entradas almacenadas en la tabla de direcciones MAC (FDB):
- El dispositivo reenvía paquetes con una dirección MAC de destino conocida directamente a los puertos que ya han recibido paquetes de datos de esta dirección MAC.
- El dispositivo desborda paquetes de datos con direcciones de destino desconocidas, es decir, el dispositivo reenvía estos paquetes de datos a cada puerto.

10.1.2 Antigüedad de las direcciones MAC aprendidas

Las direcciones que no han sido detectadas por el dispositivo durante un período de tiempo ajustable (tiempo de caducidad) son eliminadas por el dispositivo de la tabla de direcciones MAC (FDB). El reinicio o restablecimiento de la tabla de direcciones MAC permite eliminar las entradas de la tabla de direcciones MAC (FDB).

10.1.3 Entradas de direcciones estáticas

Además de aprender la dirección MAC del remitente, el dispositivo también ofrece la opción de ajustar manualmente las direcciones MAC. Estas direcciones MAC permanecen configuradas y sobreviven al restablecimiento de la tabla de direcciones MAC (FDB), así como al reinicio del dispositivo.

Las entradas de direcciones estáticas permiten al dispositivo reenviar paquetes de datos directamente a los puertos seleccionados. Si no especifica un puerto de destino, el dispositivo descarta los paquetes de datos correspondientes.

Administra las entradas de direcciones estáticas en la interfaz gráfica de usuario o en la Interfaz de línea de comando.

Lleve a cabo los siguientes pasos:

☐ Cree una entrada de dirección estática.

☐ Abra el cuadro de diálogo *Switching > Filter for MAC Addresses*.

☐ Añada una dirección MAC configurable por el usuario:

- Haga clic en el botón  .
  El cuadro de diálogo muestra la ventana *Create*.
- En el campo *Address*, especifique la dirección MAC de destino.
- En el campo *VLAN ID*, especifique el ID de VLAN.
- En la lista *Port*, seleccione los puertos a los que el dispositivo reenviará los paquetes de datos con la dirección MAC de destino especificada en la VLAN establecida.
  Si ha definido una dirección MAC Unicast en el campo *Address*, seleccione solamente un puerto.
  Si ha definido una dirección MAC Multicast en el campo *Address*, seleccione uno o más puertos.
  Si desea que el dispositivo descarte paquetes de datos con la dirección MAC de destino, no seleccione ningún puerto.
- Haga clic en el botón *Ok*.

☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón  .

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`mac-filter <MAC address>  <VLAN ID>`	Crear el filtro de direcciones MAC, compuesto por una dirección MAC y un ID de VLAN.
`interface 1/1`	Cambiar al modo de configuración de la interfaz `1/1`.
`mac-filter <MAC address>  <VLAN ID>`	Asignar el puerto a un filtro de direcciones MAC creado previamente.
`save`	Guardar los ajustes en el perfil de configuración "seleccionado" de la memoria no volátil (`nvm`).

☐ Convierta una dirección MAC aprendida en una entrada de dirección estática.

- ☐ Abra el cuadro de diálogo *Switching > Filter for MAC Addresses*.
- ☐ Para convertir una dirección MAC aprendida en una entrada de dirección estática, seleccione el valor `permanent` en la columna *Status*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✔.

☐ Desactive una entrada de dirección estática.

- ☐ Abra el cuadro de diálogo *Switching > Filter for MAC Addresses*.
- ☐ Para desactivar una entrada de dirección estática, seleccione el valor `invalid` en la columna *Status*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✔.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`interface 1/1`	Cambiar al modo de configuración de la interfaz `1/1`.
`no mac-filter <MAC address>  <VLAN ID>`	Cancelar la asignación del filtro de direcciones MAC en el puerto.
`exit`	Cambiar al modo de configuración.
`no mac-filter <MAC address>  <VLAN ID>`	Eliminar el filtro de direcciones MAC, compuesto por una dirección MAC y un ID de VLAN.
`exit`	Cambiar al modo Privileged EXEC.
`save`	Guardar los ajustes en el perfil de configuración "seleccionado" de la memoria no volátil (`nvm`).

☐ Elimine las direcciones MAC aprendidas.

- ☐ Para eliminar las direcciones aprendidas de la tabla de direcciones MAC (FDB), abra el cuadro de diálogo *Basic Settings > Restart* y haga clic en el botón *Reset MAC address table*.

`clear mac-addr-table`	Eliminar las direcciones MAC aprendidas de la tabla de direcciones MAC (FDB).

10.2 Multicasts

Por defecto, el dispositivo desborda paquetes de datos con direcciones Multicast, es decir, el dispositivo reenvía estos paquetes de datos a cada puerto. Esto provoca un aumento de la carga de la red.

El uso de IGMP Snooping puede reducir la carga de la red provocada por el tráfico de datos Multicast. IGMP Snooping permite al dispositivo enviar paquetes de datos Multicast solamente en los puertos a los que están conectados los dispositivos "interesados" en Multicast.

10.2.1 Ejemplo de una aplicación Multicast

Las cámaras de vigilancia transmiten imágenes a los monitores de la sala de máquinas y de la sala de supervisión. Mediante la transmisión IP Multicast, las cámaras transmiten sus datos gráficos a través de la red en paquetes Multicast.

El protocolo IGMP (Internet Group Management Protocol, Protocolo de gestión de grupos de Internet) organiza el tráfico de datos Multicast entre los monitores y los enrutadores Multicast. Los switches de la red situados entre los monitores y los enrutadores Multicast supervisan el tráfico de datos de IGMP de manera continua ("IGMP Snooping").

Los switches registran los inicios de sesión para recibir un flujo de Multicast (informe de IGMP). A continuación, el dispositivo crea una entrada en la tabla de direcciones MAC (FDB) y reenvía paquetes Multicast solamente a los puertos en los que ha recibido informes de IGMP previamente.

10.2.2 IGMP Snooping

El protocolo IGMP (Internet Group Management Protocol, Protocolo de gestión de grupos de Internet) describe la distribución de información de Multicast entre los enrutadores y receptores conectados en la Capa 3. IGMP Snooping describe la función de un switch de supervisión continua de tráfico IGMP y optimización de sus propios ajustes de transmisión para este tráfico de datos.

La función *IGMP Snooping* del dispositivo opera conforme a RFC 4541 (Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches).

Los enrutadores Multicast con una función *IGMP* activa solicitan (consultan) periódicamente el registro de flujos Multicast para determinar los miembros de los grupos IP Multicast asociados. Los miembros de grupos IP Multicast responden con un mensaje de informe. Este mensaje de informe contiene los parámetros requeridos por la función *IGMP*. El enrutador Multicast introduce la dirección del grupo IP Multicast en su tabla de enrutamiento a partir del mensaje de informe. Esto provoca el reenvío de los paquetes de datos con este grupo IP Multicast al campo de dirección de destino conforme a su tabla de enrutamiento.

Al abandonar un grupo Multicast (versión IGMP 2 y posteriores), los receptores cierran sesión con el mensaje "Leave" y no envían ningún mensaje de informe adicional. Si no recibe ningún mensaje de informe adicional de este receptor en un determinado período de tiempo (tiempo de caducidad), el enrutador Multicast eliminará la entrada de la tabla de enrutamiento de un receptor.

Si hay varios enrutadores Multicast IGMP en la misma red, el dispositivo con la dirección IP inferior asumirá la función de consulta. Si no hay ningún enrutador Multicast en la red, tendrá la opción de activar la función de consulta en un switch adecuadamente equipado.

Un switch que conecta un receptor Multicast con un enrutador Multicast analiza la información de IGMP con el método IGMP Snooping.

El método IGMP Snooping también permite a los switches utilizar la función *IGMP*. Un switch almacena las direcciones MAC derivadas de direcciones IP de los receptores Multicast como direcciones Multicast reconocidas en su tabla de direcciones MAC (FDB). Además, el switch identifica los puertos en los que ha recibido informes para una dirección Multicast específica. De este modo, el switch reenvía paquetes Multicast solamente a puertos a los que los receptores Multicast están conectados. Los otros puertos no reciben estos paquetes.

Una función especial del dispositivo consiste en la posibilidad de determinar el procesamiento de paquetes de datos con direcciones Multicast desconocidas. En función del ajuste, el dispositivo descarta estos paquetes de datos o los reenvía a cada puerto. Por defecto, el dispositivo transmite los paquetes de datos solo a los puertos con dispositivos conectados, que a su vez reciben paquetes de consultas. También existe la posibilidad de enviar los paquetes Multicast conocidos a los puertos de consulta.

Configuración de IGMP Snooping

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Switching > IGMP Snooping > Global*.
- ☐ Para activar la función, seleccione el botón de opción `On` en el cuadro *Operation*.

Cuando la función *IGMP Snooping* está desactivada, el dispositivo se comporta del modo siguiente:

- El dispositivo ignora la consulta recibida y los mensajes de informes.
- El dispositivo reenvía (desborda) paquetes de datos recibidos con una dirección Multicast como dirección de destino a cada puerto.

- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✓.

☐ Especificación de la configuración de un puerto:

- ☐ Abra el cuadro de diálogo *Switching > IGMP Snooping > Configuration*, pestaña *Port*.
- ☐ Para activar la función *IGMP Snooping* en un puerto, marque la casilla de la columna *Active* del puerto correspondiente.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✓.

☐ Especificación de la configuración de una VLAN:

- ☐ Abra el cuadro de diálogo *Switching > IGMP Snooping > Configuration*, pestaña *VLAN ID*.
- ☐ Para activar la función *IGMP Snooping* de una VLAN específica, marque la casilla de la columna *Active* para la VLAN correspondiente.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✓.

Configuración de la función IGMP Querier

El propio dispositivo tiene la opción de enviar mensajes de consulta activos; también puede responder a mensajes de consulta o detectar otros solicitantes Multicast en la red (función *IGMP Snooping Querier*).

Requisito previo:

Que la función *IGMP Snooping* esté activada globalmente.

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Switching > IGMP Snooping > Querier*.
- ☐ En el cuadro *Operation*, active/desactive la función *IGMP Snooping Querier* del dispositivo globalmente.
- ☐ Para activar la función *IGMP Snooping Querier* de una VLAN específica, marque la casilla de la columna *Active* para la VLAN correspondiente.
- ▶ El dispositivo lleva a cabo un proceso de selección sencillo: cuando la dirección de origen IP del otro solicitante Multicast es inferior a la suya, el dispositivo pasa a estado pasivo, en el que no envía ninguna solicitud de consulta más.
- ▶ En la columna *Address*, especifique la dirección IP Multicast que el dispositivo inserta como dirección del remitente en solicitudes de consulta generadas. Utilice la dirección del enrutador Multicast.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón .

Mejoras de IGMP Snooping (tabla)

El cuadro de diálogo *Switching > IGMP Snooping > Snooping Enhancements* proporciona acceso a ajustes mejorados para la función *IGMP Snooping*. Active o desactive los ajustes en función del puerto en una VLAN.

Es posible establecer los siguientes ajustes:

▶ `Static`
Utilice esta configuración para ajustar el puerto como puerto de consulta estática. El dispositivo reenvía todos los mensajes IGMP a través de un puerto de consulta estática, aunque no haya recibido anteriormente ningún mensaje de consulta IGMP en este puerto. Cuando la opción estática esté desactivada y el dispositivo haya recibido previamente mensajes de consulta IGMP, reenviará los mensajes IGMP a través de este puerto. En tal caso, la entrada mostrará `L` ("learned").

- `Learn by LLDP`
  Un puerto con esta configuración descubre automáticamente los otros dispositivos Schneider Electric que usan LLDP (Link Layer Discovery Protocol, Protocolo de descubrimiento de capa de enlace). A continuación, el dispositivo aprende el estado de la consulta IGMP de este puerto a partir de estos dispositivos Schneider Electric y configura la función *IGMP Snooping Querier* en consecuencia. La entrada `ALA` indica que la función `Learn by LLDP` está activada. Cuando el dispositivo ha encontrado otro dispositivo Schneider Electric en este puerto de esta VLAN, la entrada también muestra una `A` ("automatic").
- `Forward All`
  Con este ajuste, el dispositivo reenvía los paquetes de datos dirigidos a una dirección Multicast a este puerto. El ajuste es adecuado en las siguientes situaciones, por ejemplo:
  - Para fines de diagnóstico.
  - Para dispositivos situados en un anillo MRP: una vez conmutado el anillo, la función `Forward All` permite reconfigurar la red rápidamente para paquetes de datos con direcciones de destino Multicast registradas. Active la función `Forward All` en cada puerto del anillo.

Requisito previo:

Que la función *IGMP Snooping* esté activada globalmente.

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Switching > IGMP Snooping > Snooping Enhancements*.
- ☐ Haga doble clic en el puerto deseado de la VLAN deseada.
- ☐ Para activar una o más funciones, seleccione las opciones correspondientes.
- ☐ Haga clic en el botón *Ok*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✔.

`enable`	Cambiar al modo Privileged EXEC.
`vlan database`	Cambiar al modo de configuración de VLAN.
`igmp-snooping vlan-id 1 forward-all 1/1`	Active la función `Forward All` para el puerto `1/1` de la VLAN `1`.

Configuración de Multicasts

El dispositivo le permite configurar el intercambio de paquetes de datos Multicast. El dispositivo ofrece diferentes opciones dependiendo de si desea enviar los paquetes de datos a receptores Multicast desconocidos o conocidos.

Los ajustes de direcciones Multicast desconocidas son globales para todo el dispositivo. Es posible seleccionar las siguientes opciones:
- El dispositivo descarta Multicasts desconocidos.
- El dispositivo reenvía Multicasts desconocidos a cada puerto.

Nota: Los ajustes de intercambio de direcciones Multicast desconocidas también se aplican a las direcciones IP reservadas de "Local Network Control Block" (`224.0.0.0..224.0.0.255`). Este comportamiento puede afectar a los protocolos de enrutamiento de mayor nivel.

Para cada VLAN, especifica el envío de paquetes Multicast a direcciones Multicast conocidas individualmente. Es posible seleccionar las siguientes opciones:

- El dispositivo reenvía Multicasts conocidos a los puertos que han recibido mensajes de consulta previamente (puertos de consulta) y a los puertos registrados. Los puertos registrados son puertos con receptores Multicast registrados con el grupo Multicast correspondiente. Esta opción ayuda a garantizar que la transferencia funciona con aplicaciones básicas sin configuración adicional.
- El dispositivo reenvía Multicasts conocidos solamente a los puertos registrados. Esta configuración tiene la ventaja de utilizar de forma óptima el ancho de banda disponible mediante un envío localizado.

Requisito previo:

Que la función *IGMP Snooping* esté activada globalmente.

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Switching > IGMP Snooping > Multicasts*.
- ☐ En el cuadro *Configuration*, especifique cómo desea que envíe el dispositivo paquetes de datos a direcciones Multicast desconocidas.
  - *send to registered ports*
    El dispositivo reenvía paquetes con direcciones Multicast desconocidas a cada puerto de consulta.
- ☐ En la columna *Known multicasts*, especifique cómo desea que envíe el dispositivo paquetes de datos a direcciones Multicast conocidas en la VLAN correspondiente. Haga clic en el campo correspondiente y seleccione el valor que desee.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón .

10.3 Rate limiter ‹Limitador de carga›

La función de limitador de carga ayuda a garantizar un funcionamiento estable incluso con volúmenes de tráfico elevados limitando el tráfico en los puertos. La limitación de carga se lleva a cabo individualmente para cada puerto y por separado para el tráfico entrante y saliente.

Si la velocidad de transferencia de un puerto supera un límite definido, el dispositivo descarta la sobrecarga en este puerto.

La limitación de la velocidad se produce por completo en la Capa 2. Durante el proceso, la función de limitador de carga ignora la información del protocolo en niveles superiores, como IP o TCP. Esto puede afectar al tráfico TCP.

Para minimizar estos efectos, utilice las siguientes opciones:
- Limite la limitación de carga a determinados tipos de paquetes, por ejemplo, Broadcasts, Multicasts y Unicasts con una dirección de destino desconocida.
- Limite el tráfico de datos saliente en lugar del tráfico entrante. La limitación de la carga saliente funciona mejor con el control de flujo de TCP debido al almacenamiento en búfer interno del dispositivo de los paquetes de datos.
- Aumente el intervalo de validez de las direcciones Unicast aprendidas.

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Switching > Rate Limiter*.
- Active el limitador de carga y establezca límites para la velocidad de transferencia. Los ajustes se aplican en función del puerto y se dividen por tipo de tráfico:
  - Paquetes de datos Broadcast recibidos
  - Paquetes de datos Multicast recibidos
  - Paquetes de datos Unicast recibidos con una dirección de destino desconocida

  Para activar el limitador de carga en un puerto, marque la casilla de al menos una categoría. En la columna *Threshold unit*, especifique si desea que el dispositivo interprete los valores umbrales como porcentaje del ancho de banda del puerto o como paquetes por segundo. El valor umbral `0` desactiva el limitador de carga.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✓.

10.4 QoS/prioridad

QoS (Quality of Service, Calidad de servicio) es un procedimiento definido en el estándar IEEE 802.1D que se utiliza para distribuir recursos en la red. QoS le permite priorizar los datos de las aplicaciones necesarias.

Cuando existe una carga de red importante, la priorización ayuda a evitar que el tráfico de datos con una prioridad inferior interfiera con el tráfico de datos sensibles a los retardos. Dentro del tráfico de datos sensibles a los retardos, se incluye, por ejemplo, voz, vídeo y datos en tiempo real.

10.4.1 Descripción de priorización

Para la priorización del tráfico de datos, las clases de tráfico se definen en el dispositivo. El dispositivo prioriza las clases de tráfico más elevadas por encima de las de tráfico inferior. El número de clases de tráfico depende del tipo de dispositivo.

Para permitir un flujo de datos óptimo para los datos sensibles a los retardos, debe asignar clases de tráfico más elevadas a estos datos. Asigne clases de tráfico inferior a los datos menos sensibles a los retardos.

Asignación de clases de tráfico a los datos

El dispositivo asigna automáticamente clases de tráfico a datos entrantes (clasificación del tráfico). El dispositivo tiene en cuenta los siguientes criterios de clasificación:

- Métodos según los cuales el dispositivo lleva a cabo la asignación de paquetes de datos recibidos a clases de tráfico:
  - `trustDot1p`
    El dispositivo utiliza la prioridad del paquete de datos contenido en la etiqueta VLAN.
  - `trustIpDscp`
    El dispositivo utiliza la información de QoS contenida en el encabezado IP (ToS/DiffServ).
  - `untrusted`
    El dispositivo ignora posible información sobre la prioridad contenida en los paquetes de datos y utiliza la prioridad del puerto de recepción directamente.
- La prioridad asignada al puerto de recepción.

Ambos criterios de clasificación son configurables.

Durante la clasificación del tráfico, el dispositivo utiliza las siguientes normas:

- Si el puerto de recepción está ajustado en `trustDot1p` (configuración por defecto), el dispositivo utiliza la prioridad del paquete de datos contenida en la etiqueta VLAN. Si los paquetes de datos no contienen una etiqueta VLAN, el dispositivo es dirigido por la prioridad del puerto de recepción.
- Si el puerto de recepción está ajustado en `trustIpDscp`, el dispositivo utiliza la información de QoS (ToS/DiffServ) contenida en el encabezado IP. Si los paquetes de datos no contienen paquetes de IP, el dispositivo es dirigido por la prioridad del puerto de recepción.
- Si el puerto de recepción está ajustado en `untrusted`, el dispositivo es dirigido por la prioridad del puerto de recepción.

Priorización de las clases de tráfico

Para la priorización de las clases de tráfico, el dispositivo utiliza los siguientes métodos:

- `Strict`
  Si la transmisión de los datos de una clase de tráfico superior ha dejado de realizarse o si los datos relevantes se encuentran todavía en cola, el dispositivo envía datos de la clase de tráfico correspondiente. Si se da prioridad a todas las clases de tráfico conforme al método `Strict`, con una carga de red elevada, el dispositivo puede bloquear permanentemente los datos de clases de tráfico inferiores.
- `Weighted Fair Queuing`
  Se asignará un ancho de banda específico a la clase de tráfico. Esto ayudará a garantizar que el dispositivo envíe el tráfico de datos de esta clase de tráfico, aunque haya mucho tráfico de datos en clases de tráfico superiores.

10.4.2 Manejo de información de prioridad recibida

Las aplicaciones etiquetan los paquetes de datos con la siguiente información de priorización:

- Prioridad de VLAN basada en IEEE 802.1Q/ 802.1D (Capa 2)
- Tipo de servicio (ToS, Type-of-Service) o DiffServ (DSCP) para paquetes de IP de gestión de VLAN (Capa 3)

El dispositivo le permite evaluar esta información sobre prioridades utilizando las siguientes opciones:

- `trustDot1p`
  El dispositivo asigna paquetes de datos etiquetados para VLAN a las diferentes clases de tráfico conforme a sus prioridades de VLAN. La asignación correspondiente se puede configurar. El dispositivo asigna la prioridad del puerto receptor a los paquetes de datos que recibe sin una etiqueta VLAN.
- `trustIpDscp`
  El dispositivo asigna los paquetes de IP a las diferentes clases de tráfico conforme al valor de DSCP que figure en el encabezado IP, aunque el paquete también esté etiquetado para VLAN. La asignación correspondiente se puede configurar. El dispositivo prioriza paquetes que no son de IP conforme a la prioridad del puerto receptor.
- `untrusted`
  El dispositivo ignora la información sobre la prioridad contenida en los paquetes de datos y asigna la prioridad del puerto de recepción a ellos.

10.4.3 Etiquetado VLAN

Para las funciones de priorización y de VLAN, el estándar IEEE 802.1Q permite la integración de un marco de MAC en la etiqueta VLAN. La etiqueta VLAN está compuesta por 4 bytes y se encuentra entre el campo de dirección de origen ("Source Address Field") y el campo de tipo ("Length / Type Field").

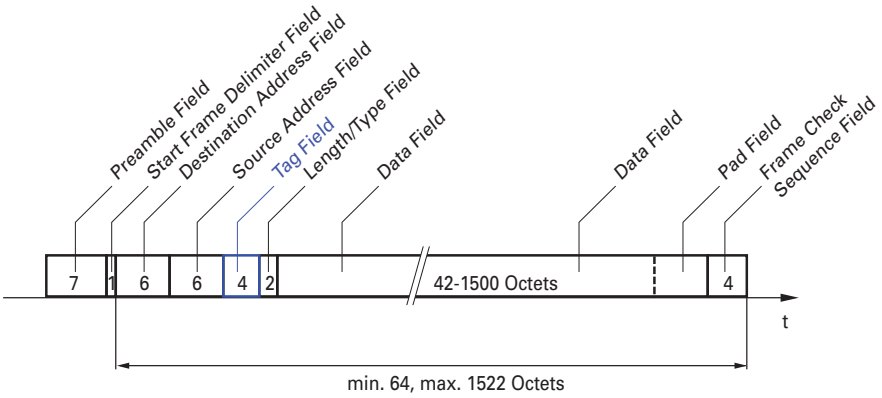


Figura 23: Paquete de datos de Ethernet con etiqueta

Para paquetes de datos con etiquetas VLAN, el dispositivo evalúa la siguiente información:
- Información de prioridad
- Cuando las VLAN están configuradas, el etiquetado VLAN

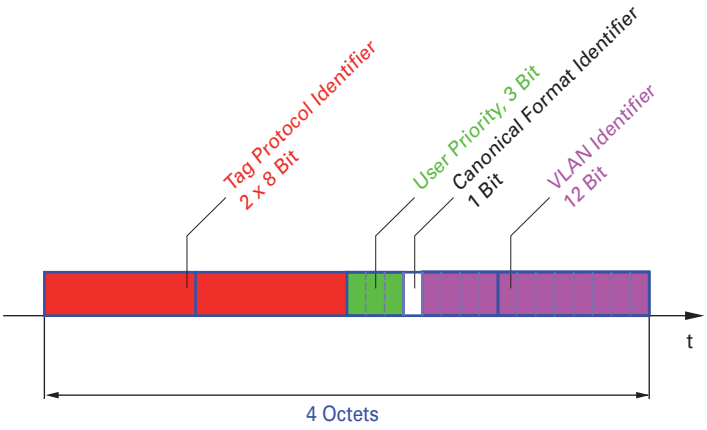


Figura 24: Estructura del etiquetado VLAN

Los paquetes de datos con etiquetas VLAN que contienen información sobre prioridad, pero no información de VLAN (ID de VLAN = 0), se conocen como tramas con etiquetas de prioridad.

Nota: Los protocolos de red y los mecanismos de redundancia utilizan la clase de tráfico más alta: 7. Por ello, seleccione otras clases de tráfico para los datos de aplicaciones.

Cuando utilice la priorización de la VLAN, tenga en cuenta las siguientes funciones especiales:
- Una prioridad de extremo a extremo requiere la transmisión de etiquetas VLAN en toda la red. Es imprescindible que todos los componentes de la red sean compatibles con la VLAN.
- Los enrutadores no son capaces de enviar y recibir paquetes con etiquetas VLAN a través de interfaces de enrutador basadas en puertos.

10.4.4 IP ToS (Tipo de servicio)

El campo Tipo de servicio (ToS, Type-of-Service) del encabezado IP ya formaba parte del protocolo IP desde el principio y se utiliza para diferenciar servicios en las redes IP. Incluso entonces, existían ideas partidarias del tratamiento diferenciado de paquetes IP debido al limitado ancho de banda disponible y a la presencia de rutas de conexión no fiables. A causa del aumento continuo del ancho de banda disponible, no se necesitaba utilizar el campo ToS.

Únicamente con los requisitos de tiempo real de las redes actuales, se ha vuelto importante de nuevo el campo ToS. Una marca en el byte ToS del encabezado IP posibilita distinguir entre servicios diferentes. No obstante, este campo no se utiliza mucho en la práctica.

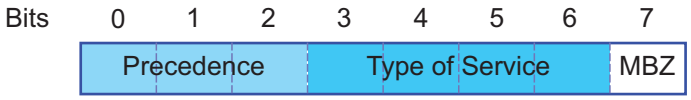


Tabla 22: Campo ToS en el encabezado IP

Bits (0-2): IP Precedence Defined	Bits (3-6): Type of Service Defined	Bit (7)
111 - Network Control	0000 - [all normal]	0 - Zero
110 - Internetwork Control	1000 - [minimize delay]	
101 - CRITIC / ECP	0100 - [maximize throughput	
100 - Flash Override	0010 - [maximize reliability]	
011 - Flash	0001 - [minimize monetary cost]	
010 - Immediate		
001 - Priority		
000 - Routine		

10.4.5 Uso de las clases de tráfico

El dispositivo le ofrece las siguientes posibilidades para manejar las clases de tráfico:
- Strict Priority
- Weighted Fair Queuing
- Strict Priority en combinación con Weighted Fair Queuing
- Administración de colas

Descripción de Strict Priority

Con el ajuste Strict Priority, el dispositivo transmite en primer lugar los paquetes de datos con clase de tráfico superior (prioridad superior) antes de transmitir paquetes de datos de la siguiente clase de tráfico. Cuando no haya ningún otro paquete de datos en la cola, el dispositivo transmitirá un paquete de datos con la clase de tráfico mínima (prioridad mínima). En casos desafortunados, si existe un volumen elevado de tráfico de alta prioridad esperando a enviarse en este puerto, el dispositivo no enviará paquetes de datos con una prioridad baja.

En aplicaciones sensibles a retardos, como VoIP o vídeo, Strict Priority permite el envío de datos inmediatamente.

Descripción de Weighted Fair Queuing

Con Weighted Fair Queuing, también llamado Weighted Round Robin (WRR), el usuario asigna un ancho de banda mínimo o reservado a cada clase de tráfico. Esto ayuda a garantizar que los paquetes de datos con una prioridad inferior también se envíen aunque la red esté muy ocupada.

Los valores reservados varían entre el 0% y el 100% del ancho de banda disponible, en pasos de 1%.
- Una reserva de 0 es equivalente al ajuste "no bandwidth".
- La suma de anchos de banda individuales puede equivaler a un máximo de 100%.

Si asigna Weighted Fair Queuing a todas las clases de tráfico, tendrá a su disposición el ancho de banda completo del puerto correspondiente.

Combinación de Strict Priority y Weighted Fair Queuing

Cuando combine Weighted Fair Queuing con Strict Priority, compruebe que la clase de tráfico máxima de Weighted Fair Queuing sea inferior a la clase de tráfico mínima de Strict Priority.

Si combina Weighted Fair Queuing con Strict Priority, una carga de red Strict Priority alta podrá reducir de manera significativa el ancho de banda disponible para Weighted Fair Queuing.

10.4.6 Administración de colas

Queue Shaping

Queue Shaping acelera la velocidad a la que las colas transmiten paquetes. Por ejemplo, al utilizar Queue Shaping, pone un límite de velocidad a la cola con prioridad estricta más alta para que la cola con prioridad estricta más baja pueda enviar paquetes a pesar de que los de mayor prioridad sigan disponibles para la transmisión. El dispositivo le permite configurar Queue Shaping para cualquier cola. Asigne un porcentaje como ancho de banda disponible para especificar Queue Shaping como la velocidad máxima a la cual el tráfico se transfiere a través de una cola.

Definición de ajustes para la gestión de colas

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Switching > QoS/Priority > Queue Management*.

El ancho de banda total asignado en la columna *Min. bandwidth [%]* es del 100%.

- ☐ Para activar Weighted Fair Queuing para *Traffic class* = `0`, haga lo siguiente:
  - Desmarque la casilla de la columna *Strict priority*.
  - En la columna *Min. bandwidth [%]*, especifique el valor `5`.
- ☐ Para activar Weighted Fair Queuing para *Traffic class* = `1`, haga lo siguiente:
  - Desmarque la casilla de la columna *Strict priority*.
  - En la columna *Min. bandwidth [%]*, especifique el valor `20`.

- ☐ Para activar Weighted Fair Queuing para *Traffic class* = 2, haga lo siguiente:
  - Desmarque la casilla de la columna *Strict priority*.
  - En la columna *Min. bandwidth [%]*, especifique el valor 30.
- ☐ Para activar Weighted Fair Queuing para *Traffic class* = 3, haga lo siguiente:
  - Desmarque la casilla de la columna *Strict priority*.
  - En la columna *Min. bandwidth [%]*, especifique el valor 20.
- ☐ Para activar Weighted Fair Queuing y Queue Shaping para *Traffic class* = 4, haga lo siguiente:
  - Desmarque la casilla de la columna *Strict priority*.
  - En la columna *Min. bandwidth [%]*, especifique el valor 10.
  - En la columna *Max. bandwidth [%]*, especifique el valor 10.

  Al utilizar la combinación Weighted Fair Queuing y Queue Shaping para una clase de tráfico específica, especifique un valor más alto en la columna *Max. bandwidth [%]* que en el de la columna *Min. bandwidth [%]*.
- ☐ Para activar Weighted Fair Queuing para *Traffic class* = 5, haga lo siguiente:
  - Desmarque la casilla de la columna *Strict priority*.
  - En la columna *Min. bandwidth [%]*, especifique el valor 5.
- ☐ Para activar Weighted Fair Queuing para *Traffic class* = 6, haga lo siguiente:
  - Desmarque la casilla de la columna *Strict priority*.
  - En la columna *Min. bandwidth [%]*, especifique el valor 10.
- ☐ Para activar Strict Priority y Queue Shaping para *Traffic class* = 7, haga lo siguiente:
  - Marque la casilla de la columna *Strict priority*.
  - En la columna *Max. bandwidth [%]*, especifique el valor 10.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✔.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`cos-queue weighted 0`	Activar Weighted Fair Queuing para la clase de tráfico 0.
`cos-queue min-bandwidth: 0 5`	Asignar un peso de 5 % a la clase de tráfico 0.
`cos-queue weighted 1`	Activar Weighted Fair Queuing para la clase de tráfico 1.
`cos-queue min-bandwidth: 1 20`	Asignar un peso de 20 % a la clase de tráfico 1.
`cos-queue weighted 2`	Activar Weighted Fair Queuing para la clase de tráfico 2.
`cos-queue min-bandwidth: 2 30`	Asignar un peso de 30 % a la clase de tráfico 2.
`cos-queue weighted 3`	Activar Weighted Fair Queuing para la clase de tráfico 3.
`cos-queue min-bandwidth: 3 20`	Asignar un peso de 20 % a la clase de tráfico 3.

```
show cos-queue
Queue Id  Min. bandwidth  Max. bandwidth  Scheduler type
--------  --------------  --------------  --------------
0         5               0               weighted
1         20              0               weighted
2         30              0               weighted
3         20              0               weighted
4         0               0               strict
5         0               0               strict
6         0               0               strict
7         0               0               strict
```

Combinación de Weighted Fair Queuing y Queue Shaping

Lleve a cabo los siguientes pasos:

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`cos-queue weighted 4`	Activar Weighted Fair Queuing para la clase de tráfico `4`.
`cos-queue min-bandwidth: 4 10`	Asignar un peso de `10` % a la clase de tráfico `4`.
`cos-queue max-bandwidth: 4 10`	Asignar un peso de `10` % a la clase de tráfico `4`.
`cos-queue weighted 5`	Activar Weighted Fair Queuing para la clase de tráfico `5`.
`cos-queue min-bandwidth: 5 5`	Asignar un peso de `5` % a la clase de tráfico `5`.
`cos-queue weighted 6`	Activar Weighted Fair Queuing para la clase de tráfico `6`.
`cos-queue min-bandwidth: 6 10`	Asignar un peso de `10` % a la clase de tráfico `6`.

```
show cos-queue
Queue Id  Min. bandwidth  Scheduler type
--------  --------------  --------------  --------------
0         5               0               weighted
1         20              0               weighted
2         30              0               weighted
3         20              0               weighted
4         10              10              weighted
5         5               0               weighted
6         10              0               weighted
7         0               0               strict
```

Configuración de Queue Shaping

Lleve a cabo los siguientes pasos:

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`cos-queue max-bandwidth: 7 10`	Asignar un peso de `10` % a la clase de tráfico `7`.

```
show cos-queue
Queue Id  Min. bandwidth  Scheduler type
--------  --------------  --------------  --------------
0         5               0               weighted
1         20              0               weighted
2         30              0               weighted
3         20              0               weighted
4         10              10              weighted
5         5               0               weighted
6         10              0               weighted
7         0               10              strict
```

10.4.7 Priorización de la administración

Para que disponga de acceso constante a la gestión del dispositivo, aunque haya una carga de red elevada, el dispositivo le permitirá priorizar los paquetes de administración.

Al priorizar los paquetes de administración, el dispositivo envía estos con información de prioridad.

- En la Capa 2, el dispositivo modifica la prioridad de la VLAN en la etiqueta VLAN.
  El requisito previo de esta función consiste en que los puertos correspondientes estén ajustados para permitir el envío de paquetes con una etiqueta VLAN.
- En la Capa 3, el dispositivo modifica el valor de DSCP de IP.

10.4.8 Configuración de la priorización

Asignación de una prioridad de puerto

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Switching > QoS/Priority > Port Configuration*.
- ☐ En la columna *Port priority*, especifique la prioridad con la que desea que el dispositivo reenvíe los paquetes de datos recibidos en este puerto sin una etiqueta VLAN.
- ☐ En la columna *Trust mode*, especifique los criterios que desea que utilice el dispositivo para asignar una clase de tráfico a los paquetes de datos recibidos.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✔.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`interface 1/1`	Cambiar al modo de configuración de la interfaz `1/1`.
`vlan priority 3`	Asignar a la interfaz `1/1` la prioridad del puerto `3`.
`exit`	Cambiar al modo de configuración.

Asignación de la prioridad de la VLAN a una clase de tráfico

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Switching > QoS/Priority > 802.1D/p Mapping*.
- ☐ Para asignar una clase de tráfico a una prioridad de VLAN, introduzca el valor asociado en la columna *Traffic class*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✔.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`classofservice dot1p-mapping 0 2`	Asignar una prioridad de VLAN de `0` a la clase de tráfico `2`.

`classofservice dot1p-mapping 1 2`	Asignar una prioridad de VLAN de `1` a la clase de tráfico `2`.
`exit`	Cambiar al modo Privileged EXEC.
`show classofservice dot1p-mapping`	Mostrar la asignación.

Asignación de la prioridad del puerto a los paquetes de datos recibidos

Lleve a cabo los siguientes pasos:

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`interface 1/1`	Cambiar al modo de configuración de la interfaz `1/1`.
`classofservice trust untrusted`	Asignar el modo `untrusted` a la interfaz.
`classofservice dot1p-mapping 0 2` `classofservice dot1p-mapping 1 2`	Asignar una prioridad de VLAN de `0` a la clase de tráfico `2`. Asignar una prioridad de VLAN de `1` a la clase de tráfico `2`.
`vlan priority 1`	Especificar el valor `1` para la prioridad del puerto.
`exit`	Cambiar al modo de configuración.
`exit`	Cambiar al modo Privileged EXEC.
`show classofservice trust`	Visualizar el modo Trust de los puertos/interfaces.

```
 Interface Trust Mode
 --------- -------------
 1/1       untrusted
 1/2       dot1p
 1/3       dot1p
 1/4       dot1p
 1/5       dot1p
 1/6       dot1p
 1/7       dot1p
```

Asignación de DSCP a una clase de tráfico

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Switching > QoS/Priority > IP DSCP Mapping*.
- ☐ Especifique el valor deseado en la columna *Traffic class*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✔.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.

```
classofservice  ip-dscp-mapping cs1 1
```
Asignar el valor DSCP `CS1` a la clase de tráfico `1`.

```
show classofservice  ip-dscp-mapping
```
Visualizar las asignaciones de IP DSCP

```
    IP DSCP       Traffic Class
-------------    -------------
  be                  2
  1                   2
  .                   .
  .                   .
  (cs1)               1
  .                   .
```

Asignación de la prioridad de DSCP a los paquetes de datos de IP recibidos

Lleve a cabo los siguientes pasos:

```
enable
```
Cambiar al modo Privileged EXEC.

```
configure
```
Cambiar al modo de configuración.

```
interface 1/1
```
Cambiar al modo de configuración de la interfaz `1/1`.

```
classofservice trust ip-dscp
```
Asignar el modo `trust ip-dscp` globalmente.

```
exit
```
Cambiar al modo de configuración.

```
show classofservice trust
```
Visualizar el modo Trust de los puertos/interfaces.

```
Interface     Trust Mode
----------    -------------
1/1           ip-dscp
1/2           dot1p
1/3           dot1p
.             .
.             .
1/5           dot1p
.             .
```

Configuración de la formación de tráfico en un puerto

Lleve a cabo los siguientes pasos:

```
enable
```
Cambiar al modo Privileged EXEC.

```
configure
```
Cambiar al modo de configuración.

```
interface 1/2
```
Cambiar al modo de configuración de la interfaz `1/2`.

```
traffic-shape bw 50
```
Limitar el ancho de banda máximo del puerto `1/2` al 50%

```
exit
```
Cambiar al modo de configuración.

```
exit
```
Cambiar al modo Privileged EXEC.

```
show traffic-shape
```
Mostrar la configuración de la formación de tráfico.

```
Interface  Shaping rate
---------  ------------
1/1        0  %
1/2        50 %
1/3        0  %
1/4        0  %
```

Configuración de la prioridad de administración de Capa 2

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Switching > QoS/Priority > Global*.
- ☐ En el campo *VLAN priority for management packets*, especifique la prioridad de VLAN con la que el dispositivo envía paquetes de datos de administración.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✔.

```
enable
```
Cambiar al modo Privileged EXEC.

```
network management priority dot1p 7
```
Asignar la prioridad de VLAN de 7 a paquetes de administración. El dispositivo envía paquetes de administración con la prioridad máxima.

```
show network parms
```
Visualizar la prioridad de VLAN en la que se encuentra la administración del dispositivo.

```
IPv4 Network
------------
...
Management VLAN priority.....................7
...
```

Configuración de la prioridad de administración de Capa 3

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Switching > QoS/Priority > Global*.
- ☐ En el campo *IP DSCP value for management packets*, especifique el valor DSCP con el que el dispositivo envía paquetes de datos de administración.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✔.

```
enable
```
Cambiar al modo Privileged EXEC.

```
network management priority ip-dscp 56
```

Asignar el valor DSCP de 56 a paquetes de administración. El dispositivo envía paquetes de administración con la prioridad máxima.

```
show network parms
```

Visualizar la prioridad de VLAN en la que se encuentra la administración del dispositivo.

```
IPv4 Network
------------
...
Management IP-DSCP value.....................56
```

10.5 Flow control ‹Control de flujo›

Si se recibe un número elevado de paquetes de datos en la cola de prioridad de un puerto al mismo tiempo, esto puede provocar un desbordamiento de la memoria del puerto. Esto sucede, por ejemplo, cuando el dispositivo recibe datos en un puerto Gigabit y los reenvía a un puerto con un ancho de banda inferior. El dispositivo descarta paquetes de datos sobrantes.

El mecanismo de control de flujo descrito en el estándar IEEE 802.3 ayuda a garantizar que no se pierdan paquetes de datos debido a un desbordamiento de la memoria del puerto. Poco antes de que la memoria de un puerto esté completamente llena, el dispositivo señala a los dispositivos conectados que no acepta ningún paquete de datos adicional de ellos.

- En el modo Full-Dúplex, el dispositivo envía un paquete de datos en pausa.
- En el modo Half-Dúplex, el dispositivo simula una colisión.

En la siguiente figura, se muestra el funcionamiento del control de flujo. Las estaciones de trabajo 1, 2 y 3 quieren transmitir simultáneamente una gran cantidad de datos a la estación de trabajo 4. El ancho de banda combinado de las estaciones de trabajo 1, 2 y 3 es superior al ancho de banda de la estación de trabajo 4. Esto provoca un desbordamiento en la cola de recepción del puerto 4. El embudo izquierdo simboliza este estado.

Cuando la función de control de flujo de los puertos 1, 2 y 3 del dispositivo está activada, el dispositivo reacciona antes de que el embudo se desborde. El embudo de la derecha ilustra a los puertos 1, 2 y 3 enviando un mensaje a los dispositivos de transmisión para controlar la velocidad de transmisión. Esto provoca que el puerto de recepción no se vuelva a colapsar y que pueda procesar el tráfico entrante.

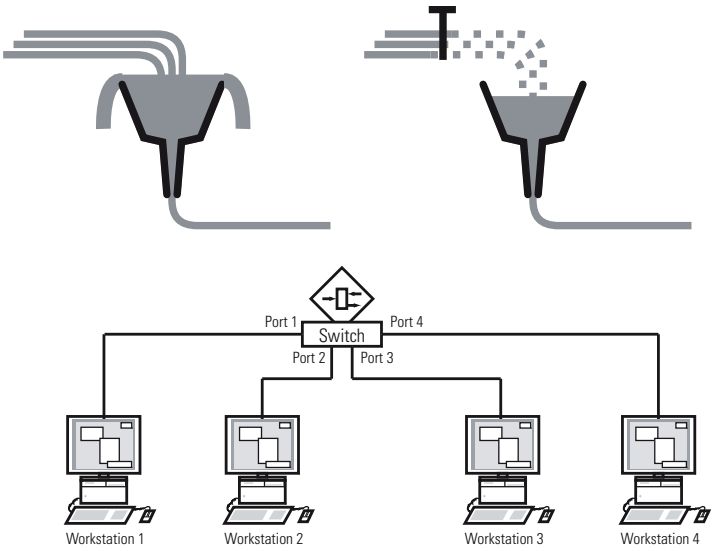


Figura 25: Ejemplo de control de flujo

10.5.1 Conexión Half-Dúplex o Full-Dúplex

Control de flujo con conexión Half-Dúplex

En el ejemplo, existe una conexión Half-Dúplex entre la estación de trabajo 2 y el dispositivo.

Antes de que se desborde la cola de envío del puerto 2, el dispositivo envía datos de vuelta a la estación de trabajo 2. La estación de trabajo 2 detecta una colisión y deja de transmitir.

Control de flujo con conexión Full-Dúplex

En el ejemplo, existe una conexión Full-Dúplex entre la estación de trabajo 2 y el dispositivo.

Antes de que se desborde la cola de envío del puerto 2, el dispositivo envía una solicitud a la estación de trabajo 2 para incluir una pequeña pausa en la transmisión de envío.

10.5.2 Configuración del control de flujo

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Switching > Global*.
- ☐ Marque la casilla *Flow control*.
  Con este ajuste activará el control de flujo en el dispositivo.
- ☐ Abra el cuadro de diálogo *Basic Settings > Port*, pestaña *Configuration*.
- ☐ Para activar el control de flujo en un puerto, marque la casilla de la columna *Flow control*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✓.

Nota: si utiliza una función de redundancia, desactive el control de flujo en los puertos implicados. Si el control de flujo y la función de redundancia están activos al mismo tiempo, es posible que la función de redundancia opere de un modo distinto al deseado.

11 Configuración de TSN basado en plantillas

11.1 Hechos subyacentes

Cuando utiliza la función *TSN*, se aplican las siguientes condiciones básicas:

- El dispositivo funciona utilizando el método "Store and Forward". Por consiguiente, el dispositivo tiene que recibir el paquete de datos completo antes de tomar una decisión de reenvío.
- Especifique la hora base y el tiempo de ciclo una vez en el dispositivo. Ambos ajustes son válidos para cada puerto participante en TSN.
- Configure una Lista de control de puertas por puerto basada en las plantillas predefinidas para disfrutar de una configuración más sencilla.
- Compruebe que la suma de los tiempos de entrada de la Lista de control de puertas es inferior o igual al tiempo de ciclo especificado.
- El dispositivo utiliza una banda de protección para ayudar a proteger la franja de tiempo para paquetes de prioridad alta de paquetes derivados de la franja horaria anterior. El factor decisivo para la duración del intervalo de la banda de protección es la velocidad del puerto de envío. Es recomendable utilizar las siguientes duraciones de intervalo para la banda de protección. Los valores se basan en la velocidad del puerto y el tamaño máximo permitido de los paquetes de Ethernet:
  - 2.5 Gbit/s: 5 µs
  - 1 Gbit/s: 13 µs
  - 100 Mbit/s: 124 µs
- El rango del Tiempo del ciclo equivale a 50 000..10 000 000 ns.
- El rango del intervalo de la Lista de control de puertas equivale a 1 000..10 000 000 ns.
- Compruebe que el Tiempo del ciclo y los intervalos de la Lista de control de puertas sean múltiplos de 1 µs, 2 µs o 4 µs.

Tabla 23: Dependencia entre el Tiempo del ciclo y la granularidad

Tiempo del ciclo	Granularidad
50 µs..4 ms	1 µs
4.002 ms..8 ms	2 µs
8.004 ms..10 ms	4 µs

11.2 Ejemplo

En este ejemplo se describe cómo configurar los dispositivos para un escenario con las siguientes condiciones:
- Tiempo del ciclo =1 ms
- Franja de tiempo para paquetes con prioridad alta =500 µs
- Franja de tiempo para paquetes con prioridad baja =487 µs

En este ejemplo, cada dispositivo está conectado a la red con una velocidad de puerto de 1 Gbit/s.

Tabla 24: Estructura del ciclo

Franja horaria	Clases de tráfico	Duración
Paquetes con prioridad alta	7	500 µs
Paquetes con prioridad baja	0,1,2,3,4,5,6	487 µs
Banda de protección	–	13 µs

11.2.1 Cálculo del tiempo

El dispositivo calcula automáticamente la duración de la franja horaria para los paquetes con prioridad baja. El cálculo se basa en los siguientes parámetros:
- Tiempo del ciclo
- Duración de la franja horaria para paquetes con prioridad alta
- Duración de la banda de protección

11.2.2 Configure los dispositivos

Configure los dispositivos con los tiempos especificados anteriormente mediante la interfaz gráfica de usuario o la interfaz de línea de comandos. En cada dispositivo implicado, lleve a cabo los siguientes pasos.

Compruebe y ajuste el Tiempo del ciclo

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Switching > TSN > Configuration*.
- ☐ Compruebe en el cuadro *Configuration* el valor del campo *Cycle time [ns]*.
- ☐ Si es necesario, ajuste el valor.

- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✓.

```
enable                                          Cambiar al modo Privileged EXEC.
configure                                       Cambiar al modo de configuración.
show tsn configuration
Port  Status                 Conf. cycle time[ns]  Conf. base time
      Default gate states    Curr. cycle time[ns]  Curr. base time
      Config change pending                        Time of last activation
----  ---------------------  --------------------  ------------------------------
 1/1  [x]           disabled              1000000  1970-01-01 00:00:00.000000000
      7,6,5,4,3,2,1,0                     1000000  1970-01-01 00:00:00.000000000
      [ ]                                          2018-07-12 08:10:58.813000000

 1/2  [x]           disabled              1000000  1970-01-01 00:00:00.000000000
      7,6,5,4,3,2,1,0                     1000000  1970-01-01 00:00:00.000000000
      [ ]                                          2018-07-11 07:24:35.204000000

 1/3  [ ]           disabled              1000000  1970-01-01 00:00:00.000000000
      7,6,5,4,3,2,1,0                           0  1970-01-01 00:00:00.000000000
      [ ]                                          1970-01-01 00:00:00.000000000

 1/4  [ ]           disabled              1000000  1970-01-01 00:00:00.000000000
      7,6,5,4,3,2,1,0                           0  1970-01-01 00:00:00.000000000
      [ ]                                          1970-01-01 00:00:00.000000000

tsn cycle-time 1000000                          Si es necesario, ajuste el valor.
```

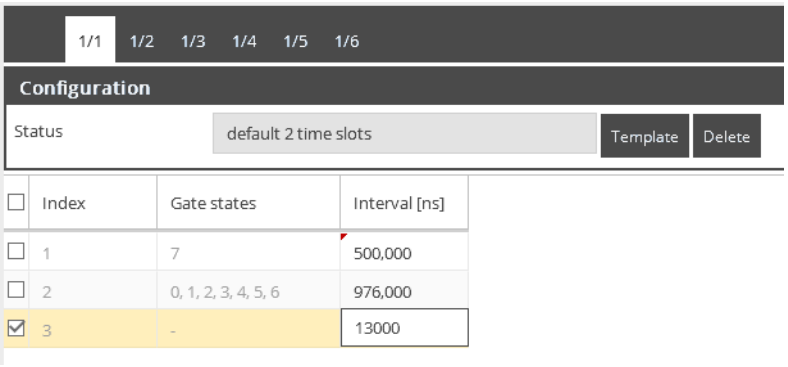
Seleccione una plantilla y configure la Lista de control de puertas

El dispositivo proporciona plantillas predefinidas para ayudarle a configurar la Lista de control de puertas. En este ejemplo, utilizamos la plantilla *default 2 time slots*. Tras seleccionar la plantilla, puede ajustar la duración de las franjas horarias. Lleve a cabo los pasos siguientes en cada uno de los puertos en los que desee utilizar la función *TSN*.

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Switching > TSN > Gate Control List > Configured*.
- ☐ Seleccione la pestaña correspondiente al puerto cuya configuración desee especificar.

- ☐ Seleccione una plantilla en el cuadro *Configuration*.
  Lleve a cabo los siguientes pasos:
  - Haga clic en el botón *Template*.
  - Seleccione el elemento `default 2 time slots`.
  - Haga clic en el botón *Ok*.
- ☐ Ajuste los valores de la columna *Interval [ns]*:
  - Introduzca el valor `500000` en la fila para los paquetes de prioridad alta.
  - Introduzca el valor `13000` en la fila para la banda de protección.
  - El dispositivo calcula el tercer valor automáticamente al guardar los cambios.



- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ☑.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`interface 1/1`	Cambiar al modo de configuración de la interfaz `1/1`.
`tsn gcl modify 1 interval 500000`	Ajuste la duración en nanosegundos de la franja horaria para paquetes con prioridad alta.
`tsn gcl modify 3 interval 13000`	Ajuste la duración de la franja horaria de la banda de protección en nanosegundos. El dispositivo calcula automáticamente la duración de la franja horaria para paquetes con prioridad baja. No puede establecer la franja horaria para paquetes con prioridad baja.

12 VLAN

En el caso más sencillo, una LAN virtual (VLAN) consiste en un grupo de participantes de red en un segmento de red que pueden comunicarse entre sí como si pertenecieran a una LAN individual.

Las VLAN más complejas se extienden a lo largo de varios segmentos de red y se basan adicionalmente en conexiones lógicas (en vez de solo físicas) entre los participantes de red. Las VLAN constituyen un elemento para estructurar de forma flexible una red. Es más sencillo reconfigurar las conexiones lógicas de manera central que las conexiones de cable.

El dispositivo admite el aprendizaje VLAN independiente de acuerdo con la norma IEEE 802.1Q, que define la función *VLAN*.

La utilización de VLAN aporta muchas ventajas. La siguiente lista muestra las ventajas principales:

- Limitación de la carga de red
  Las VLAN reducen considerablemente la carga de red cuando el dispositivo transmite paquetes Broadcast, Multicast y Unicast con direcciones de destino desconocidas (no aprendidas) únicamente dentro de la LAN virtual. El resto de la red de datos reenvía el tráfico con normalidad.
- Flexibilidad
  Tiene la posibilidad de formar grupos de trabajo de usuarios que se basen en la función de los participantes más allá de su medio o ubicación física.
- Visión de conjunto
  Las VLAN aportan a las redes una estructura clara y facilitan el mantenimiento.

12.1 Ejemplos de VLAN

Los siguientes ejemplos prácticos ofrecen una introducción rápida a la estructura de una VLAN.

Nota: Al configurar redes VLAN, utilice una interfaz para acceder a la administración del dispositivo, que permanecerá inalterada. En este ejemplo, utilice la interfaz 1/6 o la conexión en serie para configurar las VLAN.

12.1.1 Ejemplo 1

El ejemplo muestra una configuración VLAN mínima (VLAN basada en puerto). Un administrador ha conectado varios dispositivos finales a un dispositivo de comunicación y los ha asignado a 2 VLAN. De este modo, se prohíbe de manera efectiva la transferencia de datos entre las VLAN, cuyos miembros se comunican exclusivamente entre sus propias VLAN.

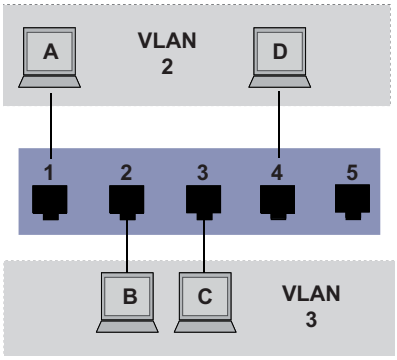


Figura 26: Ejemplo de una VLAN sencilla basada en puerto

Durante la creación de la VLAN, se crean reglas de comunicación para cada puerto y se registran en una tabla de entrada (entrante) y otra de salida (saliente).

La tabla de entrada define qué ID de VLAN asigna un puerto a los paquetes de datos entrantes. De esta forma, asigna al dispositivo final una VLAN mediante la dirección de puerto.

La tabla de salida especifica a qué puertos envía los paquetes el dispositivo desde esta VLAN.
- `T` = Etiquetado (con campo de etiqueta, marcada)
- `U` = No etiquetado (sin campo de etiqueta, no marcada)

En este ejemplo, el estado del campo TAG de los paquetes de datos no tiene importancia, así que puede utilizar el ajuste `U`.

Tabla 25: Tabla de entrada

Terminal	Puerto	Identificador de VLAN del puerto (PVID)
A	1	2
B	2	3
C	3	3
D	4	2
	5	1

Tabla 26: Tabla de salida

ID de VLAN	Puerto				
	1	2	3	4	5
1					U
2	U			U	
3		U	U		

Lleve a cabo los siguientes pasos:

☐ Configuración de la VLAN

- ☐ Abra el cuadro de diálogo *Switching > VLAN > Configuration*.
- ☐ Haga clic en el botón .
  El cuadro de diálogo muestra la ventana *Create*.
- ☐ En el campo *VLAN ID*, especifique el valor `2`.
- ☐ Haga clic en el botón *Ok*.
- ☐ Para la VLAN, especifique el nombre `VLAN2`:
  Haga doble clic en la columna *Name* y especifique el nombre.
  Para la VLAN `1`, en la columna *Name*, cambie el valor `Default` a `VLAN1`.
- ☐ Repita los pasos anteriores para crear una VLAN `3` con el nombre `VLAN3`.

`enable`	Cambiar al modo Privileged EXEC.
`vlan database`	Cambiar al modo de configuración de VLAN.
`vlan add 2`	Genera una nueva VLAN con el ID de VLAN `2`.
`name 2 VLAN2`	Asignar el nombre `2` a la VLAN `VLAN2`.
`vlan add 3`	Genera una nueva VLAN con el ID de VLAN `3`.
`name 3 VLAN3`	Asignar el nombre `3` a la VLAN `VLAN3`.
`name 1 VLAN1`	Asignar el nombre `1` a la VLAN `VLAN1`.
`exit`	Cambiar al modo Privileged EXEC.
`show vlan brief`	Mostrar la configuración de VLAN actual.

```
Max. VLAN ID..................................... 4042
Max. supported VLANs............................. 128
Number of currently configured VLANs............ 3
vlan unaware mode................................ disabled
VLAN ID VLAN Name                       VLAN Type VLAN Creation Time
---- -------------------------------- --------- -------------------
1       VLAN1                           default    0 days, 00:00:05
2       VLAN2                           static     0 days, 02:44:29
3       VLAN3                           static     0 days, 02:52:26
```

☐ Configuración de los puertos

- ☐ Abra el cuadro de diálogo *Switching > VLAN > Port*.
- ☐ Para asignar el puerto a una VLAN, especifique el valor deseado en la columna correspondiente.
  Valores posibles:
  - `T` = El puerto es miembro de la VLAN. El puerto transmite paquetes de datos etiquetados.
  - `U` = El puerto es miembro de la VLAN. El puerto transmite paquetes de datos no etiquetados.
  - `F` = El puerto no es miembro de la VLAN.
    Los cambios mediante la función *GVRP* están desactivados.
  - `-` = El puerto no es miembro de esta VLAN.
    Los cambios mediante la función *GVRP* están permitidos.

  Puesto que, normalmente, los dispositivos finales interpretan los paquetes de datos sin etiquetar, especifique el valor `U`.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón .

- ☐ Abra el cuadro de diálogo *Switching > VLAN > Port*.
- ☐ En el columna *Port-VLAN ID*, especifique el ID de VLAN de la VLAN correspondiente: `2` o `3`
- ☐ Puesto que, normalmente, los dispositivos finales interpretan los paquetes de datos sin etiquetar, en la columna *Acceptable packet types*, especifique el valor `admitAll` para los puertos del dispositivo final.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✔.

El valor de la columna *Ingress filtering* no tiene ningún efecto sobre las funciones de este ejemplo.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`interface 1/1`	Cambiar al modo de configuración de la interfaz `1/1`.
`vlan participation include 2`	El puerto `1/1` pasa a ser miembro de la VLAN `2` y transmite los paquetes de datos sin una etiqueta VLAN.
`vlan pvid 2`	Asignar el ID de VLAN del puerto `1/1` al puerto `2`.
`exit`	Cambiar al modo de configuración.
`interface 1/2`	Cambiar al modo de configuración de la interfaz `1/2`.
`vlan participation include 3`	El puerto `1/2` pasa a ser miembro de la VLAN `3` y transmite los paquetes de datos sin una etiqueta VLAN.
`vlan pvid 3`	Asignar el ID de VLAN del puerto `1/2` al puerto `3`.
`exit`	Cambiar al modo de configuración.
`interface 1/3`	Cambiar al modo de configuración de la interfaz `1/3`.
`vlan participation include 3`	El puerto `1/3` pasa a ser miembro de la VLAN `3` y transmite los paquetes de datos sin una etiqueta VLAN.
`vlan pvid 3`	Asignar el ID de VLAN del puerto `1/3` al puerto `3`.
`exit`	Cambiar al modo de configuración.
`interface 1/4`	Cambiar al modo de configuración de la interfaz `1/4`.
`vlan participation include 2`	El puerto `1/4` pasa a ser miembro de la VLAN `2` y transmite los paquetes de datos sin una etiqueta VLAN.
`vlan pvid 2`	Asignar el ID de VLAN del puerto `1/4` al puerto `2`.
`exit`	Cambiar al modo de configuración.

```
exit                                    Cambiar al modo Privileged EXEC.
show vlan id 3                          Muestra detalles de la VLAN 3.
VLAN ID           : 3
VLAN Name         : VLAN3
VLAN Type         : Static
Interface   Current   Configured   Tagging
----------  --------  -----------  --------
1/1            -      Autodetect   Tagged
1/2         Include   Include      Untagged
1/3         Include   Include      Untagged
1/4            -      Autodetect   Tagged
1/5            -      Autodetect   Tagged
```

12.1.2 Ejemplo 2

El segundo ejemplo muestra una configuración más compleja con 3 VLAN (1 a 3). Junto con el switch del ejemplo 1, utilice un segundo switch (a la derecha en el ejemplo).

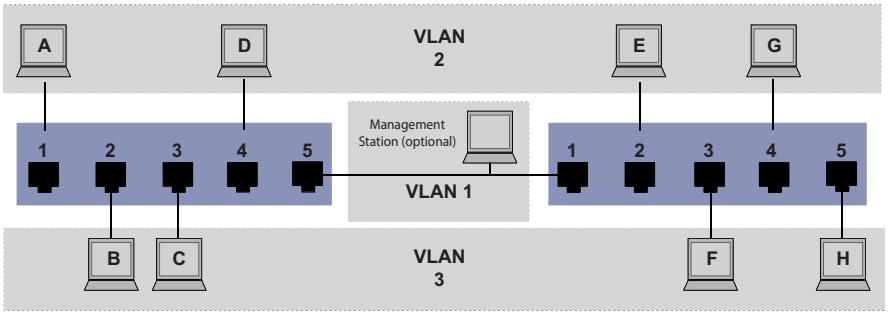


Figura 27: Ejemplo de una configuración de VLAN más compleja

Los dispositivos finales de cada una de las VLAN (de A a H) abarcan 2 dispositivos de comunicación (switches). Tales VLAN se llaman, por esta razón, VLAN distribuidas. Si la VLAN está configurada correctamente, también se muestra una estación de administración de red opcional que permite el acceso a cada componente de la red.

Nota: En este caso, la VLAN 1 no tiene importancia en la comunicación del dispositivo final, pero es necesaria para la administración de los dispositivos de comunicación a través de lo que se conoce como VLAN de administración.

Asigne los puertos con dispositivos finales conectados de forma unívoca a una VLAN como en el ejemplo anterior. En caso de conexión directa entre los 2 dispositivos de comunicación (Uplink), los puertos transportan paquetes para ambas VLAN. Para diferenciar estos Uplinks, utilice el "etiquetado VLAN", que gestiona los paquetes de datos de la manera correspondiente. De este modo, mantiene la asignación a las VLAN correspondientes.

Lleve a cabo los siguientes pasos:
- ☐ Añada el puerto Uplink 5 a las tablas de entrada y de salida del ejemplo 1.
- ☐ Cree nuevas tablas de entrada y de salida para el switch de la derecha, tal y como se describe en el primer ejemplo.

La tabla de salida especifica a qué puertos envía los paquetes el dispositivo desde esta VLAN.
- ▶ `T` = Etiquetado (con campo de etiqueta, marcada)
- ▶ `U` = No etiquetado (sin campo de etiqueta, no marcada)

En este ejemplo, los paquetes etiquetados se usan en la comunicación entre dispositivos de comunicación (Uplink), ya que en estos puertos se distinguen paquetes de VLAN diferentes.

Tabla 27: Tabla de entrada del dispositivo de la izquierda

Terminal	Puerto	Identificador de VLAN del puerto (PVID)
A	1	2
B	2	3
C	3	3
D	4	2
Uplink	5	1

Tabla 28: Tabla de entrada del dispositivo de la derecha

Terminal	Puerto	Identificador de VLAN del puerto (PVID)
Uplink	1	1
E	2	2
F	3	3
G	4	2
H	5	3

Tabla 29: Tabla de salida del dispositivo de la izquierda

ID de VLAN	Puerto				
	1	2	3	4	5
1					U
2	U			U	T
3		U	U		T

Tabla 30: Tabla de salida del dispositivo de la derecha

ID de VLAN	Puerto				
	1	2	3	4	5
1	U				
2	T	U		U	
3	T		U		U

Las relaciones de comunicación en este caso son las siguientes: los dispositivos finales de los puertos 1 y 4 del dispositivo de la izquierda y los dispositivos finales de los puertos 2 y 4 del dispositivo de la derecha son miembros de la VLAN 2 y, por tanto, se pueden comunicar entre sí. El comportamiento es el mismo para los dispositivos finales de los puertos 2 y 3 del dispositivo de la izquierda y los dispositivos finales de los puertos 3 y 5 del dispositivo de la derecha. Estos pertenecen a la VLAN 3.

Los dispositivos finales "ven" sus partes correspondientes de la red. No se puede acceder a los participantes que estén fuera de esta VLAN. El dispositivo también transmite paquetes Broadcast, Multicast y Unicast con direcciones de destino desconocidas (no aprendidas) únicamente dentro de una VLAN.

En este caso, los dispositivos utilizan el etiquetado VLAN (IEE.801.1Q) en la VLAN con el ID de VLAN 1 (Uplink). La letra `T` de la tabla de salida de los puertos indica el etiquetado VLAN.

La configuración del ejemplo es la misma para el dispositivo de la derecha. Proceda de forma análoga para adaptar al entorno nuevo el dispositivo de la izquierda configurado previamente usando las tablas de entrada y salida generadas más arriba.

Lleve a cabo los siguientes pasos:

☐ Configuración de la VLAN

- ☐ Abra el cuadro de diálogo *Switching > VLAN > Configuration*.
- ☐ Haga clic en el botón  .
  El cuadro de diálogo muestra la ventana *Create*.
- ☐ En el campo *VLAN ID*, especifique el ID de VLAN, por ejemplo, `2`.
- ☐ Haga clic en el botón *Ok*.
- ☐ Para la VLAN, especifique el nombre `VLAN2`:
  Haga doble clic en la columna *Name* y especifique el nombre.
  Para la VLAN `1`, en la columna *Name*, cambie el valor `Default` a `VLAN1`.
- ☐ Repita los pasos anteriores para crear una VLAN `3` con el nombre `VLAN3`.

`enable`	Cambiar al modo Privileged EXEC.
`vlan database`	Cambiar al modo de configuración de VLAN.
`vlan add 2`	Genera una nueva VLAN con el ID de VLAN `2`.
`name 2 VLAN2`	Asignar el nombre `2` a la VLAN `VLAN2`.
`vlan add 3`	Genera una nueva VLAN con el ID de VLAN `3`.
`name 3 VLAN3`	Asignar el nombre `3` a la VLAN `VLAN3`.
`name 1 VLAN1`	Asignar el nombre `1` a la VLAN `VLAN1`.
`exit`	Cambiar al modo Privileged EXEC.
`show vlan brief`	Mostrar la configuración de VLAN actual.

```
Max. VLAN ID..................................... 4042
Max. supported VLANs............................. 128
Number of currently configured VLANs........... 3
vlan unaware mode................................ disabled
VLAN ID VLAN Name                       VLAN Type VLAN Creation Time
---- -------------------------------- --------- -------------------
1       VLAN1                           default    0 days, 00:00:05
2       VLAN2                           static     0 days, 02:44:29
3       VLAN3                           static     0 days, 02:52:26
```

☐ Configuración de los puertos

☐ Abra el cuadro de diálogo *Switching > VLAN > Port*.

☐ Para asignar el puerto a una VLAN, especifique el valor deseado en la columna correspondiente.
Valores posibles:
- `T` = El puerto es miembro de la VLAN. El puerto transmite paquetes de datos etiquetados.
- `U` = El puerto es miembro de la VLAN. El puerto transmite paquetes de datos no etiquetados.
- `F` = El puerto no es miembro de la VLAN.
  Los cambios mediante la función *GVRP* están desactivados.
- `-` = El puerto no es miembro de esta VLAN.
  Los cambios mediante la función *GVRP* están desactivados.

Puesto que, normalmente, los dispositivos finales interpretan los paquetes de datos sin etiquetar, especifique el valor `U`.
Especifique el ajuste `T` en el puerto Uplink a través del cual las VLAN se comunican entre sí.

☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✔.

☐ Abra el cuadro de diálogo *Switching > VLAN > Port*.

☐ En el columna *Port-VLAN ID*, especifique el ID de VLAN de la VLAN correspondiente: `1`, `2` o `3`

☐ Puesto que, normalmente, los dispositivos finales interpretan los paquetes de datos sin etiquetar, en la columna *Acceptable packet types*, especifique el valor `admitAll` para los puertos del dispositivo final.

☐ Para el puerto Uplink, en la columna *Acceptable packet types*, especifique el valor `admitOnlyVlanTagged`.

☐ Marque la casilla de la columna *Ingress filtering* para que los puertos Uplink evalúen las etiquetas de este puerto.

☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✔.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`interface 1/1`	Cambiar al modo de configuración de la interfaz `1/1`.
`vlan participation include 1`	El puerto `1/1` pasa a ser miembro de la VLAN `1` y transmite los paquetes de datos sin una etiqueta VLAN.
`vlan participation include 2`	El puerto `1/1` pasa a ser miembro de la VLAN `2` y transmite los paquetes de datos sin una etiqueta VLAN.
`vlan tagging 2 enable`	El puerto `1/1` pasa a ser miembro de la VLAN `2` y transmite los paquetes de datos con una etiqueta VLAN.
`vlan participation include 3`	El puerto `1/1` pasa a ser miembro de la VLAN `3` y transmite los paquetes de datos sin una etiqueta VLAN.
`vlan tagging 3 enable`	El puerto `1/1` pasa a ser miembro de la VLAN `3` y transmite los paquetes de datos con una etiqueta VLAN.
`vlan pvid 1`	Asignar el ID de VLAN del puerto `1` al puerto `1/1`.
`vlan ingressfilter`	Activar el filtrado de ingreso en el puerto `1/1`.
`vlan acceptframe vlanonly`	El puerto `1/1` solo reenvía los paquetes con una etiqueta VLAN.
`exit`	Cambiar al modo de configuración.
`interface 1/2`	Cambiar al modo de configuración de la interfaz `1/2`.
`vlan participation include 2`	El puerto `1/2` pasa a ser miembro de la VLAN `2` y transmite los paquetes de datos sin una etiqueta VLAN.
`vlan pvid 2`	Asignar el ID de VLAN del puerto `2` al puerto `1/2`.
`exit`	Cambiar al modo de configuración.
`interface 1/3`	Cambiar al modo de configuración de la interfaz `1/3`.
`vlan participation include 3`	El puerto `1/3` pasa a ser miembro de la VLAN `3` y transmite los paquetes de datos sin una etiqueta VLAN.
`vlan pvid 3`	Asignar el ID de VLAN del puerto `3` al puerto `1/3`.
`exit`	Cambiar al modo de configuración.
`interface 1/4`	Cambiar al modo de configuración de la interfaz `1/4`.
`vlan participation include 2`	El puerto `1/4` pasa a ser miembro de la VLAN `2` y transmite los paquetes de datos sin una etiqueta VLAN.
`vlan pvid 2`	Asignar el ID de VLAN del puerto `2` al puerto `1/4`.
`exit`	Cambiar al modo de configuración.
`interface 1/5`	Cambiar al modo de configuración de la interfaz `1/5`.
`vlan participation include 3`	El puerto `1/5` pasa a ser miembro de la VLAN `3` y transmite los paquetes de datos sin una etiqueta VLAN.

```
vlan pvid 3
```
Asignar el ID de VLAN del puerto 3 al puerto 1/5.

```
exit
```
Cambiar al modo de configuración.

```
exit
```
Cambiar al modo Privileged EXEC.

```
show vlan id 3
```
Muestra detalles de la VLAN 3.

```
VLAN ID.....................3
VLAN Name...................VLAN3
VLAN Type...................Static
VLAN Creation Time..........0 days, 00:07:47 (System Uptime)
VLAN Routing................disabled

Interface   Current   Configured   Tagging
----------  --------  -----------  --------
1/1         Include   Include      Tagged
1/2         -         Autodetect   Untagged
1/3         Include   Include      Untagged
1/4         -         Autodetect   Untagged
1/5         Include   Include      Untagged
```

12.2 VLAN invitada/VLAN no autenticada

Una VLAN invitada permite a un dispositivo proporcionar control de acceso a la red basado en puerto (IEEE 802.1x) a solicitantes sin capacidad 802.1x. Esta función ofrece un mecanismo para permitir a los invitados acceder únicamente a las redes externas. Si conecta solicitantes sin capacidad 802.1x a un puerto 802.1x activo no autorizado, los solicitantes no enviarán respuestas a las solicitudes 802.1x. Puesto que los solicitantes no envían respuestas, el puerto permanece en el estado no autorizado. Los solicitantes no tienen acceso a las redes externas.

El solicitante de la VLAN invitada tiene una configuración para cada puerto. Si configura un puerto como VLAN invitada y conecta solicitantes sin capacidad 802.1x a dicho puerto, el dispositivo asigna los solicitantes a la VLAN invitada. Al añadir solicitantes a una VLAN invitada, el puerto cambia al estado autorizado y permite a los solicitantes acceder a las redes externas.

Una VLAN no autenticada permite al dispositivo dar servicio a solicitantes con capacidad 802.1x que se autentiquen de forma incorrecta. Esta función permite a los solicitantes no autorizados acceder a servicios limitados. Si configura una VLAN no autenticada en un puerto con autenticación de puertos 802.1x y el funcionamiento global está activo, el dispositivo coloca el puerto en una VLAN no autenticada. Si un solicitante con capacidad 802.1x se autentica de manera incorrecta en el puerto, el dispositivo añade el solicitante a la VLAN no autenticada. Si configura una VLAN invitada en el puerto, los solicitantes sin capacidad 802.1x utilizan la VLAN invitada.

Si el puerto tiene una VLAN no autenticada asignada, el temporizador de reautenticación empieza a correr. Si vence el tiempo especificado en la columna *Reauthentication period [s]* y los solicitantes están presentes en el puerto, la VLAN no autenticada vuelve a autenticarse. Si no hay solicitantes presentes, el dispositivo coloca el puerto en la VLAN invitada configurada.

El siguiente ejemplo explica cómo crear una VLAN invitada. Cree una VLAN no autorizada de la misma manera.

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Switching > VLAN > Configuration*.
- ☐ Haga clic en el botón .
  El cuadro de diálogo muestra la ventana *Create*.
- ☐ En el campo *VLAN ID*, especifique el valor `10`.
- ☐ Haga clic en el botón *Ok*.
- ☐ Para la VLAN, especifique el nombre `Guest`:
  Haga doble clic en la columna *Name* y especifique el nombre.
- ☐ Haga clic en el botón .
  El cuadro de diálogo muestra la ventana *Create*.
- ☐ En el campo *VLAN ID*, especifique el valor `20`.
- ☐ Haga clic en el botón *Ok*.
- ☐ Para la VLAN, especifique el nombre `Not authorized`:
  Haga doble clic en la columna *Name* y especifique el nombre.
- ☐ Abra el cuadro de diálogo *Network Security > 802.1X Port Authentication > Global*.
- ☐ Para activar la función, seleccione el botón de opción `On` en el cuadro *Operation*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón .

- ☐ Abra el cuadro de diálogo *Network Security > 802.1X Port Authentication > Port Configuration*.
- ☐ Especifique los siguientes ajustes para el puerto `1/4`:
  - El valor `auto` en la columna *Port control*
  - El valor `10` en la columna *Guest VLAN ID*
  - El valor `20` en la columna *Unauthenticated VLAN ID*
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✔.

`enable`	Cambiar al modo Privileged EXEC.
`vlan database`	Cambiar al modo de configuración de VLAN.
`vlan add 10`	Crea la VLAN `10`.
`vlan add 20`	Crea la VLAN `20`.
`name 10 Guest`	Cambia el nombre de la VLAN `10` a `Guest`.
`name 20 Unauth`	Cambia el nombre de la VLAN `20` a `Unauth`.
`exit`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`dot1x system-auth-control enable`	Activar la función *802.1X Port Authentication* globalmente.
`dot1x port-control auto`	Activa el control del puerto en el puerto `1/4`.
`interface 1/4`	Cambiar al modo de configuración de la interfaz `1/4`.
`dot1x guest-vlan 10`	Asignar la VLAN invitada al puerto `1/4`.
`dot1x unauthenticated-vlan 20`	Asignar la VLAN no autorizada al puerto `1/4`.
`exit`	Cambiar al modo de configuración.

12.3 Asignación de VLAN de RADIUS

La función de asignación de VLAN de RADIUS hace posible que un atributo ID de VLAN de RADIUS se asocie con un cliente autenticado. Si un cliente se autentica correctamente, y el servidor RADIUS envía un atributo VLAN, el dispositivo asocia el cliente con la VLAN asignada a RADIUS. Como resultado, el dispositivo añade el puerto físico como miembro a la VLAN adecuada y establece el ID VLAN del puerto (PVID) con el valor dado. El puerto transmite los paquetes de datos sin etiqueta de VLAN.

12.4 Creación de Voice VLAN

Utilice la función Voice VLAN para separar el tráfico de voz y datos de un puerto por VLAN y/o prioridad. Una de las principales ventajas de utilizar Voice VLAN es que protege la calidad del sonido de un teléfono IP cuando hay un tráfico de datos elevado en el puerto.

El dispositivo utiliza la dirección MAC de origen para identificar y priorizar el flujo de datos de voz. Con el uso de la dirección MAC para identificar los dispositivos, se evita que un cliente no autorizado se conecte al mismo puerto y provoque que el tráfico de voz se deteriore.

Otra ventaja de la función Voice VLAN es que el teléfono VoIP obtiene el ID de VLAN o la información de prioridad a través de LLDP-MED. Como resultado, el teléfono VoIP envía datos de voz como etiquetados, etiquetados con prioridad o sin etiquetar. Esto depende de la configuración de interfaz de Voice VLAN.

Son posibles los siguientes modos de interfaz de Voice VLAN. Los 3 primeros métodos separan y priorizan el tráfico de datos y de voz. La separación de tráfico permite un incremento de la calidad del tráfico de voz durante los periodos de tráfico elevado.

- Configurar el puerto para que utilice el modo `vlan` permite al dispositivo etiquetar los datos de voz que provengan de un teléfono VoIP con el ID de Voice VLAN definido por el usuario. El dispositivo asigna los datos regulares al ID de VLAN del puerto por defecto.
- Configurar el puerto para que utilice el modo `dot1p-priority` permite al dispositivo etiquetar los datos que provengan de un teléfono VoIP con la VLAN 0 y la prioridad definida por el usuario. El dispositivo asigna la prioridad por defecto del puerto a los datos regulares.
- Configure tanto el ID de Voice VLAN como la prioridad mediante el modo `vlan/dot1p-priority`. En este modo, el teléfono VoIP envía los datos de voz con el ID de Voice VLAN y la información de prioridad definidos por el usuario. El dispositivo asigna el PVID y la prioridad por defecto del puerto a los datos regulares.
- Si se configura como `untagged`, el teléfono envía paquetes sin etiquetar.
- Si se configura como `none`, el teléfono utiliza su propia configuración para enviar tráfico de voz.

13 Redundancy ‹Redundancia›

13.1 Topología de red frente a Protocolos de redundancia

Al utilizar Ethernet, un requisito previo que se debe tener en cuenta es que los paquetes de datos siguen una ruta individual (única) desde el emisor hasta el receptor. Las siguientes topologías de red son compatibles con este requisito previo:

- Topología en línea
- Topología en estrella
- Topología en árbol

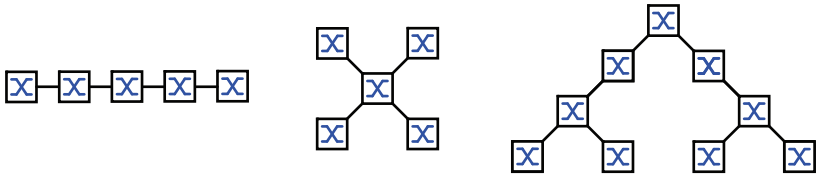


Figura 28: Red con topologías en línea, estrella y árbol

Para mantener la comunicación en caso de que se detecte un fallo de la conexión, instale conexiones físicas adicionales entre los nodos de red. Los protocolos de redundancia ayudan a garantizar que las conexiones adicionales permanezcan apagadas mientras que la conexión original aún esté en funcionamiento. Si se detecta un fallo de la conexión, el protocolo de redundancia genera una nueva ruta desde el emisor hasta el receptor a través de la conexión alternativa.

Para introducir la redundancia en la Capa 2 de una red, primero debe definir qué topología de red se requiere. En función de la topología de red seleccionada, elija a continuación los protocolos de redundancia que desea utilizar con esta topología de red.

13.1.1 Topologías de red

Topología de malla

Para redes con topologías en estrella o en árbol, los procesos de redundancia solo son posibles en conexión con la creación de un bucle físico. Como resultado, se origina una topología de malla.

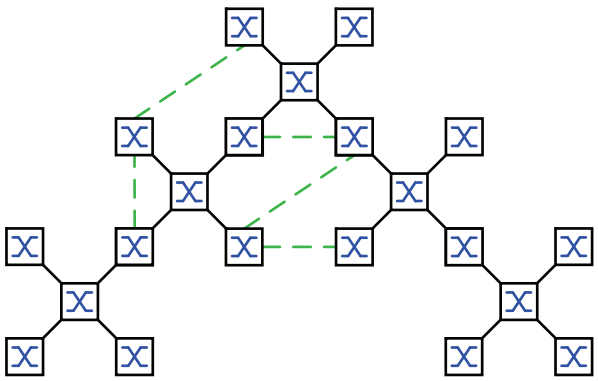


Figura 29: Topología de malla: topología en árbol con bucles físicos

Para el funcionamiento de esta topología de red, el dispositivo le ofrece los siguientes protocolos de redundancia:
- Rapid Spanning Tree (RSTP)

Topología en anillo

En redes con una topología en línea, puede utilizar procesos de redundancia al conectar los extremos de la línea. De este modo se crea una topología en anillo.

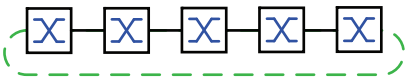


Figura 30: Topología en anillo: topología en línea con los extremos conectados

Para el funcionamiento de esta topología de red, el dispositivo le ofrece los siguientes protocolos de redundancia:
- Protocolo de redundancia de medios (MRP)
- Rapid Spanning Tree (RSTP)

13.1.2 Protocolos de redundancia

Para el funcionamiento en diferentes topologías de red, el dispositivo le ofrece los siguientes protocolos de redundancia:

Tabla 31: Vista general de los protocolos de redundancia

Protocolo de redundancia	Topología de red	Observaciones
MRP	Ring ‹Anillo›	El intervalo de conmutación se puede seleccionar y es prácticamente independiente del número de dispositivos. Un anillo MRP está compuesto por hasta 50 dispositivos compatibles con el protocolo MRP conforme al estándar IEC 62439. Si solo utiliza los dispositivos Schneider Electric, el anillo MRP admite hasta 100 dispositivos.
Subring ‹Anillo secundario›	Ring ‹Anillo›	La función *Sub Ring* le permite acoplar fácilmente segmentos de red a anillos de redundancia existentes.
Ring/Network coupling ‹Acoplamiento de red/anillo›	Ring ‹Anillo›	
RCP	Ring ‹Anillo›	
RSTP	Estructura aleatoria	El intervalo de conmutación depende de la topología de red y del número de dispositivos. - tip. < 1 s con RSTP - tip. < 30 s con STP
Agregación de enlaces	Estructura aleatoria	Un grupo de agregación de enlaces consiste en la combinación de 2 o más enlaces de punto a punto Full-Dúplex que funcionan a la misma velocidad en un solo switch para aumentar el ancho de banda.

Tabla 31: Vista general de los protocolos de redundancia (cont

Protocolo de redundancia	Topología de red	Observaciones
Link Backup	Estructura aleatoria	Si el dispositivo detecta un error en el enlace principal, el dispositivo transfiere el tráfico al enlace de reserva. Por lo general, Link Backup se utiliza en redes empresariales o de proveedor de servicios.
Cliente de anillo HIPER	Ring ‹Anillo›	Amplíe un anillo HIPER existente o sustituya un dispositivo que ya esté participando como cliente en un anillo HIPER.
HIPER Ring a través de LAG	Ring ‹Anillo›	Vincule dispositivos entre sí a través de un grupo de agregación de enlaces (LAG). Los clientes del anillo y el gestor de anillos se comportan de la misma manera que un anillo sin una instancia LAG.

Si el control de flujo y la función de redundancia están activos al mismo tiempo, es posible que la función de redundancia opere de un modo distinto al deseado.

⚠ ADVERTENCIA

OPERACIÓN INESPERADA DEL EQUIPO

Si está utilizando un mecanismo de redundancia, desactive el control de flujo en los puertos del dispositivo implicados.

El incumplimiento de estas instrucciones puede causar la muerte, heridas graves o daños en el equipo.

13.1.3 Combinaciones de redundancias

Tabla 32: Vista general de los protocolos de redundancia

	MRP	RSTP	Agregación de enlaces	Link Backup	Subring ‹Anillo secundario›	HIPER Ring
MRP	▲	– – –	– – –	– – –	– – –	– – –
RSTP	▲ 1)	▲	– – –	– – –	– – –	– – –
Agregación de enlaces	▲ 2)	▲ 2)	▲	– – –	– – –	– – –
Link Backup	▲	▲	▲	▲	– – –	– – –
Subring ‹Anillo secundario›	▲	▲	▲ 2)	▲	▲	– – –
HIPER Ring	▲	▲ 1)	▲ 2)	▲	▲	▲

▲ Combinación aplicable

1) Un acoplamiento redundante entre estas topologías de red probablemente provocará bucles.
Para acoplar estas topologías de manera redundante, consulte el capítulo “FuseNet” en página 224.

2) Combinación aplicable en el mismo puerto

13.2 Protocolo de redundancia de medios (MRP)

Desde mayo de 2008, el protocolo de redundancia de medios (MRP, Media Redundancy Protocol) ha sido la solución estandarizada para la redundancia de anillo en el entorno industrial.

MRP es compatible con el acoplamiento redundante entre anillos, admite VLAN y se distingue por unos tiempos de reconfiguración muy breves.

Un anillo MRP está compuesto por hasta 50 dispositivos compatibles con el protocolo MRP conforme al estándar IEC 62439. Si solo utiliza los dispositivos Schneider Electric, el anillo MRP admite hasta 100 dispositivos.

Si utiliza el puerto redundante MRP fijo (Fixed Backup) y se detecta un fallo del enlace del anillo principal, Ring Manager reenvía los datos al enlace del anillo secundario. Cuando el enlace principal se restaure, el enlace secundario continuará utilizándose.

13.2.1 Estructura de red

El concepto de la redundancia de anillo le permite construir estructuras de red de alta disponibilidad y con forma de anillo.

Con la ayuda de la función RM (**R**ing**M**anager) se pueden conectar los dos extremos de un backbone de una estructura lineal para formar un anillo redundante. Ring Manager mantiene abierto el trayecto redundante cuando la estructura lineal permanece intacta. Si un segmento deja de estar disponible, Ring Manager cierra inmediatamente el trayecto redundante y la estructura lineal vuelve a quedar intacta.

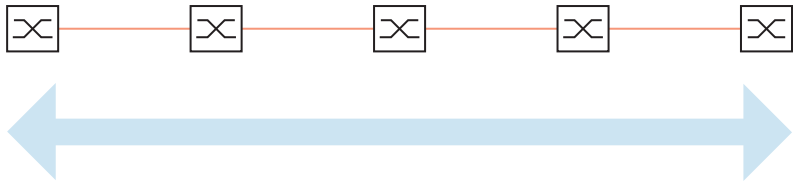


Figura 31: Estructura lineal

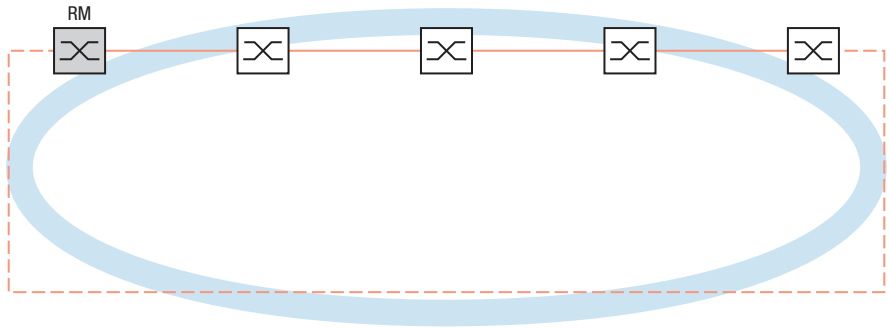


Figura 32: Estructura del acoplamiento redundante entre anillos
RM = Ring Manager
—— línea principal
- - - línea redundante

13.2.2 Tiempo de reconfiguración

Si se detecta un fallo de la sección de línea, Ring Manager vuelve a cambiar el anillo MRP a una estructura lineal. Puede definir el tiempo máximo para la reconfiguración de la línea en Ring Manager.

Valores posibles para tiempo de retardo máximo:
- *500ms*
- *30ms*

Nota: Si todos los dispositivos del anillo admiten el tiempo de retardo más breve, puede configurar el tiempo de reconfiguración con un valor inferior a *500ms*.

De lo contrario, es posible que los dispositivos que solo admitan tiempos de retardo más largos no sean accesibles debido a una sobrecarga. Como consecuencia, pueden producirse bucles.

13.2.3 Modo avanzado

Para intervalos aún más breves que los tiempos de reconfiguración especificados, el dispositivo proporciona el modo avanzado. Cuando los participantes del anillo informan a Ring Manager sobre interrupciones en el anillo a través de mensajes link-down, el modo avanzado acelera el reconocimiento de errores de enlace.

Los dispositivos Schneider Electric admiten mensajes link-down. Por lo tanto, generalmente, puede activar el modo avanzado en Ring Manager.

Si utiliza dispositivos que no admiten mensajes link-down, Ring Manager reconfigura la línea de acuerdo con el tiempo de reconfiguración máximo seleccionado.

13.2.4 Requisitos previos para MRP

Antes de instalar un anillo MRP, verifique que las siguientes condiciones se cumplan:
- Todos los participantes del anillo son compatibles con MRP.
- Los participantes del anillo están conectados entre sí a través de los puertos del anillo. Además de los vecinos del dispositivo, no hay otros participantes del anillo conectados al dispositivo correspondiente.
- Todos los participantes del anillo admiten el tiempo de configuración especificado en Ring Manager.
- Hay solamente un Ring Manager en el anillo.

Si utiliza redes VLAN, debe configurar cada puerto del anillo con los siguientes ajustes:

- Desactive el filtrado de ingreso: consulte el cuadro de diálogo *Switching > VLAN > Port*.
- Defina el ID de VLAN del puerto (PVID): consulte el cuadro de diálogo *Switching > VLAN > Port*.
  - PVID = `1` en los casos en los que el dispositivo transmite los paquetes de datos MRP sin etiquetar (ID de VLAN = `0` en el cuadro de diálogo *Switching > L2-Redundancy > MRP*)
    Al establecer el PVID = `1`, el dispositivo asigna automáticamente los paquetes recibidos sin etiquetar a la VLAN 1.
  - PVID = `any` en los casos en los que el dispositivo transmite los paquetes de datos MRP en una VLAN (ID VLAN ≥ `1` en el cuadro de diálogo *Switching > L2-Redundancy > MRP*)
- Defina las reglas de salida: consulte el cuadro de diálogo *Switching > VLAN > Configuration*.
  - `U` (sin etiquetar) para los puertos del anillo de la VLAN 1 en los casos en los que el dispositivo transmita los paquetes de datos MRP sin etiquetar (ID de VLAN = `0` en el cuadro de diálogo *Switching > L2-Redundancy > MRP*, el anillo MRP no se asigna a una VLAN).
  - `T` (etiquetado) para los puertos del anillo de la VLAN que asigna al anillo MRP. Seleccione `T` en los casos en los que el dispositivo transmite los paquetes de datos MRP sin etiquetar en una VLAN (ID de VLAN ≥ `1` en el cuadro de diálogo *Switching > L2-Redundancy > MRP*).

13.2.5 Configuración de ejemplo

Una red backbone contiene 3 dispositivos en una estructura lineal. Para aumentar la disponibilidad de la red, convierta la estructura lineal en una estructura del acoplamiento redundante entre anillos. Se utilizan dispositivos de diferentes fabricantes. Todos los dispositivos son compatibles con MRP. En cada dispositivo, defina los puertos 1.1 y 1.2 como puertos del anillo.

Si se detecta un fallo del enlace del anillo principal, Ring Manager envía los datos a través del enlace del anillo secundario. Cuando el enlace principal se restaure, el enlace secundario volverá al modo de reserva.

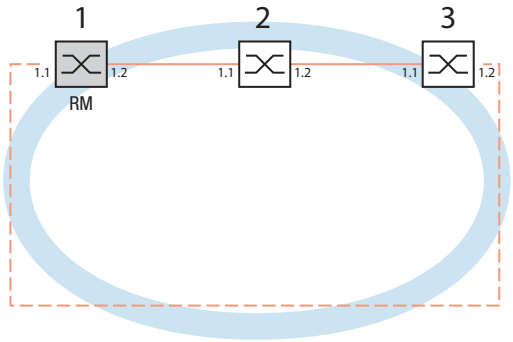


Figura 33: Ejemplo de anillo MRP
RM = Ring Manager
—— línea principal
- - - línea redundante

El siguiente ejemplo describe la configuración del dispositivo Ring Manager (1). Los otros 2 dispositivos (2 a 3) se configuran de la misma forma, sin tener que activar la función *Ring manager*. Este ejemplo no utiliza una VLAN. Especifique el valor `30ms` como tiempo de recuperación del anillo. Todos los dispositivos son compatibles con el modo avanzado de Ring Manager.

- ☐ Configure la red para que cumpla con sus requisitos.
- ☐ Configure cada puerto para que la velocidad de transmisión y los ajustes dúplex de las líneas correspondan con la siguiente tabla:

Tabla 33: Configuración de puertos de anillo

Tipo de puerto	Velocidad de bits	Port on	Automatic configuration	Manual configuration
TX	100 Mbit/s	`marcado`	`sin marcar`	*`100 Mbit/s FDX`*
TX	1 Gbit/s	`marcado`	`marcado`	–
Óptico	100 Mbit/s	`marcado`	`sin marcar`	*`100 Mbit/s FDX`*
Óptico	1 Gbit/s	`marcado`	`marcado`	–
Óptico	2.5 Gbit/s	`marcado`	–	*`2.5 Gbit/s FDX`*

Nota: Configure los puertos ópticos sin soporte para autonegociación (configuración automática) con Full-Dúplex de 100 Mbits/s (FDX) o Full-Dúplex de 1000 Mbits/s (FDX).

Nota: Configure los puertos ópticos sin soporte para autonegociación (configuración automática) con Full-Dúplex de 100 Mbits/s (FDX).

Nota: Configure uno a uno todos los dispositivos del anillo MRP. Antes de conectar el trayecto redundante, verifique que ha completado la configuración de cada dispositivo del anillo MRP. De esta forma, ayuda a evitar bucles durante la fase de configuración.

⚠ ADVERTENCIA

OPERACIÓN INESPERADA DEL EQUIPO

Para ayudar a evitar bucles durante la fase de configuración, configure cada dispositivo de la configuración *MRP* individualmente. Antes de conectar los trayectos redundantes, complete la configuración de los otros dispositivos de la configuración del anillo.

El incumplimiento de estas instrucciones puede causar la muerte, heridas graves o daños en el equipo.

Desactive el control de flujo de los puertos participantes.

Si el control de flujo y la función de redundancia están activos al mismo tiempo, es posible que la función de redundancia opere de un modo distinto al deseado. (Configuración por defecto: control de flujo desactivado globalmente y activado en todos los puertos).

Desactive la función *Spanning Tree* en cada dispositivo de la red. Para ello, siga los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Switching > L2-Redundancy > Spanning Tree > Global*.
- ☐ Desactive la función.
  En la configuración por defecto, Spanning Tree está activado en el dispositivo.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`no spanning-tree operation`	Desconecta Spanning Tree.
`show spanning-tree global`	Muestra los parámetros para la comprobación.

Active MRP en cada dispositivo de la red. Para ello, siga los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Switching > L2-Redundancy > MRP*.
- ☐ Especifique los puertos de anillo deseados.

En la interfaz de línea de comando, deberá definir primero un parámetro adicional, los identificadores de dominio de MRP. Configure los anillos participantes con los mismos identificadores de dominio de MRP. Los identificadores de dominio de MRP consisten en una sucesión de 16 grupos numéricos (valores de 8 bits).

En la configuración con la interfaz gráfica de usuario, el dispositivo utiliza el valor por defecto `255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255`.

`mrp domain add default-domain`	Genera un nuevo dominio de MRP con el ID `default-domain`.
`mrp domain modify port primary 1/1`	Especifica el puerto *1/1* como puerto del anillo `1`.
`mrp domain modify port secondary 1/2`	Especifica el puerto *1/2* como puerto del anillo `2`.

Active el puerto *Fixed backup*. Para ello, siga los siguientes pasos:

- ☐ Active Ring Manager.
  Para los otros dispositivos del anillo, deje la configuración en *Off*.
- ☐ Para permitir que el dispositivo continúe enviando datos a través del puerto secundario una vez que el anillo se ha restaurado, marque la casilla *Fixed backup*.

Nota: Cuando el dispositivo vuelve al puerto principal, se puede superar el tiempo de recuperación máximo del anillo.

Si desactiva la casilla *Fixed backup* y el anillo se restaura, Ring Manager bloquea el puerto secundario y desbloquea el puerto principal.

`mrp domain modify port secondary 1/2 fixed-backup enable`	Activa la función *Fixed backup* en el puerto secundario. El puerto secundario continúa enviando datos una vez que el anillo se ha restaurado.

- ☐ Active Ring Manager.
  Para los otros dispositivos del anillo, deje la configuración en *Off*.

`mrp domain modify mode manager`	Especifique que el dispositivo actúa como *Ring manager*. Para los otros dispositivos del anillo, deje la configuración por defecto.

☐ Seleccione la casilla del campo *Advanced mode*.

```
mrp domain modify   advanced-mode
enabled
```

Activa el modo avanzado.

☐ En el campo *Ring recovery*, seleccione el valor `30ms`.

```
mrp domain modify   recovery-delay
200ms
```

Especifica el valor `30ms` como el tiempo de retardo máximo para la reconfiguración del anillo.

Nota: Si al seleccionar el valor `30ms` para la recuperación del anillo no se obtiene la estabilidad del anillo necesaria para cumplir con los requisitos de su red, seleccione el valor `500ms`.

☐ Active la función del anillo MRP.
☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ☑.

```
mrp domain modify operation   enable
```

Activa el anillo MRP.

Cuando se hayan configurado todos los participantes del anillo, cierre la línea del anillo. Para ello, conecte los dispositivos de los extremos de la línea mediante los puertos del anillo.

Compruebe los mensajes del dispositivo. Para ello, siga los siguientes pasos:

```
show mrp
```

Muestra los parámetros para la comprobación.

El campo *Operation* muestra el modo de funcionamiento del puerto del anillo.

Valores posibles:
- `forwarding`
  El puerto está activado, existe una conexión.
- `blocked`
  El puerto está bloqueado, existe una conexión.
- `disabled`
  El puerto está desactivado.
- `not-connected`
  No existe conexión.

El campo *Information* muestra mensajes para la configuración de la redundancia y las posibles causas de los errores.

Cuando el dispositivo actúa como Ring Client o Ring Manager, es posible que se muestren los siguientes mensajes:
- *Redundancy available*
  La redundancia está configurada. Cuando un componente del anillo está inactivo, la línea redundante asume su función.
- *Configuration error: Error on ringport link.*
  Se ha detectado un error en el cableado de los puertos del anillo.

Cuando el dispositivo actúa como Ring Manager, es posible que se muestren los siguientes mensajes:
- *Configuration error: Packets from another ring manager received.*
  Existe otro dispositivo en el anillo que actúa como Ring Manager.
  Active la función *Ring manager* exactamente en un dispositivo del anillo.
- *Configuration error: Ring link is connected to wrong port.*
  Una línea del anillo está conectada con un puerto diferente en lugar de con un puerto del anillo. El dispositivo solamente recibe paquetes de datos de prueba en un puerto de anillo.

En caso necesario, integre el anillo MRP en una VLAN. Para ello, siga los siguientes pasos:

- ☐ En el campo *VLAN ID*, defina el ID VLAN de MRP. El ID VLAN de MRP determina en qué redes VLAN configuradas el dispositivo puede transmitir los paquetes MRP.
  Para establecer el ID VLAN de MRP, configure primero las VLAN y las reglas de salida correspondientes en el cuadro de diálogo *Switching > VLAN > Configuration*.
  - Si el anillo MRP no está asignado a una VLAN (como en este ejemplo), deje el ID VLAN como `0`.
    En el cuadro de diálogo *Switching > VLAN > Configuration*, especifique la pertenencia de VLAN como `U` (no etiquetada) para los puertos del anillo en la VLAN `1`.
  - Si el anillo MRP no está asignado a una VLAN, introduzca el ID VLAN > `0`.
    En el cuadro de diálogo *Switching > VLAN > Configuration*, especifique la pertenencia de VLAN como `T` (etiquetada) para los puertos del anillo en la VLAN seleccionada.

`mrp domain modify vlan <0..4042>`	Asigna el ID VLAN.

13.2.6 MRP a través de LAG

Schneider Electric los dispositivos le permiten combinar grupos de agregación de enlaces (LAG) para incrementar el ancho de banda con el Protocolo de redundancia de medios (MRP) proporcionando redundancia. La función le permite incrementar el ancho de banda en segmentos individuales o en toda la red.

La función *Link Aggregation* le permite superar las limitaciones de ancho de banda de los puertos individuales. LAG le permite combinar 2 o más enlaces en paralelo, creando un enlace lógico entre 2 dispositivos. Los enlaces paralelos aumentan el ancho de banda para el flujo de datos entre los 2 dispositivos.

Un anillo MRP está compuesto por hasta 50 dispositivos compatibles con el protocolo MRP conforme al estándar IEC 62439. Si solo utiliza dispositivos Schneider Electric, el protocolo le permite configurar anillos MRP con hasta 100 dispositivos.

Utilice MRP a través de LAG en los casos siguientes:
- para aumentar el ancho de banda solamente en segmentos específicos de un anillo MRP
- para aumentar el ancho de banda en todo el anillo MRP

Estructura de red

Al configurar un anillo MRP con LAG, el Ring Manager (RM) supervisa la continuidad de ambos extremos de la red backbone. El RM bloquea los datos en el puerto secundario (redundante) siempre que la red backbone esté intacta. Cuando el RM detecta una interrupción del flujo de datos en el anillo, comienza a desviar datos en el puerto secundario, lo cual restablece la continuidad de la red backbone.

Utilice instancias LAG en anillos MRP solamente para aumentar el ancho de banda; en este caso MRP proporciona la redundancia.

Para que el RM detecte una interrupción en el anillo, MRP requiere que un dispositivo bloquee cada puerto de la instancia LAG en casos en los que un puerto de la instancia no esté disponible.

LAG en un único segmento de un anillo MRP

El dispositivo le permite configurar una instancia LAG en segmentos específicos de un anillo MRP.

Utilice el método de un solo switch LAG para los dispositivos del anillo MRP. El método de un solo switch ofrece un método asequible para hacer crecer su red utilizando tan solo un dispositivo en cada parte de un segmento para proporcionar los puertos físicos. Agrupe los puertos del dispositivo en una instancia LAG para proporcionar un mayor ancho de banda en segmentos específicos cuando sea necesario.

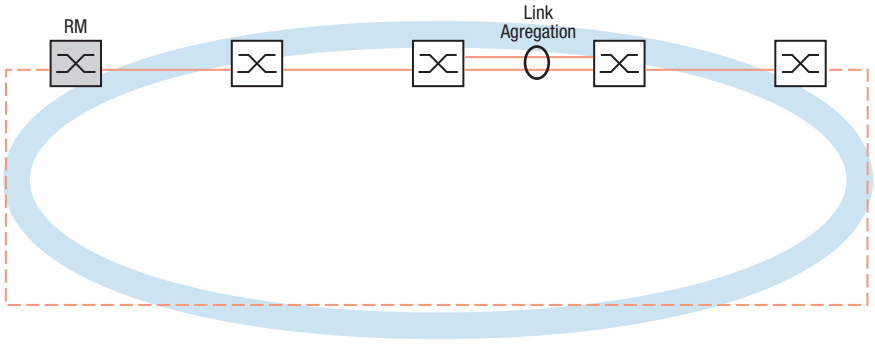


Figura 34: Agregación de enlaces a través de un único enlace de un anillo MRP.

LAG en un anillo MRP completo

Además de permitir configurar una instancia LAG en segmentos específicos de un anillo MRP, los dispositivos Schneider Electric también le permiten configurar instancias LAG en cada segmento, lo cual permite aumentar el ancho de banda en todo el anillo MRP.

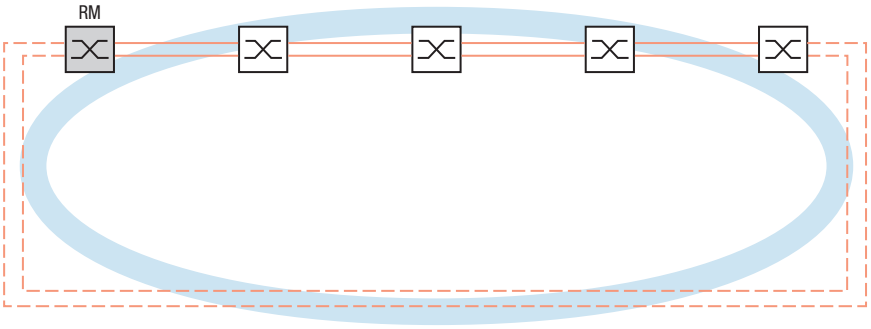


Figura 35: Agregación de enlaces a través del anillo MRP completo.

Detección de interrupciones en el anillo

Al configurar la instancia LAG, especifique el valor *Active ports (min.)* para igualar el número total de puertos utilizados en la instancia LAG. Cuando un dispositivo detecte una interrupción en un puerto de la instancia LAG, bloquea datos en los demás puertos de la instancia. Con cada puerto de una instancia bloqueada, el RM detecta que el anillo está abierto y comienza a desviar datos en el puerto secundario. De este modo, el RM es capaz de restablecer la continuidad con los dispositivos del otro lado del segmento interrumpido.

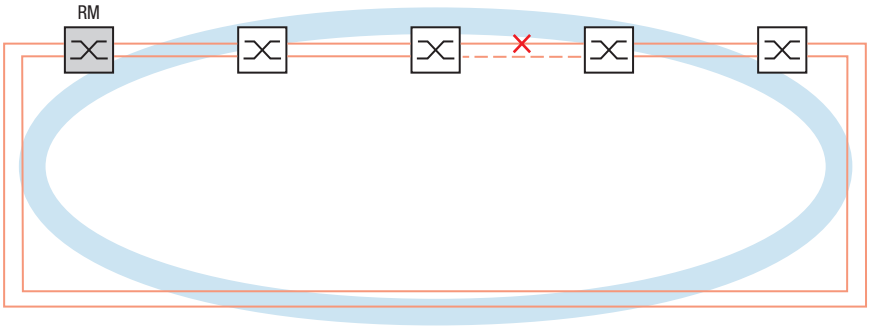


Figura 36: Interrupción de un enlace de un anillo MRP.

Configuración de ejemplo

En el siguiente ejemplo, el switch A y el switch B vinculan dos departamentos entre sí. Los departamentos producen un tráfico demasiado elevado para el ancho de banda del puerto individual. Configure una instancia LAG para el segmento individual del anillo MRP, aumentando el ancho de banda del segmento.

Como requisito previo para la configuración de ejemplo debe comenzar con un anillo MRP operativo.

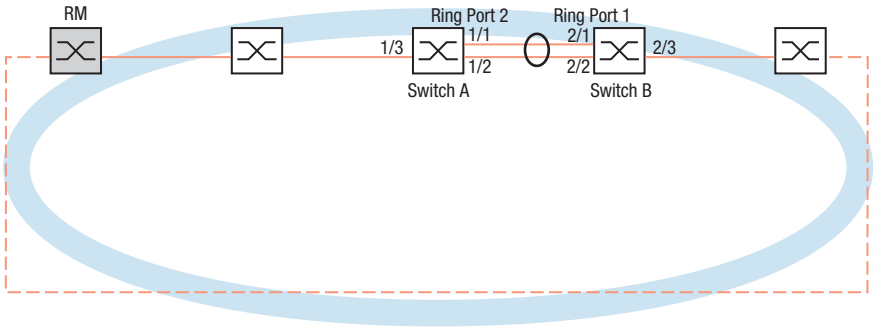


Figura 37: Ejemplo de configuración de MRP a través de LAG

Configure el interruptor A en primer lugar. Para ello, siga los siguientes pasos: A continuación, configure el switch B mediante los mismos pasos, sustituyendo los números de puerto y de puerto de anillo correspondientes.

- ☐ Abra el cuadro de diálogo *Switching > L2-Redundancy > Link Aggregation*.
- ☐ Haga clic en el botón .
  El cuadro de diálogo muestra la ventana *Create*.
- ☐ En la lista desplegable *Trunk port*, seleccione el número de instancia del grupo de agregación de enlaces.
- ☐ En la lista desplegable *Port*, seleccione el puerto *1/1*.

- ☐ Haga clic en el botón *Ok*.
- ☐ Repita los pasos anteriores y seleccione el puerto *1/2*.
- ☐ Haga clic en el botón *Ok*.
- ☐ En la columna *Active ports (min.)*, introduzca `2`, que en este caso se corresponde con el número total de puertos de la instancia. Al combinar MRP y LAG especificará el número total de puertos como *Active ports (min.)*. Cuando el dispositivo detecta una interrupción en un puerto, bloquea los otros puertos de la instancia, lo que hace que el anillo se abra. El Ring Manager detecta que el anillo está abierto y comienza a desviar los datos de su puerto de anillo secundario, lo cual restablece la conectividad con los otros dispositivos de la red.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✔.
- ☐ Abra el cuadro de diálogo *Switching > L2-Redundancy > MRP*.
- ☐ En el cuadro *Ring port 2*, seleccione el puerto `lag/1` en la lista desplegable *Port*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✔.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`link-aggregation add lag/1`	Crea un grupo de agregación de enlaces `lag/1`.
`link-aggregation modify lag/1 addport 1/1`	Añade el puerto *1/1* al grupo de agregación de enlaces.
`link-aggregation modify lag/1 addport 1/2`	Añade el puerto *1/2* al grupo de agregación de enlaces.
`mrp domain modify port secondary lag/1`	Especifica el puerto `lag/1` como puerto del anillo `2`.
`copy config running-config nvm`	Guardar la configuración actual en la memoria no volátil (`nvm`) del perfil de configuración "seleccionado".

13.3 Cliente de anillo HIPER

⚠ ADVERTENCIA

OPERACIÓN INESPERADA DEL EQUIPO

Para ayudar a evitar bucles durante la fase de configuración, configure cada dispositivo de la configuración *HIPER Ring* individualmente. Antes de conectar los trayectos redundantes, complete la configuración de los otros dispositivos de la configuración del anillo.

El incumplimiento de estas instrucciones puede causar la muerte, heridas graves o daños en el equipo.

El concepto de la redundancia de anillo HIPER posibilita la creación de estructuras de red de alta disponibilidad y con forma de anillo. La función de cliente *HIPER Ring* le permite al administrador de red ampliar un anillo HIPER existente o sustituir un dispositivo de cliente que ya esté participando en un anillo HIPER.

Cuando el dispositivo detecta que el enlace de un puerto del anillo se interrumpe, el dispositivo envía un paquete LinkDown a Ring Manager (RM) y vacía la tabla FDB. Una vez que RM recibe el paquete LinkDown, reenvía inmediatamente el flujo de datos a través de los puertos principal y secundario del anillo. De este modo, RM puede mantener la integridad del anillo HIPER.

El dispositivo solamente admite puertos Fast Ethernet y Gigabit Ethernet como puertos de anillo. Además, puede incluir los puertos del anillo en una instancia LAG.

En el estado por defecto, el cliente del anillo HIPER está inactivo, y los puertos principal y secundario están configurados como `no Port`.

Nota: Desactive el Protocolo Spanning Tree (STP) para los puertos del anillo en el cuadro de diálogo *Switching > L2-Redundancy > Spanning Tree > Port*, puesto que los anillos HIPER y STP presentan diferentes tiempos de reacción.

Tabla 34: Configuración de puertos de anillo

Tipo de puerto	Velocidad de bits	Port on	Automatic configuration	Manual configuration
TX	100 Mbit/s	`marcado`	`sin marcar`	*`100 Mbit/s FDX`*
TX	1 Gbit/s	`marcado`	`marcado`	–
Óptico	100 Mbit/s	`marcado`	`sin marcar`	*`100 Mbit/s FDX`*
Óptico	1 Gbit/s	`marcado`	`marcado`	–
Óptico	2.5 Gbit/s	`marcado`	–	*`2.5 Gbit/s FDX`*

13.3.1 Redes VLAN del anillo HIPER

El dispositivo le permite reenviar datos de VLAN a través del anillo HIPER. De este modo, el dispositivo proporciona redundancia para sus datos de VLAN. El dispositivo del anillo reenvía los datos de administración alrededor del anillo, por ejemplo, en la VLAN 1. Para que los datos alcancen la estación de administración de red, los dispositivos del anillo reenvían los datos de administración sin etiquetar a través de los puertos del anillo. Además, especifican los puertos del anillo como miembros de la VLAN 1.

Si cuenta con otras VLAN que transmitan datos por los dispositivos del anillo, estos reenvían los otros datos de VLAN como etiquetados.

Especifique la configuración de la VLAN. Para ello, siga los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Switching > VLAN > Configuration*.
- ☐ Reenvie datos de administración de VLAN sin etiquetar a través de los puertos del anillo.
  En la fila VLAN 1, seleccione el elemento `U` en la lista desplegable en las columnas relacionadas con el puerto del anillo.
- ☐ Bloquee el reenvío de los paquetes de administración a los puertos que no pertenezcan al anillo.
  En la fila VLAN 1, seleccione el elemento `-` en la lista desplegable en las columnas **no** relacionadas con el puerto del anillo.
- ☐ Permita que el dispositivo del anillo reenvíe datos de VLAN hacia y desde puertos que sean miembros de VLAN.
  En la fila VLAN, seleccione el elemento `T` de la lista desplegable en las columnas relacionadas con el puerto del anillo.
- ☐ Abra el cuadro de diálogo *Switching > VLAN > Port*.
- ☐ Asignar la suscripción de VLAN 1 a los puertos del anillo
  Introduzca el valor `1` en la columna *Port-VLAN ID* de las filas de los puertos del anillo.
- ☐ Asigne la suscripción de VLAN a los puertos que no pertenezcan al anillo.
  Introduzca el ID VLAN adecuado en la columna *Port-VLAN ID* de las filas de los puertos que no pertenezcan al anillo.

13.3.2 HIPER Ring a través de LAG

La función *HIPER Ring* permite vincular los dispositivos entre sí a través de un grupo de agregación de enlaces (LAG). Los clientes del anillo y el gestor de anillos se comportan de la misma manera que un anillo sin una instancia LAG.

Si un enlace LAG deja de estar disponible, el otro enlace de la instancia también dejará de estarlo provocando una interrupción en el anillo. Tras detectar una interrupción en el anillo, los puertos afectados envían un paquete Link Down al Ring Manager. El Ring Manager desbloquea el puerto secundario, enviando datos en ambas direcciones alrededor del anillo y responde con un paquete Delete. Tras recibir un paquete Delete, el anillo participa vaciando su FDB.

13.4 Spanning Tree

Nota: El protocolo Spanning Tree es un protocolo para puentes MAC. Por esta razón, en la siguiente descripción se utiliza el concepto "puente" para el dispositivo.

Las redes locales son cada vez mayores. Esto se refiere tanto a la expansión geográfica como a la cantidad de participantes de la red. Por tanto, resulta ventajoso utilizar varios puentes, por ejemplo:

- para reducir la carga de la red en áreas secundarias,
- para establecer conexiones redundantes y
- para superar limitaciones por la distancia.

Sin embargo, el uso de varios puentes con conexiones múltiples y redundantes entre las subredes puede causar bucles y, con ello, la interrupción de la comunicación en la red. Para evitarlo, puede utilizar el protocolo Spanning Tree. Spanning Tree consigue evitar la formación de bucles desactivando, en caso necesario, las conexiones redundantes. La redundancia permite la reactivación sistemática de las conexiones individuales según sea necesario.

RSTP es un desarrollo posterior del protocolo Spanning Tree (STP) y es compatible con el mismo. Si una conexión o un puente no está operativo, el STP requiere un máximo de 30 segundos para reconfigurarse. Esta situación ya no es aceptable en aplicaciones que dependan del factor tiempo. RSTP alcanza tiempos de reconfiguración medios menores de un segundo. Cuando utiliza el RSTP en una topología de anillo con entre 10 y 20 dispositivos, puede incluso obtener tiempos de reconfiguración en milisegundos.

Nota: RSTP convierte una topología de red de Capa 2 con segmentos redundantes en una estructura de árbol (Spanning Tree) que ya no presenta segmentos redundantes. En este caso, uno de los dispositivos asume el rol de puente raíz. El número máximo de dispositivos permitidos en una rama activa (desde el puente raíz hasta la punta de la rama) está especificado por la variable *Max age* para el puente raíz actual. El valor preestablecido para *Max age* es `20`, y puede incrementarse hasta `40`.

Si el dispositivo que funciona como raíz no está operativo y otro dispositivo asume su función, entonces el ajuste *Max age* del nuevo puente raíz determina el número máximo de dispositivos permitidos en una rama.

Nota: El estándar RSTP requiere que todos los dispositivos dentro de una red funcionen con el algoritmo (Rapid) Spanning Tree. Cuando se utilizan simultáneamente STP y RSTP, los segmentos de red mixtos no se benefician de la ventaja de una reconfiguración más rápida que ofrece RSTP.

Un dispositivo que solo admita RSTP funciona junto con los dispositivos MSTP sin asignarse una región MST a sí mismo, sino CST (Common Spanning Tree).

13.4.1 Conceptos básicos

Puesto que el RSTP es un desarrollo posterior del STP, cada una de las siguientes descripciones del STP también se aplican al RSTP.

Funciones del STP

El algoritmo Spanning Tree reduce las topologías de red creadas con puentes y que contengan estructuras de anillo a una estructura de árbol debido a los enlaces redundantes. Durante este proceso, el STP abre estructuras de anillo según las reglas preconfiguradas desactivando las rutas redundantes. Cuando una ruta se interrumpe a causa de que un componente de la red no esté operativo, el STP reactiva de nuevo la ruta previamente desconectada. De este modo se permite que los enlaces redundantes aumenten la disponibilidad de la comunicación.

El STP determina un puente que representa la base de la estructura de árbol del STP. Este puente recibe el nombre de puente raíz.

Características del algoritmo STP:
- reconfiguración automática de la estructura de árbol en caso de que un puente no esté operativo o se interrumpa una ruta de datos,
- la estructura de árbol se estabiliza hasta el tamaño de red máximo,
- estabilización de la topología dentro de un breve período de tiempo,
- la topología predefinible y reproducible mediante el administrador,
- transparencia para los dispositivos finales,
- carga de red baja relativa a la capacidad de transmisión disponible debido a la estructura de árbol creada.

Parámetros del puente

En el contexto del Spanning Tree, cada puente y sus conexiones se describen de manera unívoca con los siguientes parámetros:
- Bridge Identifier ‹Identificación del puente›
- Costes de la ruta raíz de los puertos del puente,
- Port Identifier ‹Identificación del puerto›

Bridge Identifier ‹Identificación del puente›

La identificación del puente se compone de 8 bytes. Los 2 bytes de mayor valor son la prioridad. Al configurar la red, el administrador puede cambiar la configuración por defecto por el número de prioridad, que es `32768` (8000H). Los 6 bytes de menor valor de la identificación del puente son la dirección MAC del puente. La dirección MAC permite que cada puente tenga una identificación única.

El puente con el menor número de identificación tiene la prioridad más alta.

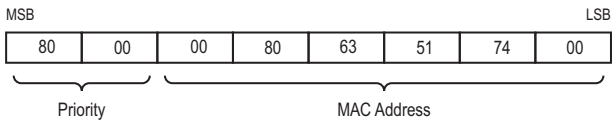


Figura 38: Identificación del puente, ejemplo (valores en notación hexadecimal)

Costes de las ruta raíz

Cada ruta que conecta 2 puentes tiene asignado un coste para la transmisión (coste de ruta). El dispositivo determina este valor en función de la velocidad de transmisión (ver la tabla 35). El dispositivo asigna un coste de ruta más alto con velocidades de transmisión más bajas.

De forma alternativa, el administrador también podrá establecer los costes de ruta. Tal y como hace el dispositivo, el administrador asigna un coste de ruta más alto con velocidades de transmisión más bajas. Puesto que, a fin de cuentas, puede elegir libremente este valor, dispone de una herramienta con la que da preferencia a una ruta determinada en el caso de rutas redundantes.

El coste de ruta raíz es la suma de los costes individuales de aquellas rutas que un paquete de datos debe atravesar desde un puerto de puente conectado hasta el puente raíz.

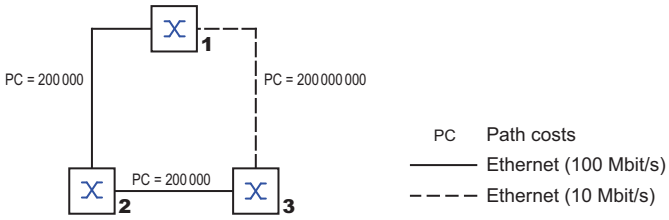


Figura 39: Costes de ruta

Tabla 35: Costes de ruta recomendados para RSTP en función de la velocidad de transferencia.

Velocidad de transferencia	Valor recomendado	Intervalo recomendado	Intervalo posible
≤100 kbit/s	200 000000[1]	20000000-200000000	1-200000000
1 Mbit/s	20000000[a]	2000000-200000000	1-200000000
10 Mbit/s	2000000[a]	200000-20000000	1-200000000
100 Mbit/s	200000[a]	20000-2000000	1-200000000
1 Gbit/s	20000	2000-200000	1-200000000
10 Gbit/s	2000	200-20000	1-200 000000
100 Gbit/s	200	20-2000	1-200000000
1 TBit/s	20	2-200	1-200000000
10 TBit/s	2	1-20	1-200000000

1. Verifique que los puentes de red conformes a IEEE 802.1D-1998 soportando solamente costes de ruta con valores de 16 bits, utilicen el valor 65535 (FFFFH) para los costes de ruta si se utilizan en combinación con puentes que soporten valores de 32 bits.

Port Identifier ‹Identificación del puerto›

La identificación del puerto se compone de 2 bytes. Una parte, el byte de menor valor, contiene el número de puerto físico. Esta parte proporciona una identificación única para el puerto de este puente. La segunda, la parte de mayor valor, es la prioridad del puerto, que el administrador especifica (valor por defecto: `128` También se da en este caso que el puente con el menor número de identificación tiene la prioridad más alta.

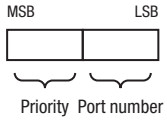


Figura 40: Port Identifier ‹Identificación del puerto›

Max Age y Diámetro

Los valores "Max Age" y "Diámetro" determinan a grandes rasgos la expansión máxima de una red Spanning Tree.

Diámetro

El número de conexiones entre los dispositivos de la red que están más alejados entre sí es conocido como diámetro de la red.

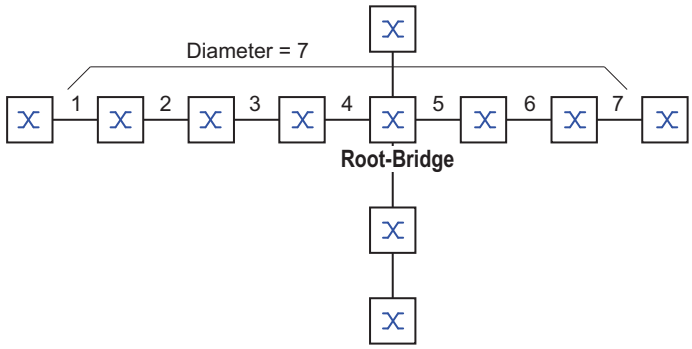


Figura 41: Definición del diámetro

El diámetro de la red que puede lograrse en la red es MaxAge-1.

En la configuración por defecto, MaxAge = 20 y el diámetro máximo que puede lograrse es = 19. Si establece el valor máximo de 40 para MaxAge, el diámetro máximo que puede lograrse es = 39.

MaxAge

Cada BPDU de STP contiene un contador de "MessageAge". Si un puente es atravesado, el contador aumenta en 1.

Antes de reenviar un BPDU de STP, el puente compara el contador "MessageAge" con el valor "MaxAge" especificado en el dispositivo:
- Si MessageAge < MaxAge, el puente reenvía el BPDU de STP al siguiente puente.
- Si MessageAge = MaxAge, el puente descarta el BPDU de STP.

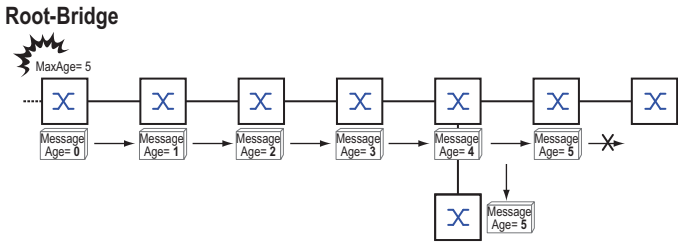


Figura 42: Transmisión de un BPDU de STP en función de MaxAge

13.4.2 Reglas para crear una estructura de árbol

Información del puente

Para determinar la estructura de árbol, los puentes requieren más información sobre los otros puentes que se encuentran en la red.

Para obtener esta información, cada puente envía un BPDU (Unidad de datos de protocolo de puente, Bridge Protocol Data Unit) a otros puentes.

Entre los componentes de un BPDU se encuentran:
- Identificación del puente
- Costes de la ruta raíz
- Identificación del puerto

(véase IEEE 802.1D).

Instalación de la estructura de árbol

El puente con el número de identificación más bajo se denomina puente raíz. Es (o pasará a ser) la raíz de la estructura de árbol.

La estructura del árbol depende de los costes de la ruta raíz. Spanning Tree selecciona la estructura para que los costes de la ruta entre cada puente y el puente raíz sean lo más bajos posible.

- Si hay múltiples rutas con los mismos costes de ruta raíz, el puente más alejado de la raíz decide qué puerto bloquea. Para este fin, utiliza las identificaciones del puente más cercano a la raíz. El puente bloquea el puerto que conduce al puente con el ID más alto numéricamente (un ID numéricamente alto es lógicamente el peor). Si 2 puentes tienen la misma prioridad, el puente con la dirección MAC numéricamente más alta tiene el ID numéricamente más alto, que es lógicamente el peor.
- Si múltiples rutas con los mismos costes de ruta raíz conducen de un puente al mismo puente, el puente más alejado de la raíz utiliza la identificación del puerto del otro puente como último criterio (ver la figura 40). Durante el proceso, el puente bloquea el puerto que conduce al puerto con el ID más alto numéricamente (un ID numéricamente alto es lógicamente el peor). Si 2 puertos tienen la misma prioridad, el puerto con el número de puerto más alto tiene el ID numéricamente más alto, que es lógicamente el peor.

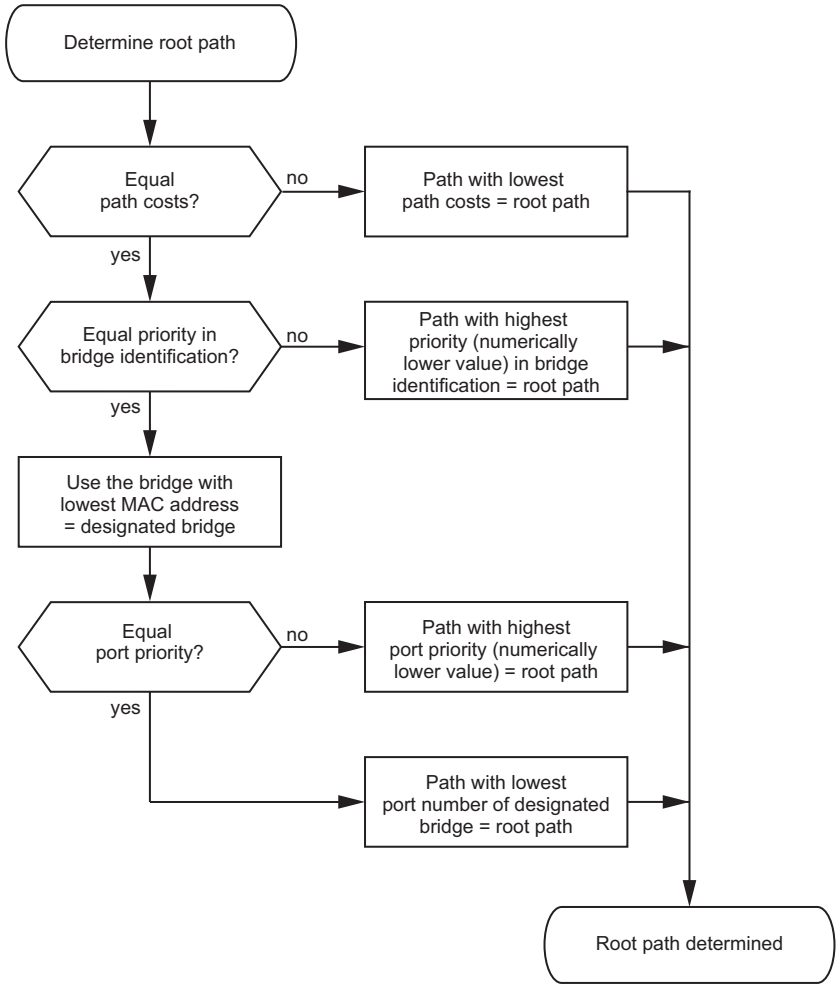


Figura 43: Diagrama de flujo para especificar la ruta raíz

13.4.3 Ejemplos

Ejemplo de cómo determinar la ruta raíz

Puede utilizar el plano de la red (ver la figura 44) para seguir el diagrama de flujo (ver la figura 43) a fin de determinar la ruta raíz. El administrador ha especificado una prioridad para cada puente en la identificación del puente. El puente con el valor numérico más bajo para la identificación de puente asume el rol de puente raíz, en este caso, el puente 1. En el ejemplo, cada ruta secundaria tiene los mismos costes de ruta. El protocolo bloquea la ruta entre el puente 2 y el puente 3, puesto que una conexión del puente 3 a través del puente 2 con el puente raíz daría como resultado mayores costes de ruta.

Cabe destacar la ruta desde el puente 6 hasta el puente raíz:
- La ruta mediante el puente 5 y el puente 3 causa los mismos costes de la ruta raíz que la ruta mediante el puente 4 y el puente 2.
- STP selecciona la ruta a partir del puente que tiene la dirección MAC más baja en la identificación del puente (puente 4 en la ilustración).
- También hay 2 rutas entre el puente 6 y el puente 4.
  Aquí decide la identificación del puerto (Puerto 1 < Puerto 3).

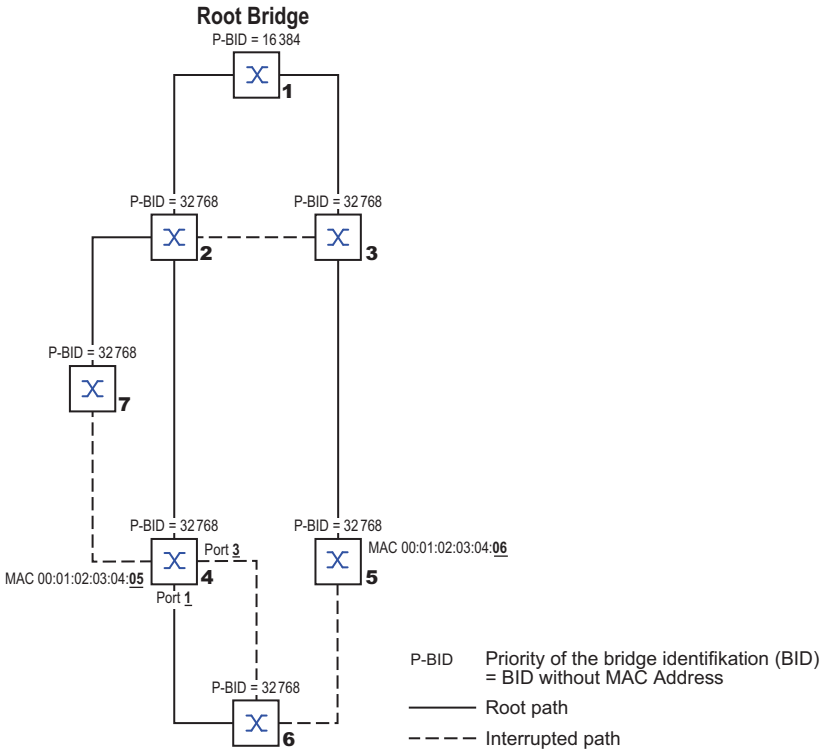


Figura 44: Ejemplo de cómo determinar la ruta raíz

Nota: Si el puente raíz actual deja de estar disponible, la dirección MAC de la identificación del puente determina por sí misma qué puente debe convertirse en el nuevo puente raíz, dado que el administrador no modifica los valores por defecto de las prioridades de los puentes en la identificación del puente, excepto para el puente raíz.

Ejemplo de manipulación de la ruta raíz

Puede utilizar el plano de la red (ver la figura 45) para seguir el diagrama de flujo (ver la figura 43) a fin de determinar la ruta raíz. El administrador ha llevado a cabo los siguientes pasos:

- Ha dejado la configuración por defecto de 32768 (8000H) para cada puente, excepto para el puente 1 y el puente 5
- Ha asignado al puente 1 el valor 16384 (4000H), por lo que ahora es el puente raíz.
- Para el puente 5, ha asignado el valor 28672 (7000H).

El protocolo bloquea la ruta entre el puente 2 y el puente 3, puesto que una conexión del puente 3 a través del puente 2 con el puente raíz daría como resultado mayores costes de ruta.

Cabe destacar la ruta desde el puente 6 hasta el puente raíz:

▶ Los puentes seleccionan una ruta a través del puente 5, puesto que el valor 28672 para la prioridad en la identificación del puente es menor que el valor 32768.

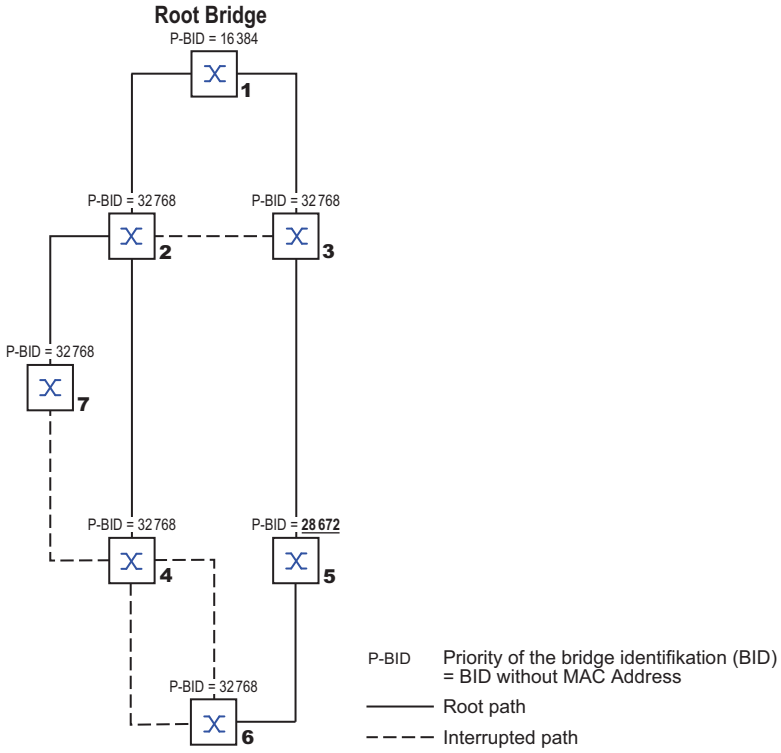


Figura 45: Ejemplo de manipulación de la ruta raíz

Ejemplo de manipulación de la estructura de árbol

El administrador pronto se da cuenta de que esta configuración con el puente 1 como puente raíz no es válida. En las rutas desde el puente 1 hasta el puente 2 y desde el puente 1 hasta el puente 3, los paquetes de control que el puente raíz envía a los otros puentes se agrupan.

Si el administrador configura el puente 2 como el puente raíz, la carga de los paquetes de control en las subredes se distribuye de manera más uniforme. El resultado es la configuración que se muestra aquí (ver la figura 46). Los costes de ruta para la mayoría de los puentes hasta el puente raíz han disminuido.

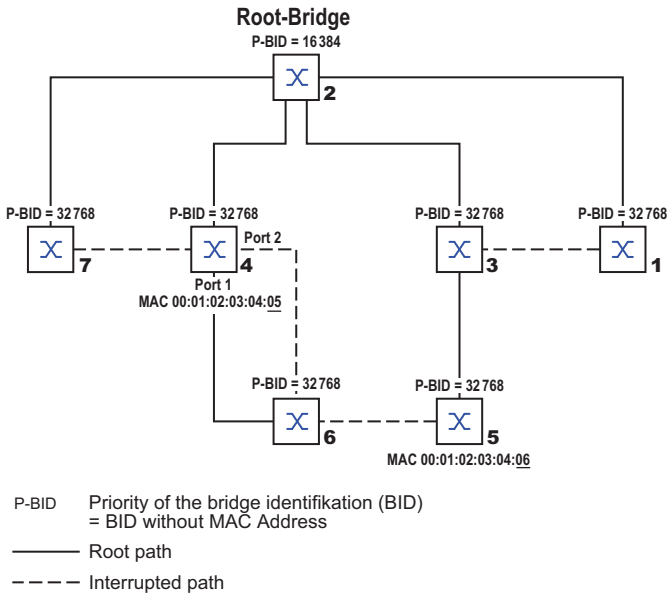


Figura 46: Ejemplo de manipulación de la estructura de árbol

13.5 Protocolo Rapid Spanning Tree

El RSTP utiliza el mismo algoritmo que el STP para determinar la estructura de árbol. Si un enlace o un puente no está operativo, RSTP solo cambia los parámetros y añade nuevos parámetros y mecanismos que aceleran la reconfiguración.

Los puertos desempeñan un papel importante en este sentido.

13.5.1 Roles del puerto

RSTP asigna a cada puerto del puente los siguientes roles (ver la figura 47):

- Puerto raíz:
  Este es el puerto en el que el puente recibe los paquetes de datos con los costes de ruta más bajos desde el puente raíz.
  Si hay múltiples puertos con costes de ruta igual de bajos, el ID del puente que lleva hasta la raíz (puente designado) decide a cuál de sus puertos se le asigna el rol de puerto raíz por el puente más alejado de la raíz.
  Si un puente tienen múltiples puertos con costes de ruta igual de bajos hasta el mismo puente, el puente utiliza el ID del puerto del puente que lleva hasta la raíz (puente designado) para decidir qué puerto selecciona localmente como puerto raíz (ver la figura 43).
  El propio puente raíz no tienen un puerto raíz.
- Puerto designado:
  El puente de un segmento de red que tiene los costes de ruta más bajos es el puente designado.
  Si más de un puente tiene los mismos costes de ruta raíz, el puente con el valor de identificación del puente más bajo se convierte en el puente designado. El puerto designado de este puente es el que conecta un segmento de red que conduzca lejos del puente raíz. Si un puente está conectado a un segmento de red con más de un puerto (a través de un concentrador, por ejemplo), el puente asigna el rol de puerto designado al puerto con mejor ID del puerto.
- Edge port ‹Puerto periférico›
  Cada segmento de red sin puentes RSTP adicionales se conecta con exactamente un puerto designado. En este caso, este puerto designado es, al mismo tiempo, un puerto periférico. Un puerto periférico se distingue por el hecho de que no recibe BPDU de RST (Unidades de datos de protocolo de puente de Rapid Spanning Tree).
- Alternate port ‹Puerto alternativo›
  Si la conexión al puente raíz se pierde, este puerto bloqueado asume la tarea de puerto raíz. El puerto alternativo proporciona un apoyo para la conexión con el puente raíz.

- Backup port ‹Puerto de reserva›
  Se trata de un puerto bloqueado que sirve como reserva en caso de que la conexión con el puerto designado de este segmento de red se pierda (sin puentes RSTP).
- Disabled port ‹Puerto desactivado›
  Se trata de un puerto que no participa en la operación Spanning Tree, es decir, el puerto está desconectado o no tiene conexión.

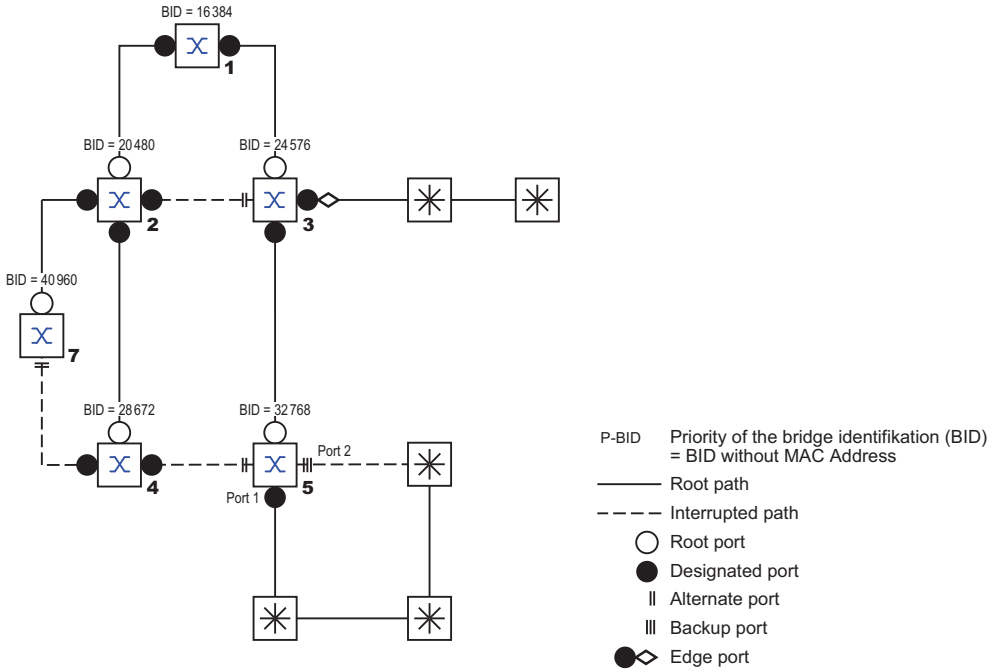


Figura 47: Asignación de roles de puertos

13.5.2 Estados de los puertos

En función de la estructura de árbol y del estado de las rutas de conexión seleccionadas, el RSTP asigna a los puertos un estado.

Tabla 36: Relación entre los valores de estado de los puertos en STP y RSTP

Estado del puerto STP	Estado del puerto del puente administrador	Operatividad MAC	Estado del puerto RSTP	Topología activa (rol del puerto)
DISABLED	Desactivado	FALSE	Discarding[1]	Excluido (desactivado)
DISABLED	Activado	FALSE	Discarding[a]	Excluido (desactivado)
BLOCKING	Activado	TRUE	Discarding[2].	Excluido (alternativo, reserva)
LISTENING	Activado	TRUE	Discarding[b]	Incluido (raíz, designado)
LEARNING	Activado	TRUE	Learning	Incluido (raíz, designado)
FORWARDING	Activado	TRUE	Forwarding	Incluido (raíz, designado)

1. El dot1d-MIB muestra "Desactivado".
2. El dot1d-MIB muestra "Bloqueado"

Significado de los estados del puerto RSTP:
- Desactivado: el puerto no pertenece a la topología activa
- Descartado: no se recibe ninguna dirección en FDB, no hay tráfico de datos excepto para los BPDU de STP
- Aprendizaje: aprendizaje de direcciones activo (FDB), no hay tráfico de datos excepto por los BPDU de STP
- Reenvío: aprendizaje de direcciones activo (FDB), envío y recepción de cada tipo de paquete (no solo BPDU de STP)

13.5.3 Vector de prioridad de Spanning Tree

Para repartir roles a los puertos, los puentes RSTP intercambian la información de configuración. Esta información se denomina Spanning Tree Priority Vector (vector de prioridad de Spanning Tree). Forma parte de los BPDU de RSTP y contiene la siguiente información:
- Identificación del puente raíz
- Costes de la ruta raíz del puente emisor
- Identificación del puente emisor
- Identificación del puerto a través del cual fue enviado el mensaje
- Identificación del puerto a través del cual fue recibido el mensaje

En función de esta información, los puentes que participan en RSTP pueden determinar los roles de puerto por sí mismos y definir los estados de sus propios puertos.

13.5.4 Reconfiguración rápida

¿Por qué RST reacciona más rápido que STP ante una interrupción de la ruta raíz?
- Introducción de los puertos periféricos:
  Durante una reconfiguración, RSTP establece un puerto periférico en el modo de transmisión una vez transcurridos 3 segundos (configuración por defecto). Para comprobar que ningún puerto que envíe BPDU está conectado, RSTP espera a que pase el valor "Hello Time". Cuando verifica que un dispositivo final está y permanece conectado a este puerto, no hay intervalos de espera en caso de reconfiguración en este puerto.
- Introducción de los puertos alternativos:
  Como las funciones del puerto están ya distribuidas en un funcionamiento normal, un puente puede cambiar inmediatamente del puerto raíz al puerto alternativo después de que se haya perdido la conexión con el puente raíz.
- Comunicación con puentes vecinos (conexiones punto a punto):
  La comunicación descentralizada y directa entre puentes vecinos permite la reacción sin intervalos de espera ante los cambios de estado en la topología Spanning Tree.
- Tabla de direcciones:
  Con STP, la antigüedad de las entradas en la FDB determina la actualización de la comunicación. El RSTP borra inmediatamente y envía las entradas de los puertos implicados al cambiar la configuración.
- Reacción ante eventos:
  Sin tener que adherirse a especificaciones de tiempo, RSTP reacciona inmediatamente a eventos como interrupciones de conexión, restablecimientos de conexión, etc.

Nota: Los paquetes de datos pueden duplicarse o enviarse al receptor en el pedido equivocado durante la fase de reconfiguración de la topología RSTP. También puede usar el Protocolo Spanning Tree o seleccionar otro procedimiento de redundancia descrito en este manual.

13.5.5 Configuración del dispositivo

⚠ ADVERTENCIA

OPERACIÓN INESPERADA DEL EQUIPO

Para ayudar a evitar bucles durante la fase de configuración, configure cada dispositivo de la configuración *Spanning Tree* individualmente. Antes de conectar los trayectos redundantes, complete la configuración de los otros dispositivos de la configuración *Spanning Tree*.

El incumplimiento de estas instrucciones puede causar la muerte, heridas graves o daños en el equipo.

RSTP configura la topología de red de manera completamente autónoma. El dispositivo con la menor prioridad se convierte automáticamente en el puente raíz. Sin embargo, para definir una estructura de red específica, debe especificar un dispositivo como puente raíz. En general, un dispositivo del backbone debe asumir este rol.

Lleve a cabo los siguientes pasos:
- ☐ Cree la red según sus necesidades, inicialmente sin líneas redundantes.
- ☐ Desactive el control de flujo de los puertos participantes.
  Si el control de flujo y la función de redundancia están activos al mismo tiempo, es posible que la función de redundancia opere de un modo distinto al deseado. (Configuración por defecto: control de flujo desactivado globalmente y activado en todos los puertos).
- ☐ Desactive MRP en cada dispositivo.
- ☐ Active la función Spanning Tree en cada dispositivo de la red.
  En la configuración por defecto, Spanning Tree está activado en el dispositivo.

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Switching > L2-Redundancy > Spanning Tree > Global*.
- ☐ Active la función.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✓.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`spanning-tree operation`	Activa Spanning Tree.
`show spanning-tree global`	Muestra los parámetros para la comprobación.

Conecte ahora las líneas redundantes.

Defina los ajustes para el dispositivo que asume el papel de puente raíz.

Lleve a cabo los siguientes pasos:

- ☐ En el campo *Priority*, introduzca un valor numérico inferior.
  El puente con el ID de puente numéricamente más bajo tiene la prioridad más alta y pasa a ser el puente raíz de la red.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✓.

`spanning-tree mst priority 0 <0..61440>`	Especifica la prioridad del puente del dispositivo. **Nota:** Especifique la prioridad del puente dentro del rango de `0..61440` en pasos de 4096.

Después de guardar, el cuadro de diálogo muestra la siguiente información:
- La casilla *Bridge is root* está marcada.
- El campo *Root port* muestra el valor `0.0`.
- El campo *Root path cost* muestra el valor `0`.

`show spanning-tree global`	Muestra los parámetros para la comprobación.

- ☐ Si es necesario, cambie los valores en los campos *Forward delay [s]* y *Max age*.
  - – El puente raíz transmite los valores modificados a los otros dispositivos.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✓.

`spanning-tree forward-time <4..30>`	Especifica el tiempo que desea que transcurra para el cambio de estado en segundos.
`spanning-tree max-age <6..40>`	Especifica la longitud máxima admisible de una rama, por ejemplo, el número de dispositivos que hay hasta el puente raíz.
`show spanning-tree global`	Muestra los parámetros para la comprobación.

Nota: Los parámetros *Forward delay [s]* y *Max age* tienen la siguiente relación:

Forward delay [s] ≥ (*Max age*/2) + 1

Si especifica valores en los campos que contradicen esta relación, el dispositivo los sustituye por los últimos valores válidos o por el valor por defecto.

Nota: Si es posible, no cambie el valor en el campo "Hello Time".

Compruebe los siguientes valores en los otros dispositivos:
- ID del puerto (prioridad del puerto y dirección MAC) del dispositivo correspondiente y el puente raíz.
- Número del puerto del dispositivo que lleva al puente raíz.
- Coste de la ruta del puerto raíz del dispositivo hasta el puente raíz.

Lleve a cabo los siguientes pasos:

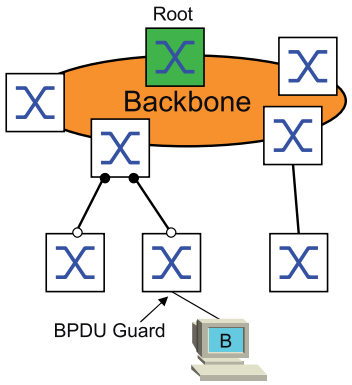
`show spanning-tree global`	Muestra los parámetros para la comprobación.

13.5.6 Guards

El dispositivo le permite activar varias funciones de protección (guards) en los puertos del dispositivo.

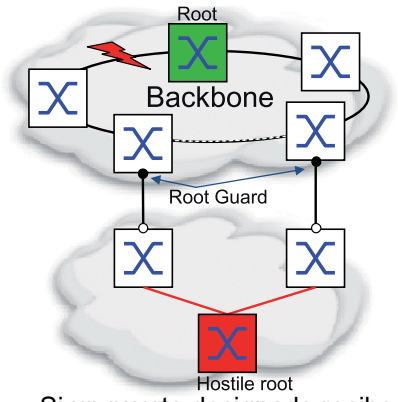
La siguiente protección ayuda a proteger su red frente a configuraciones incorrectas, bucles y ataques con BPDU de STP:

- BPDU Guard: para puertos periféricos especificados manualmente (puertos del dispositivo final)
  Active esta función de protección globalmente en el dispositivo.



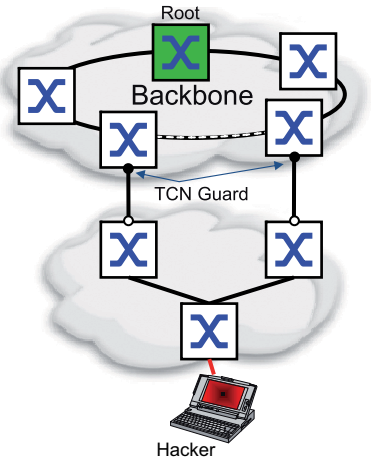
Normalmente, los puertos del dispositivo final no reciben ningún BPDU de STP. Si, aun así, un atacante intenta introducir BPDU de STP en este puerto, el dispositivo desactiva el puerto.

- Root Guard: para puertos designados
  Active esta función de protección de manera individual para cada puerto del dispositivo.



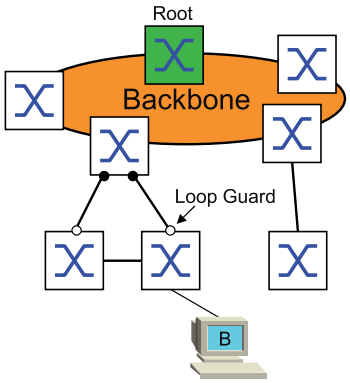
Si un puerto designado recibe un BPDU de STP con información de una ruta mejor al puente raíz, el dispositivo descartará el BPDU de STP y establecerá el estado de la transmisión del puerto en `discarding` en lugar de `root`.
Si no recibe paquetes BPDU de STP con información de una ruta mejor al puente raíz, tras 2 x *Hello time [s]*, el dispositivo vuelve a establecer el estado del puerto en un valor indicado según el rol del puerto.

- TCN Guard – para puertos que reciben BPDU de STP con una marca de cambio de topología
  Active esta función de protección de manera individual para cada puerto del dispositivo.



Si la función de protección está activada, el dispositivo ignorará las marcas de cambio de topología en los BPDU de STP recibidos. Esto no cambia el contenido de la tabla de direcciones (FDB) del puerto del dispositivo. Sin embargo, la información adicional del BPDU que cambia la topología es procesada por el dispositivo.

- Loop Guard: para puertos raíz, alternativos y de reserva
  Active esta función de protección de manera individual para cada puerto del dispositivo.



Si el puerto no recibe ningún BPDU de STP, la función de protección ayuda a evitar la transmisión del estado de un puerto que se haya modificado involuntariamente a `forwarding`. Si esta situación se produce, el dispositivo designa el estado de bucle del puerto como incoherente, pero no reenvía paquetes de datos.

Activación del BPDU Guard

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Switching > L2-Redundancy > Spanning Tree > Global*.
- ☐ Marque la casilla *BPDU guard*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ☑.

`enable`	Cambiar al modo Privileged EXEC.

`configure`	Cambiar al modo de configuración.
`spanning-tree bpdu-guard`	Activa el BPDU Guard.
`show spanning-tree global`	Muestra los parámetros para la comprobación.

- ☐ Abra el cuadro de diálogo *Switching > L2-Redundancy > Spanning Tree > Port*.
- ☐ Cambie a la pestaña *CIST*.
- ☐ Para los puertos del dispositivo final, marque la casilla de la columna *Admin edge port*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✔.

`interface <x/y>`	Cambiar al modo de configuración de la interfaz `<x/y>`.
`spanning-tree edge-port`	Designa el puerto como puerto de dispositivo final (puerto periférico).
`show spanning-tree port x/y`	Muestra los parámetros para la comprobación.
`exit`	Abandona el modo de interfaz.

Cuando un puerto periférico recibe un BPDU de STP, el dispositivo reacciona de la siguiente manera:

- ▶ El dispositivo desactiva este puerto.
  En la pestaña *Configuration* del cuadro de diálogo *Basic Settings > Port*, la casilla para este puerto de la columna *Port on* está en la posición `unmarked`.
- ▶ El dispositivo designa el puerto.

Puede determinar si un puerto se ha desactivado porque ha recibido un BPDU. Para ello, siga los siguientes pasos:

En la pestaña *Guards* del cuadro de diálogo *Switching > L2-Redundancy > Spanning Tree > Port*, la casilla de la columna *BPDU guard effect* está en la posición `marked`.

`show spanning-tree port x/y`	Muestra los parámetros del puerto para su comprobación. El valor del parámetro *BPDU guard effect* es `enabled`.

Restablezca el estado del puerto del dispositivo al valor `forwarding`. Para ello, siga los siguientes pasos:

- ☐ Si el puerto aún recibe BPDU:
  - – Elimine la definición manual como puerto periférico (puerto de dispositivo final).
    o bien
  - – Desactive el BPDU Guard.
- ☐ Active el puerto del dispositivo de nuevo.

Activación de Root Guard / TCN Guard / Loop Guard

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Switching > L2-Redundancy > Spanning Tree > Port*.
- ☐ Cambie a la pestaña *Guards*.
- ☐ Para los puertos designados, seleccione la casilla de la columna *Root guard*.
- ☐ Para los puertos que reciban BPDU de STP con la marca de cambio de topología, seleccione la casilla de la columna *TCN guard*.
- ☐ Para puertos raíz, alternativos o de reserva, marque la casilla de la columna *Loop guard*.

Nota: Las funciones *Root guard* y *Loop guard* son mutuamente exclusivas. Si intenta activar la función *Root guard* mientras la función *Loop guard* está activa, el dispositivo desactiva la función *Loop guard*.

- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✔.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`interface <x/y>`	Cambiar al modo de configuración de la interfaz `<x/y>`.
`spanning-tree guard-root`	Activa Root Guard en el puerto designado.
`spanning-tree guard-tcn`	Activa TCN Guard en los puertos que reciben BPDU de STP con una marca de cambio de topología.
`spanning-tree guard-loop`	Activa Loop Guard en un puerto raíz, alternativo o de reserva.
`exit`	Abandona el modo de interfaz.
`show spanning-tree port x/y`	Muestra los parámetros del puerto para su comprobación.

13.6 Dual RSTP (MCSESM-E)

Las aplicaciones industriales requieren que sus redes tengan una alta disponibilidad. Esto también implica mantener tiempos de interrupción breves y determinísticos para la comunicación en casos en los que uno de los componentes de la red no esté operativo.

Las topologías en anillo permiten ofrecer tiempos de interrupción breves con un uso mínimo de los recursos. Mediante el protocolo *Spanning Tree*, el tiempo de interrupción depende del tamaño de la red. Para optimizar el tiempo de interrupción, puede separar grandes redes *Spanning Tree* en segmentos de anillo más pequeños.

La función *Dual RSTP* se utiliza con la función *RCP*. Si utiliza la función *RCP*, tendrá la opción de acoplar uno o más anillos RSTP con la instancia RSTP en un anillo principal. Al acoplar dos segmentos *Spanning Tree*, el anillo secundario representa una instancia de RSTP independiente para la que se aplica la configuración de la función *Dual RSTP*. Esta instancia de *Dual RSTP* funciona de manera independiente de la instancia de RSTP del anillo principal y de los demás anillos secundarios. Si el protocolo RSTP es utilizado en tan solo uno de los anillos que desea acoplar, no necesitará la función *Dual RSTP*.

13.7 Agregación de enlaces

La función *Link Aggregation* mediante el método de un solo switch le permite superar las 2 limitaciones con los enlaces de Ethernet, es decir, el ancho de banda y la redundancia

La función *Link Aggregation* le permite superar las limitaciones de ancho de banda de los puertos individuales. La función *Link Aggregation* le permite combinar 2 o más enlaces en paralelo, creando 1 enlace lógico entre 2 dispositivos. Los enlaces paralelos aumentan el ancho de banda para el tráfico entre 2 dispositivos.

Normalmente puede utilizar la función *Link Aggregation* en el backbone de la red. La función proporciona una forma económica de aumentar el ancho de banda.

Además, la función *Link Aggregation* proporciona una tolerancia a errores de redundancia sin contratiempos. Si un enlace deja de estar disponible, con 2 o más enlaces configurados en paralelo, los otros enlaces del grupo continuarán reenviando el tráfico.

La configuración por defecto para una nueva instancia de *Link Aggregation* es la siguiente:
- En la columna *Active*, la casilla está marcada.
- En la columna *Send trap (Link up/down)*, la casilla está marcada.
- En la columna *Static link aggregation*, la casilla no está marcada.
- En la columna *Active ports (min.)*, el valor es `1`.

13.7.1 Métodos de funcionamiento

El dispositivo funciona con el método de un solo switch. El método de un solo switch proporciona una forma económica de aumentar su red. El método de un solo switch especifica que es necesario un dispositivo en cada lado de un enlace para proporcionar los puertos físicos. El dispositivo equilibra la carga de tráfico a través de los puertos miembros del grupo.

El dispositivo también utiliza el método de misma velocidad de enlace en el que los puertos miembros del grupo son enlaces Full-Dúplex punto a punto con la misma velocidad de transmisión. El primer puerto que añade al grupo es el puerto principal, y determina el ancho de banda para los otros puertos miembros del grupo de agregación de enlaces.

El dispositivo le permite configurar hasta 2 grupos de agregación de enlaces. El número de puertos disponibles por grupo de agregación de enlaces depende del dispositivo.

13.7.2 Ejemplo de agregación de enlaces

⚠ ADVERTENCIA

OPERACIÓN INESPERADA DEL EQUIPO

Para ayudar a evitar bucles durante la fase de configuración, configure cada dispositivo de la configuración *Link Aggregation* individualmente. Antes de conectar los trayectos redundantes, complete la configuración de los otros dispositivos de la configuración *Link Aggregation*.

El incumplimiento de estas instrucciones puede causar la muerte, heridas graves o daños en el equipo.

Conecte varias estaciones de trabajo mediante un grupo de enlace agregado entre el switch 1 y el 2. Al agregar varios enlaces, se consiguen velocidades más altas sin tener que mejorar el hardware.

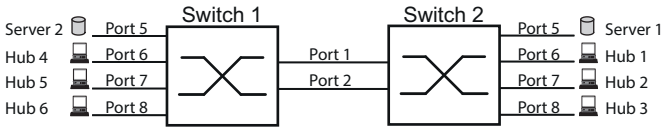


Figura 48: Red de switch a switch de agregación de enlaces

Configure los switches 1 y 2 en la interfaz gráfica de usuario. Para ello, siga los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Switching > L2-Redundancy > Link Aggregation*.
- ☐ Haga clic en el botón .
  El cuadro de diálogo muestra la ventana *Create*.
- ☐ En la lista desplegable *Trunk port*, seleccione el número de instancia del grupo de agregación de enlaces.
- ☐ En la lista desplegable *Port*, seleccione el puerto *1/1*.
- ☐ Haga clic en el botón *Ok*.
- ☐ Repita los pasos anteriores y seleccione el puerto *1/2*.
- ☐ Haga clic en el botón *Ok*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón .

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`link-aggregation add lag/1`	Crea un grupo de agregación de enlaces `lag/1`.
`link-aggregation modify lag/1 addport 1/1`	Añade el puerto *1/1* al grupo de agregación de enlaces.
`link-aggregation modify lag/1 addport 1/2`	Añade el puerto *1/2* al grupo de agregación de enlaces.

13.8 Link Backup

Link Backup proporciona un enlace redundante para el tráfico en dispositivos de Capa 2. Si el dispositivo detecta un error en el enlace principal, el dispositivo transfiere el tráfico al enlace de reserva. Por lo general, Link Backup se utiliza en redes empresariales o de proveedor de servicios.

Establezca los enlaces de reserva en parejas, uno como principal y otro como reserva. Al proporcionar redundancia para las redes empresariales, por ejemplo, el dispositivo le permite establecer más de una pareja. El número máximo de parejas de Link Backup es: número total de puertos físicos / 2. Además, cuando cambia el estado de un puerto participante en una pareja de Link Backup, el dispositivo envía una trampa SNMP.

Al configurar las parejas de Link Backup, recuerde las siguientes reglas:
- Una pareja de enlaces consiste en una combinación de puertos físicos. Por ejemplo, un puerto de 100 Mbits y otro puerto SFP de 1000 Mbits.
- Un puerto específico es miembro de una pareja de Link Backup en un determinado momento.
- Verifique que los puertos de una pareja de Link Backup son miembros de la misma VLAN con el mismo ID VLAN. Si el puerto principal o el puerto de reserva son miembros de una VLAN, asigne el segundo puerto de la pareja a la misma VLAN.

La configuración por defecto para esta función no se activa sin parejas de Link Backup.

Nota: Verifique que el protocolo Spanning Tree está desactivado en los puertos de Link Backup.

13.8.1 Descripción de conmutación por recuperación

Link Backup también le permite configurar una opción de conmutación por recuperación. Si activa la función de conmutación por recuperación y el enlace principal vuelve a funcionar de manera normal, el dispositivo primero bloqueará el tráfico en el puerto de reserva y, a continuación, lo desviará al puerto principal. Este proceso ayuda a evitar que el dispositivo provoque bucles en la red.

Si el puerto principal vuelve al estado activo del enlace, el dispositivo admite los 2 modos de funcionamiento:
- Si desactiva *Fail back*, el puerto principal permanece en estado de bloqueo hasta que el enlace de reserva falla.
- Si activa *Fail back*, y una vez finalizado el temporizador de *Fail back delay [s]*, el puerto principal vuelve al estado de reenvío y el puerto de reserva cambia a desactivado.

En los casos referidos anteriormente, el puerto que obliga a su enlace a reenviar el tráfico, primero envía un paquete "flush FDB" al dispositivo remoto. El paquete flush permite que el dispositivo remoto aprenda de nuevo las direcciones MAC.

13.8.2 Configuración de ejemplo

⚠ ADVERTENCIA

OPERACIÓN INESPERADA DEL EQUIPO

Para ayudar a evitar bucles durante la fase de configuración, configure cada dispositivo de la configuración *Link Backup* individualmente. Antes de conectar los trayectos redundantes, complete la configuración de los otros dispositivos de la configuración *Link Backup*.

El incumplimiento de estas instrucciones puede causar la muerte, heridas graves o daños en el equipo.

En el ejemplo de red a continuación, se conectan los puertos *2/3* y *2/4* en el switch A con los switches Uplink B y C. Al establecer los puertos como pareja de Link Backup, uno de los puertos reenvía el tráfico y el otro puerto permanece en el modo de bloqueo.

El principal, el puerto *2/3* del switch A, es el puerto activo y reenvía el tráfico al puerto 1 del switch B. El puerto *2/4* del switch A es el puerto de reserva y bloquea el tráfico.

Si el switch A desactiva el puerto *2/3* a causa de un error reconocido, el puerto *2/4* del switch A comienza a reenviar el tráfico al puerto 2 del switch C.

Si el puerto *2/3* vuelve al estado activo, "no shutdown", con *Fail back* activado, y *Fail back delay [s]* ajustado en 30 segundos. Una vez que finalice el temporizador, el puerto *2/4* primero bloquea el tráfico y, a continuación, el puerto *2/3* comienza a reenviar el tráfico.

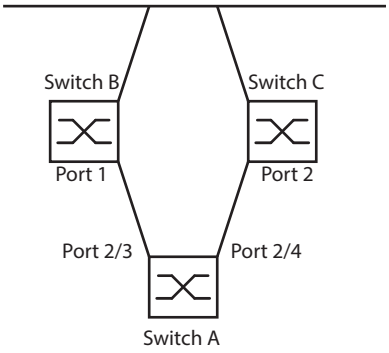


Figura 49: Ejemplo de red Link Backup

Las siguientes tablas incluyen ejemplos de los parámetros para la configuración del switch A.

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Switching > L2-Redundancy > Link Backup*.
- ☐ Introduzca una nueva pareja de Link Backup en la tabla:
  - ☐ Haga clic en el botón .
    El cuadro de diálogo muestra la ventana *Create*.
  - ☐ En la lista desplegable *Primary port*, seleccione el puerto *2/3*.
    En la lista desplegable *Backup port*, seleccione el puerto *2/4*.
  - ☐ Haga clic en el botón *Ok*.
- ☐ En el cuadro de texto *Description*, introduzca `Link_Backup_1` como nombre de la pareja de reserva.

- ☐ Para activar la función *Fail back* de la pareja de Link Backup, marque la casilla *Fail back*.
- ☐ Establezca el temporizador de conmutación por recuperación de la pareja de Link Backup e introduzca `30` en *Fail back delay [s]*.
- ☐ Para activar la pareja de Link Backup, marque la casilla *Active*.
- ☐ Para activar la función, seleccione el botón de opción *On* en el cuadro *Operation*.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`interface 2/3`	Cambie al modo de configuración de la interfaz *2/3*.
`link-backup add 2/4`	Crea una instancia de Link Backup en la que el puerto *2/3* es el puerto principal y el puerto *2/4* es el puerto de reserva.
`link-backup modify 2/4 description Link_Backup_1`	Especifica la secuencia `Link_Backup_1` como el nombre de la pareja de reserva.
`link-backup modify 2/4 failback-status enable`	Activar el temporizador de conmutación por recuperación.
`link-backup modify 2/4 failback-time 30`	Especificar el tiempo de retardo de conmutación por recuperación en `30` s.
`link-backup modify 2/4 status enable`	Activar la instancia de Link Backup.
`exit`	Cambiar al modo de configuración.
`link-backup operation`	Activar la función *Link Backup* globalmente en el dispositivo.

13.9 FuseNet

Los protocolos *FuseNet* permiten acoplar anillos que están funcionando con uno de los siguientes protocolos de redundancia:

- MRP
- Anillo HIPER
- RSTP

Nota: El requisito previo para acoplar una red al anillo principal mediante el protocolo *Ring/Network Coupling* es que la red conectada contenga solamente dispositivos de red que admitan el protocolo *Ring/Network Coupling*.

Utilice la tabla siguiente para seleccionar el protocolo de acoplamiento *FuseNet* que desee utilizar en su red:

Anillo principal	**Red conectada**		
	MRP	**Anillo HIPER**	**RSTP**
MRP	*Sub Ring*[1)]	– *Redundant Coupling Protocol* – *Ring/Network Coupling*	– *Redundant Coupling Protocol* – *Ring/Network Coupling*
Anillo HIPER	*Sub Ring*	*Ring/Network Coupling*	– *Redundant Coupling Protocol* – *Ring/Network Coupling*
RSTP	*Redundant Coupling Protocol*	*Redundant Coupling Protocol*	*Dual RSTP* + *Redundant Coupling Protocol*

– ningún protocolo de acoplamiento adecuado

1) con *MRP* configurado en VLAN diferentes

13.10 Subring ‹Anillo secundario›

La función *Sub Ring* es una extensión del Protocolo de redundancia de medios (MRP, Media Redundancy Protocol). Esta función le permite acoplar un anillo secundario a un anillo principal mediante varias estructuras de red.

El protocolo de anillo secundario proporciona redundancia a los dispositivos al acoplar al anillo principal los dos extremos de una red que, de lo contrario, sería plana.

El establecimiento de anillos secundarios tiene las siguientes ventajas:
- Integración del nuevo segmento de red en el concepto de redundancia mediante el acoplamiento.
- Los anillos secundarios permiten la integración sencilla de nuevas áreas en las redes existentes.
- Los anillos secundarios le permiten realizar una asignación de la estructura organizativa de un área en una topología de red.
- En un anillo MRP, en caso de redundancia, los intervalos de conmutación del anillo secundario son del tipo < 100 ms.

13.10.1 Descripción del anillo secundario

El concepto de anillo secundario le permite acoplar nuevos segmentos de red a los dispositivos aptos en un anillo existente (anillo principal). Los dispositivos con los que acopla el anillo secundario al anillo principal son administradores de anillo secundario o Subring Managers (SRM).

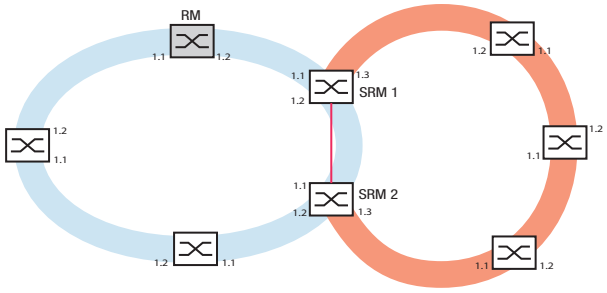


Figura 50: Ejemplo de estructura de anillo secundario
anillo azul = anillo principal
anillo naranja = anillo secundario
línea roja = enlace redundante de anillo secundario
SRM = Subring Manager
RM = Ring Manager

Los dispositivos que pueden actuar como Subring Managers admiten hasta 8 instancias y, por tanto, administran hasta 8 anillos secundarios a la vez.

La función *Sub Ring* le permite integrar dispositivos que admitan MRP como participantes. Los dispositivos con los que acopla el anillo secundario al anillo principal requieren la función *Sub Ring* Manager.

Cada anillo secundario puede comprender hasta 200 participantes, sin incluir a los propios Subring Managers y a los dispositivos entre los Subring Managers y el anillo principal.

Las siguientes figuras muestran ejemplos de posibles topologías de anillo secundario:

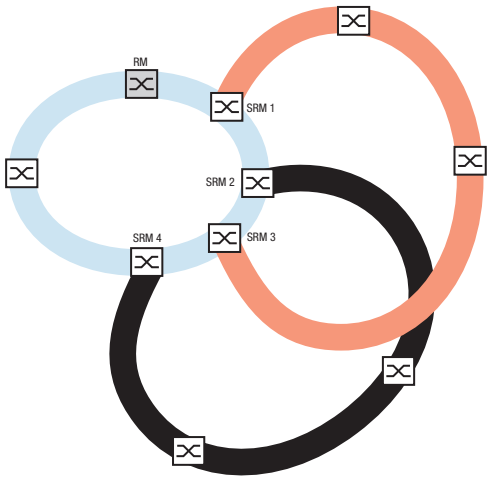


Figura 51: Ejemplo de una estructura solapada de anillo secundario

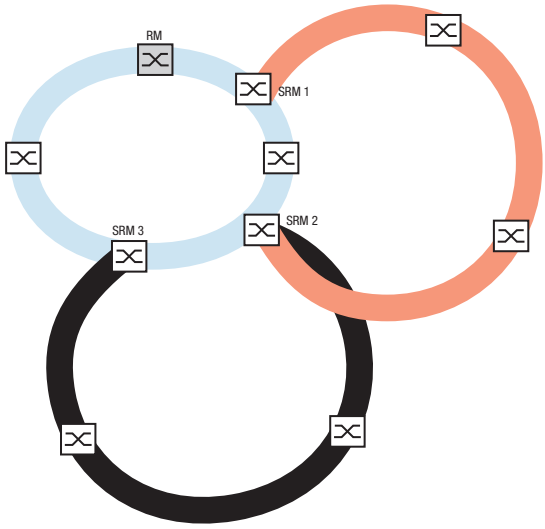


Figura 52: Caso especial: un Subring Manager administra 2 anillos secundarios (2 instancias). El Subring Manager puede administrar hasta 8 instancias.

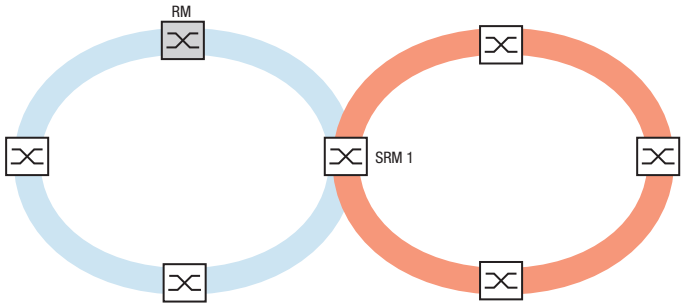


Figura 53: Caso especial: un Subring Manager administra los dos extremos de un anillo secundario en puertos diferentes (Single Subring Manager).

Nota: En los ejemplos anteriores, los Subring Managers solo acoplan anillos secundarios a anillos principales existentes. La función *Sub Ring* prohíbe los anillos secundarios en cascada, por ejemplo, el acoplamiento de un nuevo anillo secundario con un anillo secundario existente.

Si utiliza MRP para el anillo principal y el secundario, especifique la configuración de la VLAN del siguiente modo:

- VLAN X para el anillo principal
  - en los puertos de anillo de los participantes del anillo principal
  - en los puertos del anillo principal del Subring Manager
- VLAN Y para el anillo secundario
  - en los puertos de anillo de los participantes del anillo secundario
  - en los puertos del anillo secundario del Subring Manager

  Puede utilizar la misma VLAN para varios anillos secundarios.

13.10.2 Ejemplo de anillo secundario

En el siguiente ejemplo, se acopla un nuevo segmento de red con 3 dispositivos en un anillo principal existente que utiliza el protocolo MRP. Al acoplar la red en ambos extremos en lugar de en solo uno, el anillo secundario proporciona una mayor disponibilidad con la configuración correspondiente.

Acople el nuevo segmento de red como anillo secundario. Acople el anillo secundario a los dispositivos existentes del anillo principal que utilicen los siguientes tipos de configuración.

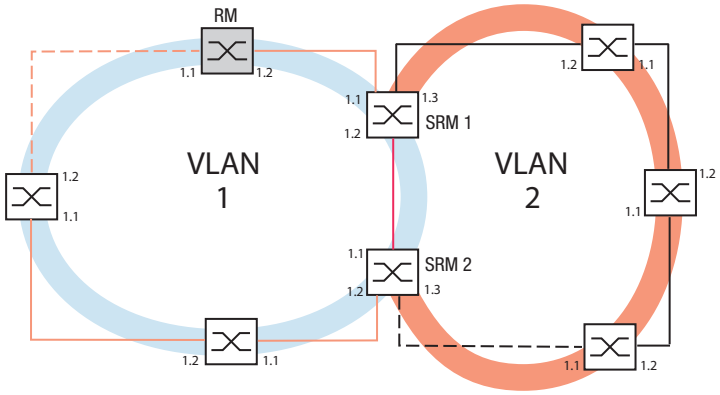


Figura 54: Ejemplo de estructura de anillo secundario
línea naranja = miembros del anillo principal en la VLAN 1
línea negra = miembros del anillo secundario en la VLAN 2
línea naranja discontinua = bucle del anillo principal abierto
línea negra discontinua = bucle del anillo secundario abierto
línea roja = miembro del enlace redundante en la VLAN 1
SRM = Subring Manager
RM = Ring Manager

Para configurar el anillo secundario, realice los siguientes pasos:

- ☐ Configure los tres dispositivos del nuevo segmento de red como participantes en un anillo MRP:
  - Configure la velocidad de transmisión y el modo dúplex para los puertos de anillo según la siguiente tabla:

Tabla 37: Configuración de los puertos para crear puertos de anillo secundario

Tipo de puerto	Velocidad de bits	Port on	Automatic configuration	Manual configuration
TX	100 Mbit/s	marcado	sin marcar	*100 Mbit/s FDX*
TX	1 Gbit/s	marcado	marcado	–

Tabla 37: Configuración de los puertos para crear puertos de anillo secundario

Tipo de puerto	Velocidad de bits	Port on	Automatic configuration	Manual configuration
Óptico	100 Mbit/s	marcado	sin marcar	*100 Mbit/s FDX*
Óptico	1 Gbit/s	marcado	marcado	–
Óptico	2.5 Gbit/s	marcado	–	*2.5 Gbit/s FDX*

Los siguientes pasos contienen ajustes adicionales para la configuración del anillo secundario:

- ☐ Para evitar bucles durante la configuración, desactive la función de Subring Manager en los dispositivos del anillo principal y del anillo secundario. Tras configurar por completo cada dispositivo participante en el anillo principal y los anillos secundarios, active la función *Sub Ring* globalmente y los Subring Managers.
- ☐ Desactive la función RSTP en los puertos del anillo MRP utilizados en el anillo secundario.
- ☐ Verifique que la función *Link Aggregation* no está activa en los puertos participantes en el anillo principal y el anillo secundario.
- ☐ Especifique una suscripción a VLAN diferente para los puertos del anillo principal y los puertos del anillo secundario, aunque el anillo principal utilice el protocolo MRP. Por ejemplo, utilice el ID VLAN 1 para el anillo principal y el enlace redundante y, a continuación, utilice el ID VLAN 2 para el anillo secundario.
  - Para los dispositivos participantes en el anillo principal, por ejemplo, abra el cuadro de diálogo *Switching > VLAN > Configuration*. Cree la VLAN 1 en la tabla de VLAN estática. Para etiquetar los puertos del anillo principal para la suscripción a la VLAN 1, seleccione el elemento T en la lista desplegable de las columnas de los puertos correspondientes.
  - Para los dispositivos participantes en el anillo secundario, siga el paso anterior y añada los puertos a la VLAN 2 en la tabla de VLAN estática.
- ☐ Active la función *MRP* para los dispositivos del anillo principal y del anillo secundario.
  - En el cuadro de diálogo *Switching > L2-Redundancy > MRP*, configure los 2 puertos de anillo participantes en el anillo principal en los dispositivos del anillo principal.
  - Para los dispositivos participantes en el anillo secundario, siga el paso anterior y configure los 2 puertos de anillo participantes en el anillo secundario en los dispositivos del anillo secundario.
  - Asigne a los dispositivos del anillo principal y del anillo secundario el mismo identificador de dominio de MRP. Si solo utiliza Schneider Electric dispositivos, son suficientes los valores predeterminados para el identificador de dominio de MRP.

Nota: El *MRP domain* es una secuencia de 16 números en un rango de 0 a 255. El valor por defecto es 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255. Un *MRP domain* compuesto íntegramente por ceros no es válido.

El cuadro de diálogo *Sub Ring* le permite cambiar el identificador de dominio de MRP. También puede utilizar la interfaz de línea de comando. Para ello, siga los siguientes pasos:

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`mrp domain delete`	Borra los dominios de MRP actuales.
`mrp domain add domain-id 0.0.1.1.2.2.3.4.4.111.222.123.0.0.66.99`	Genera un nuevo dominio de MRP con el ID de dominio de MRP indicado. Cualquier cambio posterior de dominio MRP se aplicará a este identificador de dominio.

13.10.3 Configuración de ejemplo de anillo secundario

⚠ ADVERTENCIA

OPERACIÓN INESPERADA DEL EQUIPO

Para ayudar a evitar bucles durante la fase de configuración, configure cada dispositivo de la configuración *Sub Ring* individualmente. Antes de conectar los trayectos redundantes, complete la configuración de los otros dispositivos de la configuración del anillo.

El incumplimiento de estas instrucciones puede causar la muerte, heridas graves o daños en el equipo.

Nota: Así se evitan bucles durante la fase de configuración. Configure uno a uno todos los dispositivos del anillo secundario. Antes de activar el enlace redundante, configure por completo todos los dispositivos del anillo secundario.

Configure los 2 Subring Managers del ejemplo: Para ello, siga los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Switching > L2-Redundancy > Sub Ring*.
- ☐ Para añadir una entrada de tabla, haga clic en el botón .
- ☐ En la columna *Port*, seleccione el puerto que acoplará el dispositivo con el anillo secundario.
  Utilice el puerto *1/3* para este ejemplo.
  Para llevar a cabo el acoplamiento, utilice uno de los puertos disponibles a excepción de los puertos que ya estén conectados al anillo principal.
- ☐ En la columna *Name*, asigne un nombre al anillo secundario.
  Para este ejemplo, introduzca `Test`.
- ☐ En la columna *SRM mode*, seleccione el modo Subring Manager.
  De esta forma, especifica qué puerto se convierte en el administrador redundante para el acoplamiento del anillo secundario con el anillo principal.
  Las posibilidades de acoplamiento son:
  - `manager`
    Si especifica ambos Subring Managers con el mismo valor, el dispositivo con la dirección MAC más alta administra el enlace redundante.
  - `redundant manager`
    Este dispositivo administra el enlace redundante siempre que haya especificado el otro Subring Manager como `manager`. De lo contrario, el dispositivo con la dirección MAC más alta administra el enlace redundante.

  Especifique el Subring Manager 1 como `manager`, de acuerdo con la figura de este ejemplo.
- ☐ Deje los valores de la columna *VLAN* y la columna *MRP domain* como están.
  Los valores por defecto son correctos para la configuración del ejemplo.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón .

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`sub-ring add 1`	Genera un nuevo anillo secundario con el ID de anillo secundario `1`.
`sub-ring modify 1 port 1/3`	Especificar el puerto *1/3* como puerto del anillo secundario.

`sub-ring modify 1 name Test`	Asignar el nombre `Test` al anillo secundario `1`.
`sub-ring modify 1 mode manager`	Asignar el modo `manager` al anillo secundario `1`.
`show sub-ring ring`	Mostrar el estado de los anillos secundarios en este dispositivo.
`show sub-ring global`	Mostrar el estado global de los anillos secundarios en este dispositivo.

- ☐ Configure de la misma forma el segundo Subring Manager.
  Especifique el Subring Manager 2 como `redundant manager`, de acuerdo con la figura de este ejemplo.

- ☐ Para activar la función Subring Manager, marque la casilla *Active* de la fila correspondiente.
- ☐ Tras configurar ambos Subring Managers y los dispositivos participantes en el anillo secundario, active la función y cierre el enlace redundante.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✓.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`sub-ring enable 1`	Active el anillo secundario `1`.
`sub-ring enable 2`	Active el anillo secundario `2`.
`exit`	Cambiar al modo Privileged EXEC.
`show sub-ring ring <Domain ID>`	Mostrar los ajustes de los anillos secundarios seleccionados.
`show sub-ring global`	Mostrar los ajustes globales del anillo secundario.
`copy config running-config nvm profile Test`	Guardar los ajustes actuales en el perfil de configuración de nombre `Test` en la memoria no volátil (`nvm`).

13.11 Anillo secundario con LAG

⚠ ADVERTENCIA

OPERACIÓN INESPERADA DEL EQUIPO

Para ayudar a evitar bucles durante la fase de configuración, configure cada dispositivo de la configuración *Sub Ring* individualmente. Antes de conectar los trayectos redundantes, complete la configuración de los otros dispositivos de la configuración del anillo.

El incumplimiento de estas instrucciones puede causar la muerte, heridas graves o daños en el equipo.

Si existen al menos dos líneas de conexión redundantes paralelas (conocidas como troncos) entre dos dispositivos y estas líneas se combinan en una conexión lógica, esta es una conexión de agregación de enlaces (LAG).

El dispositivo le permite utilizar los puertos LAG como puertos de anillo con el protocolo *Sub Ring*.

13.11.1 Ejemplo

El siguiente ejemplo es una configuración sencilla entre un anillo MRP y un anillo secundario.

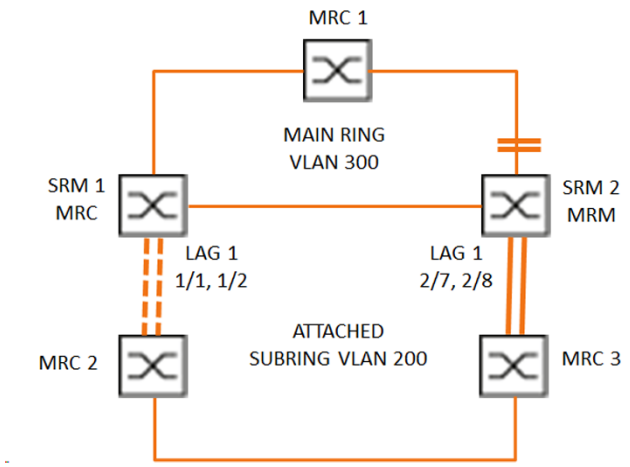


Figura 55: Anillo secundario con agregación de enlace

En la tabla siguiente se describen los roles de los dispositivos tal y como se ven en la ilustración anterior. La tabla proporciona información sobre cómo utilizar los puertos de los anillos y los de anillos secundarios como puertos LAG.

Tabla 38: Dispositivos, puertos y roles

Nombre del dispositivo	Puerto del anillo	Rol de anillo principal	Rol de anillo secundario	Puerto de anillo secundario
MRC1	1/3, 1/4	MRP client ‹Cliente MRP›	-	-
SRM1	1/3, 1/4	MRP client ‹Cliente MRP›	Administrador redundante	lag/1
SRM2	2/4, 2/5	Administrador de MRP	Manager	lag/1
MRC2	lag/1, 1/3	-	MRP client ‹Cliente MRP›	-
MRC3	lag/1, 1/3	-	MRP client ‹Cliente MRP›	-

Configuración de anillo MRP

Los dispositivos que participan en el anillo principal son miembros de la VLAN 300.

Lleve a cabo los siguientes pasos:

`SRM2`

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`mrp domain add default-domain`	Genera un nuevo dominio de MRP con el ID `default-domain`.
`mrp domain modify port primary 2/4`	Especifica el puerto *2/4* como puerto del anillo `1`.
`mrp domain modify port secondary 2/5`	Especifica el puerto *2/5* como puerto del anillo `2`.
`mrp domain modify mode manager`	Especifique que el dispositivo actúa como *Ring manager*. No active la función *Ring manager* en ningún otro dispositivo.
`mrp domain modify operation enable`	Activa el anillo MRP.
`mrp domain modify vlan 300`	Especifica el ID VLAN `300`.
`mrp operation`	Active la función *MRP* en el dispositivo.

`MRC1, SRM1`

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`mrp domain add default-domain`	Genera un nuevo dominio de MRP con el ID `default-domain`.
`mrp domain modify port primary 1/3`	Especifica el puerto *1/3* como puerto del anillo `1`.
`mrp domain modify port secondary 1/4`	Especifica el puerto *1/4* como puerto del anillo `2`.

`mrp domain modify mode client`	Especifica el rol de dispositivo como cliente del anillo.
`mrp domain modify operation enable`	Activa el anillo MRP.
`mrp domain modify vlan 300`	Especifica el ID VLAN `300`.
`mrp operation`	Active la función *MRP* en el dispositivo.

Configuración de anillo secundario

Los dispositivos que participan en el anillo secundario adjunto son miembros de la VLAN 200.

Lleve a cabo los siguientes pasos:

`SRM1`

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`link-aggregation add lag/1`	Crea un grupo de agregación de enlaces `lag/1`.
`link-aggregation modify lag/1 addport 1/1`	Añade el puerto *1/1* al grupo de agregación de enlaces.
`link-aggregation modify lag/1 addport 1/2`	Añade el puerto *1/2* al grupo de agregación de enlaces.
`link-aggregation modify lag/1 adminmode`	Active el grupo de agregación de enlaces.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`sub-ring add 1`	Genera un nuevo anillo secundario con el ID de anillo secundario `1`.
`sub-ring modify 1 name SRM1`	Asigne el nombre `SRM1` al anillo secundario `1`.
`sub-ring modify 1 mode redundant-manager vlan 200 port lag/1`	Asigne al dispositivo el rol de `Sub-ring redundant manager`en el anillo secundario `1`. Si se cierra el anillo secundario, el dispositivo bloqueará el puerto del anillo. La VLAN `200` es la establecida para el ID VLAN del dominio. El puerto `lag/1` se establece como miembro en la VLAN `200`.
`sub-ring enable 1`	Active el anillo secundario `1`.
`sub-ring operation`	Active la funcionalidad de Subring Manager global en este dispositivo.

`SRM2`

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`link-aggregation add lag/1`	Crea un grupo de agregación de enlaces `lag/1`.

`link-aggregation modify lag/1 addport 2/7`	Añade el puerto *2/7* al grupo de agregación de enlaces.
`link-aggregation modify lag/1 addport 2/8`	Añade el puerto *2/8* al grupo de agregación de enlaces.
`link-aggregation modify lag/1 adminmode`	Active el grupo de agregación de enlaces.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`sub-ring add 1`	Genera un nuevo anillo secundario con el ID de anillo secundario `1`.
`sub-ring modify 1 mode manager vlan 200 port lag/1`	Asigne al dispositivo el rol de `Subring manager` en el anillo secundario `1`. La VLAN `200` es la establecida para el ID VLAN del dominio. El puerto `lag/1` se establece como miembro en la VLAN `200`.
`sub-ring modify 1 name SRM2`	Asignar el nombre `SRM2` al anillo secundario `1`.
`sub-ring enable 1`	Active el anillo secundario `1`.
`sub-ring operation`	Active la funcionalidad de Subring Manager global en este dispositivo.

`MRC 2, 3`

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`mrp domain add default-domain`	Genera un nuevo dominio de MRP con el ID `default-domain`.
`mrp domain modify port primary lag/1`	Especifica el puerto `lag/1` como puerto del anillo `1`.
`mrp domain modify port secondary 1/3`	Especifica el puerto *1/3* como puerto del anillo `2`.
`mrp domain modify mode client`	Especifica el rol de dispositivo como cliente del anillo.
`mrp domain modify operation enable`	Activa el anillo MRP.
`mrp domain modify vlan 200`	Especifica el ID VLAN `200`.
`mrp operation`	Active la función *MRP* en el dispositivo.

Desactivar STP

Desactive la función *Spanning Tree* en cada puerto que haya especificado como MRP o puerto de anillo secundario. En el siguiente ejemplo se utiliza el puerto *1/3*.

Lleve a cabo los siguientes pasos:

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`interface 1/3`	Cambie al modo de configuración de la interfaz *1/3*.
`no spanning-tree operation`	Desactive la función *Spanning Tree* en el puerto.

13.12 Ring/Network Coupling

Basándose en un anillo, la función *Ring/Network Coupling* acopla los anillos o segmentos de red de manera redundante. *Ring/Network Coupling* conecta 2 anillos/segmentos de red a través de 2 rutas diferentes.

Si los dispositivos en la red acoplada son Schneider Electric, la función *Ring/Network Coupling* admite el acoplamiento según los protocolos del anillo en los anillos principal y secundario:
- HIPER Ring
- Anillo Fast HIPER
- MRP

La función *Ring/Network Coupling* también puede acoplar segmentos de red de estructuras de bus y de malla.

13.12.1 Métodos de Ring/Network Coupling

Acoplamiento de un switch

Dos puertos de **un** dispositivo del primer anillo/red se conectan a un puerto cada uno de dos dispositivos del segundo anillo/red (ver la figura 56). Con el método de acoplamiento de un switch, la línea principal reenvía datos y el dispositivo bloquea la línea redundante.

Si la línea principal ya no está en funcionamiento, el dispositivo desbloquea inmediatamente la línea redundante. Cuando la línea principal se restaura, el dispositivo bloquea los datos en la línea redundante. La línea principal reenvía datos de nuevo.

El acoplamiento de anillo detecta y gestiona los errores en 500 ms (por lo general, 150 ms).

Acoplamiento de dos switches

Un puerto de cada uno de los **dos** dispositivos del primer anillo/red se conecta a un puerto cada uno de los dos dispositivos del segundo anillo/segmento de red (ver la figura 58).

El dispositivo de la línea redundante y el dispositivo de la línea principal utilizan paquetes de control para informar al otro sobre sus estados operativos mediante Ethernet o la línea de control.

Si la línea principal ya no está en funcionamiento, el dispositivo redundante (Stand-by) desbloquea inmediatamente la línea redundante. En cuanto la línea principal se restaure, el dispositivo de la línea principal informa al dispositivo redundante. El dispositivo Stand-by bloquea los datos en la línea redundante. La línea principal reenvía datos de nuevo.

El acoplamiento de anillo detecta y gestiona los errores en 500 ms (por lo general, 150 ms).

El tipo de configuración de acoplamiento se determina principalmente mediante la topología de la red y el nivel deseado de disponibilidad (ver la tabla 39).

Tabla 39: Criterios de selección de los tipos de configuración para acoplamiento redundante

	Acoplamiento de un switch	Acoplamiento de dos switches	Acoplamiento de dos switches con línea de control
Application	Los 2 dispositivos implicados no están distribuidos de forma favorable en cuanto a la topología. Por tanto, establecer un enlace entre ellos implicaría un gran esfuerzo en un acoplamiento de dos switches.	Los 2 dispositivos implicados están distribuidos de forma favorable en cuanto a la topología. La instalación de una línea de control implicaría un gran esfuerzo.	Los 2 dispositivos implicados están distribuidos de forma favorable en cuanto a la topología. La instalación de una línea de control no implicaría un gran esfuerzo.
Desventaja	En caso de no estar disponible el switch configurado para el acoplamiento redundante, no habrá conexión entre las redes.	Mayor esfuerzo para la conexión de 2 dispositivos a la red (en comparación con el acoplamiento de un switch).	Mayor esfuerzo para la conexión de los dos dispositivos a la red (en comparación con el acoplamiento de un switch y el acoplamiento de dos switches).
Ventaja	Menor esfuerzo para la conexión de los 2 dispositivos a la red (en comparación con el acoplamiento de dos switches).	Si uno de los dispositivos configurados para el acoplamiento redundante deja de estar disponible, las redes acopladas seguirán conectadas.	Si uno de los dispositivos configurados para el acoplamiento redundante deja de estar disponible, las redes acopladas seguirán conectadas. La determinación de socios entre los dispositivos acoplados se produce de manera más segura y rápida que sin línea de control.

13.12.2 Preparación del Ring/Network Coupling

⚠ ADVERTENCIA

OPERACIÓN INESPERADA DEL EQUIPO

Para ayudar a evitar bucles durante la fase de configuración, configure cada dispositivo de la configuración *Ring/Network Coupling* individualmente. Antes de conectar los trayectos redundantes, complete la configuración de los otros dispositivos de la configuración del anillo.

Para ayudar a evitar bucles, utilice la función *Ring/Network Coupling* únicamente en puertos en los que el protocolo Rapid Spanning Tree esté inactivo.

El incumplimiento de estas instrucciones puede causar la muerte, heridas graves o daños en el equipo.

Mediante las imágenes del cuadro de diálogo, defina el rol de los dispositivos en el *Ring/Network Coupling*.

En las siguientes capturas de pantalla y diagramas, se utilizan las siguientes convenciones:
- Los cuadros y las líneas en azul marcan los dispositivos o conexiones de los elementos que se describen.
- Las líneas continuas indican una conexión principal.
- Las líneas discontinuas indican una conexión en stand-by.
- La línea de puntos designa la línea de control.

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Switching > L2-Redundancy > Ring/Network Coupling*.
- ☐ En el cuadro *Mode*, en la lista de opciones *Type*, seleccione el botón de opción requerido.
  - `one-switch coupling`
  - `two-switch coupling, master`
  - `two-switch coupling, slave`
  - `two-switch coupling with control line, master`
  - `two-switch coupling with control line, slave`

Acoplamiento de un switch

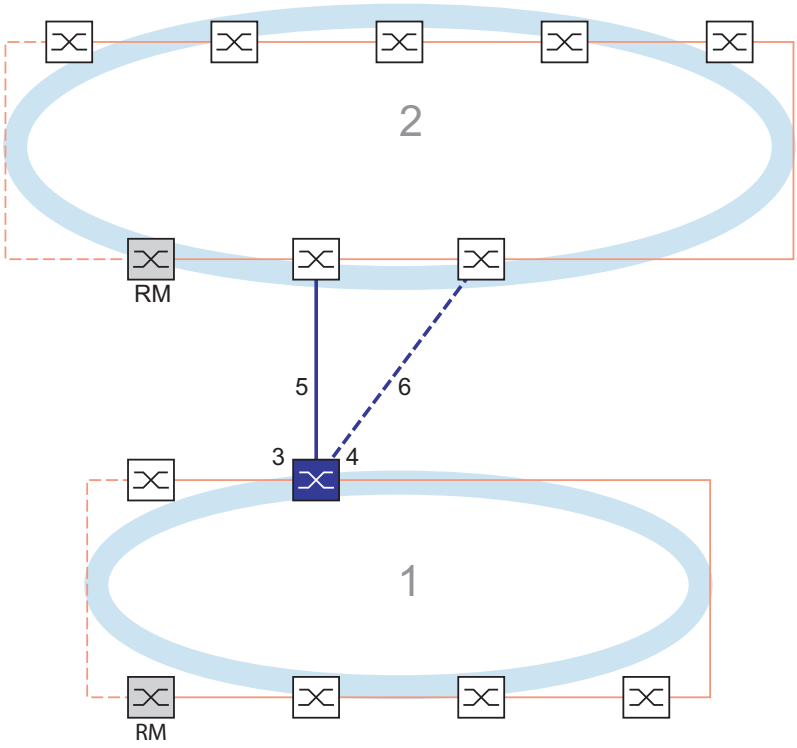


Figura 56: Ejemplo de acoplamiento de Un Switch
1: Anillo
2: Backbone
3: Puerto de acoplamiento socio
4: Puerto de acoplamiento
5: Línea principal
6: Línea redundante

La línea principal conectada al puerto de acoplamiento socio, que se indica mediante la línea azul continua, permite el acoplamiento entre las dos redes en el modo de funcionamiento normal. Si la línea principal deja de estar operativa, la línea redundante conectada al puerto de acoplamiento, que se indica mediante la línea azul discontinua, asume la función de acoplamiento del anillo/red. **Un** switch lleva a cabo el cambio de acoplamiento.

Los siguientes ajustes se aplican al dispositivo que se muestra en azul en el gráfico seleccionado.

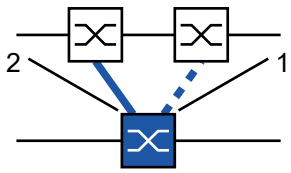


Figura 57: Acoplamiento de un switch
1: Puerto de acoplamiento
2: Puerto de acoplamiento socio

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Switching > L2-Redundancy > Ring/Network Coupling*.
- ☐ En el cuadro *Mode*, en la lista de opciones *Type*, seleccione el botón de opción `one-switch coupling`.

Nota: Configure el *Partner coupling port* y los puertos de anillo en puertos diferentes.

- ☐ En el cuadro *Coupling port*, seleccione el puerto al que conecta la línea redundante en la lista desplegable *Port*.
- ☐ En el cuadro *Partner coupling port*, seleccione el puerto al que conecta la línea principal en la lista desplegable *Port*.
- ☐ Para activar la función, seleccione el botón de opción *On* en el cuadro *Operation*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✔.
- ☐ Conecte la línea redundante al puerto de acoplamiento socio.
  En el cuadro *Partner coupling port*, el campo *State* muestra el estado actual del puerto de acoplamiento socio.
- ☐ Conecte la línea principal al puerto de acoplamiento.
  En el cuadro *Coupling port*, el campo *State* muestra el estado actual del puerto de acoplamiento.

En el cuadro *Information*, el campo *Redundancy available* muestra si la redundancia está disponible. El campo *Configuration failure* muestra si los ajustes están completos y son correctos.

Para los puertos de acoplamiento, lleve a cabo los siguientes pasos:

Nota: Para los puertos de acoplamiento, se requiere la siguiente configuración:

- ☐ Abra el cuadro de diálogo *Basic Settings > Port*, pestaña *Configuration*.
- ☐ Para los puertos seleccionados como puertos de acoplamiento, especifique los ajustes de acuerdo con los parámetros de la siguiente tabla.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✔.

Tabla 40: Configuración de puertos de anillo

Tipo de puerto	Velocidad de bits	Port on	Automatic configuration	Manual configuration
TX	100 Mbit/s	marcado	sin marcar	*100 Mbit/s FDX*
TX	1 Gbit/s	marcado	marcado	–
Óptico	100 Mbit/s	marcado	sin marcar	*100 Mbit/s FDX*
Óptico	1 Gbit/s	marcado	marcado	–
Óptico	2.5 Gbit/s	marcado	–	*2.5 Gbit/s FDX*

Si ha configurado VLAN en los puertos de acoplamiento, especifique los ajustes de VLAN en los puertos de acoplamiento y los puertos de acoplamiento socios: Para ello, siga los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Switching > VLAN > Port*.
- ☐ Cambie la configuración de *Port-VLAN ID* al valor del ID VLAN configurado en los puertos.
- ☐ Desactive la casilla *Ingress filtering* para ambos puertos de acoplamiento.
- ☐ Abra el cuadro de diálogo *Switching > VLAN > Configuration*.
- ☐ Para etiquetar las conexiones redundantes para la `VLAN 1` y la asignación de VLAN, introduzca el valor `T` en las celdas correspondientes para ambos puertos de acoplamiento en la fila `VLAN 1`.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✓.

Los dispositivos del acoplamiento envían paquetes redundantes con la prioridad máxima en `VLAN 1`.

- ☐ En el cuadro *Configuration*, en la lista de opciones *Redundancy mode*, especifique el tipo de redundancia:
  - ▶ Con la configuración *redundant ring/network coupling*, la línea principal o la redundante está activa. La configuración permite que los dispositivos alternen entre ambas líneas.
  - ▶ Si activa la configuración *extended redundancy*, la línea principal y la redundante están activas simultáneamente. Esta configuración le permite añadir redundancia a la red de acoplamiento. Si la conexión entre los dispositivos del acoplamiento en la segunda red deja de estar operativa, los dispositivos del acoplamiento siguen trasmitiendo y recibiendo datos.

Nota: Durante el intervalo de reconfiguración, es posible que se produzcan duplicaciones en los paquetes. Por esa razón, si sus dispositivos detectan duplicaciones de los paquetes, seleccione esta configuración.

El modo *Coupling mode* describe el tipo de red backbone a la que conecta la red en anillo (ver la figura 56).

- ☐ En el cuadro *Configuration*, en la lista de opciones *Coupling mode*, especifique el tipo de la segunda red:
  - ☐ Si se conecta a una red en anillo, seleccione el botón de opción *ring coupling*.
  - ☐ Si se conecta a una estructura de bus o malla, seleccione el botón de opción *network coupling*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✓.

Restablezca los ajustes de acoplamiento al estado por defecto. Para ello, siga los siguientes pasos:

- ☐ Haga clic en el botón ☰ y, a continuación, en el elemento *Reset*.

Acoplamiento de dos switches

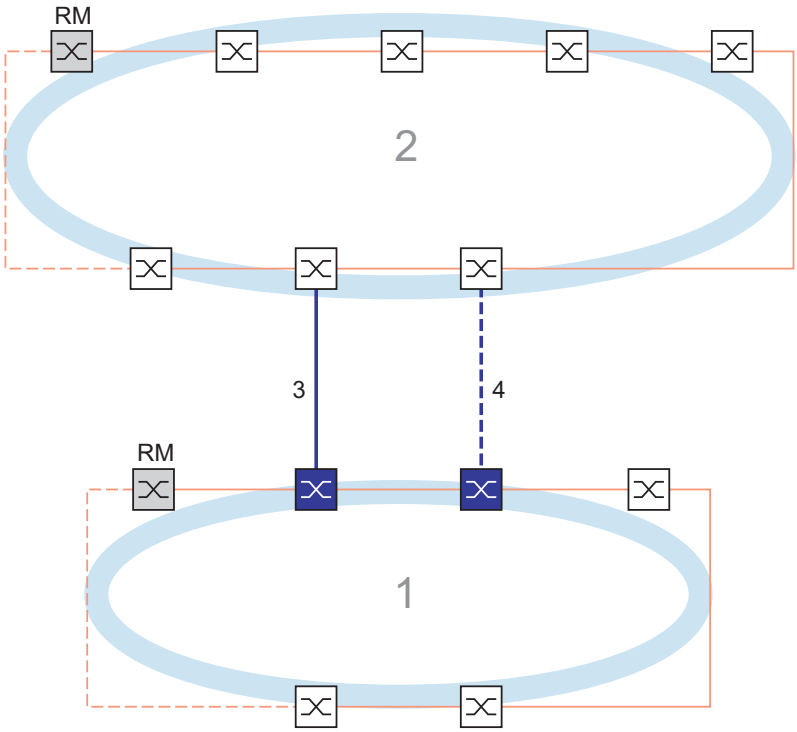


Figura 58: Ejemplo de acoplamiento de Dos Switches
1: Anillo
2: Backbone
3: Línea principal
4: Línea redundante

El acoplamiento entre 2 redes se lleva a cabo mediante la línea principal, indicada por la línea azul continua. Si la línea principal o uno de los dispositivos adyacentes dejan de estar operativos, la línea redundante, que se indica mediante la línea azul discontinua, asume la función de acoplamiento de la red. El acoplamiento se lleva a cabo mediante los 2 dispositivos.

Los dispositivos se envían paquetes de control entre sí a través de Ethernet.

El dispositivo principal conectado a la línea principal y el dispositivo stand-by conectado a la línea redundante son socios en lo que respecta al acoplamiento.
☐ Conecte los 2 socios mediante los puertos del anillo.

Acoplamiento de dos switches, dispositivo principal

Los siguientes ajustes se aplican al dispositivo que se muestra en azul en el gráfico seleccionado.

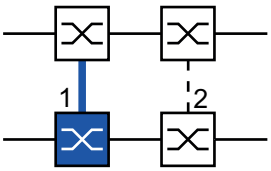


Figura 59: Acoplamiento de Dos Switches, Dispositivo primario
1: Puerto de acoplamiento
2: Puerto de acoplamiento socio

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Switching > L2-Redundancy > Ring/Network Coupling*.
- ☐ En el cuadro *Mode*, en la lista de opciones *Type*, seleccione el botón de opción `two-switch coupling, master`.
- ☐ En el cuadro *Coupling port*, seleccione el puerto al que conecta los segmentos de red en la lista desplegable *Port*.
  Configure el *Coupling port* y los puertos de anillo en puertos diferentes.
- ☐ Para activar la función, seleccione el botón de opción *On* en el cuadro *Operation*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✔.
- ☐ Conecte la línea principal al *Coupling port*.
  En el cuadro *Coupling port*, el campo *State* muestra el estado actual del puerto de acoplamiento.
  Si el socio ya está operando en la red, el campo *IP address* del cuadro *Partner coupling port* muestra la dirección IP del puerto socio.

En el cuadro *Information*, el campo *Redundancy available* muestra si la redundancia está disponible. El campo *Configuration failure* muestra si los ajustes están completos y son correctos.

Nota: Si activa la función *Ring manager* y la función de acoplamiento de dos switches en el mismo dispositivo, existe la posibilidad de crear un bucle.

Para evitar la creación de bucles continuos mientras las conexiones están en funcionamiento en los puertos de acoplamiento del anillo, lleve a cabo una de las siguientes acciones. El dispositivo ajusta el estado del puerto de acoplamiento en "off":

- desactivar el funcionamiento
- cambiar la configuración

Para los puertos de acoplamiento, lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Basic Settings > Port*, pestaña *Configuration*.
- ☐ Para los puertos seleccionados como puertos de acoplamiento, especifique los ajustes de acuerdo con los parámetros de la siguiente tabla.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✔.

Tabla 41: Configuración de puertos de anillo

Tipo de puerto	Velocidad de bits	Port on	Automatic configuration	Manual configuration
TX	100 Mbit/s	`marcado`	`sin marcar`	*`100 Mbit/s FDX`*
TX	1 Gbit/s	`marcado`	`marcado`	–
Óptico	100 Mbit/s	`marcado`	`sin marcar`	*`100 Mbit/s FDX`*
Óptico	1 Gbit/s	`marcado`	`marcado`	–
Óptico	2.5 Gbit/s	`marcado`	–	*`2.5 Gbit/s FDX`*

Si ha configurado VLAN en los puertos de acoplamiento, especifique los ajustes de VLAN en los puertos de acoplamiento y los puertos de acoplamiento socios: Para ello, siga los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Switching > VLAN > Port*.
- ☐ Cambie la configuración de *Port-VLAN ID* al valor del ID VLAN configurado en los puertos.
- ☐ Desactive la casilla *Ingress filtering* para ambos puertos de acoplamiento.

- ☐ Abra el cuadro de diálogo *Switching > VLAN > Configuration*.
- ☐ Para etiquetar las conexiones redundantes para la `VLAN 1` y la asignación de VLAN, introduzca el valor `T` en las celdas correspondientes para ambos puertos de acoplamiento en la fila `VLAN 1`.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✔.

Los dispositivos del acoplamiento envían paquetes redundantes con la prioridad máxima en `VLAN 1`.

Acoplamiento de dos switches, dispositivo stand-by

Los siguientes ajustes se aplican al dispositivo que se muestra en azul en el gráfico seleccionado.

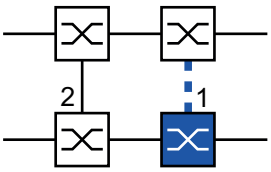


Figura 60: Acoplamiento de Dos Switches, dispositivo de stand-by
1: Puerto de acoplamiento
2: Puerto de acoplamiento socio

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Switching > L2-Redundancy > Ring/Network Coupling*.
- ☐ En el cuadro *Mode*, en la lista de opciones *Type*, seleccione el botón de opción *`two-switch coupling, slave`*.
- ☐ En el cuadro *Coupling port*, seleccione el puerto al que conecta los segmentos de red en la lista desplegable *Port*.
  Configure el *Coupling port* y los puertos de anillo en puertos diferentes.
- ☐ Para activar la función, seleccione el botón de opción *On* en el cuadro *Operation*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✔.
- ☐ Conecte la línea redundante al *Coupling port*.
  En el cuadro *Coupling port*, el campo *State* muestra el estado actual del puerto de acoplamiento.
  Si el socio ya está operando en la red, el campo *IP address* del cuadro *Partner coupling port* muestra la dirección IP del puerto socio.

En el cuadro *Information*, el campo *Redundancy available* muestra si la redundancia está disponible. El campo *Configuration failure* muestra si los ajustes están completos y son correctos.

Nota: Si activa la función *Ring manager* y la función de acoplamiento de dos switches en el mismo dispositivo, existe la posibilidad de crear un bucle.

Para evitar la creación de bucles continuos mientras las conexiones están en funcionamiento en los puertos de acoplamiento del anillo, lleve a cabo una de las siguientes acciones. El dispositivo ajusta el estado del puerto de acoplamiento en "off":

- desactivar el funcionamiento
- cambiar la configuración

Para los puertos de acoplamiento, lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Basic Settings > Port*, pestaña *Configuration*.
- ☐ Para los puertos seleccionados como puertos de acoplamiento, especifique los ajustes de acuerdo con los parámetros de la siguiente tabla.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✓.

Tabla 42: Configuración de puertos de anillo

Tipo de puerto	Velocidad de bits	Port on	Automatic configuration	Manual configuration
TX	100 Mbit/s	marcado	sin marcar	*100 Mbit/s FDX*
TX	1 Gbit/s	marcado	marcado	–
Óptico	100 Mbit/s	marcado	sin marcar	*100 Mbit/s FDX*
Óptico	1 Gbit/s	marcado	marcado	–
Óptico	2.5 Gbit/s	marcado	–	*2.5 Gbit/s FDX*

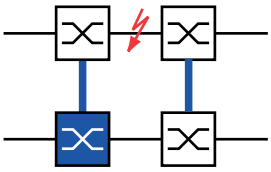
Si ha configurado VLAN en los puertos de acoplamiento, especifique los ajustes de VLAN en los puertos de acoplamiento y los puertos de acoplamiento socios: Para ello, siga los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Switching > VLAN > Port*.
- ☐ Cambie la configuración de *Port-VLAN ID* al valor del ID VLAN configurado en los puertos.
- ☐ Desactive la casilla *Ingress filtering* para ambos puertos de acoplamiento.
- ☐ Abra el cuadro de diálogo *Switching > VLAN > Configuration*.
- ☐ Para etiquetar las conexiones redundantes para la `VLAN 1` y la asignación de VLAN, introduzca el valor `T` en las celdas correspondientes para ambos puertos de acoplamiento en la fila `VLAN 1`.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✓.

Los dispositivos del acoplamiento envían paquetes redundantes con la prioridad máxima en `VLAN 1`.

Especifique la configuración de *Redundancy mode* y *Coupling mode*. Para ello, siga los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Switching > L2-Redundancy > Ring/Network Coupling*.
- ☐ En el cuadro *Configuration*, en la lista de opciones *Redundancy mode*, seleccione uno de los siguientes botones de opción:
  - ▶ `redundant ring/network coupling`
    Con este ajuste, la línea principal o la redundante está activa. La configuración permite que los dispositivos alternen entre ambas líneas.
  - ▶ `extended redundancy`
    Con este ajuste, la línea principal y la redundante están activas simultáneamente. Esta configuración le permite añadir redundancia a la segunda red. Si la conexión entre los dispositivos del acoplamiento en la segunda red deja de estar operativa, los dispositivos del acoplamiento siguen trasmitiendo y recibiendo datos.

    Durante el intervalo de reconfiguración, es posible que se produzcan duplicaciones en los paquetes. Por esa razón, seleccione esta configuración solo si sus dispositivos detectan duplicaciones de los paquetes.
- ☐ En el cuadro *Configuration*, en la lista de opciones *Coupling mode*, seleccione uno de los siguientes botones de opción:
  - ☐ Si se conecta a una red en anillo, seleccione el botón de opción *ring coupling*.
  - ☐ Si se conecta a una estructura de bus o malla, seleccione el botón de opción *network coupling*.

  El modo *Coupling mode* describe el tipo de red backbone a la que conecta la red en anillo (ver la figura 58).
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón .

Restablezca los ajustes de acoplamiento al estado por defecto. Para ello, siga los siguientes pasos:

- ☐ Haga clic en el botón y, a continuación, en el elemento *Reset*.

Acoplamiento de dos switches con línea de control

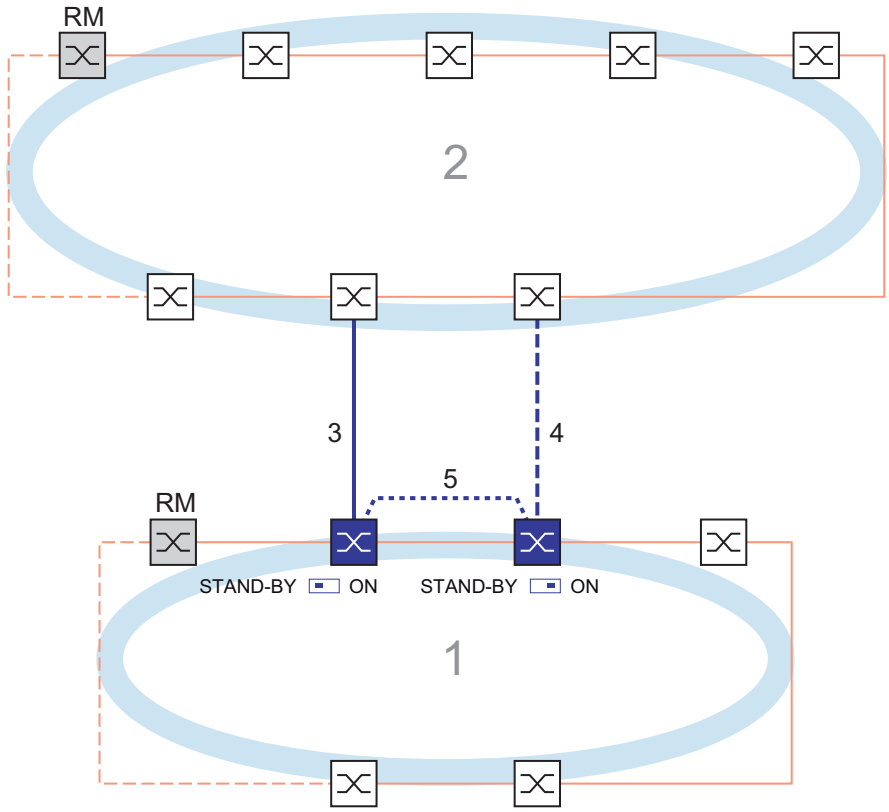


Figura 61: Ejemplo de acoplamiento de Dos Switches con línea de control
1: Anillo
2: Backbone
3: Línea principal
4: Línea redundante
5: Línea de control

El acoplamiento entre 2 redes se lleva a cabo mediante la línea principal, indicada por la línea azul continua. Si la línea principal o uno de los dispositivos adyacentes dejan de estar operativos, la línea redundante, que se indica mediante la línea azul discontinua, asume la función de acoplamiento de las 2 redes. El acoplamiento de anillo se lleva a cabo mediante los 2 dispositivos.

Los dispositivos envían paquetes de control a través de la línea de control, indicada mediante la línea azul de puntos en la figura de abajo (ver la figura 62).

El dispositivo principal conectado a la línea principal y el dispositivo stand-by conectado a la línea redundante son socios en lo que respecta al acoplamiento.
☐ Conecte los 2 socios mediante los puertos del anillo.

Acoplamiento de dos switches con línea de control, dispositivo principal

Los siguientes ajustes se aplican al dispositivo que se muestra en azul en el gráfico seleccionado.

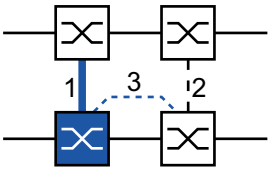


Figura 62: Acoplamiento de dos switches con línea de control, dispositivo primario
1: puerto de acoplamiento
2: puerto de acoplamiento socio
3: línea de control

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Switching > L2-Redundancy > Ring/Network Coupling*.
- ☐ En el cuadro *Mode*, en la lista de opciones *Type*, seleccione el botón de opción `two-switch coupling with control line, master`.
- ☐ En el cuadro *Coupling port*, seleccione el puerto al que conecta los segmentos de red en la lista desplegable *Port*.
  Configure el *Coupling port* y los puertos de anillo en puertos diferentes.
- ☐ En el cuadro *Control port*, seleccione el puerto al que conecta la línea de control en la lista desplegable *Port*.
  Configure el *Coupling port* y los puertos de anillo en puertos diferentes.
- ☐ Para activar la función, seleccione el botón de opción *On* en el cuadro *Operation*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✓.
- ☐ Conecte la línea redundante al puerto de acoplamiento.
  En el cuadro *Coupling port*, el campo *State* muestra el estado actual del puerto de acoplamiento.
  Si el socio ya está operando en la red, el campo *IP address* del cuadro *Partner coupling port* muestra la dirección IP del puerto socio.
- ☐ Conecte la línea de control al puerto de control.
  En el cuadro *Control port*, el campo *State* muestra el estado del puerto de control.
  Si el socio ya está operando en la red, el campo *IP address* del cuadro *Partner coupling port* muestra la dirección IP del puerto socio.

En el cuadro *Information*, el campo *Redundancy available* muestra si la redundancia está disponible. El campo *Configuration failure* muestra si los ajustes están completos y son correctos.

Nota: Si activa la función *Ring manager* y la función de acoplamiento de dos switches en el mismo dispositivo, existe la posibilidad de crear un bucle.

Para evitar la creación de bucles continuos mientras las conexiones están en funcionamiento en los puertos de acoplamiento del anillo, lleve a cabo una de las siguientes acciones. El dispositivo ajusta el estado del puerto de acoplamiento en "off":
- desactivar el funcionamiento
- cambiar la configuración

Para los puertos de acoplamiento, lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Basic Settings > Port*, pestaña *Configuration*.
- ☐ Para los puertos seleccionados como puertos de acoplamiento, especifique los ajustes de acuerdo con los parámetros de la siguiente tabla.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✓.

Tabla 43: Configuración de puertos de anillo

Tipo de puerto	Velocidad de bits	Port on	Automatic configuration	Manual configuration
TX	100 Mbit/s	marcado	sin marcar	*100 Mbit/s FDX*
TX	1 Gbit/s	marcado	marcado	–
Óptico	100 Mbit/s	marcado	sin marcar	*100 Mbit/s FDX*
Óptico	1 Gbit/s	marcado	marcado	–
Óptico	2.5 Gbit/s	marcado	–	*2.5 Gbit/s FDX*

Si ha configurado VLAN en los puertos de acoplamiento, especifique los ajustes de VLAN en los puertos de acoplamiento y los puertos de acoplamiento socios: Para ello, siga los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Switching > VLAN > Port*.
- ☐ Cambie la configuración de *Port-VLAN ID* al valor del ID VLAN configurado en los puertos.
- ☐ Desactive la casilla *Ingress filtering* para ambos puertos de acoplamiento.
- ☐ Abra el cuadro de diálogo *Switching > VLAN > Configuration*.
- ☐ Para etiquetar las conexiones redundantes para la `VLAN 1` y la asignación de VLAN, introduzca el valor `T` en las celdas correspondientes para ambos puertos de acoplamiento en la fila `VLAN 1`.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✓.

Los dispositivos del acoplamiento envían paquetes redundantes con la prioridad máxima en `VLAN 1`.

Acoplamiento de dos switches con línea de control, dispositivo stand-by

Los siguientes ajustes se aplican al dispositivo que se muestra en azul en el gráfico seleccionado.

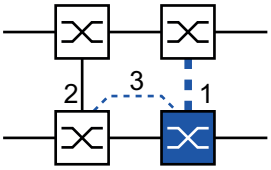


Figura 63: Acoplamiento de dos switches con línea de control, dispositivo stand-by
1: puerto de acoplamiento
2: puerto de acoplamiento socio
3: línea de control

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Switching > L2-Redundancy > Ring/Network Coupling*.
- ☐ En el cuadro *Mode*, en la lista de opciones *Type*, seleccione el botón de opción `two-switch coupling with control line, slave`.
- ☐ En el cuadro *Coupling port*, seleccione el puerto al que conecta los segmentos de red en la lista desplegable *Port*.
  Configure el *Coupling port* y los puertos de anillo en puertos diferentes.
- ☐ En el cuadro *Control port*, seleccione el puerto al que conecta la línea de control en la lista desplegable *Port*.
  Configure el *Coupling port* y los puertos de anillo en puertos diferentes.
- ☐ Para activar la función, seleccione el botón de opción *On* en el cuadro *Operation*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✔.
- ☐ Conecte la línea redundante al puerto de acoplamiento.
  En el cuadro *Coupling port*, el campo *State* muestra el estado actual del puerto de acoplamiento.
  Si el socio ya está operando en la red, el campo *IP address* del cuadro *Partner coupling port* muestra la dirección IP del puerto socio.
- ☐ Conecte la línea de control al puerto de control.
  En el cuadro *Control port*, el campo *State* muestra el estado del puerto de control.
  Si el socio ya está operando en la red, el campo *IP address* del cuadro *Partner coupling port* muestra la dirección IP del puerto socio.

En el cuadro *Information*, el campo *Redundancy available* muestra si la redundancia está disponible. El campo *Configuration failure* muestra si los ajustes están completos y son correctos.

Nota: Si activa la función *Ring manager* y la función de acoplamiento de dos switches en el mismo dispositivo, existe la posibilidad de crear un bucle.

Para evitar la creación de bucles continuos mientras las conexiones están en funcionamiento en los puertos de acoplamiento del anillo, lleve a cabo una de las siguientes acciones. El dispositivo ajusta el estado del puerto de acoplamiento en "off":

- desactivar el funcionamiento
- cambiar la configuración

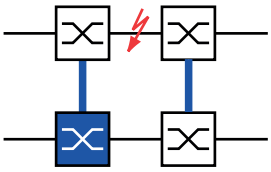
Para los puertos de acoplamiento, lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Switching > VLAN > Port*.
- ☐ Cambie la configuración de *Port-VLAN ID* al valor del ID VLAN configurado en los puertos.
- ☐ Desactive la casilla *Ingress filtering* para ambos puertos de acoplamiento.
- ☐ Abra el cuadro de diálogo *Switching > VLAN > Configuration*.
- ☐ Para etiquetar las conexiones redundantes para la `VLAN 1` y la asignación de VLAN, introduzca el valor `T` en las celdas correspondientes para ambos puertos de acoplamiento en la fila `VLAN 1`.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✔.

Los dispositivos del acoplamiento envían paquetes redundantes con la prioridad máxima en `VLAN 1`.

Especifique la configuración de *Redundancy mode* y *Coupling mode*. Para ello, siga los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Switching > L2-Redundancy > Ring/Network Coupling*.
- ☐ En el cuadro *Configuration*, en la lista de opciones *Redundancy mode*, seleccione uno de los siguientes botones de opción:
  - ▶ `redundant ring/network coupling`
    Con este ajuste, la línea principal o la redundante está activa. La configuración permite que los dispositivos alternen entre ambas líneas.
  - ▶ `extended redundancy`
    Con este ajuste, la línea principal y la redundante están activas simultáneamente. Esta configuración le permite añadir redundancia a la segunda red. Si la conexión entre los dispositivos del acoplamiento en la segunda red deja de estar operativa, los dispositivos del acoplamiento siguen trasmitiendo y recibiendo datos.

    Durante el intervalo de reconfiguración, es posible que se produzcan duplicaciones en los paquetes. Por esa razón, seleccione esta configuración solo si sus dispositivos detectan duplicaciones de los paquetes.
- ☐ En el cuadro *Configuration*, en la lista de opciones *Coupling mode*, seleccione uno de los siguientes botones de opción:
  - ☐ Si se conecta a una red en anillo, seleccione el botón de opción *ring coupling*.
  - ☐ Si se conecta a una estructura de bus o malla, seleccione el botón de opción *network coupling*.

  El modo *Coupling mode* describe el tipo de red backbone a la que conecta la red en anillo (ver la figura 61).
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón .

Restablezca los ajustes de acoplamiento al estado por defecto. Para ello, siga los siguientes pasos:

- ☐ Haga clic en el botón y, a continuación, en el elemento *Reset*.

13.13 RCP

Las aplicaciones industriales requieren que sus redes tengan una alta disponibilidad. Esto también implica mantener tiempos de interrupción breves y determinísticos para la comunicación en casos en los que un dispositivo de la red no esté operativo.

Las topologías en anillo ofrecen tiempos de transición breves con un uso mínimo de los recursos. Sin embargo, las topologías en anillo suponen el reto de acoplar estos anillos de manera redundante.

El Protocolo de acoplamiento redundante*RCP* le permite acoplar anillos que están funcionando con uno de los siguientes protocolos de redundancia:

- MRP
- Anillo HIPER
- RSTP

La función *RCP* también le permite acoplar varios anillos secundarios en un anillo principal (ver la figura 64). Solo los switches que acoplan los anillos requieren la función *RCP*.

También puede utilizar dispositivos diferentes a los dispositivos Schneider Electric en las redes acopladas.

La función *RCP* utiliza un dispositivo maestro y un dispositivo esclavo para transmitir datos entre las redes. Solo el dispositivo maestro reenvía cuadros entre los anillos.

Al utilizar los mensajes Multicast exclusivos Schneider Electric, los dispositivos maestro y esclavo de *RCP* informan entre sí sobre su modo de funcionamiento. Configure los dispositivos del anillo que no sean dispositivos de acoplamiento para que reenvíen las siguientes direcciones Multicast:

- `01:80:63:07:00:09`
- `01:80:63:07:00:0A`

Conecte los dispositivos maestro y esclavo como vecinos directos.

Utilice 4 puertos por dispositivo para crear un acoplamiento redundante. Instale los dispositivos del acoplamiento con 2 puertos interiores y 2 puertos exteriores en cada red.

- El puerto interior conecta los dispositivos maestro y esclavo.
- El puerto exterior conecta los dispositivos a la red.

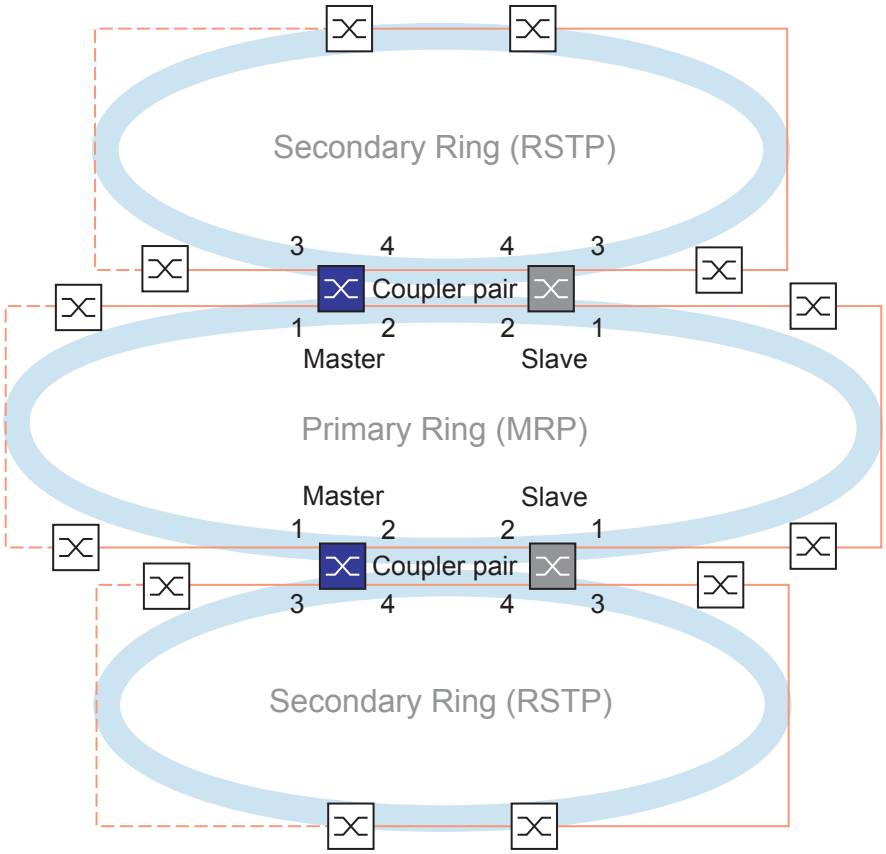


Figura 64: Ejemplo de acoplamiento redundante de dos switches
1: puerto de acoplamiento exterior en el anillo principal
2: puerto de acoplamiento interior en el anillo principal
3: puerto de acoplamiento exterior en el anillo secundario
4: puerto de acoplamiento interior en el anillo secundario

Si el rol se establece en el valor *auto*, los dispositivos acopladores seleccionan por sí solos su rol como *master* o *slave*. Si desea disponer de un dispositivo maestro o esclavo permanente, configure los roles manualmente.

Nota: El rol `single` solo se utiliza junto con la función *Dual RSTP*. Ver “Acoplamiento de 2 anillos RSTP mediante la función Dual RSTP” en página 256.

Si ya no se puede acceder al maestro mediante los puertos de acoplamiento interiores, el dispositivo esclavo espera a que transcurra el intervalo de tiempo de espera antes de asumir el rol de maestro. Durante el intervalo de tiempo de espera especificado, el esclavo intenta acceder al maestro mediante los puertos de acoplamiento exteriores. Si el maestro sigue sin estar accesible, el esclavo asume el rol de maestro. Para mantener la estabilidad en la red conectada a los puertos de acoplamiento exteriores, configure el intervalo de tiempo de espera en una duración mayor que el tiempo de recuperación de los anillos acoplados.

Nota: Desactive el protocolo RSTP en los puertos interiores y exteriores de acoplamiento redundante *RCP* que no estén conectados al anillo RSTP. En la configuración de ejemplo, desactive el RSTP en los puertos `1` y `2` de cada dispositivo.

13.13.1 Ejemplo de aplicación para el acoplamiento RCP

⚠ ADVERTENCIA

OPERACIÓN INESPERADA DEL EQUIPO

Para ayudar a evitar bucles durante la fase de configuración, configure cada dispositivo de la configuración *RCP* individualmente. Antes de conectar los trayectos redundantes, complete la configuración de los otros dispositivos de la configuración del anillo.

El incumplimiento de estas instrucciones puede causar la muerte, heridas graves o daños en el equipo.

Los dispositivos Schneider Electric admiten el método de Protocolo de acoplamiento redundante de dos switches. Puede utilizar la función *RCP* para proporcionar una red instalada en un tren, por ejemplo. La red proporciona información a los pasajeros sobre la ubicación del tren o las diferentes paradas de la línea. La red también permite ofrecer a los pasajeros seguridad, por ejemplo, mediante la vigilancia por vídeo.

Los anillos principales de la figura representan una red en anillo *MRP* en un coche. Los anillos secundarios de la figura son redes en anillo RSTP. Cada anillo contiene 4 dispositivos (ver la figura 65).

Para simplificar la topología del tren en la figura, a los puertos de anillo *MRP* y a los puertos interiores y exteriores *RCP* se les asigna los mismos números de puerto. Especifique los mismos valores para los parámetros de los puertos según su función en la red. Por ejemplo, especifique los puertos *1/1* y *1/2* de los switches 1D y 1C como puertos de anillo MRP. El puerto *1/4* como puerto interior *RCP*, y el puerto *1/3* como puerto exterior *RCP*.

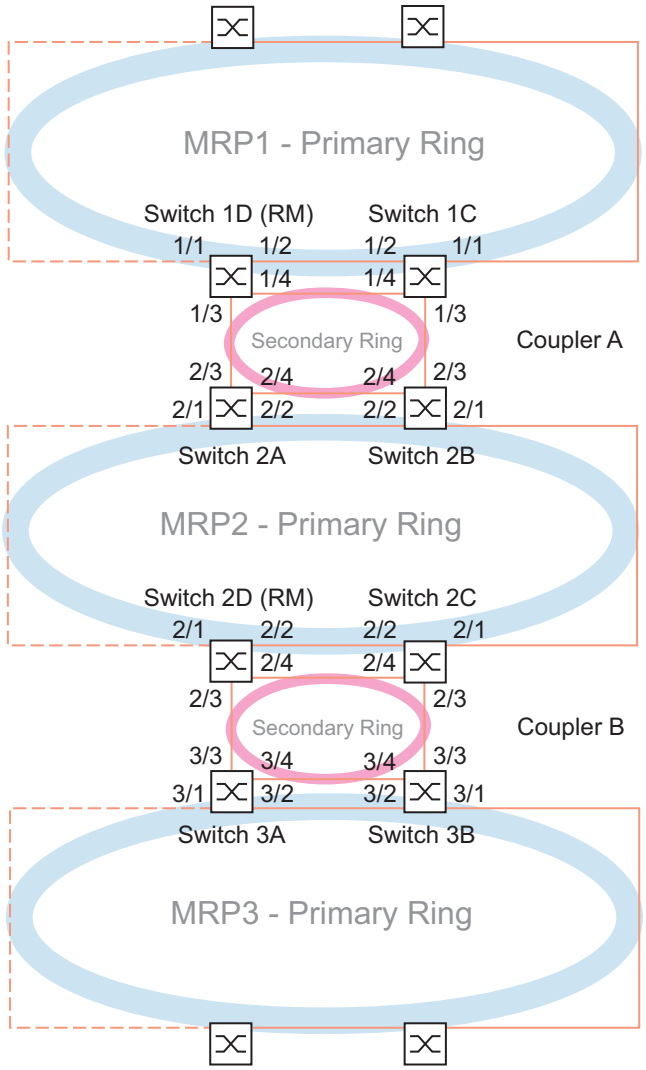


Figura 65: Topología del tren Protocolo de acoplamiento redundante

La siguiente lista especifica roles de los puertos de cada dispositivo.
1: los puertos 1 y 2 son puertos de anillo MRP
2: el puerto 3 es un puerto exterior RCP
3: el puerto 4 es un puerto interior RCP

Los siguientes pasos describen cómo especificar los parámetros para el switch 1D en el acoplador A. Configure los otros dispositivos utilizados para el acoplador A y los dispositivos utilizados en el acoplador B del mismo modo.

Desactivación de la función RSTP en el anillo MRP

MRP y RSTP no funcionan juntos. Por tanto, desactive la función RSTP en los puertos *RCP* utilizados en el anillo *MRP*. En la configuración de ejemplo, los puertos `x/1` y `x/2` se utilizan en el anillo *MRP*. Active la función RSTP solo en los puertos interiores y exteriores *RCP* utilizados en el anillo secundario. Por ejemplo, active la función RSTP en los puertos `x/3` y `x/4`.

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Switching > L2-Redundancy > Spanning Tree > Port*, pestaña *CIST*.
- ☐ En la configuración por defecto, la función RSTP está activa en los puertos. Para desactivar la función RSTP en los puertos del anillo *MRP*, desactive las casillas *STP active* para los puertos `x/1` y `x/2`.
- ☐ Abra el cuadro de diálogo *Switching > L2-Redundancy > Spanning Tree > Global*.
- ☐ Para activar la función, seleccione el botón de opción *On* en el cuadro *Operation*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✓.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`interface x/1`	Cambiar al modo de configuración de la interfaz `x/1`.
`no spanning-tree mode`	Desactive la función *Spanning Tree* en el puerto.
`exit`	Cambiar al modo de configuración.
`interface x/2`	Cambiar al modo de configuración de la interfaz `x/2`.
`no spanning-tree mode`	Desactive la función *Spanning Tree* en el puerto.
`exit`	Cambiar al modo de configuración.
`spanning-tree operation`	Activar la función *Spanning Tree*.

Especificar el anillo maestro en el anillo MRP

En la figura, el switch D de cada anillo *MRP* es designado como Ring Manager(ver la figura 65). Especifique los otros switches de los anillos como clientes del anillo.

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Switching > L2-Redundancy > MRP*.
- ☐ Especifique el primer puerto de anillo en el cuadro *Ring port 1*.
  En la lista desplegable *Port*, seleccione el puerto `x/1`.
- ☐ Especifique el segundo puerto de anillo en el cuadro *Ring port 2*.
  En la lista desplegable *Port*, seleccione el puerto `x/2`.
- ☐ Para designar el dispositivo como Ring Manager, active la función en el cuadro *Ring manager*.
- ☐ Para activar la función, seleccione el botón de opción *On* en el cuadro *Operation*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✓.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`mrp domain add default-domain`	Generar un nuevo dominio de *MRP* con el ID `default-domain`.
`mrp domain modify port primary x/1`	Especificar el puerto `x/1` como puerto del anillo `1`.
`mrp domain modify port secondary x/2`	Especificar el puerto `x/2` como puerto del anillo `2`.
`mrp domain modify mode manager`	Especificar que el dispositivo actúa como *Ring manager*. Para los otros dispositivos del anillo, deje la configuración por defecto.
`mrp domain modify operation enable`	Activar la función *MRP*.

Especificación de los dispositivos en el acoplador redundante

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Switching > L2-Redundancy > RCP*.
- ☐ Especifique el *Inner port* en el cuadro *Primary ring/network*. Seleccione el puerto `x/2`.
- ☐ Especifique el *Outer port* en el cuadro *Primary ring/network*. Seleccione el puerto `x/1`.
- ☐ Especifique el *Inner port* en el cuadro *Secondary ring/network*. Seleccione el puerto `x/4`.
- ☐ Especifique el *Outer port* en el cuadro *Secondary ring/network*. Seleccione el puerto `x/3`.

- ☐ Para activar la función, seleccione el botón de opción *On* en el cuadro *Operation*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✓.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`redundant-coupling port primary inner x/2`	Especificar el puerto `x/2` como el puerto interior principal.
`redundant-coupling port primary outer x/1`	Especificar el puerto `x/1` como el puerto exterior principal.
`redundant-coupling port secondary inner x/4`	Especificar el puerto `x/4` como el puerto interior secundario.
`redundant-coupling port secondary outer x/3`	Especificar el puerto `x/3` como el puerto exterior secundario.
`redundant-coupling operation`	Active la función *RCP* en el dispositivo.
`copy config running-config nvm`	Guardar la configuración actual en la memoria no volátil (`nvm`) del perfil de configuración "seleccionado".

13.13.2 Acoplamiento de 2 anillos RSTP mediante la función Dual RSTP

Si desea utilizar el RSTP para los anillos principal y secundario, la función *RCP* asigna los puertos del anillo secundario a la instancia *Dual RSTP*. Esto permite crear dos redes RSTP independientes acopladas mediante *RCP*.

Tiene la opción de utilizar hasta 16 dispositivos MCSESM-E en un anillo secundario. Se incluyen los 2 dispositivos del anillo principal que están conectados al anillo secundario. Si un componente de la red en el anillo secundario cambia a estado inoperativo, la función *RCP* puede lograr normalmente un tiempo de reconfiguración de menos de 50 ms.

También tiene la opción de utilizar hasta 16 dispositivos MCSESM-E en un anillo principal. De esta manera, la función*RCP* y *Dual RSTP* también pueden obtener un tiempo de reconfiguración típico de menos de 50 ms en el anillo principal. Puede conectar hasta 8 anillos secundarios a un anillo principal. De esta manera, puede conectar hasta 128 puentes (8 × 14 + 16). En esta red, puede obtener un tiempo habitual de reconfiguración de extremo a extremo de 50 ms con redundancia de dispositivo.

Si los requisitos del tiempo de reconfiguración del anillo principal son inferiores, tiene las siguientes opciones:
- Aumentar el número de puentes del anillo principal.
- Conectar más anillos secundarios al anillo principal.

También puede utilizar dispositivos diferentes a los dispositivos MCSESM-E en los anillos, pero solo en los casos en los que los dispositivos actualicen los cambios de topología RSTP con la velocidad suficiente. Por ejemplo, si un componente de la red deja de estar operativo.

Propiedades de los puertos principales y secundarios de la instancia

Para los puertos de una instancia principal o secundaria, tenga en cuenta las siguientes consideraciones:
- Solo aquellos puertos del puente *RCP* que estén configurados como puertos de anillo exteriores o interiores del anillo secundario pertenecen a la instancia *Dual RSTP*. Los otros puertos pertenecen a la instancia principal del puente.
- Tiene la opción de conectar dispositivos finales o redes que no ejecuten *Spanning Tree* en un puerto que pertenezca implícitamente a una instancia principal del puente *RCP*.
  Estas topologías no proporcionan ni la redundancia del dispositivo ni la redundancia del enlace.
- Tiene la opción de crear una red en malla en el anillo principal o secundario al establecer más enlaces entre los puertos de la misma instancia.
  En estas topologías, no se aplica un tiempo máximo definido de reconfiguración de extremo a extremo de 50 ms.

Acoplamiento de 2 anillos RSTP solo mediante un puente RCP

Si desea acoplar 2 anillos RSTP utilizando solo un puente, utilice el rol `single`.

Para el puente *RCP* con el rol `single`, los puertos interiores y exteriores tienen la misma función. Puede intercambiar los puertos interiores y exteriores de una instancia específica.

Si utiliza un puente para conectar los anillos, puede conectar hasta 16 anillos secundarios a un anillo principal. Aquí se incluye al puente *RCP* que conecta los anillos. De esta manera, puede conectar hasta 256 puentes (16 × 15 + 16). En esta red, puede obtener un tiempo máximo de reconfiguración de extremo a extremo de 50 ms en una red con redundancia de conexión.

Si los requisitos del tiempo de reconfiguración del anillo principal son inferiores, tiene las siguientes opciones:

- Aumentar el número de puentes del anillo principal.
- Conectar más anillos secundarios al anillo principal.

Opciones de topología para la función Dual RSTP

El siguiente ejemplo muestra la estructura básica de un anillo principal conectado a 3 anillos secundarios. Los anillos secundarios 1 y 2 están conectados al anillo principal mediante 2 puentes *RCP* cada uno, y el anillo secundario 3 mediante 1 puente *RCP*. Se entiende que los costes de ruta son los mismos para cada conexión de anillo.

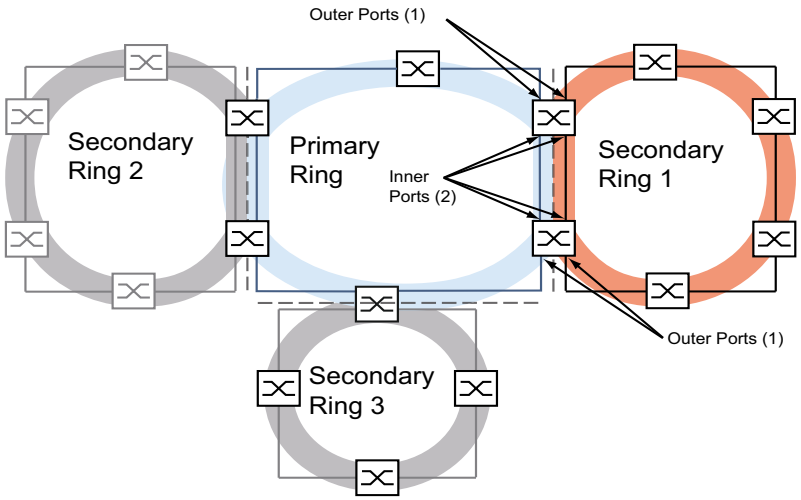


Figura 66: Anillo principal con 3 anillos secundarios conectados mediante RCP

Configuración del anillo principal

Los siguientes capítulos describen la configuración en principio y, de esta manera, no incluyen pasos de trabajo.

⚠ ADVERTENCIA

OPERACIÓN INESPERADA DEL EQUIPO

Al ejecutar la configuración actual, lleve a cabo los pasos para evitar la creación de bucles.

El incumplimiento de estas instrucciones puede causar la muerte, heridas graves o daños en el equipo.

Para especificar el puente raíz y el puente raíz de reserva en el anillo principal, configure sus prioridades de puente globales de RSTP. Si el puente raíz y el puente raíz de reserva se oponen entre sí en el anillo principal, obtendrá un tiempo de reconfiguración muy breve en el anillo principal. Esto se produce si el puente raíz de reserva tiene 2 rutas hacia el puente raíz cuyo número de dispositivos al puente raíz es diferente en un máximo de 1.

Configure los otros puentes del anillo principal ubicados entre el puente raíz y el puente raíz de reserva para que las prioridades de puente disminuyan (es decir, aumenten numéricamente) a medida que su distancia con respecto al puente raíz aumenta.

La figura muestra un ejemplo con los detalles de RSTP para el anillo principal. La topología se reduce al anillo principal y al anillo secundario. Durante la configuración, la estación de administración de red está conectada al anillo principal para evitar interrupciones de comunicación con los puentes en el anillo secundario.

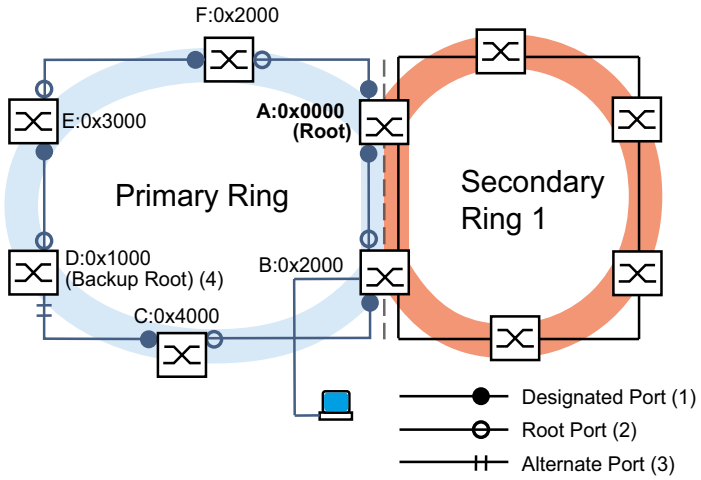


Figura 67: Anillo principal conectado a un anillo secundario con detalles del anillo principal
A..F: identificación del puente
0x0000..0x4000: prioridades del puente en el anillo principal

Configuración del anillo secundario

Para especificar el puente raíz y el puente raíz de reserva en el anillo secundario, configure la prioridad del puente *Dual RSTP* para los puentes *RCP*. Para el resto de puentes del anillo secundario, configure solo su prioridad de puente global de RSTP. Si el puente raíz y el puente raíz de reserva se oponen entre sí en el anillo secundario, obtendrá un tiempo de reconfiguración muy breve en el anillo secundario.

Configure también los otros puentes del anillo secundario para que las prioridades de puente disminuyan (es decir, aumenten numéricamente) a medida que su distancia con respecto al puente raíz aumenta.

La figura muestra un ejemplo con los detalles de RSTP para el anillo secundario.

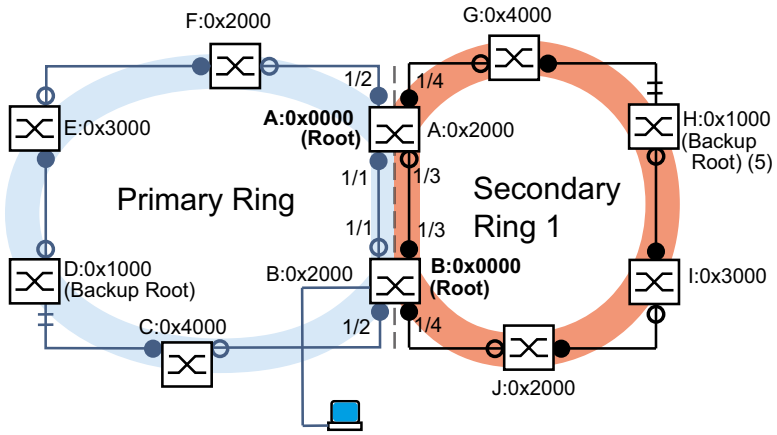


Figura 68: Anillo principal conectado a un anillo secundario con detalles del anillo secundario
A, B, G a J: identificaciones del puente en el anillo secundario
0x0000..0x4000: prioridades del puente
para los puentes A y B: Dual RSTP prioridad del puente
para los puentes G a J: prioridades de puente globales de RSTP
5: puerto raíz de reserva del anillo secundario

Los roles del puente raíz del anillo principal y del anillo secundario son independientes los unos de los otros. Un puente puede ser la raíz de RSTP para:

- Ambos anillos
- Un anillo
- Ningún anillo

Utilice el anillo secundario solo con RSTP.

Configuración del acoplamiento de los anillos

Para los puentes *RCP*, defina los puertos interiores y exteriores para el anillo principal y el secundario.

Tabla 44: Puertos de anillo para los puentes RCP

Puertos	RCP maestro (B)	RCP esclavo (A)
Anillo principal		
Puerto interior	1/1	1/1
Puerto exterior	1/2	1/2
Anillo secundario		
Puerto interior	1/3	1/3
Puerto exterior	1/4	1/4

Después, configure el rol para cada puente *RCP*.

La figura muestra un ejemplo.

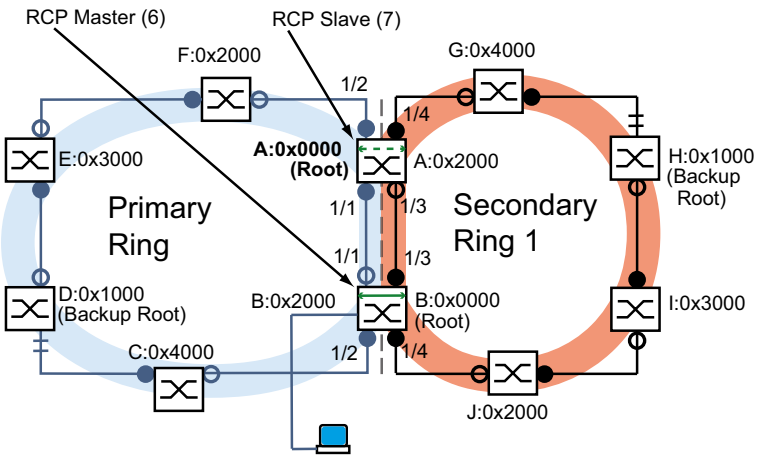


Figura 69: Anillo principal conectado a un anillo secundario, con los números de puerto y los roles RCP
6: RCP maestro
7: RCP esclavo

Los roles del puente raíz y los roles de acoplamiento son independientes los unos de los otros. Un puente puede ser *RCP* maestro y operar al mismo tiempo que el RSTP raíz para:
- Ambos anillos
- Un anillo
- Ningún anillo

Lo mismo sucede con el *RCP*esclavo.

Después, active la función *RCP*.

13.13.3 Ejemplo de aplicación para el acoplamiento RCP mediante Dual RSTP

En una planta de producción, hay varias células de producción. Los dispositivos de una célula de producción están conectados en una estructura de red en línea. Esta red está conectada a la red de mayor nivel de la planta de producción. La red de la planta de producción esta interconectada de manera redundante y funciona como RSTP. Todos los dispositivos son del tipo MCSESM-E.

Requisitos:
- Ajuste la red en línea existente en las células de producción con una redundancia de dispositivo rápida.
- Conecte las células de producción de manera redundante a la red de la planta de producción.
- Reconfigure la red de la planta de producción para que proporcione tiempos de reconfiguración breves y determinísticos.

Topología de red existente, reducida a una célula de producción:

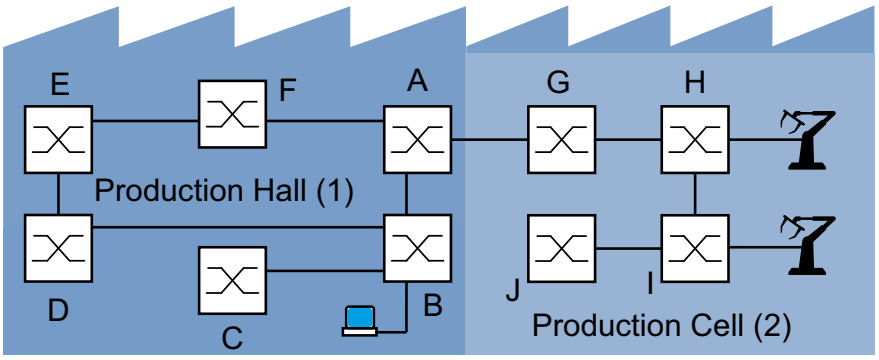


Figura 70: Ejemplo de una célula de producción en una planta de producción; topología antes de usar el RCP y la función Dual RSTP.
1: planta de producción
2: célula de producción

Topología de red *Dual RSTP* deseada:

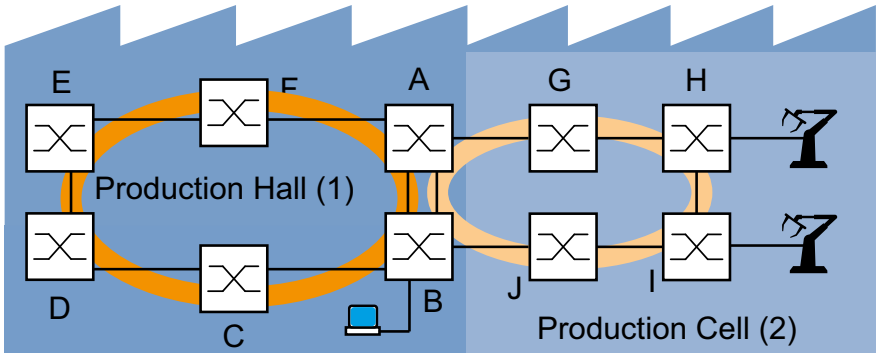


Figura 71: Ejemplo de una célula de producción en una planta de producción; topología al usar el RCP y la función Dual RSTP
1: planta de producción
2: célula de producción

Representación esquemática de la topología de red *Dual RSTP* deseada:

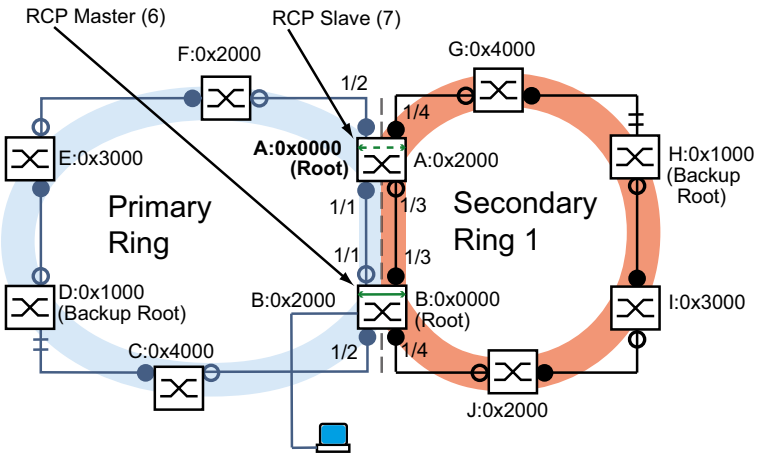


Figura 72: Representación esquemática de la topología de red Dual RSTP:
6: RCP maestro
7: RCP esclavo

La siguiente tabla muestra que el número reducido de ajustes son suficientes para configurar la nueva topología. Introduzca los ajustes *Dual RSTP* solo en los dispositivos A y B.

Tabla 45: Valores para la configuración de los switches del ejemplo Dual RSTP

Parámetro	A	B	C	D	E	F	G	H	I	J
Configuración de RSTP										
Prioridad del puente (hex.)[1]	0x0000	0x2000	0x4000	0x1000	0x3000	0x2000	0x4000	0x1000	0x3000	0x2000
Configuración de Dual RSTP										
Prioridad del puente (hex.)[a]	0x2000	0x0000	-	-	-	-	-	-	-	-
Configuración de RCP										
Anillo principal, puerto interior	1/1	1/1	-	-	-	-	-	-	-	-
Anillo principal, puerto exterior	1/2	1/2	-	-	-	-	-	-	-	-
Anillo secundario, puerto interior	1/3	1/3	-	-	-	-	-	-	-	-
Anillo secundario, puerto exterior	1/4	1/4	-	-	-	-	-	-	-	-
Rol de acoplamiento	Slave	Master	-	-	-	-	-	-	-	-

1. Para las prioridades de puente en notación hexadecimal y decimal, consulte tabla 46.

Tabla 46: Posibles prioridades del puente en notación hexadecimal y decimal

Prioridad del puente								
Hexadecimal	0x0000	0x1000	0x2000	0x3000	0x4000	0x5000	0x6000	0x7000
Decimal	0	4096	8192	12288	16384	20480	24576	28672

Hexadecimal	0x8000	0x9000	0xA000	0xB000	0xC000	0xD000	0xE000	0xF000
Decimal	32768	36864	40960	45056	49152	53248	57344	61440

Requisitos para una configuración adicional:

- La conexión para la interconexión existente entre los puentes B y D está inactiva en la topología anterior del anillo secundario. Puede llevar a cabo esto, por ejemplo, desactivando manualmente los puertos correspondientes de los puentes B y D o desconectando el enlace.
- Las conexiones entre los puentes C y D y entre los puentes J y B están inactivas. Puede llevar a cabo esto, por ejemplo, desactivando manualmente los puertos correspondientes de los puentes antes de conectar los enlaces.
- La conexión para el anillo secundario entre los puentes A y B está inactiva.
- RSTP está activo en todos los dispositivos y los parámetros están en el estado de la configuración por defecto.
- Su estación de administración está conectada al anillo principal.

- Ha abierto la interfaz gráfica de usuario o la interfaz de línea de comando para los dispositivos A y B.
- Tiene acceso a las interfaces de usuario de los dispositivos C a J.

⚠ ADVERTENCIA

PELIGRO DE CREACIÓN DE BUCLES

- Defina cada dispositivo de la configuración de *RCP* y *Dual RSTP* individualmente. Antes de conectar los trayectos redundantes, complete la configuración de los otros dispositivos de la configuración del anillo.
- En la configuración del acoplamiento de *RCP*, defina un tiempo límite (timeout) mayor que el mayor tiempo de interrupción previsto de la instancia más rápida del protocolo de redundancia.
- En una topología con 2 puentes de acoplamiento, configure los roles de ambos dispositivos en el acoplamiento solamente como `master`, `slave` o `auto`.
- Acople la instancia principal y secundaria solamente mediante 1 puente *RCP* (para topologías con 1 puente *RCP*) o mediante 2 puentes *RCP* (para topologías con 2 puentes *RCP*). Mantenga los puertos de la instancia principal separados de los puertos de cada instancia secundaria.
- Active el ajuste *Admin edge port* en un puerto solamente en los casos en los que haya un dispositivo terminal conectado al puerto.

El incumplimiento de estas instrucciones puede causar la muerte, heridas graves o daños en el equipo.

Configuración de los parámetros globales RSTP de los puentes RCP

De las especificaciones de tareas de la tabla 45, necesitará las prioridades de puente RSTP para el puente A y el puente B. La siguiente tabla contiene un resumen de estos valores.

Tabla 47: Prioridades de puente RSTP para los puentes A y B.

Parámetro RSTP	A	B
Prioridad del puente (hex.)	0x0000	0x2000
Prioridad del puente (dec.)	0	8192

Nota: Las siguientes instrucciones describen la configuración de los puentes *RCP* (A y B) en detalle; las del resto de puentes (C a J) solo figuran de forma abreviada.

Configurar dispositivo A. Para ello, siga los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Switching > L2-Redundancy > Spanning Tree > Global*.
- ☐ En el cuadro *Bridge configuration*, seleccione el valor 0 en la lista desplegable *Priority*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ☑.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`spanning-tree mst priority 0 0`	Establecer la prioridad del puenteRSTP de la instancia MST 0 al valor 0. La instancia MST0 es la instancia MST global o la instancia por defecto.

Configurar dispositivo B. Para ello, siga los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Switching > L2-Redundancy > Spanning Tree > Global*.
- ☐ En el cuadro *Bridge configuration*, seleccione el valor `8192` en la lista desplegable *Priority*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✓.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`spanning-tree mst priority 0 8192`	Establecer la prioridad del puenteRSTP de la instancia MST global al valor `8192`.

Configuración de los parámetros globales RSTP de los otros puentes

Configure ahora los otros puentes. De las especificaciones de tareas, necesitará las prioridades de puenteRSTP. La siguiente tabla contiene un resumen de estos valores.

Tabla 48: Prioridades de puente RSTP para los puentes C a J.

Parámetro RSTP	C	D	E	F	G	H	I	J
Prioridad del puente (hex.)	0x4000	0x1000	0x3000	0x2000	0x4000	0x1000	0x3000	0x2000
Prioridad del puente (dec.)	16384	4096	12288	8192	16384	4096	12288	8192

Lleve a cabo los siguientes pasos:

- ☐ Establezca la prioridad del puenteRSTP del dispositivo C a `16384 (0x4000)` y active la configuración.
- ☐ Establezca la prioridad del puenteRSTP del dispositivo D a `4096 (0x1000)` y active la configuración.
- ☐ Establezca la prioridad del puenteRSTP del dispositivo E a `12288 (0x3000)` y active la configuración.
- ☐ Establezca la prioridad del puenteRSTP del dispositivo F a `8192 (0x2000)` y active la configuración.
- ☐ Establezca la prioridad del puenteRSTP del dispositivo G a `16384 (0x4000)` y active la configuración.
- ☐ Establezca la prioridad del puenteRSTP del dispositivo H a `4096 (0x1000)` y active la configuración.
- ☐ Establezca la prioridad del puenteRSTP del dispositivo I a `12288 (0x3000)` y active la configuración.
- ☐ Establezca la prioridad del puenteRSTP del dispositivo J a `8192 (0x2000)` y active la configuración.

Configuración de los parámetros Dual RSTP de los puentes RCP

De las especificaciones de tareas, necesitará los parámetros *Dual RSTP* específicos para los puentes A y B. Estos son las prioridades del puente *Dual RSTP*, los puertos de anillo y los roles de acoplamiento. Las siguientes tablas contienen un resumen de estos valores.

Tabla 49: Parámetros Dual RSTP para los puentes A y B

Parámetro Dual RSTP	A	B
Prioridad del puente *Dual RSTP* (hex.)	`0x2000`	`0x0000`
Prioridad del puente *Dual RSTP* (dec.)	`8192`	`0`

Tabla 50: Parámetros RCP para los puentes A y B

Parámetro Dual RSTP	A	B
Anillo principal, puerto interior	`1/1`	`1/1`
Anillo principal, puerto exterior	`1/2`	`1/2`
Anillo secundario, puerto interior	`1/3`	`1/3`
Anillo secundario, puerto exterior	`1/4`	`1/4`
Rol de acoplamiento	`Slave`	`Master`

Configurar dispositivo A. Para ello, siga los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Switching > L2-Redundancy > FuseNet > RCP*.
- ☐ En el cuadro *Primary ring/network*, seleccione el valor `1/1` en la lista desplegable *Inner port*.
- ☐ En el cuadro *Primary ring/network*, seleccione el valor `1/2` en la lista desplegable *Outer port*.
- ☐ En el cuadro *Secondary ring/network*, seleccione el valor `1/3` en la lista desplegable *Inner port*.
- ☐ En el cuadro *Secondary ring/network*, seleccione el valor `1/4` en la lista desplegable *Outer port*.
- ☐ En el cuadro *Coupler configuration*, seleccione el valor *`slave`* en la lista desplegable *Role*.
- ☐ Para activar la función, seleccione el botón de opción *On* en el cuadro *Operation*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ☑.
- ☐ Abra el cuadro de diálogo *Switching > L2-Redundancy > Spanning Tree > Dual RSTP*.
- ☐ En el cuadro *Bridge configuration*, seleccione el valor `8192` en la lista desplegable *Priority*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ☑.

`spanning-tree drstp mst priority 0 8192`	Establecer la prioridad del puenteRSTP de la instancia *Dual RSTP* al valor `8192`.
`redundant-coupling port primary inner 1/1`	Seleccionar el puerto *1/1* como el puerto interior para el anillo principal *RCP*.
`redundant-coupling port primary outer 1/2`	Seleccionar el puerto *1/2* como el puerto exterior para el anillo principal *RCP*.
`redundant-coupling port secondary inner 1/3`	Seleccionar el puerto *1/3* como el puerto interior para el anillo secundario *RCP*.
`redundant-coupling port secondary outer 1/4`	Seleccionar el puerto *1/4* como el puerto exterior para el anillo secundario *RCP*.
`redundant-coupling role slave`	Configurar este dispositivo como el *RCP*esclavo.
`exit`	Cambiar al modo Privileged EXEC.

Configurar dispositivo B. Para ello, siga los siguientes pasos:

- Abra el cuadro de diálogo *Switching > L2-Redundancy > FuseNet > RCP*.
- En el cuadro *Primary ring/network*, seleccione el valor `1/1` en la lista desplegable *Inner port*.
- En el cuadro *Primary ring/network*, seleccione el valor `1/2` en la lista desplegable *Outer port*.
- En el cuadro *Secondary ring/network*, seleccione el valor `1/3` en la lista desplegable *Inner port*.
- En el cuadro *Secondary ring/network*, seleccione el valor `1/4` en la lista desplegable *Outer port*.
- En el cuadro *Coupler configuration*, seleccione el valor `master` en la lista desplegable *Role*.
- Para activar la función, seleccione el botón de opción *On* en el cuadro *Operation*.
- Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✓.
- Abra el cuadro de diálogo *Switching > L2-Redundancy > Spanning Tree > Dual RSTP*.
- En el cuadro *Bridge configuration*, seleccione el valor `0` en la lista desplegable *Priority*.
- Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✓.

`spanning-tree drstp mst priority 0 0`	Establecer la prioridad del puenteRSTP de la instancia *Dual RSTP* al valor `0`.
`redundant-coupling port primary inner 1/1`	Seleccionar el puerto *1/1* como el puerto interior para el anillo principal *RCP*.
`redundant-coupling port primary outer 1/2`	Seleccionar el puerto *1/2* como el puerto exterior para el anillo principal *RCP*.
`redundant-coupling port secondary inner 1/3`	Seleccionar el puerto *1/3* como el puerto interior para el anillo secundario *RCP*.
`redundant-coupling port secondary outer 1/4`	Seleccionar el puerto *1/4* como el puerto exterior para el anillo secundario *RCP*.
`redundant-coupling role master`	Configurar este dispositivo como el *RCP*maestro.
`exit`	Cambiar al modo Privileged EXEC.

Comprobación de la configuración

Active las nuevas conexiones redundantes:
- La conexión de los puertos interiores para el anillo secundario entre el dispositivo A, puerto *1/3*, y el dispositivo B, puerto *1/3*.
- El cierre del anillo para el anillo secundario entre los dispositivos G y H.
- El cierre del anillo para el anillo principal entre los dispositivos C y D.

Compare los roles del puente actual en el anillo principal con los roles de puente necesarios:

El puente A debería ser el puente raíz.

Lleve a cabo los siguientes pasos:

- Abra el cuadro de diálogo *Switching > L2-Redundancy > Spanning Tree > Global*.
- En el cuadro *Topology information*, marque la configuración de la casilla *Bridge is root*.

```
show spanning-tree global

Spanning Tree Information:
--------------------------
Spanning Tree Mode.........................RSTP
Spanning Tree Trap Mode....................enabled
Bridge is root.............................true
...
```

Compare los 4 puertos que configuró como puertos interiores y exteriores en el anillo principal y el secundario con las especificaciones de la tabla 45.

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Switching > L2-Redundancy > FuseNet > RCP*.
- ☐ En los cuadros *Primary ring/network* y *Secondary ring/network*, compruebe los puertos que se muestran.

```
show redundant-coupling global

Redundant coupling protocol global settings
-------------------------------------------
RCP global state...........................enabled
RCP device configured role..................slave
RCP inner primary interface.................1/1
RCP outer primary interface.................1/2
RCP inner secondary interface...............1/3
RCP outer secondary interface...............1/4
RCP timeout................................45 milliseconds
```

Compare los roles del puente actual en el anillo secundario con los roles de puente necesarios. El puente B deberá ser el puente raíz.

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Switching > L2-Redundancy > Spanning Tree > Dual RSTP*.
- ☐ En el cuadro *Topology information*, marque la configuración de la casilla *Bridge is root*.

```
show spanning-tree drstp

Dual Spanning Tree Information:
-------------------------------
Spanning Tree Mode.........................RSTP
Spanning Tree Trap Mode....................enabled
Bridge is root.............................true
...
```

Compare los roles de puerto actuales de los puentes del anillo principal con los roles de puerto necesarios:

- ▶ Para los puertos del puente D que llevan al puente C:
  Rol `alternate`

- Para el resto de puertos de los puentes que dirigen en la dirección del puente raíz A:
  Rol *root*
- Para el resto de puertos de los puentes que dirigen en la dirección del puente raíz de reserva D:
  Rol *designated*

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Switching > L2-Redundancy > Spanning Tree > Port*.
- ☐ En la columna *Port role*, compruebe el valor *alternate*, *root* o *designated* tal y como se describió anteriormente.

```
show spanning-tree mst port 0 1/<port>
```

Compare los roles de puerto actuales de los puentes del anillo secundario con los roles de puerto necesarios:

- Para los puertos del puente H que llevan al puente G:
  Rol *alternate*
- Para el resto de puertos de los puentes que dirigen en la dirección del puente raíz B:
  Rol *root*
- Para el resto de puertos de los puentes que dirigen en la dirección del puente raíz de reserva H:
  Rol *designated*

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Switching > L2-Redundancy > Spanning Tree > Port*.
- ☐ En la columna *Port role*, compruebe el valor *alternate*, *root* o *designated* tal y como se describió anteriormente.

```
show spanning-tree mst port 0 1/<port>
```

Si está desactivada la función *RCP* o *Spanning Tree*, el dispositivo desconecta automáticamente la función *Dual RSTP*.

Comprobar el estado de la función *Dual RSTP*.

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Switching > L2-Redundancy > Spanning Tree > Dual RSTP*.
  En el marco *Operation*, el botón radio *Off* está seleccionado.

```
show redundant-coupling status

Redundant coupling protocol status
----------------------------------------
RCP global state.........................forwarding
RCP device actual role...................disabled
Redundancy state availability............redNotAvailable
Primary ring protocol....................NONE
Secondary ring protocol..................NONE
```

Finalización de la configuración

Para los dispositivos A a J, guarde la configuración en la memoria no volátil. Siga las instrucciones de la sección “Grabación de un perfil de configuración” en página 101.

14 Diagnóstico de funcionamiento

El dispositivo le ofrece las siguientes herramientas de diagnóstico:
- Enviar trampas SNMP
- Monitorizar el estado del dispositivo
- Señalizar Out-of-Band mediante el contacto de señalización.
- Indicación del estado del puerto
- Contador de eventos en el nivel de puerto
- Detectar la falta de coincidencia de los modos dúplex
- Auto-Disable
- Mostrar el estado de SFP
- Detección de la topología
- Detectar conflictos de direcciones IP
- Detectar bucles
- Ayuda a proteger frente a bucles de red de capa 2
- Informes
- Supervisar el tráfico de datos de un puerto (duplicación de puertos)
- Syslog
- Event log ‹Registro de eventos›
- Gestión de causas y acciones durante el autodiagnóstico

14.1 Enviar trampas SNMP

El dispositivo informa inmediatamente sobre eventos no habituales que se produzcan durante el funcionamiento normal de la estación de administración de red. Este proceso se lleva a cabo mediante mensajes denominados trampas SNMP que omiten el procedimiento de sondeo ("sondeo" se refiere a la consulta de estaciones de datos a intervalos regulares). Las trampas SNMP le permiten reaccionar con rapidez ante eventos no habituales.

Algunos ejemplos de tales eventos son:
- Hardware reset ‹Restablecimiento de hardware›
- Cambios en la configuración
- Segmentación de un puerto

El dispositivo envía trampas SNMP a diferentes hosts para elevar la seguridad de transmisión de los mensajes. Un mensaje de trampa SNMP no confirmado consiste en un paquete con información sobre un evento no habitual.

El dispositivo envía trampas SNMP a los host introducidos en la tabla de destino de las trampas. El dispositivo le permite configurar la tabla de destino de las trampas con la estación de administración de red mediante SNMP.

14.1.1 Lista de trampas SNMP

La siguiente tabla muestra las posibles trampas SNMP enviadas por el dispositivo.

Tabla 51: Posibles trampas SNMP

Nombre de la trampa SNMP	Significado
authenticationFailure	Si una estación intenta acceder a un agente sin autorización, se envía esta trampa.
coldStart	Enviado después de un reinicio.
sa2DevMonSenseExtNvmRemoval	Si se ha eliminado una memoria externa, se envía esta trampa.
linkDown	Si se interrumpe la conexión a un puerto, se envía esta trampa.
linkUp	Si se establece la conexión a un puerto, se envía esta trampa.
sa2DevMonSensePSState	Si el estado de una fuente de alimentación cambia, se envía esta trampa.
sa2SigConStateChange	Si el estado del contacto de señalización en la monitorización de funcionamiento cambia, se envía esta trampa.
newRoot	Si el agente emisor pasa a ser la nueva raíz del Spanning Tree, se envía esta trampa.
topologyChange	Si el puerto cambia de blocking a forwarding o de forwarding a blocking, se envía esta trampa.
alarmRisingThreshold	Si la entrada RMON sobrepasa el umbral superior, se envía esta trampa.
alarmFallingThreshold	Si la entrada RMON se encuentra por debajo del umbral inferior, se envía esta trampa.
sa2AgentPortSecurityViolation	Si una dirección MAC detectada en este puerto no coincide con los ajustes actuales del parámetro sa2AgentPortSecurityEntry, se envía esta trampa.
sa2DiagSelftestActionTrap	Si se realiza un autodiagnóstico para las cuatro categorías "tarea", "recurso", "software" y "hardware" según los ajustes configurados, se envía esta trampa.
sa2MrpReconfig	Si la configuración del anillo MRP cambia, se envía esta trampa.
sa2DiagIfaceUtilizationTrap	Si se sobrepasa el umbral de la interfaz o se reduce el umbral especificado superior o inferior, se envía esta trampa.
sa2LogAuditStartNextSector	Si, tras completar un sector, el código de auditoría comienza uno nuevo, se envía esta trampa.
sa2PtpSynchronizationChance	Si el estado de la sincronización PTP cambia, se envía esta trampa.
sa2ConfigurationSavedTrap	Si el dispositivo ha guardado satisfactoriamente su configuración a nivel local, se envía esta trampa.
sa2ConfigurationChangedTrap	Si cambia por primera vez la configuración del dispositivo después de guardarla a nivel local, se envía esta trampa.
sa2PlatformStpInstanceLoopInconsistentStartTrap	Si el puerto de esta instancia STP cambia al estado "loop inconsistent", se envía esta trampa.
sa2PlatformStpInstanceLoopInconsistentEndTrap	Si el puerto de esta instancia STP abandona el estado "loop inconsistent" y recibe un paquete BPDU, se envía esta trampa.

14.1.2 Trampas SNMP para actividades de configuración

Después de guardar una configuración en la memoria, el dispositivo envía una `sa2Configura-tionSavedTrap`. Esta trampa SNMP contiene tanto las variables de estado de la memoria no volátil (*NVM*) como de la memoria no volátil externa (*ENVM*), que indican si la configuración que se está ejecutando está sincronizada con la memoria no volátil y con la memoria no volátil externa. También puede activar esta trampa SNMP copiando un archivo de configuración en el dispositivo y sustituyendo la configuración guardada activa.

Además, el dispositivo envía una `sa2ConfigurationChangedTrap` cada vez que cambie la configuración local, indicando una falta de coincidencia entre la configuración en ejecución y la configuración guardada.

14.1.3 Configuración de trampas SNMP

El dispositivo le permite enviar una trampa SNMP como reacción ante eventos específicos. Cree al menos un destino de trampas para la recepción de trampas SNMP.

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Diagnostics > Status Configuration > Alarms (Traps)*.
- ☐ Haga clic en el botón .
  El cuadro de diálogo muestra la ventana *Create*.
- ☐ En el cuadro *Name*, especifique el nombre que el dispositivo utiliza para identificarse como el origen de la trampa SNMP.
- ☐ En el cuadro *Address*, especifique la dirección IP del destino de trampas al que el dispositivo envía las trampas SNMP.
- ☐ En la columna *Active*, seleccione las entradas que el dispositivo tendrá en cuenta al enviar las trampas SNMP.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón .

Por ejemplo, en los siguientes cuadros de diálogo, especifique el momento en que el dispositivo debe activar una trampa SNMP:

- Cuadro de diálogo *Basic Settings > Port*
- Cuadro de diálogo *Basic Settings > Power over Ethernet > Global*
- Cuadro de diálogo *Network Security > Port Security*
- Cuadro de diálogo *Switching > L2-Redundancy > Link Aggregation*
- Cuadro de diálogo *Diagnostics > Status Configuration > Device Status*
- Cuadro de diálogo *Diagnostics > Status Configuration > Security Status*
- Cuadro de diálogo *Diagnostics > Status Configuration > Signal Contact*
- Cuadro de diálogo *Diagnostics > Status Configuration > MAC Notification*
- Cuadro de diálogo *Diagnostics > System > IP Address Conflict Detection*
- Cuadro de diálogo *Diagnostics > System > Selftest*
- Cuadro de diálogo *Diagnostics > Ports > Port Monitor*
- Cuadro de diálogo *Advanced > Digital IO Module*

14.1.4 Mensajes ICMP

El dispositivo le permite utilizar el Protocolo de control de mensajes de Internet (ICMP, Internet Control Message Protocol) para las aplicaciones de diagnóstico, por ejemplo, la ruta ping y trace. El dispositivo también utiliza el ICMP para los mensajes de período de vida y de descarte en los que el dispositivo reenvía un mensaje ICMP al dispositivo de origen del paquete.

Utilice la herramienta de red ping para realizar la prueba de la ruta hasta un host en particular a través de la red IP. La herramienta de diagnóstico Traceroute muestra las rutas y retrasos de tránsito de los paquetes a través de la red.

14.2 Monitorizar el estado del dispositivo

El estado del dispositivo proporciona un resumen de la condición general del dispositivo. Muchos sistemas de visualización de procesos registran el estado del dispositivo para presentar su condición en forma de gráfico.

El dispositivo muestra su estado actual como `error` o `ok` en el cuadro *Device status*. El dispositivo determina este estado a partir de los resultados de la supervisión individual.

El dispositivo le permite:
- Señalizar Out-of-Band mediante un contacto de señalización
- señalar el estado modificado del dispositivo mediante el envío de una trampa SNMP
- detectar el estado del dispositivo en el cuadro de diálogo *Basic Settings* > *System* de la interfaz gráfica de usuario
- solicitar el estado del dispositivo en la interfaz de línea de comando

La pestaña *Global* del cuadro de diálogo *Diagnostics* > *Status Configuration* > *Device Status* le permite configurar el dispositivo para enviar una trampa a la estación de administración en los siguientes casos:
- Tensión de alimentación incorrecta
  - al menos una de las 2 tensiones de alimentación no funciona
  - la tensión de alimentación interna no funciona
- Si el dispositivo está funcionando fuera del umbral de temperatura definido por el usuario
- Pérdida de la redundancia (en el modo Ring Manager)
- La interrupción de las conexiones de enlace
  Configure al menos un puerto para esta función. Si el enlace se cae, especifique qué puertos indica el dispositivo en la pestaña *Port* del cuadro de diálogo *Diagnostics* > *Status Configuration* > Device Status de la fila *Propagate connection error*.
- La extracción de la memoria externa.
  La configuración de la memoria externa no está sincronizada con la configuración del dispositivo.

Seleccione las entradas correspondientes para decidir qué eventos incluye el estado del dispositivo.

Nota: En caso de una alimentación no redundante de la tensión de alimentación, el dispositivo informa de falta de tensión. Para desactivar este mensaje, suministre la tensión de alimentación a través de las dos entradas o ignore la monitorización.

14.2.1 Eventos que pueden monitorizarse

Tabla 52: Eventos de Device Status

Nombre	Significado
Temperature	Supervisión en caso de que la temperatura sobrepase o no alcance el valor especificado.
Ring redundancy	En caso de haya redundancia de anillo, active esta función.
Connection errors	Active esta función para monitorizar los eventos de enlace de puertos en los que la casilla *Propagate connection error* esté marcada.

Tabla 52: Eventos de Device Status (cont

Nombre	Significado
External memory removal	Active esta función para monitorizar la presencia de un dispositivo de almacenamiento externo.
External memory not in sync	El dispositivo supervisa la sincronización entre la configuración del dispositivo y la configuración almacenada en la memoria externa (*ENVM*).
Power supply	Active esta función para monitorizar la alimentación eléctrica.

14.2.2 Configuración del estado del dispositivo

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Diagnostics > Status Configuration > Device Status*, pestaña *Global*.
- ☐ Para seleccionar los parámetros que se deben monitorizar, marque la casilla de la columna *Monitor*.
- ☐ Para enviar una trampa SNMP a la estación de administración, active la función *Send trap* en el cuadro *Traps*.
- ☐ En el cuadro de diálogo *Diagnostics > Status Configuration > Alarms (Traps)* cree al menos un destino de trampa para la recepción de trampas SNMP.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✓.
- ☐ Abra el cuadro de diálogo *Basic Settings > System*.
- ☐ Para monitorizar la temperatura, en la parte inferior del cuadro *System data*, especifique los umbrales de temperatura.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✓.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`device-status trap`	Si el estado del dispositivo cambia, envíe una trampa SNMP.
`device-status monitor envm-not-in-sync`	Supervisar los perfiles de configuración en el dispositivo y en la memoria externa. El *Device status* cambia a `error` en las siguientes situaciones: • El perfil de configuración solo existe en el dispositivo. • El perfil de configuración en el dispositivo difiere del perfil de configuración en la memoria externa.
`device-status monitor envm-removal`	Supervisar la memoria externa activa. Si extrae la memoria externa activa del dispositivo, el valor del cuadro *Device status* cambia a `error`.

`device-status monitor power-supply 1`	Supervisar la fuente de alimentación `1`. Si el dispositivo detecta un error de alimentación eléctrica, el valor del cuadro *Device status* cambia a `error`.
`device-status monitor ring-redundancy`	Supervisa la redundancia de anillo. El *Device status* cambia a `error` en las siguientes situaciones: • La función de redundancia pasa a estar activa (pérdida de la reserva de redundancia). • El dispositivo consiste en un anillo normal participante y detecta un error en su configuración.
`device-status monitor temperature`	Supervisa la temperatura del dispositivo. En caso de que la temperatura sobrepase o no alcance el valor especificado, el valor del cuadro *Device status* cambia a `error`.

Para que el dispositivo pueda supervisar un enlace activo sin conexión, primero debe activar la función global y, a continuación, activar los puertos individuales.

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Diagnostics > Status Configuration > Device Status*, pestaña *Global*.
- ☐ Para el parámetro *Connection errors*, marque la casilla de la columna *Monitor*.
- ☐ Abra el cuadro de diálogo *Diagnostics > Status Configuration > Device Status*, pestaña *Port*.
- ☐ Para el parámetro *Propagate connection error*, marque la casilla en la columna de los puertos que deben supervisarse.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✔.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`device-status monitor link-failure`	Supervisar el enlace de interfaces/puertos. Si el enlace se interrumpe en un puerto/interfaz supervisado, el valor del cuadro *Device status* cambia a `error`.
`interface 1/1`	Cambiar al modo de configuración de la interfaz `1/1`.
`device-status link-alarm`	Supervisar el enlace de interfaz/puerto. Si el enlace se interrumpe en el puerto/interfaz, el valor del cuadro *Device status* cambia a `error`.

Nota: Los comandos anteriores activan el control y el trapping de los componentes compatibles. Si desea activar o desactivar el control para componentes por separado, consulte la sintaxis correspondiente en el manual de referencia "Interfaz de línea de comando" o en la ayuda de la consola de la interfaz de línea de comando. Para mostrar la ayuda en la interfaz de línea de comando, introduzca un signo de interrogación `?` y pulse la tecla <Intro>.

14.2.3 Visualización del estado del dispositivo

Lleve a cabo los siguientes pasos:

☐ Abra el cuadro de diálogo *Basic Settings > System*.

`show device-status all`	En el modo EXEC Privilege: muestra el estado del dispositivo y la configuración para determinarlo.

14.3 Estado de seguridad

El estado de seguridad ofrece una vista general sobre la seguridad del dispositivo en conjunto. Muchos procesos asisten en la visualización del sistema mediante el registro del estado de seguridad del dispositivo y su presentación posterior en forma de gráfico. El dispositivo muestra el estado de seguridad general en el cuadro de diálogo *Basic Settings > System*, cuadro *Security status*.

En la pestaña *Global* del cuadro de diálogo *Diagnostics > Status Configuration > Security Status*, el dispositivo muestra su estado actual como `error` o `ok` en el cuadro *Security status*. El dispositivo determina este estado a partir de los resultados de la supervisión individual.

El dispositivo le permite:
- Señalizar Out-of-Band mediante un contacto de señalización
- señalar el estado modificado de seguridad mediante el envío de una trampa SNMP
- detectar el estado de seguridad en el cuadro de diálogo *Basic Settings > System* de la interfaz gráfica de usuario
- solicitar el estado de seguridad en la interfaz de línea de comando

14.3.1 Eventos que pueden monitorizarse

Lleve a cabo los siguientes pasos:
- ☐ Especifique los eventos que el dispositivo supervisará.
- ☐ Para el parámetro correspondiente, marque la casilla de la columna *Monitor*.

Tabla 53: Eventos de Security Status

Nombre	Significado
Password default settings unchanged	Tras finalizar la instalación, cambie las contraseñas para aumentar la seguridad. Si las contraseñas activas y predeterminadas no cambian, el dispositivo muestra una alarma.
Min. password length < 8	Cree contraseñas de más de 8 caracteres para mantener una posición de alta seguridad. Cuando está activo, el dispositivo controla la configuración de *Min. password length*.
Password policy settings deactivated	El dispositivo controla la configuración ubicada en el cuadro de diálogo *Device Security > User Management* para los requisitos de la política de contraseñas.
User account password policy check deactivated	El dispositivo controla la configuración de la casilla *Policy check*. Cuando *Policy check* está inactivo, el dispositivo envía una trampa SNMP.
Telnet server active	El dispositivo realiza la monitorización cuando activa la función *Telnet*.
HTTP server active	El dispositivo realiza la monitorización cuando activa la función *HTTP*.
SNMP unencrypted	El dispositivo realiza la monitorización cuando activa la función *SNMPv1* o *SNMPv2*.
Access to system monitor with serial interface possible	El dispositivo realiza la monitorización del estado de supervisión del sistema.
Saving the configuration profile on the external memory possible	El dispositivo realiza la monitorización de la posibilidad de guardar las configuraciones en la memoria no volátil externa.
Link interrupted on enabled device ports	El dispositivo realiza la monitorización del estado de enlace de los puertos activos.

Tabla 53: Eventos de Security Status (cont

Nombre	Significado
Access with Ethernet Switch Configurator possible	El dispositivo realiza la monitorización cuando activa la función de lectura/escritura Ethernet Switch Configurator.
Load unencrypted config from external memory	El dispositivo realiza la monitorización de las configuraciones de seguridad para la carga de la configuración desde una NVM externa.
IEC61850-MMS active	El dispositivo realiza la monitorización de la configuración de activación del protocolo IEC 61850-MMS
Modbus TCP active	El dispositivo controla la configuración de activación del protocolo Modbus TCP/IP.
Self-signed HTTPS certificate present	El dispositivo realiza la monitorización del servidor HTTPS para certificados digitales creados de forma autónoma.

14.3.2 Configuración del estado de seguridad

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Diagnostics > Status Configuration > Security Status*, pestaña *Global*.
- ☐ Para seleccionar los parámetros que se deben monitorizar, marque la casilla de la columna *Monitor*.
- ☐ Para enviar una trampa SNMP a la estación de administración, active la función *Send trap* en el cuadro *Traps*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✔.
- ☐ En el cuadro de diálogo *Diagnostics > Status Configuration > Alarms (Traps)* cree al menos un destino de trampa para la recepción de trampas SNMP.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`security-status monitor pwd-change`	Supervisar la contraseña para las cuentas de usuario configuradas localmente `user` y `admin`. Si la contraseña tiene la configuración por defecto para las cuentas de usuario `user` o `admin`, el valor del cuadro *Security status* cambia a *`error`*.
`security-status monitor pwd-min-length`	Supervisar el valor especificado en la política *Min. password length*. Si el valor de la política *Min. password length* es menor a `8`, el valor del cuadro *Security status* cambia a *`error`*.
`security-status monitor pwd-policy-config`	Supervisar la configuración de la política de contraseñas. Si el valor de al menos una de las siguientes políticas se establece en `0`, el valor del cuadro *Security status* cambia a *`error`*. • *Upper-case characters (min.)* • *Lower-case characters (min.)* • *Digits (min.)* • *Special characters (min.)*

`security-status monitor pwd-policy-inactive`	Supervisar la configuración de la política de contraseñas. Si el valor de al menos una de las siguientes políticas se establece en `0`, el valor del cuadro *Security status* cambia a `error`.
`security-status monitor telnet-enabled`	Supervisar el servidor Telnet. Si activa el servidor Telnet, el valor del cuadro *Security status* cambia a `error`.
`security-status monitor http-enabled`	Supervisar el servidor HTTP. Si activa el servidor HTTP, el valor del cuadro *Security status* cambia a `error`.
`security-status monitor snmp-unsecure`	Supervisar el servidor SNMP. Si al menos una de las siguientes condiciones se cumple, el valor del cuadro *Security status* cambia a `error`: • La función *SNMPv1* está activada. • La función *SNMPv2* está activada. • La encriptación para SNMPv3 está desactivada. Active la encriptación en el cuadro de diálogo *Device Security > User Management*, en el campo *SNMP encryption type*.
`security-status monitor sysmon-enabled`	Supervise la activación de la función System Monitor en el dispositivo.
`security-status monitor extnvm-upd-enabled`	Supervise la activación de la actualización de la memoria no volátil externa.
`security-status monitor iec61850-mms-enabled`	Realiza la monitorización de la función *IEC61850-MMS*. Si activa la función *IEC61850-MMS*, el valor del cuadro *Security status* cambia a `error`.
`security-status trap`	Si el estado del dispositivo cambia, envía una trampa SNMP.

Para que el dispositivo pueda supervisar un enlace activo sin conexión, primero debe activar la función global y, a continuación, activar los puertos individuales.

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Diagnostics > Status Configuration > Security Status*, pestaña *Global*.
- ☐ Para el parámetro *Link interrupted on enabled device ports*, marque la casilla de la columna *Monitor*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✓.
- ☐ Abra el cuadro de diálogo *Diagnostics > Status Configuration > Device Status*, pestaña *Port*.
- ☐ Para el parámetro *Link interrupted on enabled device ports*, marque la casilla en la columna de los puertos que deben supervisarse.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✓.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.

`security-status monitor no-link-enabled`	Supervisar el enlace de los puertos activos. Si el enlace se interrumpe en el puerto activo, el valor del cuadro *Security status* cambia a `error`.
`interface 1/1`	Cambiar al modo de configuración de la interfaz `1/1`.
`security-status monitor no-link`	Supervisar el enlace de la interfaz/puerto `1`.

14.3.3 Visualización del estado de seguridad

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Basic Settings > System*.

`show security-status all`	En el modo EXEC Privilege, se muestra el estado de seguridad y la configuración para determinarlo.

14.4 Señalización Out-of-Band

El dispositivo utiliza los contactos de señalización para controlar dispositivos externos y para la monitorización de las funciones del dispositivo. La monitorización de las funciones le permite realizar diagnósticos remotos.

El dispositivo informa del estado de funcionamiento a través de la interrupción del contacto de señalización libre de potencial (contacto de relé, circuito de corriente de reposo) para el modo seleccionado: El dispositivo realiza la monitorización de las siguientes funciones:

- Tensión de alimentación incorrecta
  - al menos una de las 2 tensiones de alimentación no funciona
  - la tensión de alimentación interna no funciona
- Si el dispositivo está funcionando fuera del umbral de temperatura definido por el usuario
- Eventos de redundancia de anillo
  Pérdida de la redundancia (en el modo Ring Manager)
  En la configuración por defecto, la supervisión de la redundancia de anillo está inactiva. El dispositivo consiste en un anillo normal participante y detecta un error en la configuración local.
- La interrupción de las conexiones de enlace
  Configure al menos un puerto para esta función. En el cuadro *Propagate connection error*, especifique qué puertos señala el dispositivo para una interrupción de enlace. En la configuración por defecto, el control de enlace está inactivo.
- La extracción de la memoria externa.
  La configuración de la memoria externa no coincide con la configuración del dispositivo.

Seleccione las entradas correspondientes para decidir qué eventos incluye el estado del dispositivo.

Nota: En caso de una alimentación no redundante de la tensión de alimentación, el dispositivo informa de falta de tensión. Para desactivar este mensaje, suministre la tensión de alimentación a través de las dos entradas o ignore la monitorización.

14.4.1 Control del contacto de señalización

Con el modo `Manual setting`, puede controlar a distancia este contacto de señalización.

Posibilidades de aplicación:

- Simulación de un error detectado en un control de errores del PLC.
- Mando a distancia de un dispositivo mediante SNMP como, por ejemplo, la activación de una cámara

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Diagnostics* > *Status Configuration* > *Signal Contact*, pestaña *Global*.
- ☐ Para controlar el contacto de señalización manualmente, en el cuadro *Configuration*, seleccione el elemento `Manual setting` en la lista desplegable *Mode*.
- ☐ Para abrir el contacto de señalización, seleccione el botón de opción `open` en el cuadro *Configuration*.
- ☐ Para cerrar el contacto de señalización, seleccione el botón de opción `close` en el cuadro *Configuration*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ☑.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`signal-contact 1 mode manual`	Seleccionar el modo de configuración manual para el contacto de señalización `1`.
`signal-contact 1 state open`	Abrir el contacto de señalización `1`.
`signal-contact 1 state closed`	Cerrar el contacto de señalización `1`.

14.4.2 Supervisión de los estados de dispositivo y seguridad

En el campo *Configuration*, especifique qué eventos debe indicar el contacto de señalización.

- *`Device status`*
  Con esta configuración, el contacto de señalización indica el estado de los parámetros supervisados en el cuadro de diálogo *Diagnostics > Status Configuration > Device Status*.
- *`Security status`*
  Con esta configuración, el contacto de señalización indica el estado de los parámetros supervisados en el cuadro de diálogo *Diagnostics > Status Configuration > Security Status*.
- *`Device/Security status`*
  Con esta configuración, el contacto de señalización indica el estado de los parámetros supervisados en los cuadros de diálogo *Diagnostics > Status Configuration > Device Status* y *Diagnostics > Status Configuration > Security Status*.

Configuración de la monitorización

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Diagnostics > Status Configuration > Signal Contact*, pestaña *Global*.
- ☐ Para monitorizar las funciones del dispositivo mediante el contacto de señalización, en el cuadro *Configuration*, especifique el valor *`Monitoring correct operation`* en el campo *Mode*.
- ☐ Para seleccionar los parámetros que se deben monitorizar, marque la casilla de la columna *Monitor*.
- ☐ Para enviar una trampa SNMP a la estación de administración, active la función *Send trap* en el cuadro *Traps*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✓.
- ☐ En el cuadro de diálogo *Diagnostics > Status Configuration > Alarms (Traps)* cree al menos un destino de trampa para la recepción de trampas SNMP.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✓.
- ☐ Especifique los umbrales de temperatura para la monitorización de temperatura en el cuadro de diálogo *Basic Settings > System*.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`signal-contact 1 monitor temperature`	Supervisa la temperatura del dispositivo. Si la temperatura excede o no alcanza los valores límite, el contacto de señalización se abre.

`signal-contact 1 monitor ring-redundancy`	Supervisa la redundancia de anillo. El contacto de señalización se abre en las siguientes situaciones: • La función de redundancia pasa a estar activa (pérdida de la reserva de redundancia). • El dispositivo consiste en un anillo normal participante y detecta un error en su configuración.
`signal-contact 1 monitor link-failure`	Supervisar el enlace de interfaces/puertos. Si el enlace se interrumpe en un puerto/interfaz monitorizado, el contacto de señalización se abre.
`signal-contact 1 monitor envm-removal`	Supervisar la memoria externa activa. Si extrae la memoria externa activa del dispositivo, el contacto de señalización se abre.
`signal-contact 1 monitor envm-not-in-sync`	Supervisar los perfiles de configuración en el dispositivo y en la memoria externa. El contacto de señalización se abre en las siguientes situaciones: • El perfil de configuración solo existe en el dispositivo. • El perfil de configuración en el dispositivo difiere del perfil de configuración en la memoria externa.
`signal-contact 1 monitor power-supply 1`	Supervisar la fuente de alimentación `1`. Si el dispositivo detecta un error de alimentación de tensión, el contacto de señalización se abre.
`signal-contact 1 monitor module-removal 1`	Monitorizar el módulo `1`. Si extrae el módulo `1` del dispositivo, el contacto de señalización se abre.
`signal-contact 1 trap`	Permite al dispositivo enviar una trampa SNMP si el estado de la monitorización de funcionamiento cambia.
`no signal-contact 1 trap`	Desactivar la trampa SNMP

Para que el dispositivo pueda supervisar un enlace activo sin conexión, primero debe activar la función global y, a continuación, activar los puertos individuales.

Lleve a cabo los siguientes pasos:

- ☐ En la columna *Monitor*, active la función *Link interrupted on enabled device ports*.
- ☐ Abra el cuadro de diálogo *Diagnostics > Status Configuration > Device Status*, pestaña *Port*.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`signal-contact 1 monitor link-failure`	Supervisar el enlace de interfaces/puertos. Si el enlace se interrumpe en un puerto/interfaz monitorizado, el contacto de señalización se abre.
`interface 1/1`	Cambiar al modo de configuración de la interfaz `1/1`.
`signal-contact 1 link-alarm`	Supervisar el enlace de interfaz/puerto. Si el enlace se interrumpe en el puerto/interfaz, el contacto de señalización se abre.

Eventos que pueden monitorizarse

Tabla 54: Eventos de Device Status

Nombre	Significado
Temperature	Si la temperatura sobrepasa o no alcanza el valor especificado.
Ring redundancy	En caso de haya redundancia de anillo, active esta función de monitorización.
Connection errors	Active esta función para monitorizar los eventos de enlace de puertos en los que la casilla *Propagate connection error* esté marcada.
External memory not in sync with NVM	El dispositivo supervisa la sincronización entre la configuración del dispositivo y la configuración almacenada en la memoria externa (*ENVM*).
External memory removed	Active esta función para monitorizar la presencia de un dispositivo de almacenamiento externo.
Power supply	Active esta función para monitorizar la alimentación eléctrica.

Visualización del estado del contacto de señalización

El dispositivo ofrece posibilidades adicionales para representar el estado del contacto de señalización:

- Visualización en la interfaz gráfica de usuario
- Consulta en la interfaz de línea de comando

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Basic Settings > System*.
  El cuadro *Signal contact status* muestra el estado del contacto de señalización y le informa de las alarmas que se hayan producido. Si existe una alarma en este momento, el cuadro aparecerá resaltado.

`show signal-contact 1 all`	Mostrar la configuración del contacto de señalización para el contacto de señalización especificado.

14.5 Indicación del estado del puerto

Para ver el estado de los puertos, realice los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Basic Settings > System*.

El cuadro de diálogo muestra el dispositivo con la configuración actual. Además, el cuadro de diálogo indica el estado de los puertos individuales con un símbolo.

Los siguientes símbolos representan el estado de los puertos individuales. En algunas situaciones, estos símbolos interfieren entre sí. Al colocar el puntero del ratón sobre el icono del puerto, aparecerá un cuadro de ayuda con una descripción detallada sobre el estado del puerto.

Tabla 55: Símbolos que identifican el estado de los puertos

Criterio	Symbol ‹Símbolo›
Ancho de banda del puerto	10 Mbits/s Puerto activado, conexión en buen estado, modo Full-Dúplex 100 Mbits/s Puerto activado, conexión en buen estado, modo Full-Dúplex 1000 Mbits/s Puerto activado, conexión en buen estado, modo Full-Dúplex
Modo de funcionamiento	El modo Half-Dúplex está activado Consulte el cuadro de diálogo *Basic Settings > Port*, pestaña *Configuration*, casilla *Automatic configuration*, campo *Manual configuration* y campo *Manual cable crossing (Auto. conf. off)*. Autonegociación activada Consulte el cuadro de diálogo *Basic Settings > Port*, pestaña *Configuration*, casilla *Automatic configuration*. El puerto está bloqueado por una función de redundancia.
AdminLink	El puerto está desactivado, conexión en buen estado El puerto está desactivado, no se ha establecido conexión Consulte el cuadro de diálogo *Basic Settings > Port*, pestaña *Configuration*, casilla *Port on* y campo *Link/Current settings*.

14.6 Contador de eventos del puerto

La tabla de estadísticas del puerto permite a los administradores de red expertos identificar posibles problemas detectados en la red.

Esta tabla muestra los contenidos de distintos contadores de eventos. Los contadores de paquetes agrupan los eventos enviados y los eventos recibidos. En el cuadro de diálogo *Basic Settings > Restart*, puede reiniciar los contadores de eventos.

Tabla 56: Ejemplos de avisos sobre puntos débiles detectados

Contador	Aviso de un posible punto débil detectado
Fragmentos recibidos	• Controlador no operativo del dispositivo conectado • Interferencia electromagnética en el medio de transmisión
Error CRC	• Controlador no operativo del dispositivo conectado • Interferencia electromagnética en el medio de transmisión • Un componente de la red no funciona
Colisiones	• Controlador no operativo del dispositivo conectado • Red sobrecargada/líneas demasiado largas • Colisión o error reconocido con un paquete de datos

Lleve a cabo los siguientes pasos:

- ☐ Para mostrar el contador de eventos, abra el cuadro de diálogo *Basic Settings > Port*, pestaña *Statistics*.
- ☐ Para reiniciar los contadores, en el cuadro de diálogo *Basic Settings > Restart*, haga clic en el botón *Clear port statistics*.

14.6.1 Detectar la falta de coincidencia de los modos dúplex

Se producen problemas si 2 puertos directamente conectados entre sí tienen modos dúplex que no coinciden. Estos problemas son difíciles de rastrear. La función de detección automática y comunicación de esta situación tiene la ventaja de permitir la detección de falta de coincidencia de los modos dúplex antes de que se produzcan problemas.

Esta situación puede producirse por una configuración errónea, por ejemplo, si se ha desactivado la configuración automática en el puerto remoto.

Un efecto típico de esta falta de coincidencia es que la conexión parece funcionar con velocidades de transferencia de datos bajas, pero el dispositivo local cuenta gran número de errores CRC cuando el tráfico bidireccional aumenta, quedando el caudal de datos de la conexión muy por debajo del nominal.

El dispositivo le permite detectar esta situación y comunicarlo a la estación de administración de red. Para ello, el dispositivo evalúa el contador de errores del puerto en función de la configuración del mismo.

Posibles causas de error en un puerto

La tabla siguiente enumera los modos de funcionamiento dúplex de los puertos TX y los posibles eventos de errores. Los significados de los términos utilizados en la tabla son los siguientes:

- Colisiones
  En modo Half-Dúplex, las colisiones hacen referencia a un funcionamiento normal.
- Problema dúplex
  Falta de coincidencia de los modos dúplex.
- EMI
  Interferencia electromagnética.
- Expansión de red
  La expansión de la red es excesiva o hay demasiados concentradores en cascada.
- Colisiones, Late Collisions
  En el modo Full-Dúplex, no hay incremento de los contadores de puerto para colisiones o Late Collisions.
- Error CRC
  El dispositivo evalúa estos errores como modos dúplex que no coinciden en el modo Full-Dúplex manual.

Tabla 57: Evaluación de falta de coincidencia del modo dúplex

Núm.	Configuración automática	Modo dúplex actual	Errores detectados (≥ 10 después de Link Up)	Modos dúplex	Causas posibles
1	marcado	Half-Dúplex	Ninguno	OK	
2	marcado	Half-Dúplex	Colisiones	OK	
3	marcado	Half-Dúplex	Late Collisions	Detectado problema dúplex	Problema dúplex, EMI, expansión de red
4	marcado	Half-Dúplex	Error CRC	OK	EMI
5	marcado	Full-Dúplex	Ninguno	OK	
6	marcado	Full-Dúplex	Colisiones	OK	EMI
7	marcado	Full-Dúplex	Late Collisions	OK	EMI
8	marcado	Full-Dúplex	Error CRC	OK	EMI
9	sin marcar	Half-Dúplex	Ninguno	OK	
10	sin marcar	Half-Dúplex	Colisiones	OK	
11	sin marcar	Half-Dúplex	Late Collisions	Detectado problema dúplex	Problema dúplex, EMI, expansión de red
12	sin marcar	Half-Dúplex	Error CRC	OK	EMI
13	sin marcar	Full-Dúplex	Ninguno	OK	
14	sin marcar	Full-Dúplex	Colisiones	OK	EMI
15	sin marcar	Full-Dúplex	Late Collisions	OK	EMI
16	sin marcar	Full-Dúplex	Error CRC	Detectado problema dúplex	Problema dúplex, EMI

14.7 Auto-Disable

El dispositivo puede desactivar un puerto por diferentes razones de configuración. Cada razón causa que el puerto "se cierre". Para recuperar el puerto desde el estado de cierre, puede eliminar manualmente el estado que ha causado que el puerto se cierre o establecer un temporizador para que el puerto se vuelva a activar automáticamente.

Si la configuración muestra un puerto como activado pero el dispositivo detecta un error o un cambio en el estado, el software desconecta ese puerto. En otras palabras, el software del dispositivo desactiva el puerto debido a un error detectado o un cambio de estado.

Si un puerto se desactiva automáticamente, el dispositivo desconecta el puerto de manera efectiva, por lo que el puerto bloquea el tráfico. El LED del puerto parpadea en verde 3 veces por intervalo e identifica la razón por la que se ha desconectado. Además, el dispositivo crea una entrada en el archivo de registro con una lista de las causas de la desactivación. Cuando vuelva a activar el puerto tras un tiempo de espera mediante la función *Auto-Disable*, el dispositivo genera una entrada en el registro.

La función *Auto-Disable* proporciona una función de recuperación que activa automáticamente un puerto desactivado de manera automática tras un intervalo definido por el usuario. Cuando esta función activa un puerto, el dispositivo envía una trampa SNMP con el número del puerto, pero sin un valor para el parámetro *Reason*.

La función *Auto-Disable* sirve para los siguientes propósitos:
- Ayuda al administrador de red en el análisis del puerto.
- Reduce las posibilidades de que el puerto cause la inestabilidad de la red.

La función *Auto-Disable* está disponible para las siguientes funciones:
- *Link flap* (función *Port Monitor*)
- *CRC/Fragments* (función *Port Monitor*)
- Detección de Duplex Mismatch (función *Port Monitor*)
- *DHCP Snooping*
- *Dynamic ARP Inspection*
- *Spanning Tree*
- *Port Security*
- *Overload detection* (función *Port Monitor*)
- *Link speed/Duplex mode detection* (función *Port Monitor*)

En el siguiente ejemplo, configure el dispositivo para desactivar un puerto a causa de violaciones detectadas en los umbrales especificados en el cuadro de diálogo *Diagnostics > Ports > Port Monitor*, pestaña *CRC/Fragments* y, a continuación, vuelva a activar automáticamente el puerto desactivado.

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Diagnostics > Ports > Port Monitor*, pestaña *CRC/Fragments*.
- ☐ Compruebe que los umbrales especificados en la tabla concuerdan con sus preferencias para el puerto `1/1`.
- ☐ Abra el cuadro de diálogo *Diagnostics > Ports > Port Monitor*, pestaña *Global*.
- ☐ Para activar la función, seleccione el botón de opción `On` en el cuadro *Operation*.
- ☐ Para que el dispositivo desactive el puerto a causa de los errores detectados, marque la casilla de la columna *CRC/Fragments on* para el puerto `1/1`.

- En la columna *Action*, puede elegir el modo en que el dispositivo reacciona a los errores detectados. En este ejemplo, el dispositivo desactiva el puerto `1/1` por violaciones de los umbrales y, a continuación, vuelve a activar automáticamente el puerto.
  - Para permitir que el dispositivo desactive y vuelva a activar automáticamente el puerto, seleccione el valor `auto-disable` y configure la función *Auto-Disable*. El valor `auto-disable` solo funciona en combinación con la función *Auto-Disable*.

  El dispositivo también puede desactivar un puerto sin volver a activarlo de nuevo.
  - Para permitir que el dispositivo únicamente desactive el puerto, seleccione el valor `disable port`.

    Para volver a activar manualmente un puerto desactivado, destaque el puerto.

    Haga clic en el botón y, a continuación, en el elemento *Reset*.
  - Cuando configure la función *Auto-Disable*, el valor `disable port` también volverá a activar el puerto automáticamente.
- Abra el cuadro de diálogo *Diagnostics > Ports > Port Monitor*, pestaña *Auto-disable*.
- Para permitir que el dispositivo vuelva a activar automáticamente el puerto desactivado a causa de las violaciones de los umbrales detectadas, marque la casilla de la columna *CRC error*.
- Abra el cuadro de diálogo *Diagnostics > Ports > Port Monitor*, pestaña *Port*.
- Especifique el tiempo de retraso en 120 segundos en la columna *Reset timer [s]* para los puertos que desea volver a activar.

Nota: El elemento *Reset* le permite activar el puerto antes de que el tiempo especificado en la columna *Reset timer [s]* se agote.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`interface 1/1`	Cambiar al modo de configuración de la interfaz `1/1`.
`port-monitor condition crc-fragments count 2000`	Especificar el contador de fragmentos CRC a 2000 partes por millón.
`port-monitor condition crc-fragments interval 15`	Establecer el intervalo de medición en 15 segundos por cada detección de fragmentos CRC.
`auto-disable timer 120`	Especificar el tiempo de espera de `120` segundos tras el cual la función *Auto-disable* vuelve a activar el puerto.
`exit`	Cambiar al modo de configuración.
`auto-disable reason crc-error`	Activar la función CRC de desactivación automática.
`port-monitor condition crc-fragments mode`	Activar el estado de fragmentos CRC para que provoque una acción.
`port-monitor operation`	Activar la función *Port Monitor*.

Si el dispositivo desactiva un puerto a causa de violaciones de los umbrales, el dispositivo le permite utilizar los siguientes comandos para reiniciar manualmente el puerto desactivado.

Lleve a cabo los siguientes pasos:

`enable`	Cambiar al modo Privileged EXEC.

```
configure
interface 1/1

auto-disable reset
```

Cambiar al modo de configuración.

Cambiar al modo de configuración de la interfaz 1/1.

Le permite activar el puerto antes de que el temporizador se agote.

14.8 Mostrar el estado de SFP

El indicador de estado de SFP le permite ver las conexiones actuales de los módulos SFP y sus características. Estas características incluyen:

- tipo de módulo
- número de serie del módulo multimedia
- temperatura en °C
- potencia de emisión en mW
- potencia de recepción en mW

Lleve a cabo el paso siguiente:

- ☐ Abra el cuadro de diálogo *Diagnostics > Ports > SFP*.

14.9 Detección de la topología

IEEE 802.1AB define el Protocolo de descubrimiento de capa de enlace (LLDP; Link Layer Discovery Protocol). LLDP le permite detectar automáticamente la topología de red LAN.

Los dispositivos con LLDP activo:
- emiten su conexión e información de administración a los dispositivos vecinos de la misma LAN. Cuando el dispositivo receptor tiene la función *LLDP* activa, se produce la evaluación de los dispositivos.
- reciben su conexión e información de administración de los dispositivos vecinos de la misma LAN, en caso de que los dispositivos adyacentes también tengan LLDP activo.
- crean una base de datos de información de administración y definiciones de objetos para almacenar información sobre los dispositivos adyacentes con LLDP activo.

Como elemento principal, la información de la conexión contiene un identificador exacto y único para el punto de conexión final: MAC (punto de acceso de servicios). Este se compone de un identificador de dispositivo único para toda la red y un identificador de puerto único para este dispositivo.
- Identificador del dispositivo básico (su dirección MAC)
- Identificador del puerto (la dirección MAC del puerto)
- Descripción del puerto
- Nombre del sistema
- Descripción del sistema
- Capacidades del sistema compatibles
- Capacidades del sistema actualmente activas
- ID de la interfaz de la dirección de administración
- ID de VLAN del puerto
- Estado de autonegociación del puerto
- Medio, configuración Half/Full-Dúplex y ajuste de velocidad del puerto
- Información sobre las VLAN instaladas en el dispositivo (ID y nombre de VLAN, con independencia de si el puerto es participante de una VLAN).

Se puede consultar esta información desde una estación de administración de red de dispositivos con LLDP activado. Con esta información, la estación de administración de red puede representar la topología de la red.

Los dispositivos sin soporte de LLDP normalmente bloquean la dirección MAC IEEE LLDP Multicast especial utilizada para intercambiar información. Los dispositivos sin soporte de LLDP descartan los paquetes LLDP. Si coloca un dispositivo que no es compatible con LLDP entre 2 dispositivos compatibles con LLDP, el dispositivo no compatible prohíbe los intercambios de información entre los 2 dispositivos compatibles.

La Base de información de administración (MIB, Management Information Base) de un dispositivo con compatibilidad LLDP guarda la información LLDP en la MIB lldp y en la SA2-LLDP-EXT-HM-MIB y SA2-LLDP-MIB privadas.

14.9.1 Visualización de los resultados de la detección de topología

Muestre la topología de la red. Para ello, siga el siguiente paso:

- ☐ Abra el cuadro de diálogo *Diagnostics > LLDP > Topology Discovery*, pestaña *LLDP*.

Si utiliza un puerto para conectar varios dispositivos, por ejemplo, a través de un concentrador, la tabla contiene una línea por cada dispositivo conectado.

Al activar la visualización de las entradas FDB en la parte inferior de la tabla, podrá mostrar los dispositivos que no tengan compatibilidad LLDP activa en la tabla. En este caso, el dispositivo también incluye información de su FDB (Forwarding Database, Base de datos de reenvíos).

Si conecta el puerto a dispositivos con la función de detección de la topología activa, los dispositivos intercambian unidades de datos LLDP (LLDPDU) y la tabla de topología muestra estos dispositivos vecinos.

Cuando un puerto conecta únicamente dispositivos sin la detección de la topología activa, la tabla contiene una línea para que el puerto indique los dispositivos conectados. La línea contiene el número de dispositivos conectados.

La tabla de direcciones FDB contiene las direcciones MAC de los dispositivos que la tabla de topología mantiene ocultos para que sea más sencilla de comprender.

14.9.2 LLDP-Med

LLDP para dispositivos de punto final multimedia (LLDP-MED) es una extensión de LLDP que funciona entre dispositivos de punto final. Los puntos finales incluyen dispositivos como los teléfonos IP u otros dispositivos o servidores Voice over IP (VoIP), así como dispositivos de red, como switches. Proporciona específicamente soporte para las aplicaciones VoIP. LLDP-MED proporciona este soporte mediante un conjunto adicional de mensajes de advertencia tipo-longitud-valor comunes para funciones como detección, política de red, Power over Ethernet, administración de inventario e información de ubicación.

El dispositivo es compatible con los siguientes mensajes TLV:

- Funciones TLV
  Permite que los puntos finales de LLDP-MED determinen las funciones que soporta el dispositivo conectado y las funciones que el dispositivo ha activado.
- Política de red TLV
  Permite tanto a los dispositivos de conectividad de red como a los puntos finales anunciar configuraciones VLAN y atributos asociados para la aplicación específica en dicho puerto. Por ejemplo, el dispositivo notifica a un teléfono el número VLAN. El teléfono se conecta al switch, obtiene su número VLAN y, a continuación, inicia la comunicación con el control de llamadas.

LLDP-MED ofrece las siguientes funciones:

- Detección de la política de red, incluyendo el ID de VLAN, prioridad 802.1p, y el punto de código DiffServ (DSCP)
- Detección de la topología y ubicación del dispositivo según la información del puerto/MAC de nivel LAN
- Notificación de detección de movimientos de punto final, desde el dispositivo de conectividad de red hacia la aplicación de administración VoIP asociada.
- Identificación de dispositivo extendida para la administración de inventario
- Identificación de las funciones de conectividad de red de punto final, por ejemplo, un teléfono IP de varios puertos con switch integrado o función de puente
- Interacciones a nivel de aplicación con elementos de protocolo LLDP para ofrecer un proceso de inicio puntual de LLDP y permitir la rápida disponibilidad de un servicio de llamadas de emergencia.
- Aplicabilidad de LLDP-MED a entornos WLAN, soporte para Voice over Wireless WLAN

14.10 Detectar bucles

Los bucles pueden producir la interrupción de conexiones o la pérdida de datos en la red. Esto también se aplica a los bucles provisionales. La función de detección y comunicación automática de esta situación permite detectarlos y diagnosticarlos más rápidamente.

⚠ ADVERTENCIA

OPERACIÓN INESPERADA DEL EQUIPO

Para ayudar a evitar bucles durante la fase de configuración, configure cada dispositivo del anillo individualmente. Antes de conectar los trayectos redundantes, complete la configuración de los otros dispositivos de la configuración del anillo.

El incumplimiento de estas instrucciones puede causar la muerte, heridas graves o daños en el equipo.

Una configuración errónea puede producir bucles, por ejemplo, al desactivar un Spanning Tree.

El dispositivo le ofrece la posibilidad de detectar los efectos producidos generalmente por los bucles y comunicar automáticamente la situación a la estación de administración de la red. También tiene la posibilidad de definir de qué grado tienen que ser al menos los efectos de los bucles para que el dispositivo envíe un mensaje.

Un efecto típico de los bucles consiste en el envío de cuadros BPDU desde el puerto designado y su recepción tanto en un puerto diferente del mismo dispositivo como en el mismo puerto en un breve espacio de tiempo.

Para comprobar si el dispositivo ha detectado un bucle, lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Switching > L2-Redundancy > Spanning Tree > Port*, pestaña *CIST*.
- ☐ Compruebe el valor en los campos *Port state* y *Port role*. Si el campo *Port state* muestra el valor `discarding` y el campo *Port role* muestra el valor `backup`, el puerto está en estado de bucle.
  o bien
- ☐ Abra el cuadro de diálogo *Switching > L2-Redundancy > Spanning Tree > Port*, pestaña *Guards*.
- ☐ Compruebe el valor en la columna *Loop state*. Si el campo muestra el valor `true`, el puerto está en estado de bucle.

14.11 Ayuda a proteger frente a bucles de red de capa 2

El dispositivo ayuda a proteger frente a bucles de red de capa 2.

Un bucle de red puede conducir a un estancamiento de la red debido a una sobrecarga. Uno de los posibles motivos es la continua duplicación de paquetes de datos debido a un fallo de configuración. El motivo podría deberse a, por ejemplo, un cable mal conectado o un ajuste incorrecto en el dispositivo.

Por ejemplo, puede producirse un bucle de red de capa 2 en los siguientes casos, si no hay ningún protocolo de redundancia activo:
- Dos puertos del mismo dispositivo están directamente conectados entre sí.
- Hay más de una conexión activa establecida entre dos dispositivos.

⚠ ADVERTENCIA

OPERACIÓN INESPERADA DEL EQUIPO

Para ayudar a evitar bucles durante la fase de configuración, configure cada dispositivo de la red de capa 2 individualmente. Antes de conectar los trayectos redundantes, complete la configuración de los otros dispositivos de la red de capa 2.

El incumplimiento de estas instrucciones puede causar la muerte, heridas graves o daños en el equipo.

14.11.1 Ejemplo de aplicación

En la ilustración se muestran ejemplos de posibles bucles de capa 2 en una red. La función *Loop Protection* está activada en cada dispositivo.

▶ **A**: *Modo activo*
Los puertos están diseñados para conectar dispositivos finales funcionan en modo *active*. El dispositivo evalúa y envía paquetes de *detección de bucles* en estos puertos.

- **P**: *Modo pasivo*
  Los puertos que pertenecen a los anillos redundantes funcionan en modo *passive*. El dispositivo solo evalúa paquetes de *detección de bucles* en estos puertos.
- **Bucle 1**..**Bucle 4**
  Bucles de red de capa 2 configurados de manera no intencionada.

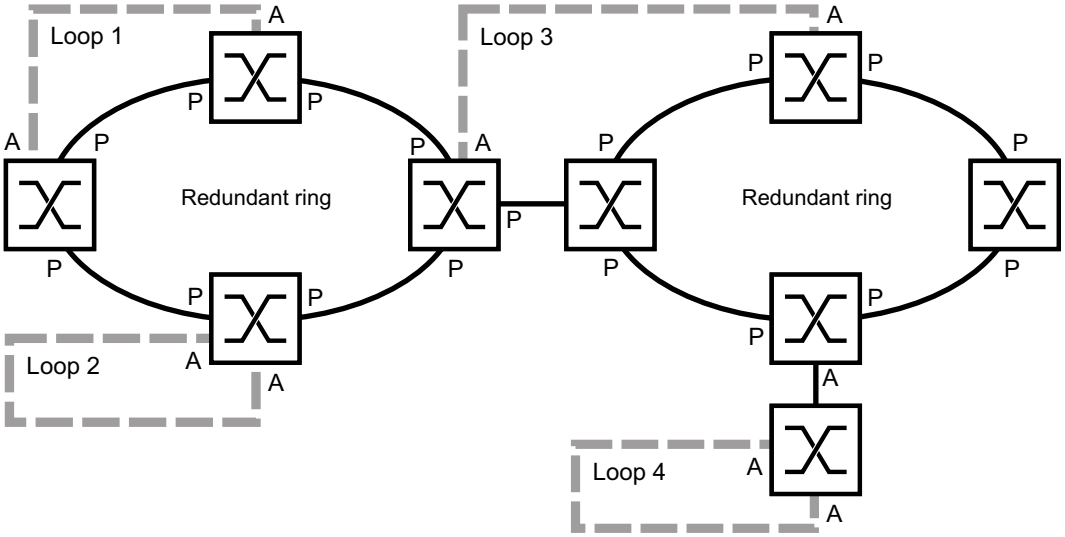


Figura 73: Ejemplos para bucles de red de capa 2 no intencionados

Asigne la configuración de Loop Protection a los puertos

Para cada puerto *activo* y *pasivo*, asigne los ajustes de la función *Loop Protection*.

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Diagnostics > Loop Protection*.
- ☐ En el cuadro *Global* del campo *Transmit interval*, ajuste el valor si es necesario.
- ☐ En el cuadro *Global* del campo *Receive threshold*, ajuste el valor si es necesario.
- ☐ En la columna *Mode*, especifique el comportamiento de la función *Loop Protection* en el puerto:
  - `active` para puertos diseñados para conectar dispositivos finales
  - `passive` para puertos que pertenecen a los anillos redundantes
- ☐ En la columna *Action*, especifique el valor *all*.
  Si el dispositivo detecta un bucle de capa 2 en este puerto, envía una trampa y desactiva el puerto mediante la función *Auto-Disable*. Si es necesario, ajuste el valor.
- ☐ Marque la casilla en la columna *Active*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✓.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`loop-protection tx-interval 5`	Especifique el intervalo de transmisión si es necesario.
`loop-protection rx-threshold 1`	Especifique el umbral de recepción si es necesario.

`interface 1/1`	Cambie al modo de interfaz. Ejemplo: puerto *1/1*.
`loop-protection mode active`	Especifique el modo `active` para puertos diseñados para conectar dispositivos finales.
`loop-protection mode passive`	Especifique el modo `passive` para puertos que pertenecen a los anillos redundantes.
`loop-protection action all`	Especifique la acción que el dispositivo lleva a cabo cuando detecta un bucle de red de capa 2 en este puerto.
`loop-protection operation`	Activar la función *Loop Protection* en el puerto.
`exit`	Cambiar al modo de configuración.

Active la función Auto-Disable

Una vez asignados los ajustes de *Loop Protection* a los puertos, active la función *Auto-Disable*.

Lleve a cabo los siguientes pasos:

- ☐ En el cuadro *Configuration*, marque la casilla *Auto-disable*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ☑.

`loop-protection auto-disable`	Activar la función *Auto-Disable*.

Active la función Loop Protection en el dispositivo

Cuando acabe, active la función *Loop Protection* en el dispositivo.

Lleve a cabo los siguientes pasos:

- ☐ En el cuadro *Operation*, seleccione el botón de opción *On*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ☑.

`loop-protection operation`	Active la función *Loop Protection* en el dispositivo.

14.11.2 Recomendaciones para puertos redundantes

Dependiendo de los ajustes de *Loop Protection*, el dispositivo desactiva puertos utilizando la función *Auto-Disable* cuando el dispositivo detecta un bucle de red de capa 2.

Si hay alguna función de redundancia activa en un puerto, no active el modo *active* en este puerto. De lo contrario, es posible que se produzcan apagados en los puertos en rutas de red redundantes. En el ejemplo anterior, estos son los puertos que pertenecen a los anillos redundantes.

Compruebe que está disponible una ruta de red redundante como soporte de respaldo. El dispositivo cambia a la ruta redundante en caso de que la ruta principal no esté disponible.

Los ajustes siguientes ayudan a evitar apagados de los puertos en rutas de red redundantes:

- ☐ Desactive la función *Loop Protection* en puertos redundantes.
  o bien
- ☐ Active el modo *passive* en puertos redundantes.

La función *Loop Protection* y *Spanning Tree* se afectan mutuamente. Los pasos siguientes ayudan a evitar comportamientos inesperados del dispositivo:

- ☐ Desactive la función *Spanning Tree* en el puerto en el que desee activar la función *Loop Protection*. Consulte el cuadro de diálogo *Switching > L2-Redundancy > Spanning Tree > Port*, columna *STP active*.
- ☐ Desactive la función *Spanning Tree* en el puerto conectado de cada dispositivo conectado. Consulte el cuadro de diálogo *Switching > L2-Redundancy > Spanning Tree*.

14.12 Utilizando la función Email Notification

El dispositivo le permite informar a los usuarios mediante correo electrónico acerca de los eventos que se han producido. Como requisito previo debe haber un servidor de correo disponible a través de la red en la que el dispositivo transfiere los correos electrónicos.

Para configurar el dispositivo para enviar correos electrónicos, lleve a cabo los pasos de los capítulos siguientes:

- ☐ Especificar la dirección del remitente
- ☐ Especificar los eventos desencadenantes
- ☐ Especificar los destinatarios
- ☐ Especificar el servidor de correo
- ☐ Activar/desactivar la función Email Notification
- ☐ Enviar un correo electrónico de prueba

14.12.1 Especificar la dirección del remitente

La dirección del remitente es la dirección de correo electrónico que indica el dispositivo que envió el correo electrónico. En el dispositivo, la configuración predeterminada es .

Cambie el valor preestablecido. Para ello, siga los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Diagnostics > Email Notification > Global*.
- ☐ En el cuadro *Sender*, cambie el valor del campo *Address*.
  Añada una dirección de correo electrónico válida.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón .

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`logging email from-addr <user@doma.in>`	Cambia la dirección del remitente.

14.12.2 Especificar los eventos desencadenantes

El dispositivo distingue entre las siguientes niveles de gravedad:

Tabla 58: Significado de los niveles de gravedad de los eventos

Severity ‹Gravedad›	Significado
`emergency`	El dispositivo no está listo para funcionar
`alert`	Se requiere la intervención inmediata del usuario
`critical`	Estado crítico
`error`	Estado de error
`warning`	Warning (advertencia)

Tabla 58: Significado de los niveles de gravedad de los eventos (cont

Severity ‹Gravedad›	Significado
`notice`	Importante, estado normal
`informational`	Mensaje informal
`debug`	Mensaje de depuración

Puede especificar los eventos de los que desea que le informe el dispositivo. Para esto, asigne el nivel de gravedad mínimo a los niveles de notificación del dispositivo.

El dispositivo informa a los destinatarios de lo siguiente:

- *Notification immediate*
  Si se produce un evento de la gravedad asignada o más graves, el dispositivo enviará un correo electrónico inmediatamente.
- *Notification periodic*
  - Si se produce un evento de la gravedad asignada o más grave, el dispositivo registra el evento en un búfer.
  - El dispositivo envía un correo electrónico con el archivo de registro periódicamente o si el búfer está lleno.
  - Si se produce un evento de una gravedad inferior, el dispositivo no registra este evento.

Lleve a cabo los siguientes pasos:

☐ Abra el cuadro de diálogo *Diagnostics > Email Notification > Global*.

En el cuadro *Notification immediate*, especifique la configuración de los correos electrónicos que el dispositivo envía inmediatamente.

☐ En el campo *Severity*, especifique el nivel de gravedad mínimo.
☐ En el campo *Subject*, especifique el asunto del correo electrónico.

En el cuadro *Notification periodic*, especifique la configuración de los correos electrónicos que el dispositivo envía periódicamente.

☐ En el campo *Severity*, especifique el nivel de gravedad mínimo.
☐ En el campo *Subject*, especifique el asunto del correo electrónico.

☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✔.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`logging email severity immediate <level>`	Especifica la gravedad mínima de los eventos para los que el dispositivo envía un correo electrónico inmediatamente.
`logging email severity periodic <level>`	Especifica la gravedad mínima de los eventos para los que el dispositivo envía periódicamente un correo electrónico.
`logging email subject add <immediate | periodic> TEXT`	Crea una línea de asunto con el contenido `TEXT`.

14.12.3 Cambiar el intervalo de envío

El dispositivo le permite especificar en qué intervalo envía correos electrónicos con el archivo de registro. El ajuste predeterminado es `30` minutos.

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Diagnostics > Email Notification > Global*.

En el cuadro *Notification periodic*, especifique la configuración de los correos electrónicos que el dispositivo envía periódicamente.

- ☐ Cambie el valor del campo *Sending interval [min]* para cambiar el intervalo.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✓.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`logging email duration <30..1440>`	Especifica el intervalo con el que el dispositivo envía correos electrónicos con el archivo de registro.

14.12.4 Especificar los destinatarios

El dispositivo le permite especificar hasta 10 destinatarios.

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Diagnostics > Email Notification > Recipients*.
- ☐ Para añadir una entrada de tabla, haga clic en el botón  .
- ☐ En la columna *Notification type*, especifique si el dispositivo envía los correos electrónicos a este destinatario de manera inmediata o periódica.
- ☐ En la columna *Address*, especifique la dirección de correo electrónico del destinatario.
- ☐ Marque la casilla en la columna *Active*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✓.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`logging email to-addr add <1..10> addr <user@doma.in> msgtype <immediately | periodically>`	Especifica el destinatario con la dirección de correo electrónico `user@doma.in`. El dispositivo gestiona la configuración de la memoria `1..10`.

14.12.5 Especificar el servidor de correo

El dispositivo admite conexiones encriptadas y no encriptadas con el servidor de correo.

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Diagnostics > Email Notification > Mail Server*.
- ☐ Para añadir una entrada de tabla, haga clic en el botón  .
- ☐ En la columna *IP address*, especifique la dirección IP o el nombre de DNS del servidor.
- ☐ En la columna *Encryption*, especifique el protocolo que encripta la conexión entre el dispositivo y el servidor de correo.
- ☐ Cuando el servidor de correo utiliza un puerto distinto del puerto conocido, especifique el puerto TCP en la columna *Destination TCP port*.

Cuando el servidor de correo solicita una autenticación:

- ☐ En las columnas *User name* y *Password*, especifique las credenciales de la cuenta que utiliza el dispositivo para autenticarse en el servidor de correo.
- ☐ En la columna *Description*, introduzca un nombre significativo para el servidor de correo.
- ☐ Marque la casilla en la columna *Active*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón  .

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`logging email mail-server add <1..5> addr <IP ADDRESS> [security <none|tlsv1>] [username <USER NAME>] [password <PASSWORD>] [port <1..65535>]`	Especifica el servidor de correo con la dirección IP `IP ADDRESS`. El dispositivo gestiona la configuración de la memoria `1..5`.

14.12.6 Activar/desactivar la función Email Notification

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Diagnostics > Email Notification > Global*.
- ☐ Para activar la función, seleccione el botón de opción `On` en el cuadro *Operation*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón  .

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`logging email operation`	Activa el envío de correos electrónicos.
`no logging email operation`	Desactiva el envío de correos electrónicos.

14.12.7 Enviar un correo electrónico de prueba

El dispositivo le permite comprobar la configuración mediante el envío de un correo electrónico de prueba.

Requisito previo:
- La configuración del correo electrónico debe estar completamente especificada.
- La función *Email Notification* está activada.

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Diagnostics > Email Notification > Mail Server*.
- ☐ Haga clic en el botón ☰ y, a continuación, en el elemento *Connection test*.
  El cuadro de diálogo muestra la ventana *Connection test*.
- ☐ En la lista desplegable de *Recipient*, seleccione a qué destinatarios desea que envíe el dispositivo el correo electrónico de prueba.
- ☐ En el campo *Message text*, especifique el texto del correo electrónico de prueba.
- ☐ Haga clic en el botón *Ok* para enviar el correo electrónico de prueba.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`logging email test msgtype <urgent|non-urgent> TEXT`	Envía un correo electrónico con el contenido `TEXT` a los destinatarios.

Si no ve ningún mensaje de error y los destinatarios obtienen el correo electrónico, significa que la configuración del dispositivo es correcta.

14.13 Informes

Los siguientes informes y botones están disponibles para el diagnóstico:

- Archivo de registro del sistema
  El archivo de registro es un archivo HTML en el que el dispositivo escribe eventos internos del dispositivo.
- Código de auditoría
  Registra de manera satisfactoria comandos y comentarios del usuario. El archivo también incluye registros SNMP.
- Registro persistente
  Si hay una memoria externa disponible, el dispositivo guarda las entradas del registro en un archivo en la memoria externa. Estos archivos están disponibles tras el apagado. Es posible configurar el tamaño y el número máximo de los archivos que se conservan y la gravedad de los eventos registrados. Una vez que el usuario defina el tamaño y el número máximo de archivos que se deben conservar, el dispositivo archiva las entradas e inicia un nuevo archivo. El dispositivo elimina el archivo más antiguo y proporciona un nuevo nombre a los otros archivos para mantener el número de archivos configurados. Para revisar estos archivos, utilice la interfaz de línea de comando o cópielos en un servidor externo para futuras referencias.
- *Download support information*
  Este botón le permite descargar información del sistema como archivo ZIP.

En caso de mantenimiento, estos informes le ofrecen al técnico la información necesaria.

14.13.1 Configuración global

Mediante este cuadro de diálogo, puede activar o desactivar a dónde se envían los informes del dispositivo, por ejemplo, a una consola, un servidor Syslog o una conexión de la interfaz de línea de comando. También puede establecer el nivel de gravedad para que el dispositivo registre los eventos en estos informes.

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Diagnostics > Report > Global*.
- ☐ Para enviar un informe a la consola, especifique el nivel deseado en el cuadro *Console logging*, campo *Severity*.
- ☐ Para activar la función, seleccione el botón de opción `On` en el cuadro *Console logging*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ☑.

El dispositivo almacena en búfer los eventos registrados en 2 áreas de almacenamiento individuales para mantener las entradas del registro para eventos urgentes. Especifique la gravedad mínima de los eventos que el dispositivo debe registrar en el área de almacenamiento en búfer con una prioridad más alta.

Lleve a cabo los siguientes pasos:

- ☐ Para enviar eventos al almacenamiento en búfer, especifique el nivel deseado en el cuadro *Buffered logging*, campo *Severity*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ☑.

Al activar el registro de las solicitudes SNMP, el dispositivo registra las solicitudes como eventos en Syslog. La función *Log SNMP get request* registra las solicitudes del usuario para la información de configuración del dispositivo. La función *Log SNMP set request* registra los eventos de configuración del dispositivo. Especifique el nivel mínimo de los eventos que el dispositivo debe registrar en Syslog.

Lleve a cabo los siguientes pasos:

- ☐ Active la función *Log SNMP get request* del dispositivo para enviar solicitudes de lectura SNMP como eventos al servidor Syslog.
  Para activar la función, seleccione el botón de opción `On` en el cuadro *SNMP logging*.
- ☐ Active la función *Log SNMP set request* del dispositivo para enviar solicitudes de escritura SNMP como eventos al servidor Syslog.
  Para activar la función, seleccione el botón de opción `On` en el cuadro *SNMP logging*.
- ☐ Seleccione el nivel de gravedad deseado para las solicitudes de recepción y ajuste.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✔.

Si está activo, el dispositivo registra los cambios de configuración realizados mediante la interfaz de línea de comando en el código de auditoría. Esta función se basa en el estándar IEEE 1686 para dispositivos electrónicos inteligentes de subestaciones.

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Diagnostics > Report > Global*.
- ☐ Para activar la función, seleccione el botón de opción `On` en el cuadro *CLI logging*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✔.

El dispositivo le permite guardar los siguientes datos de información del sistema en un archivo ZIP en su ordenador:

- `audittrail.html`
- `defaultconfig.xml`
- `script`
- `runningconfig.xml`
- `supportinfo.html`
- `systeminfo.html`
- `systemlog.html`

El dispositivo crea el nombre del archivo ZIP automáticamente en formato `<IP_address>_<system_name>.zip`.

Lleve a cabo los siguientes pasos:

- ☐ Haga clic en el botón ☰ y, a continuación, en el elemento *Download support information*.
- ☐ Seleccione el directorio en el que desea guardar la información de soporte.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✔.

14.13.2 Syslog

El dispositivo le permite enviar mensajes sobre eventos internos del dispositivo a uno o varios servidores Syslog (hasta 8). Además, puede registrar como eventos en el Syslog las consultas SNMP realizadas al dispositivo.

Nota: Para mostrar los eventos registrados, abra el cuadro de diálogo *Diagnostics > Report > Audit Trail* o el cuadro de diálogo *Diagnostics > Report > System Log*.

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Diagnostics > Syslog*.
- ☐ Para añadir una entrada de tabla, haga clic en el botón .
- ☐ En la columna *IP address*, introduzca la dirección IP o *Hostname* del servidor Syslog. Puede especificar una dirección IPv4 o IPv6 válida para el servidor Syslog.
- ☐ En la columna *Destination UDP port*, especifique el puerto TCP o UDP en el que el servidor Syslog espera las entradas del registro.
- ☐ En la columna *Min. severity*, especifique el nivel de gravedad mínimo que debe tener un evento para que el dispositivo envíe una entrada de registro al servidor Syslog.
- ☐ Marque la casilla de la columna *Active*.
- ☐ Para activar la función, seleccione el botón de opción `On` en el cuadro *Operation*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón .

En el cuadro *SNMP logging*, configure los siguientes ajustes para solicitudes de lectura y escritura SNMP:

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Diagnostics > Report > Global*.
- ☐ Active la función *Log SNMP get request* del dispositivo para enviar solicitudes de lectura SNMP como eventos al servidor Syslog.
  Para activar la función, seleccione el botón de opción `On` en el cuadro *SNMP logging*.
- ☐ Active la función *Log SNMP set request* del dispositivo para enviar solicitudes de escritura SNMP como eventos al servidor Syslog.
  Para activar la función, seleccione el botón de opción `On` en el cuadro *SNMP logging*.
- ☐ Seleccione el nivel de gravedad deseado para las solicitudes de recepción y ajuste.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón .

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`logging host add 1 addr 10.0.1.159 severity 3`	Añadir un nuevo receptor en la lista de servidores Syslog. El valor `3` especifica el nivel de gravedad del evento que el dispositivo debe registrar. El valor `3` significa `error`.
`logging host add 2 addr 2001::1 severity 4`	Añada un nuevo destinatario IPv6 en la lista de servidores Syslog. El valor `4` significa `warning`.
`logging syslog operation`	Activar la función *Syslog*.
`exit`	Cambiar al modo Privileged EXEC.

```
show logging host                          Mostrar la configuración de host de Syslog.
No.    Server IP      Port   Max. Severity   Type        Status
-----  -------------- -----  --------------  ----------  -------
1      10.0.1.159     514    error           systemlog   active
2      2001::1        514    warning         systemlog   active
configure                                  Cambiar al modo de configuración.
logging snmp-requests get operation        Registrar las solicitudes de SNMP GET.
logging snmp-requests get severity 5       El valor 5 especifica el nivel de gravedad del
                                           evento que el dispositivo debe registrar en caso de
                                           solicitudes de SNMP GET. El valor 5 significa
                                           notice.
logging snmp-requests set operation        Registra las solicitudes de SNMP SET.
logging snmp-requests set severity 5       El valor 5 especifica el nivel de gravedad del
                                           evento que el dispositivo debe registrar en caso de
                                           solicitudes de SNMP SET. El valor 5 significa
                                           notice.
exit                                       Cambiar al modo Privileged EXEC.
show logging snmp                          Mostrar la configuración de la función SNMP
                                           Logging.
Log SNMP GET requests              : enabled
Log SNMP GET severity              : notice
Log SNMP SET requests              : enabled
Log SNMP SET severity              : notice
```

14.13.3 Registro del sistema

El dispositivo le permite abrir un archivo de registro de eventos del sistema. La tabla del cuadro de diálogo *Diagnostics > Report > System Log* muestra los eventos registrados.

Lleve a cabo los siguientes pasos:

- ☐ Para actualizar el contenido del registro, haga clic en el botón .
- ☐ Para guardar el contenido del registro como un archivo html, haga clic en el botón y, a continuación, en el elemento *Reset*.
- ☐ Para eliminar el contenido del registro, haga clic en el botón y, a continuación, en el elemento *Reset*.
- ☐ Para buscar el contenido del registro con una palabra clave, utilice la función de búsqueda de su navegador web.

Nota: También tiene la opción de enviar los eventos registrados a uno o varios servidores Syslog.

14.13.4 Syslog a través de TLS

La Seguridad de capa de transporte (TLS) es un protocolo criptográfico diseñado para proporcionar seguridad en la comunicación a través de una red informática. El objetivo principal del protocolo TLS es ofrecer privacidad e integridad de datos entre dos aplicaciones informáticas en comunicación.

Tras iniciar una conexión con un servidor Syslog, utilizando un protocolo de enlace TLS, el dispositivo valida el certificado recibido del servidor. Para este objetivo, debe transferir el certificado PEM desde un servidor remoto o desde la memoria externa al dispositivo. Compruebe que la dirección IP configurada o el nombre DNS del servidor coincidan con la información facilitada en el certificado. Podrá encontrar la información en los campos Nombre común o Nombre alternativo del sujeto del certificado.

El dispositivo envía los mensajes de Syslog cifrados de TLS a través del puerto TCP especificado en la columna *Destination UDP port*.

Nota: Especifique la dirección IP o el nombre DNS en el servidor de modo que coincida con la dirección IP o el nombre DNS proporcionados en el certificado del servidor. Encontrará los valores introducidos en el certificado como Nombre común o Nombre alternativo del sujeto.

Ejemplo

El ejemplo facilitado describe la configuración de la función *Syslog*. Al seguir estos pasos, el dispositivo le permite enviar los mensajes de Syslog cifrados de TLS a través del puerto TCP especificado en la columna *Destination UDP port*.

Los mensajes Syslog que se envían desde un dispositivo a un servidor Syslog pueden atravesar redes no protegidas. Para configurar un servidor Syslog a través de TLS, transfiera el certificado de la autoridad de certificación (CA) al dispositivo.

Nota: Para que los cambios tengan efecto tras cargar un certificado nuevo, reinicie la función *Syslog*.

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Diagnostics > Syslog*.
- ☐ Para iniciar una conexión con los servidores Syslog, seleccione el botón de opción `On` en el cuadro *Operation*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✔.

El dispositivo valida el certificado recibido. El dispositivo también autentica el servidor y comienza a enviar mensajes Syslog.

- ☐ Debe transferir el certificado PEM desde el servidor remoto o desde la memoria externa al dispositivo.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`logging host add 1 addr 192.168.3.215`	Añada el índice `1` al servidor Syslog con la dirección IPv4`192.168.3.215`.
`logging host add 2 addr 2001::1`	Añada el índice `2` al servidor Syslog con la dirección IPv4`2001::1`..

`logging host modify 1 port 6512 type systemlog`	Especifique el número de puerto `6512` y registre los eventos en el registro del sistema.
`logging host modify 1 transport tls`	Especifique el tipo de transmisión como `tls`.
`logging host modify 1 severity informational`	Especifique el tipo de evento para iniciar sesión en el registro del sistema como `informational`.
`exit`	Cambiar al modo Privileged EXEC.
`copy syslogcacert evmm`	Copie certificados CA de una memoria externa al dispositivo.
`show logging host`	Mostrar la configuración de host de Syslog.

14.13.5 Código de auditoría

El cuadro de diálogo *Diagnostics > Report > Audit Trail* contiene información del sistema y cambia la configuración del dispositivo ejecutada a través de la interfaz de línea de comando y SNMP. En caso de que cambie la configuración del dispositivo, el cuadro de diálogo muestra quién, qué y cuándo se ha cambiado.

El cuadro de diálogo *Diagnostics > Syslog* le permite especificar hasta 8 servidores Syslog a los que el dispositivo puede enviar los Códigos de auditoría.

La lista siguiente contiene los eventos de registro:
- Cambios en los parámetros de configuración
- Comandos (excepto `show`) que utilizan la interfaz de línea de comando
- Comando `logging audit-trail <string>` que utiliza la interfaz de línea de comando que registra el comentario
- Cambios automáticos en la hora del sistema
- Eventos watchdog
- Bloqueo de usuario tras varios intentos de inicio de sesión incorrectos
- Inicio de sesión de usuarios, ya sea de manera local o remota, mediante la Interfaz de línea de comando
- Cierre de sesión manual iniciado por el usuario
- Cierre de sesión cronometrado después de un periodo de inactividad definido por el usuario en la Interfaz de línea de comando
- Operaciones de transferencia de archivos, incluidas actualizaciones de firmware
- Cambios de configuración mediante Ethernet Switch Configurator
- Configuración automática o actualizaciones de firmware mediante la memoria externa
- Acceso bloqueado a la gestión del dispositivo debido a un inicio de sesión no válido
- Reinicio
- Abrir y cerrar SNMP a través de túneles HTTPS
- Fallos de alimentación detectados

14.14 Análisis de red con TCPDump

TCPDump es una función UNIX de examen de paquetes utilizada por los administradores de red para examinar y analizar el tráfico de una red. Entre los motivos para examinar el tráfico de una red, se encuentran la verificación de la conectividad entre hosts o el análisis del tráfico que atraviesa la red.

TCPDump en el dispositivo proporciona la posibilidad de decodificar o capturar paquetes recibidos y transmitidos por la CPU de administración. Esta función está disponible mediante el comando `debug`. Consulte el manual de referencia "Interfaz de línea de comando" para obtener más información sobre la función TCPDump.

14.15 Monitorización del tráfico de datos

El dispositivo le permite reenviar los paquete de datos que pasan a través del dispositivo a un puerto de destino. Ahí puede monitorizar y evaluar los paquetes de datos.

El dispositivo le ofrece las siguientes opciones:
- Port Mirroring

14.15.1 Port Mirroring

La función *Port Mirroring* le permite copiar los paquetes de datos desde puertos de origen físicos a un puerto de destino físico.

Puede monitorizar el tráfico de datos a través de los puertos de origen en las direcciones de envío y recepción con una herramienta de administración conectada al puerto de destino, por ejemplo, una sonda RMON. La función no tiene efecto sobre la ejecución de tráfico de datos en los puertos de origen.

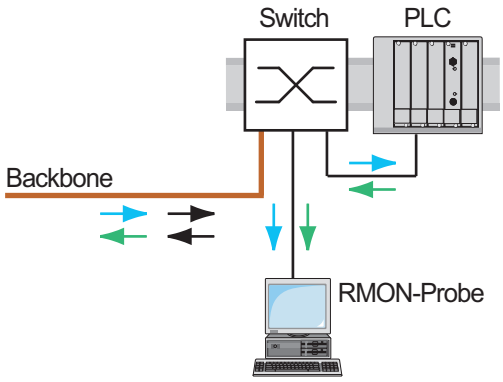


Figura 74: Ejemplo

En el puerto de destino, el dispositivo solo reenvía los paquetes de datos copiados desde los puertos de origen.

Antes de conectar la función *Port Mirroring*, marque la casilla *Allow management* para acceder a la gestión del dispositivo mediante el puerto de destino. El dispositivo permite a los usuarios acceder a la gestión del dispositivo mediante el puerto de destino sin interrumpir la sesión *Port Mirroring* activa.

Nota: El dispositivo duplica los mensajes Multicast, Broadcast y Unicast desconocidos en el puerto de destino.

Los ajustes VLAN del puerto de destino permanecen sin modificar. Un requisito previo para el acceso a la gestión del dispositivo en el puerto de destino es que el puerto de destino sea miembro de la VLAN de administración del dispositivo.

Activación de la función Port Mirroring

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Diagnostics > Ports > Port Mirroring*.
- ☐ Especifique los puertos de origen.
  Marque la casilla de la columna *Enabled* para los puertos correspondientes.
- ☐ Especifique el puerto de destino.
  En el cuadro *Destination port*, seleccione el puerto deseado de la lista desplegable *Primary port*.
  La lista desplegable solo muestra los puertos disponibles. Los puertos que ya se han especificado como puertos de origen no están disponibles.
- ☐ Cuando sea necesario, especifique un segundo puerto de destino.
  En el cuadro *Destination port*, seleccione el puerto deseado de la lista desplegable *Secondary port*.
  El requisito previo es que debe haber especificado un puerto de destino principal.
- ☐ Para acceder a la gestión del dispositivo mediante el puerto de destino:
  En el cuadro *Destination port*, marque la casilla *Allow management*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón  .

Para desactivar la función *Port Mirroring* y restaurar la configuración por defecto, haga clic en el botón  y, a continuación, en el elemento *Reset config*.

14.16 Autodiagnóstico

El dispositivo comprueba sus activos durante el proceso de inicio y, ocasionalmente, en momentos posteriores. El dispositivo comprueba la finalización o disponibilidad de tareas del sistema y el espacio de memoria disponible. Además, el dispositivo comprueba la funcionalidad de la aplicación y si hay alguna degradación de hardware en el conjunto de chips.

Si el dispositivo detecta una pérdida de integridad, responde a esta degradación con una acción definida por el usuario. Se pueden configurar las siguientes categorías.

- `task`
  Acción que se debe tomar en caso de que una tarea no sea satisfactoria.
- `resource`
  Acción que se debe tomar debido a una pérdida de recursos.
- `software`
  Acción tomada ante la pérdida de integridad del software; por ejemplo, una suma de comprobación de segmentos de código o violaciones de acceso.
- `hardware`
  Acción tomada debido a una degradación de hardware.

Configure cada categoría para que se produzca una acción en caso de que el dispositivo detecte una pérdida de integridad. Se pueden configurar las siguientes acciones.

- `log only`
  Esta acción escribe un mensaje en el archivo de registro.
- `send trap`
  Envía un trampa SNMP al destino de las trampas.
- `reboot`
  Si se activa, cualquier error detectado en la categoría provocará que el dispositivo se reinicie.

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Diagnostics > System > Selftest*.
- ☐ En la columna *Action*, especifique la acción que se debe llevar a cabo según la causa.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ☑.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`selftest action task log-only`	Enviar un mensaje al registro de eventos cuando se complete satisfactoriamente una tarea.
`selftest action resource send-trap`	Si hay insuficientes recursos, enviar una trampa SNMP.
`selftest action software send-trap`	Si se ha perdido la integridad del software, enviar una trampa SNMP.
`selftest action hardware reboot`	Reiniciar el dispositivo cuando se produce una degradación del hardware.

La desactivación de estas funciones le permite reducir el tiempo necesario para reiniciar el dispositivo tras un arranque en frío. Encontrará estas opciones en el cuadro de diálogo *Diagnostics > System > Selftest*, cuadro *Configuration*.

- *RAM test*
  Activa/desactiva la función *RAM test* durante un arranque en frío.

- *SysMon1 is available*
  Activa/desactiva la función Supervisión del sistema durante un arranque en frío.
- *Load default config on error*
  Activa/desactiva la carga de la configuración por defecto del dispositivo en caso de que no haya ninguna configuración legible disponible durante el reinicio.

Los siguientes ajustes bloquean su acceso al dispositivo de forma permanente en caso de que el dispositivo no detecte ningún perfil de configuración disponible al reiniciar.
- La casilla *SysMon1 is available* no está marcada.
- La casilla *Load default config on error* no está marcada.

Este es el caso, por ejemplo, si la contraseña del perfil de configuración que está cargando es diferente de la contraseña establecida en el dispositivo. Para desbloquear de nuevo el dispositivo, póngase en contacto con su distribuidor.

Lleve a cabo los siguientes pasos:

`selftest ramtest`	Active el autodiagnóstico de RAM en un arranque en frío.
`no selftest ramtest`	Desactivar la función "ramtest".
`selftest system-monitor`	Activar la función "SysMon1".
`no selftest system-monitor`	Desactivar la función "SysMon1".
`show selftest action`	Mostrar el estado de las acciones que se llevan a cabo en caso de degradación del dispositivo.
`show selftest settings`	Mostrar la configuración para "ramtest" y "SysMon" en caso de un arranque en frío.

14.17 Prueba del cable de cobre

Utilice esta función para comprobar si los cables de cobre conectados a una interfaz tienen un cortocircuito o circuito abierto. La prueba interrumpe el flujo de tráfico en este puerto cuando está en curso.

La tabla muestra el estado y la longitud de cada par individual. El dispositivo devuelve un resultado con el siguiente significado:

- normal: indica que el cable está funcionando correctamente
- abierto: indica una interrupción en el cable
- cortocircuito: indica que hay un cortocircuito en el cable
- sin probar: indica que no se ha comprobado el cable
- desconocido: cable no conectado

15 Funciones avanzadas del dispositivo

15.1 Uso del dispositivo como servidor DHCP

Un servidor DHCP (Dynamic Host Configuration Protocol, Protocolo de configuración dinámica de host) asigna direcciones IP, Gateways y otras definiciones de red como parámetros DNS y NTP a clientes.

Las operaciones de DHCP se dividen en 4 fases básicas: detección de IP, oferta de concesión de IP, solicitud de IP y confirmación de concesión de IP. Utilice el acrónimo DORA (Discovery, Offer, Request, and Acknowledgement; Detección, oferta, solicitud y confirmación) para ayudar a recordar las fases. El servidor recibe datos de clientes en el puerto UDP 67 y reenvía datos al cliente en el puerto UDP 68.

El servidor DHCP proporciona un grupo de direcciones IP, o "Pool", desde el que asigna direcciones IP a los clientes. El Pool consta de una lista de entradas. Una entrada permite definir una dirección IP determinada o un rango de direcciones IP.

El dispositivo le permite activar el servidor DHCP de forma global y por interfaz.

15.1.1 Direcciones IP asignadas por puerto o por VLAN

El servidor DHCP asigna una dirección IP estática o un rango dinámico de direcciones IP a un cliente conectado a un puerto o a una VLAN. El dispositivo le permite crear entradas para un puerto o una VLAN. Al crear una entrada para asignar una dirección IP a una VLAN, la entrada del puerto se atenúa. Al crear una entrada para asignar una dirección IP a un puerto, la entrada de la VLAN se atenúa.

Asignación estática significa que el servidor DHCP asigna la misma dirección IP a un cliente específico. El servidor DHCP identifica al cliente por medio de un identificador de hardware único. Una entrada de dirección estática contiene una dirección IP y la aplica a un puerto o VLAN en el que el servidor recibe una solicitud de un cliente específico. Para la asignación estática, cree una entrada de Pool para los puertos o para un puerto determinado, introduzca la dirección IP y deje la columna *Last IP address* vacía. Especifique un identificador de hardware con el que el servidor DHCP pueda identificar claramente al cliente. Este identificador puede ser una dirección MAC, un identificador de cliente, un identificador remoto o un identificador de circuito. Si un cliente se pone en contacto con el servidor con el identificador de hardware configurado, el servidor DHCP asigna la dirección IP estática.

El dispositivo también le permite asignar un rango de direcciones IP dinámico a los puertos o VLAN desde los que el servidor DHCP asigna una dirección IP libre desde un Pool. Para añadir una entrada de Pool dinámica para los puertos o VLAN, especifique las primeras y últimas direcciones IP para el rango de direcciones IP, dejando las columnas *MAC address*, *Client ID*, *Remote ID* y *Circuit ID* vacías. La creación de varias entradas de Pool le permite disponer de rangos de direcciones IP con huecos.

15.1.2 Ejemplo de dirección IP estática de servidor DHCP

En este ejemplo, configure el dispositivo para asignar una dirección IP estática a un puerto. El dispositivo reconoce clientes con identificación de hardware única. La identificación del hardware en este caso es la dirección MAC del cliente `00:24:E8:D6:50:51`. Para ello, siga los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Advanced > DHCP Server > Pool*.
- ☐ Para añadir una entrada de tabla, haga clic en el botón  .
- ☐ En la columna *IP address*, especifique el valor `192.168.23.42`.
- ☐ En la columna *Port*, especifique el valor `1/1`.
- ☐ En la columna *MAC address*, especifique el valor `00:24:E8:D6:50:51`.
- ☐ Para asignar la dirección IP al cliente de manera infinita, en la columna *Lease time [s]*, especifique el valor `4294967295`.
- ☐ Marque la casilla de la columna *Active*.
- ☐ Abra el cuadro de diálogo *Advanced > DHCP Server > Global*.
- ☐ Para el puerto `1/1`, marque la casilla de la columna *DHCP server active*.
- ☐ Para activar la función, seleccione el botón de opción `On` en el cuadro *Operation*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón  .

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`dhcp-server pool add 1 static 192.168.23.42`	Crear una entrada con el índice `1` y añadir la dirección IP `192.168.23.42` al Pool estático.
`dhcp-server pool modify 1 mode interface 1/1`	Asignar la dirección estática del índice `1` a la interfaz `1/1`.
`dhcp-server pool modify 1 mode mac 00:24:E8:D6:50:51`	Asignar la dirección IP del índice `1` al dispositivo con la dirección MAC `00:24:E8:D6:50:51`.
`dhcp-server pool mode 1`	Activar la entrada del Pool del índice `1`.
`dhcp-server pool modify 1 leasetime infinite`	Para asignar la dirección IP al cliente de manera infinita, modifique la entrada con el índice `1`.
`dhcp-server operation`	Activar el servidor DHCP de forma global.
`interface 1/1`	Cambiar al modo de configuración de la interfaz `1/1`.
`dhcp-server operation`	Activar la función del servidor *DHCP Server* en este puerto.

15.1.3 Ejemplo de rango de dirección IP dinámica del servidor DHCP

El dispositivo le permite crear rangos de direcciones IP dinámicas. Deje los campos *MAC address*, *Client ID*, *Remote ID* y *Circuit ID* vacíos. Para crear rangos de direcciones IP dinámicas con huecos entre ellos, añada varias entradas a la tabla. Para ello, siga los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Advanced* > *DHCP Server* > *Pool*.
- ☐ Para añadir una entrada de tabla, haga clic en el botón .
- ☐ En la columna *IP address*, especifique el valor `192.168.23.92`. Esta es la primera dirección IP del rango.
- ☐ En la columna *Last IP address*, especifique el valor `192.168.23.142`. Esta es la última dirección IP del rango.

En la columna *Lease time [s]*, la configuración por defecto es de 60 días.

- ☐ En la columna *Port*, especifique el valor `1/2`.
- ☐ Marque la casilla de la columna *Active*.
- ☐ Abra el cuadro de diálogo *Advanced* > *DHCP Server* > *Global*.
- ☐ Para el puerto `1/2`, marque la casilla de la columna *DHCP server active*.
- ☐ Para activar la función, seleccione el botón de opción `On` en el cuadro *Operation*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón .

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`dhcp-server pool add 2 dynamic 192.198.23.92 192.168.23.142`	Añadir un Pool dinámico con un rango IP comprendido entre `192.168.23.92` y `192.168.23.142`.
`dhcp-server pool modify 2 leasetime {seconds | infinite}`	Introducir Lease Time en segundos o equivalente a infinito.
`dhcp-server pool add 3 dynamic 192.198.23.172 192.168.23.180`	Añadir un Pool dinámico con un rango IP comprendido entre `192.168.23.172` y `192.168.23.180`.
`dhcp-server pool modify 3 leasetime {seconds | infinite}`	Introducir Lease Time en segundos o equivalente a infinito.
`dhcp-server pool mode 2`	Activar la entrada del Pool del índice `2`.
`dhcp-server pool mode 3`	Activar la entrada del Pool del índice `3`.
`dhcp-server operation`	Activar el servidor DHCP de forma global.
`interface 2/1`	Cambiar al modo de configuración de la interfaz `2/1`.
`dhcp-server operation`	Activar la función del servidor *DHCP Server* en este puerto.

15.2 DHCP L2 Relay ‹Retransmisión DHCP L2›

Encontrará el siguiente mensaje de advertencia en el panel frontal de su dispositivo:

⚠ ADVERTENCIA

OPERACIÓN INESPERADA

No cambie la posición del cable si la Opción 82 del DHCP está activada. Consulte el manual de usuario antes de efectuar el trabajo.

El incumplimiento de estas instrucciones puede causar la muerte, heridas graves o daños en el equipo.

Un administrador de red utiliza el *agente de retransmisión* DHCP de Capa 2 para añadir la información del cliente DHCP. Esta información es necesaria para que los *agentes de retransmisión* de Capa 3 y los servidores DHCP asignen una dirección y configuración a un cliente.

Cuando un servidor y un cliente DHCP están en la misma subred IP, intercambian directamente solicitudes y respuestas de dirección IP. Sin embargo, tener un servidor DHCP en cada subred es caro y, a menudo, poco factible. Una alternativa a tener un servidor DHCP en cada subred es utilizar los dispositivos de red para retransmitir paquetes entre un cliente DHCP y un servidor DHCP ubicado en una subred diferente.

Un *agente de retransmisión* de Capa 3 suele ser un enrutador que tiene interfaces IP en las subredes del cliente y del servidor, y que envía tráfico entre ellas. Sin embargo, en redes conmutadas de Capa 2, hay uno o más dispositivos de red (por ejemplo, switches) entre el cliente y el *agente de retransmisión* de Capa 3 o el servidor DHCP. En este caso, este dispositivo proporciona un *agente de retransmisión* de Capa 2 para añadir la información que el *agente de retransmisión* de Capa 3 y el servidor DHCP necesitan para cumplir con su función de asignar una dirección y configuración.

La siguiente lista contiene la configuración por defecto para esta función:
- Configuración global:
  - Configuración activa: desactivar
- Configuración de interfaz:
  - Configuración activa: desactivar
  - Puerto de confianza: desactivar
- Configuración de VLAN:
  - Configuración activa: desactivar
  - *ID de circuito*: activar
  - Tipo de *ID remoto*: mac
  - *ID remoto*: vacío

Para el protocolo DHCPv6, se utiliza un *agente de retransmisión* que añade opciones de *agente de retransmisión* a los paquetes de DHCPv6 intercambiados entre un cliente y un servidor DHCPv6. El Agente ligero de retransmisión DHCPv6 (LDRA) se describe en RFC 6221.

El LDRA procesa 2 tipos de mensajes:
- El primer tipo de mensaje es el de *Relay-Forward*, que contiene información única sobre el cliente.
- El segundo tipo de mensaje es el *Relay-Reply*, que el servidor DHCPv6 envía al *agente de retransmisión*. El *agente de retransmisión* valida a continuación los mensajes para incluir la información del mensaje *Relay-Forward* inicial y, si es válido, envía el paquete al cliente.

El mensaje *Relay-Forward* contiene información del *ID de la interfaz*, también denominado *Option 18*. Esta opción proporciona información que identifica la interfaz en la que se ha enviado la solicitud del cliente. El dispositivo descarta paquetes DHCPv6 que no contienen información de *Option 18*.

15.2.1 ID remoto y de circuito

En un entorno IPv4, antes de enviar la solicitud de un cliente al servidor DHCP, el dispositivo añade el *ID de circuito* y el *ID remoto* al campo *Option 82* del paquete de solicitud DHCP.
- El *ID de circuito* almacena en qué puerto ha recibido el dispositivo la solicitud del cliente.
- El *ID remoto* contiene la dirección MAC, la dirección IP, el nombre del sistema o una secuencia de caracteres definida por el usuario. Los dispositivos participantes la utilizan para identificar el *agente de retransmisión* que ha recibido la solicitud del cliente.

El dispositivo y otros *agentes de retransmisión* utilizan esta información para redirigir la respuesta del *agente de retransmisión* DHCP al cliente original. El servidor DHCP puede analizar estos datos, por ejemplo, para asignar al cliente una dirección IP de un grupo de direcciones específico.

Además, el paquete de retransmisión del servidor DHCP contiene el *ID de circuito* y el *ID remoto*. Antes de enviar la respuesta al cliente, el dispositivo elimina la información del campo de la *Option 82*.

15.2.2 Configuración de la retransmisión DHCP L2

El cuadro de diálogo *Advanced > DHCP L2 Relay > Configuration* le permite activar la función en los puertos activos y en las VLAN. En el cuadro *Operation*, seleccione el botón de opción *On*. A continuación, haga clic en el botón .

El dispositivo envía paquetes DHCPv4 con la información de la *Option 82* y paquetes DHCPv6 con la información de la *Option 18* a los puertos que tienen marcada la casilla en las columnas *DHCP L2 Relay* y *Trusted port*. Normalmente, son puertos de la red del servidor DHCP.

En los puertos a los que estén conectados los clientes DHCP, active la función *DHCP L2 Relay*, pero deje la casilla *Trusted port* sin marcar. En estos puertos, el dispositivo descarta paquetes DHCPv4 con información de la *Option 82* y paquetes DHCPv6 con información de la *Option 18* information.

A continuación, se muestra una configuración de ejemplo para la función de retransmisión DHCPv4 L2. Los pasos de configuración de la función de retransmisión DHCPv6 L2 son similares, excepto para las entradas de *ID del circuito* e *ID remoto* que solo se pueden especificar para *Option 82*.

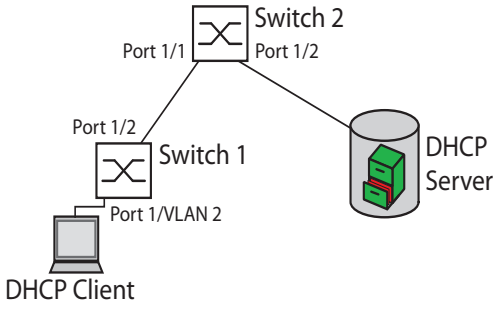


Figura 75: Ejemplo de red DHCP de Capa 2

Realice los siguientes pasos en el Switch 1:

- ☐ Abra el cuadro de diálogo *Advanced > DHCP L2 Relay > Configuration*, pestaña *Interface*.
- ☐ Especifique la configuración del puerto `1/1` del siguiente modo:
  - Marque la casilla de la columna *Active*.
- ☐ Especifique la configuración del puerto `1/2` del siguiente modo:
  - Marque la casilla de la columna *Active*.
  - Marque la casilla de la columna *Trusted port*.
- ☐ Abra el cuadro de diálogo *Advanced > DHCP L2 Relay > Configuration*, pestaña *VLAN ID*.
- ☐ Especifique la configuración de la VLAN 2 del siguiente modo:
  - Marque la casilla de la columna *Active*.
  - Marque la casilla de la columna *Circuit ID*.
  - Para usar la dirección IP del dispositivo como *ID remoto*, especifique el valor `ip` en la columna *Remote ID type*.
- ☐ Para activar la función, seleccione el botón de opción `On` en el cuadro *Operation*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✔.

Realice los siguientes pasos en el Switch 2:

- ☐ Abra el cuadro de diálogo *Advanced > DHCP L2 Relay > Configuration*, pestaña *Interface*.
- ☐ Especifique la configuración de los puertos `1/1` y `1/2` del siguiente modo:
  - Marque la casilla de la columna *Active*.
  - Marque la casilla de la columna *Trusted port*.
- ☐ Para activar la función, seleccione el botón de opción `On` en el cuadro *Operation*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✔.

Verifique que la VLAN 2 está presente. A continuación, realice los siguientes pasos en el Switch 1:

☐ Configure la VLAN 2 y especifique el puerto `1/1` como miembro de la VLAN 2.

`enable`	Cambiar al modo Privileged EXEC.
`vlan database`	Cambiar al modo de configuración de VLAN.
`dhcp-l2relay circuit-id 2`	Active el ID de circuito y la Opción 82 del DHCP en la VLAN `2`.

`dhcp-l2relay remote-id ip 2`	Especifique la dirección IP del dispositivo como ID remoto en la VLAN 2.
`dhcp-l2relay mode 2`	Active la función *DHCP L2 Relay* en la VLAN 2.
`exit`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`interface 1/1`	Cambiar al modo de configuración de la interfaz 1/1.
`dhcp-l2relay mode`	Activar la función *DHCP L2 Relay* en el puerto.
`exit`	Cambiar al modo de configuración.
`interface 1/2`	Cambiar al modo de configuración de la interfaz 1/2.
`dhcp-l2relay trust`	Especificar el puerto como *Trusted port*.
`dhcp-l2relay mode`	Activar la función *DHCP L2 Relay* en el puerto.
`exit`	Cambiar al modo de configuración.
`dhcp-l2relay mode`	Active la función *DHCP L2 Relay* en el dispositivo.

Realice los siguientes pasos en el Switch 2:

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`interface 1/1`	Cambiar al modo de configuración de la interfaz 1/1.
`dhcp-l2relay trust`	Especificar el puerto como *Trusted port*.
`dhcp-l2relay mode`	Activar la función *DHCP L2 Relay* en el puerto.
`exit`	Cambiar al modo de configuración.
`interface 1/2`	Cambiar al modo de configuración de la interfaz 1/2.
`dhcp-l2relay trust`	Especificar el puerto como *Trusted port*.
`dhcp-l2relay mode`	Activar la función *DHCP L2 Relay* en el puerto.
`exit`	Cambiar al modo de configuración.
`dhcp-l2relay mode`	Active la función *DHCP L2 Relay* en el dispositivo.

15.3 Uso del dispositivo como cliente DNS

El cliente de Sistema de nombres de dominio (DNS) consulta a los servidores DNS para resolver nombres de host y direcciones IP de dispositivos de red. De modo muy similar a una agenda de teléfonos, el cliente DNS convierte los nombres de los dispositivos en direcciones IP. Cuando el cliente DNS recibe una solicitud para resolver un nombre nuevo, el cliente DNS consulta primero su base de datos estática interna y, a continuación, los servidores DNS asignados para la información. El cliente DNS guarda la información consultada en una caché para solicitudes futuras.

El dispositivo le permite configurar el cliente DNS desde el servidor DHCP utilizando la VLAN de gestión de dispositivos. El dispositivo también le permite asignar nombres de host a direcciones IP de manera estática.

El cliente DNS ofrece las siguientes funciones de usuario:
- Lista de servidores DNS, con espacio para 4 direcciones IP de servidor de nombres de dominio
- asignación de nombre de host estático a dirección IP, con espacio para 64 hosts estáticos configurables
- caché del host, con espacio para 128 entradas

15.3.1 Configuración de un servidor DNS de ejemplo

Asigne un nombre al cliente DNS y configúrelo para consultar a un servidor DNS para resolver los nombres de host. Para ello, siga los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Advanced > DNS > Client > Static*.
- ☐ En el cuadro *Configuration*, en el campo *Configuration source*, especifique el valor `user`.
- ☐ En el cuadro *Configuration*, en el campo *Domain name*, especifique el valor `device1`.
- ☐ Para añadir una entrada de tabla, haga clic en el botón  .
- ☐ En la columna *Address*, especifique el valor `192.168.3.5` como dirección IPv4 del servidor DNS. También puede especificar una dirección IPv6 válida como dirección IP del servidor DNS.
- ☐ Marque la casilla de la columna *Active*.
- ☐ Abra el cuadro de diálogo *Advanced > DNS > Client > Global*.
- ☐ Para activar la función, seleccione el botón de opción *On* en el cuadro *Operation*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón  .

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`dns client source user`	Especifique que el usuario configura manualmente los ajustes del cliente DNS.
`dns client domain-name device1`	Especifique la cadena `device1` como nombre de dominio único para el dispositivo.
`dns client servers add 1 ip 192.168.3.5`	Para añadir un servidor de nombres DNS con una dirección IPv4 de `192.168.3.5` como índice `1`.
`dns client servers add 2 ip 2001::1`	Añada un servidor DNS con una dirección IPv6 de `2001::1` como índice `2`.
`dns client adminstate`	Activar la función *DNS Client* globalmente.

Configure el cliente DNS para asignar hosts estáticos con direcciones IP. Para ello, siga los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Advanced* > *DNS* > *Client* > *Static Hosts*.
- ☐ Para añadir una entrada de tabla, haga clic en el botón  .
- ☐ En la columna *Name*, introduzca el valor `example.com`.
  Este es un nombre de un dispositivo de la red.
- ☐ En la columna *IP address*, especifique el valor `192.168.3.9`.
- ☐ Marque la casilla de la columna *Active*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón  .

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`dns client host add 1 name example.com ip 192.168.3.9`	Añada `example.com` como host estático con una dirección IP de `192.168.3.9`.
`dns client adminstate`	Activar la función *DNS Client* globalmente.

15.4 GARP

El Protocolo de registro de atributos genérico (*GARP*, Generic Attribute Registration Protocol) está definido por el IEEE para proporcionar un marco genérico que permita que los switches puedan registrar y cancelar el registro de valores de atributos, como identificadores de VLAN y suscripciones a grupos Multicast.

Si se realiza o se cancela el registro de un atributo de un participante según la función *GARP*, se modifica el participante conforme a unas reglas específicas. Los participantes son un conjunto de estaciones terminales y dispositivos de red accesibles. El conjunto definido de participantes en un determinado momento, junto con sus atributos, es el árbol de accesibilidad correspondiente al subconjunto de la topología de red. El dispositivo reenvía los paquetes de datos solamente a las estaciones terminales registradas. El registro de las estaciones ayuda a evitar intentos de envío de datos a las estaciones terminales a las que no se puede acceder.

15.4.1 Configuración de GMRP

El protocolo de registro de multidifusión GARP (*GMRP*, GARP Multicast Registration Protocol) es un Protocolo de registro de atributos genérico (*GARP*) que proporciona un mecanismo para permitir a los dispositivos de red y a las estaciones terminales registrar las suscripciones a grupos de manera dinámica. Los dispositivos registran información de suscripción a grupos con los dispositivos conectados al mismo segmento LAN. La función *GARP* también permite a los dispositivos diseminar la información por los dispositivos de red que admiten servicios de filtrado ampliados.

Nota: Antes de activar la función *GMRP*, compruebe que la función *MMRP* esté desactivada.

El siguiente ejemplo describe la configuración de la función *GMRP*. El dispositivo ofrece una instalación de desbordamiento Multicast restringida en un puerto seleccionado. Para ello, siga los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Switching > GARP > GMRP*.
- ☐ Para ofrecer Multicast Flooding restringido en un puerto, marque la casilla de la columna *GMRP active*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✔.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`interface 1/1`	Cambiar al modo de configuración de la interfaz `1/1`.
`garp gmrp operation`	Activar la función *GMRP* en el puerto.
`exit`	Cambiar al modo de configuración.
`garp gmrp operation`	Activar la función *GMRP* globalmente.

15.4.2 Configuración de GVRP

Utilice la función *GVRP* para permitir que el dispositivo intercambie información de configuración de VLAN con otros dispositivos *GVRP*. De este modo, se reduce el tráfico Broadcast innecesario y Unicast desconocido. Además, la función *GVRP* crea y gestiona dinámicamente VLAN en dispositivos conectados a través de puertos de enlace 802.1Q.

El siguiente ejemplo describe la configuración de la función *GVRP*. El dispositivo le permite intercambiar información de configuración de VLAN con otros dispositivos *GVRP*. Para ello, siga los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Switching > GARP > GVRP*.
- ☐ Para intercambiar información de configuración de VLAN con otros dispositivos *GVRP*, marque la casilla de la columna *GVRP active* del puerto.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✔.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`interface 3/1`	Cambiar al modo de configuración de la interfaz `3/1`.
`garp gvrp operation`	Activar la función *GVRP* en el puerto.
`exit`	Cambiar al modo de configuración.
`garp gvrp operation`	Activar la función *GVRP* globalmente.

15.5 MRP-IEEE

La modificación IEEE 802.1ak al estándar IEEE 802.1Q introdujo el Protocolo de registro múltiple (MRP, Multiple Registration Protocol) para sustituir al Protocolo de registro de atributos genérico (*GARP*, Generic Attribute Registration Protocol). El IEEE también modificó y sustituyó las aplicaciones *GARP*, el Protocolo de registro de multidifusión *GARP* (*GMRP*, GARP Multicast Registration Protocol) y el Protocolo de registro de VLAN *GARP* (*GVRP*, GARP VLAN Registration Protocol) por el Protocolo de registro de MAC múltiple (*MMRP*, Multiple MAC Registration Protocol) y el Protocolo de registro de VLAN múltiple (*MVRP*, Multiple VLAN Registration Protocol).

Para confinar el tráfico a las zonas requeridas de una red, las aplicaciones MRP distribuyen valores de atributos a dispositivos compatibles con MRP a través de una LAN. Las aplicaciones MRP registran y cancelan el registro de suscripciones a grupos Multicast e identificadores de VLAN.

Nota: El Protocolo de registro múltiple (MRP, Multiple Registration Protocol) requiere una red sin bucle. Para ayudar a evitar que se produzcan bucles en su red, utilice un protocolo de red como el Protocolo de redundancia multimedia (Media Redundancy Protocol), el protocolo Spanning Tree o el protocolo Rapid Spanning Tree con MRP.

15.5.1 Funcionamiento de MRP

Cada participante contiene un componente aspirante y un componente de declaración de atributos MRP (MAD, MRP Attribute Declaration). El componente aspirante es responsable de formar los valores de atributos y del registro y su cancelación. El componente MAD genera mensajes MRP para la transmisión y procesa mensajes recibidos de otros participantes. El componente MAD codifica y transmite los atributos a otros participantes de las Unidades de datos MRP (MRPDU, MRP Data Units). En el switch, un componente de Propagación de atributos MRP (MAP, MRP Attribute Propagation) distribuye los atributos a los puertos participantes.

Existe un participante por cada aplicación MRP y por cada puerto LAN. Por ejemplo, existe una aplicación participante en un dispositivo terminal y existe otra aplicación en un puerto del switch. La máquina de estado del aspirante registra el atributo y el puerto de cada declaración de participante MRP en un dispositivo terminal o en un switch. Los cambios en la variable de la máquina de estado del aspirante provocan la transmisión de MRPDU para comunicar la declaración o la retirada.

Para establecer una instancia de *MMRP*, un dispositivo terminal envía primero un mensaje Join empty (JoinMt) con los atributos correspondientes. A continuación, el switch hace desbordar el JoinMt a los puertos participantes y a los switches próximos. Los switches próximos desbordan el mensaje a su puerto participante, y así sucesivamente, estableciendo una ruta para el tráfico del grupo.

15.5.2 Temporizadores de MRP

La configuración predeterminada del temporizador ayuda a evitar declaraciones y retiradas de atributos innecesarias. La configuración del temporizador permite a los participantes recibir y procesar mensajes MRP antes de que los temporizadores Leave (Abandono) o LeaveAll (Abandonar todo) finalicen.

Cuando reconfigure los temporizadores, mantenga las siguientes relaciones:
- Para permitir la repetición del registro tras un evento Leave (Abandono) o LeaveAll (Abandonar todo), aunque haya un mensaje perdido, ajuste el valor de LeaveTime (Hora de abandono) del modo siguiente: ≥ (2x JoinTime) + 60 in 1/100 s
- Para minimizar el volumen del tráfico de reincorporación generado tras un evento LeaveAll (Abandonar todo), especifique un valor superior para el temporizador de LeaveAll (Abandonar todo) que para el de LeaveTime (Hora de abandono).

La siguiente lista contiene varios eventos MRP que transmite el dispositivo:
- Join (Unión): controla el intervalo que desea que transcurra para la transmisión del siguiente mensaje de Join (Unión)
- Leave (Abandono): controla el tiempo que debe esperar un switch en estado Leave (Abandono) antes de cambiar al estado de retirada
- LeaveAll (Abandonar todo): controla la frecuencia con la que el switch genera mensajes LeaveAll (Abandonar todo)

Una vez finalizado, el temporizador Periodic (Periódico) inicia un mensaje MRP de solicitud de Join (Unión) que el switch envía a participantes de la LAN. Los switches utilizan este mensaje para ayudar a impedir retiradas innecesarias.

15.5.3 MMRP

Cuando un dispositivo recibe Broadcast, Multicast o tráfico desconocido en un puerto, el dispositivo desborda el tráfico a los otros puertos. Este proceso provoca el uso innecesario del ancho de banda de la LAN.

El Protocolo de registro de MAC múltiple (*MMRP*, Multiple MAC Registration Protocol) le permite controlar el desbordamiento del tráfico distribuyendo una declaración de atributos a participantes de una LAN. Los valores de los atributos que el componente MAD codifica y transmite en la LAN en mensajes MRP son información necesaria para el servicio de grupo y direcciones MAC de 48 bits.

El switch almacena los atributos en una base de datos de filtración como entradas de registro de dirección MAC. El proceso de reenvío utiliza las entradas de la base de datos de filtración solamente para transmitir datos a través de los puertos necesarios a fin de llegar a las LAN de los miembros del grupo.

Los switches facilitan los mecanismos de distribución de grupos basándose en el concepto Open Host Group (Grupo de host abierto), recibiendo paquetes en los puertos activos y reenviándolos solamente a los puertos que disponen de miembros de grupos. De este modo, los participantes de *MMRP* que requieren la transmisión de paquetes a un grupo o grupos en particular, solicitan su suscripción en el grupo. Los usuarios del servicio MAC envían paquetes a un grupo en particular desde cualquier parte de la LAN. Los grupos reciben estos paquetes en las LAN conectadas a los participantes en *MMRP* registrados. Las entradas de registro de direcciones MAC y *MMRP* restringen los paquetes a los segmentos requeridos de una LAN sin bucles.

Para mantener el estado del registro y su cancelación y para recibir tráfico, los puertos declaran su interés de manera periódica. Cada dispositivo de una LAN que disponga de la función *MMRP* activada mantiene una base de datos de filtración y desvía tráfico con direcciones MAC del grupo a los participantes enumerados.

Ejemplo de MMRP

En este ejemplo, el Host A tiene la misión de escuchar el tráfico destinado al grupo G1. El switch A procesa la solicitud de Join (Unión) de *MMRP* recibida del Host A y envía la solicitud a los dos switches vecinos. Ahora los dispositivos de la LAN reconocen que existe un host interesado en recibir tráfico destinado para el grupo G1. Cuando el Host B comienza a transmitir datos destinados al grupo G1, los datos fluyen por la ruta de registros y el Host A los recibe.

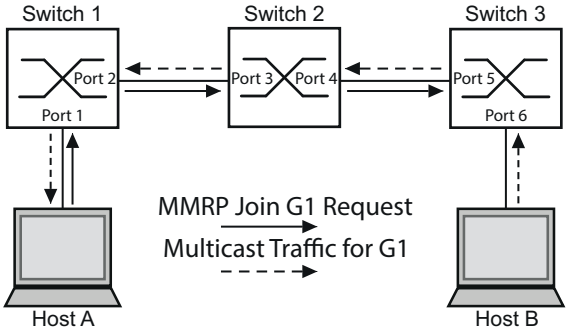


Figura 76: Red MMRP para el registro de direcciones MAC

Active la función *MMRP* en los switches. Para ello, siga los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Switching > MRP-IEEE > MMRP*, pestaña *Configuration*.
- ☐ Para activar los puertos `1` y `2` como participantes de *MMRP*, marque la casilla de verificación de la columna *MMRP* para los puertos `1` y `2` del switch 1.
- ☐ Para activar los puertos `3` y `4` como participantes de *MMRP*, marque la casilla de verificación de la columna *MMRP* para los puertos `3` y `4` del switch 2.
- ☐ Para activar los puertos `5` y `6` como participantes de *MMRP*, marque la casilla de la columna *MMRP* para los puertos `5` y `6` del switch 3.
- ☐ Para enviar eventos periódicos que permitan al dispositivo mantener el registro del grupo de direcciones MAC, active *Periodic state machine*. Seleccione el botón de opción `On` en el cuadro *Configuration*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✔.

Para activar los puertos *MMRP* del switch 1, utilice los siguientes comandos. Tras sustituir las interfaces correspondientes de los comandos, active las funciones de *MMRP* y los puertos de los switches 2 y 3.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`interface 1/1`	Cambiar al modo de configuración de la interfaz `1/1`.
`mrp-ieee mmrp operation`	Activar la función *MMRP* en el puerto.
`interface 1/2`	Cambiar al modo de configuración de la interfaz `1/2`.
`mrp-ieee mmrp operation`	Activar la función *MMRP* en el puerto.
`exit`	Cambiar al modo de configuración.
`mrp-ieee mrp periodic-state-machine`	Activar la función *Periodic state machine* globalmente.
`mrp-ieee mmrp operation`	Activar la función *MMRP* globalmente.

15.5.4 MVRP

El Protocolo de registro de VLAN múltiple (*MVRP*, Multiple VLAN Registration Protocol) es una aplicación de MRP que proporciona servicios de retirada y registro de VLAN dinámicas en una LAN.

La función *MVRP* ofrece un mecanismo de mantenimiento para las entradas de registro de VLAN dinámicas y para la transmisión de información a otros dispositivos. Esta información permite a dispositivos que detecten *MVRP* establecer y actualizar su información de suscripción a VLAN. Cuando haya miembros presentes en una VLAN, la información indicará a través de qué puertos desea que desvíe tráfico el switch para llegar a esos miembros.

El objetivo principal de la función *MVRP* es permitir a los switches descubrir parte de la información de la VLAN que, de lo contrario, configuraría manualmente. Descubrir esta información permite a los switches superar las limitaciones de consumo de banda ancha y tiempo de convergencia en redes VLAN de grandes dimensiones.

Ejemplo de MVRP

Configure una red compuesta por switches que detecten MVRP (1 - 4) conectados en topología de anillo con grupos de dispositivos finales, A1, A2, B1 y B2 en 2 VLAN diferentes, A y B. Con STP activado en los switches, los puertos que conectan los switches 1 al 4 están en estado descartado, lo cual ayuda a evitar bucles.

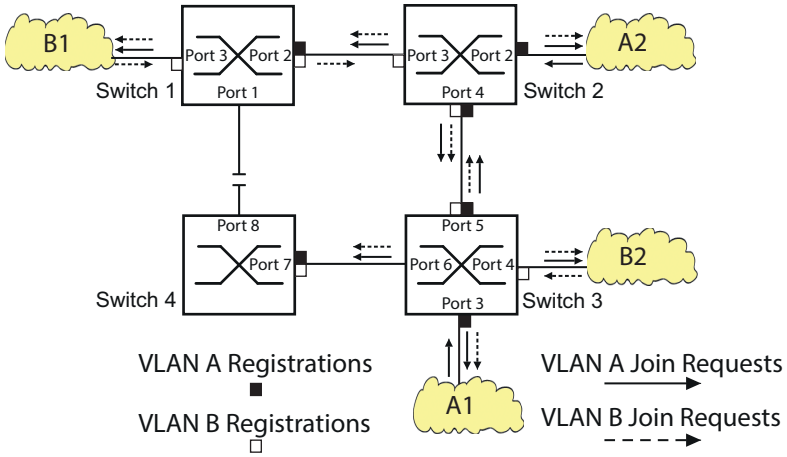


Figura 77: Red de ejemplo de MVRP para el registro de VLAN

En la red de ejemplo de MVRP, las LAN envían en primer lugar una solicitud Join (Unión) a los switches. El switch introduce el registro de la VLAN en la base de datos de desvío del puerto que recibe las tramas.

A continuación, el switch propaga la solicitud a los otros puertos y la envía a las LAN y los switches cercanos. Este proceso continúa hasta que los switches han registrado las VLAN en la base de datos de desvío del puerto de recepción.

Active MVRP en los switches. Para ello, siga los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Switching* > *MRP-IEEE* > *MVRP*, pestaña *Configuration*.
- ☐ Para activar los puertos `1` a `3` como participantes de *MVRP*, marque la casilla de la columna *MVRP* para los puertos `1` a `3` del switch 1.
- ☐ Para activar los puertos `2` a `4` como participantes de *MVRP*, marque la casilla de la columna *MVRP* para los puertos `2` a `4` del switch 2.
- ☐ Para activar los puertos `3` a `6` como participantes de *MVRP*, marque la casilla de verificación de la columna *MVRP* para los puertos `3` a `6` del switch 3.
- ☐ Para activar los puertos `7` y `8` como participantes de *MVRP*, marque la casilla de verificación de la columna *MVRP* para los puertos `7` y `8` del switch 4.
- ☐ Para mantener el registro de las VLAN, active *Periodic state machine*.
  Seleccione el botón de opción `On` en el cuadro *Configuration*.
- ☐ Para activar la función, seleccione el botón de opción `On` en el cuadro *Operation*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✔.

Para activar los puertos *MVRP* del switch 1, utilice los siguientes comandos. Tras sustituir las interfaces correspondientes de los comandos, active las funciones de *MVRP* y los puertos de los switches 2, 3 y 4.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`interface 1/1`	Cambiar al modo de configuración de la interfaz `1/1`.
`mrp-ieee mvrp operation`	Activar la función *MVRP* en el puerto.
`interface 1/2`	Cambiar al modo de configuración de la interfaz `1/2`.
`mrp-ieee mvrp operation`	Activar la función *MVRP* en el puerto.
`exit`	Cambiar al modo de configuración.
`mrp-ieee mvrp periodic-state-machine`	Activar la función *Periodic state machine* globalmente.
`mrp-ieee mvrp operation`	Activar la función *MVRP* globalmente.

16 Protocolos industriales

16.1 IEC 61850/MMS

IEC 61850/MMS es un protocolo de comunicación industrial estandarizado de la Comisión Electrotécnica Internacional (IEC). El protocolo se encuentra en la automatización de subestaciones, por ejemplo, en la tecnología de control de proveedores de energía.

Este protocolo funciona con una arquitectura orientada a paquetes, se basa en el protocolo de transporte TCP/IP y utiliza la Especificación de mensajes de fabricación (MMS, Manufacturing Messaging Specification) para la comunicación con el servidor del cliente. El protocolo está orientado a objetos y define un lenguaje de configuración estandarizado que abarca, entre otras cosas, las funciones de SCADA, los dispositivos electrónicos inteligentes (IED, Intelligent Electronic Devices) y la tecnología de control de red.

La sección 6 de la norma IEC 61850 define el lenguaje de configuración SCL (Lenguaje de configuración de subestación, Substation Configuration Language). El SCL describe las propiedades del dispositivo y la estructura del sistema de una forma automáticamente procesable. Las propiedades del dispositivo descritas con el SCL se almacenan en el archivo ICD del dispositivo.

16.1.1 Modelo de switch para IEC 61850

El informe técnico IEC 61850 90-4 especifica un modelo de puente. El modelo de puente representa las funciones de un switch como objeto de un dispositivo electrónico inteligente (IED). Un cliente MMS (por ejemplo, el software de la sala de control) utiliza estos objetos para supervisar y configurar el dispositivo.

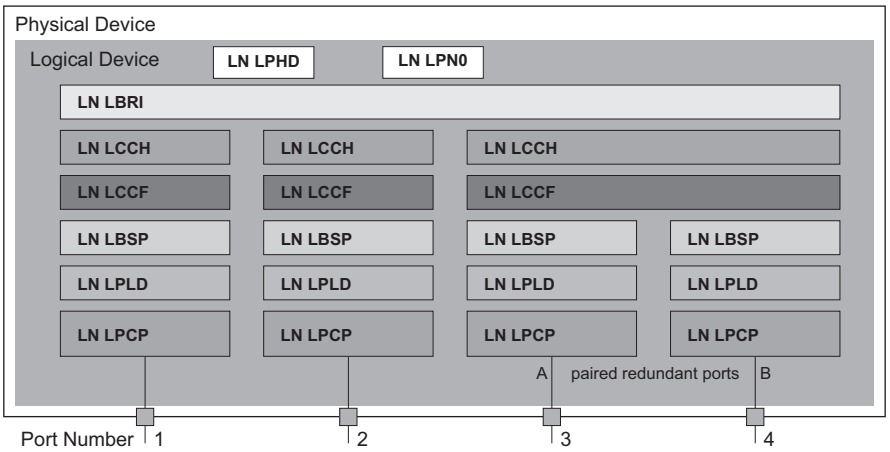


Figura 78: Modelo de puente basado en el informe técnico IEC 61850 90-4

Tabla 59: Clases de modelo de puente basadas en el informe técnico IEC 61850 90-4

Clase	Descripción
LN LLN0	Nodo lógico Zero del IED Bridge: Define las propiedades lógicas del dispositivo.
LN LPHD	Nodo lógico Physical Device del IED Bridge: Define las propiedades físicas del dispositivo.
LN LBRI	Nodo lógico Bridge: Representa la configuración general de las funciones de puente del dispositivo.
LN LCCH	Nodo lógico Communication Channel: Define el Communication Channel lógico que consiste en uno o más puertos físicos del dispositivo.
LN LCCF	Nodo lógico Channel Communication Filtering: Define la configuración de VLAN y Multicast para el Communication Channel de nivel más elevado.
LN LBSP	Nodo lógico Port Spanning Tree Protocol: Define los estados de Spanning Tree y la configuración del puerto físico del dispositivo correspondiente.
LN LPLD	Nodo lógico Port Layer Discovery: Define los estados de LLDP y la configuración del puerto físico del dispositivo correspondiente.
LN LPCP	Nodo lógico Physical Communication Port: Representa el puerto físico del dispositivo correspondiente.

16.1.2 Integración en un sistema de control

Preparación del dispositivo

Lleve a cabo los siguientes pasos:

- ☐ Compruebe que el dispositivo tenga una dirección IP asignada.
- ☐ Abra el cuadro de diálogo *Advanced > Industrial Protocols > IEC61850-MMS*.
- ☐ Para iniciar el servidor MMS, seleccione en el cuadro *Operation* el botón de opción On y haga clic en el botón ✓.
  A continuación, se puede conectar un cliente MMS al dispositivo y leer y supervisar objetos definidos en el modelo de puente.

IEC61850/MMS no brinda ningún mecanismo de autenticación. Si el acceso de escritura para IEC61850/MMS está activado, cada cliente que pueda acceder al dispositivo mediante TCP/IP podrá cambiar la configuración del dispositivo. Esto a su vez puede dar como resultado una configuración incorrecta del dispositivo y provocar posibles problemas en la red.

AVISO
RIESGO DE ACCESO NO AUTORIZADO AL DISPOSITIVO Active el acceso de escritura únicamente si ha tomado medidas adicionales (por ejemplo, un cortafuegos, VPN, etc.) para reducir posibles accesos no autorizados. **El incumplimiento de estas instrucciones puede provocar daños en el equipo.**

- ☐ Para permitir que el cliente MMS cambie la configuración, marque la casilla *Write access* y haga clic en el botón ✓.

Configuración sin conexión

El dispositivo le permite descargar el archivo ICD mediante la interfaz gráfica de usuario. Este archivo contiene las propiedades del dispositivo descritas con el SCL y le permite configurar la subestación sin conectarla directamente al dispositivo.

- ☐ Abra el cuadro de diálogo *Advanced > Industrial Protocols > IEC61850-MMS*.
- ☐ Para cargar el archivo en el PC, haga clic en el botón ☰ y, a continuación, en el elemento *Download*.

Supervisión del dispositivo

El servidor IEC61850/MMS integrado en el dispositivo le permite supervisar múltiples estados del dispositivo mediante el bloque de control de informes (RCB, Report Control Block). Se pueden registrar hasta 5 clientes MMS para un bloque de control de informes a la vez.

El dispositivo le permite supervisar los siguientes estados:

Tabla 60: Estados del dispositivo que se pueden supervisar con IEC 61850/MMS

Clase	Objeto RCB	Descripción
LN LPHD	TmpAlm	Si la temperatura medida en el dispositivo es superior o inferior a los umbrales de temperatura establecidos, el estado cambia.
	PhyHealth	Cuando el estado del objeto RCB LPHD.TmpAlm cambia, el estado cambia.
LN LPHD	TmpAlm	Si la temperatura medida en el dispositivo es superior o inferior a los umbrales de temperatura establecidos, el estado cambia.
	PwrSupAlm	Cuando una de las alimentaciones de tensión redundantes se vuelve no operativa o comienza a funcionar de nuevo, el estado cambia.
	PhyHealth	Si el estado de LPHD.PwrSupAlm o del objeto RCB LPHD.TmpAlm cambia, el estado cambia.

Tabla 60: Estados del dispositivo que se pueden supervisar con IEC 61850/MMS (cont

Clase	Objeto RCB	Descripción
LN LBRI	RstpRoot	Si el dispositivo asume o abandona el rol de puente raíz, el estado cambia.
	RstpTopoCnt	Cuando la topología cambia debido a una modificación en el puente raíz, el estado cambia.
LN LCCH	ChLiv	Cuando el estado de enlace del puerto físico cambia, el estado cambia.
LN LPCP	PhyHealth	Cuando el estado de enlace del puerto físico cambia, el estado cambia.

16.2 Modbus TCP

Modbus TCP es un protocolo de mensajería de capa de aplicación que proporciona comunicación del servidor/cliente entre el cliente y los dispositivos conectados en las redes Ethernet TCP/IP.

La función *Modbus TCP* le permite instalar el dispositivo en redes que ya utilicen *Modbus TCP* y recuperar información guardada en los registros del dispositivo.

16.2.1 Modo de Modbus TCP/IP del cliente/servidor

El dispositivo admite el modelo de cliente/servidor del Modbus TCP/IP. Este dispositivo funciona como servidor en esta constelación y responde a las solicitudes de un cliente para obtener información guardada en los registros.

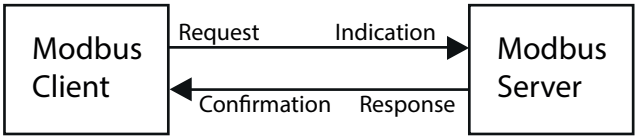


Figura 79: Modo de Modbus TCP/IP del cliente/servidor

El modelo de cliente/servidor utiliza cuatro tipos de mensajes para intercambiar datos entre el cliente y el servidor:
- Solicitud de Modbus TCP/IP, el cliente crea una solicitud de información y la envía al servidor.
- Indicación de Modbus TCP/IP, el servidor recibe una solicitud como indicación de que un cliente solicita información.
- Respuesta de Modbus TCP/IP, cuando la información solicitada está disponible, el servidor envía una respuesta que contiene la información solicitada. Si la información solicitada no está disponible, el servidor envía una Respuesta de excepción para notificar al cliente del error detectado durante el procesamiento. La Respuesta de excepción contiene un código de excepción que indica la razón del error detectado.
- Confirmación de Modbus TCP/IP, el cliente recibe una respuesta del servidor, la cual contiene la información solicitada.

16.2.2 Funciones compatibles y Mapping de la memoria

El dispositivo admite las funciones con los códigos públicos `0x03` (`Read Holding Registers`) y `0x05` (`Write Single Coil`). Los códigos le permiten leer la información guardada en los registros, como la información del sistema, incluido el nombre del sistema, la ubicación del sistema, la versión del software, la dirección IP y la dirección MAC. Los códigos también le permiten leer la información y estadísticas del puerto. El código `0x05` le permite restablecer los contadores de puerto de forma individual o global.

La siguiente lista contiene definiciones para los valores introducidos en la columna `Format`:
- Mapa de bits: un grupo de 32 bits codificado en orden de byte Big-endian y guardado en 2 registros. Los sistemas Big-endian guardan el byte más significativo de una palabra en la dirección más pequeña, y el byte menos significativo, en la dirección más grande.
- F1: 16-bit unsigned integer
- F2: Enumeration - power supply alarm
  - 0 = power supply good
  - 1 = power supply failure detected

- F3: Enumeration - OFF/ON
  - 0 = Off
  - 1 = On
- F4: Enumeration - port type
  - 0 = Giga - Gigabit Interface Converter (GBIC)
  - 1 = Copper - Twisted Pair (TP)
  - 2 = Fiber - 10 Mb/s
  - 3 = Fiber - 100 Mb/s
  - 4 = Giga - 10/100/1000 Mb/s (triple speed)
  - 5 = Giga - Copper 1000 Mb/s TP
  - 6 = Giga - Small Form-factor Pluggable (SFP)
- F9: 32-bit unsigned long
- Cadena: octetos, guardados en secuencia, 2 octetos por registro.

Códigos de Modbus TCP/IP

La tabla siguiente muestra las direcciones que permiten que el cliente restablezca los contadores del puerto y recuperar información específica de los registros del dispositivo.

Información del puerto

Tabla 61: Información del puerto

Dirección	Cant.	Descripción	Mín.	Máx.	Paso	Unidad	Formato
0400	1	Port 1 Type	0	6	1	-	F4
0401	1	Port 2 Type	0	6	1	-	F4
		...					
043F	1	Port 64 Type	0	6	1	-	F4
0440	1	Port 1 Link Status	0	1	1	-	F1
0441	1	Port 2 Link Status	0	1	1	-	F1
		...					
047F	1	Port 64 Link Status	0	1	1	-	F1
0480	1	Port 1 STP State	0	1	1	-	F1
0481	1	Port 2 STP State	0	1	1	-	F1
		...					
04BF	1	Port 64 STP State	0	1	1	-	F1
04C0	1	Port 1 Activity	0	1	1	-	F1
04C1	1	Port 2 Activity	0	1	1	-	F1
		...					
04FF	1	Port 64 Activity	0	1	1	-	F1
0500	1	Port 1 Counter Reset	0	1	1	-	F1
0501	1	Port 2 Counter Reset	0	1	1	-	F1
		...					
053F	1	Port 64 Counter Reset	0	1	1	-	F1

Estadísticas del puerto

Tabla 62: Estadísticas del puerto

Dirección	Cant.	Descripción	Mín.	Máx.	Paso	Unidad	Formato
0800	1	Port1 - Number of bytes received	0	4294967295	1	-	F9
0802	1	Port1 - Number of bytes sent	0	4294967295	1	-	F9
0804	1	Port1 - Number of frames received	0	4294967295	1	-	F9
0806	1	Port1 - Number of frames sent	0	4294967295	1	-	F9
0808	1	Port1 - Total bytes received	0	4294967295	1	-	F9
080A	1	Port1 - Total frames received	0	4294967295	1	-	F9
080C	1	Port1 - Number of broadcast frames received	0	4294967295	1	-	F9
080E	1	Port1 - Number of multicast frames received	0	4294967295	1	-	F9
0810	1	Port1 - Number of frames with CRC error	0	4294967295	1	-	F9
0812	1	Port1 - Number of oversized frames received	0	4294967295	1	-	F9
0814	1	Port1 - Number of bad fragments rcvd(<64 bytes)	0	4294967295	1	-	F9
0816	1	Port1 - Number of jabber frames received	0	4294967295	1	-	F9
0818	1	Port1 - Number of collisions occurred	0	4294967295	1	-	F9
081A	1	Port1 - Number of late collisions occurred	0	4294967295	1	-	F9
081C	1	Port1 - Number of 64-byte frames rcvd/sent	0	4294967295	1	-	F9
081E	1	Port1 - Number of 65-127 byte frames rcvd/sent	0	4294967295	1	-	F9
0820	1	Port1 - Number of 128-255 byte frames rcvd/sent	0	4294967295	1	-	F9
0822	1	Port1 - Number of 256-511 byte frames rcvd/sent	0	4294967295	1	-	F9
0824	1	Port1 - Number of 512-1023 byte frames rcvd/sent	0	4294967295	1	-	F9
0826	1	Port1 - Number of 1023-MAX byte frames rcvd/sent	0	4294967295	1	-	F9
0828	1	Port1 - Number of Mac Error Packets	0	4294967295	1	-	F9
082A	1	Port1 - Number of dropped received packets	0	4294967295	1	-	F9
082C	1	Port1 - Number of multicast frames sent	0	4294967295	1	-	F9
082E	1	Port1 - Number of broadcast frames sent	0	4294967295	1	-	F9
0830	1	Port1 - Number of <64 byte fragments w/ good CRC	0	4294967295	1	-	F9
		...					
147E	1	Port64 - Number of <64 byte fragments w/ good CRC	0	4294967295	1	-	F9

16.2.3 Configuración de ejemplo

En este ejemplo, configure el dispositivo para responder a las solicitudes del cliente. El requisito previo para esta configuración es que el dispositivo del cliente esté configurado con una dirección IP dentro del rango específico. La función *Write access* permanece inactiva en este ejemplo. Si activa la función *Write access*, el dispositivo le permite restablecer únicamente los contadores del puerto. En la configuración por defecto, las funciones *Modbus TCP* y *Write access* están inactivas.

El protocolo *Modbus TCP* no brinda ningún mecanismo de autenticación. Si está activado el acceso de escritura para *Modbus TCP*, cada cliente que pueda acceder al dispositivo mediante TCP/IP podrá cambiar la configuración del dispositivo. Esto a su vez puede dar como resultado una configuración incorrecta del dispositivo y provocar posibles problemas en la red.

AVISO
RIESGO DE ACCESO NO AUTORIZADO AL DISPOSITIVO Active el acceso de escritura únicamente si ha tomado medidas adicionales (por ejemplo, un cortafuegos, VPN, etc.) para reducir posibles accesos no autorizados. **El incumplimiento de estas instrucciones puede provocar daños en el equipo.**

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Device Security* > *Management Access* > *IP Access Restriction*.
- ☐ Añada una entrada a la tabla. Para hacer esto, haga clic en el botón .
- ☐ Especifique el rango de direcciones IP en la fila en la que la columna *Index* tiene el valor `2`. Para ello, introduzca los siguientes valores:
  - En la columna *Address*:`10.17.1.0`
  - En la columna *Netmask*:`255.255.255.248`
- ☐ Compruebe que la casilla de verificación de la columna *Modbus TCP* está marcada.
- ☐ Active el rango de direcciones IP. Para ello, marque la casilla de verificación de la columna *Active*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón .
- ☐ Abra el cuadro de diálogo *Diagnostics* > *Status Configuration* > *Security Status*, pestaña *Global*.
- ☐ Compruebe que la casilla de verificación relacionada con el parámetro *Modbus TCP active* está marcada.
- ☐ Abra el cuadro de diálogo *Advanced* > *Industrial Protocols* > *Modbus TCP*.
- ☐ El puerto de escucha estándar *Modbus TCP*, puerto `502`, es el valor por defecto. Sin embargo, si desea escuchar otro puerto TCP, introduzca el valor del puerto de escucha en el campo *TCP port*.
- ☐ Para activar la función, seleccione el botón de opción `On` en el cuadro *Operation*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón .

Si activa la función *Modbus TCP*, la función *Security Status* detecta la activación y muestra una alarma en el cuadro de diálogo *Basic Settings* > *System*, cuadro *Security status*.

`enable`	Cambiar al modo Privileged EXEC.
`network management access add 2`	Crea la entrada para el rango de direcciones de la red. Número del siguiente índice disponible en este ejemplo: `2`.
`network management access modify 2 ip 10.17.1.0`	Especifica la dirección IP.
`network management access modify 2 mask 29`	Especifica la máscara de red.
`network management access modify 2 modbus-tcp enable`	Especifica que el dispositivo permita que *Modbus TCP* tenga acceso a la gestión del dispositivo.
`network management access operation`	Permite la restricción de acceso a IP.
`configure`	Cambiar al modo de configuración.
`security-status monitor modbus-tcp-enabled`	Especifica que el dispositivo supervisa la activación del servidor *Modbus TCP*.
`modbus-tcp operation`	Activa el servidor *Modbus TCP*.
`modbus-tcp port <1..65535>`	Especificar el puerto TCP para la comunicación de *Modbus TCP* (opcional). El valor por defecto es el puerto `502`.
`show modbus-tcp`	Mostrar la configuración del servidor *Modbus TCP*.

```
Modbus TCP/IP server settings
-------------------------
Modbus TCP/IP server operation.............enabled
Write-access...............................disabled
Listening port.............................502
Max number of sessions.....................5
Active sessions............................0
```

`show security-status monitor`	Mostrar la configuración del estado de seguridad.

```
Device Security Settings
Monitor
---------------------------------
Password default settings unchanged...........monitored
...
Write access using Ethernet Switch Configurator is possible....monitored
Loading unencrypted configuration from ENVM...monitored
IEC 61850 MMS is enabled.....................monitored
Modbus TCP/IP server active..................monitored
```

`show security-status event`	Mostrar eventos de estado de seguridad ocurridos.

```
Time stamp             Event                        Info
--------------------   ----------------------    ------
2014-01-01 01:00:39   password-change(10)           -
.................................................
2014-01-01 01:00:39   ext-nvm-load-unsecure(21)     -
2014-01-01 23:47:40   modbus-tcp-enabled(23)        -
```

```
show network management access rules 1
```

Mostrar las reglas de acceso de administración restringidas para el índice 1.

```
Restricted management access settings
-------------------------------------
Index.....................................1
IP Address................................10.17.1.0
Prefix Length.............................29
HTTP......................................yes
SNMP......................................yes
Telnet....................................yes
SSH.......................................yes
HTTPS.....................................yes
IEC61850-MMS..............................yes
Modbus TCP/IP.............................yes
Active....................................[x]
```

16.3 EtherNet/IP

EtherNet/IP se acepta en todo el mundo como protocolo de comunicación industrial estandarizado y está controlado por la Open DeviceNet Vendor Association (ODVA). El protocolo se basa en los protocolos de transporte estándar Ethernet TCP/IP y UDP/IP que se emplean en todo el mundo. *EtherNet/IP* es compatible con los principales fabricantes, lo que proporciona una amplia base para la comunicación efectiva de datos en el sector industrial.

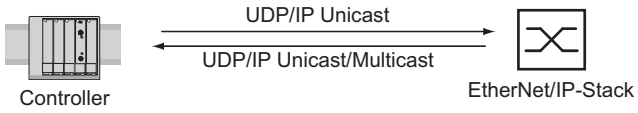


Figura 80: Red EtherNet/IP

EtherNet/IP agrega el protocolo industrial CIP (Protocolo industrial común) a los protocolos Ethernet estándar. *EtherNet/IP* implementa el CIP a la capa de Sesión y las anteriores y adapta el CIP a la tecnología *EtherNet/IP* específica en la capa de Transporte y las posteriores. En el caso de aplicaciones de automatización, *EtherNet/IP* implementa el CIP al nivel de aplicación. Por lo tanto, *EtherNet/IP* está perfectamente preparado para el sector de la tecnología de control industrial.

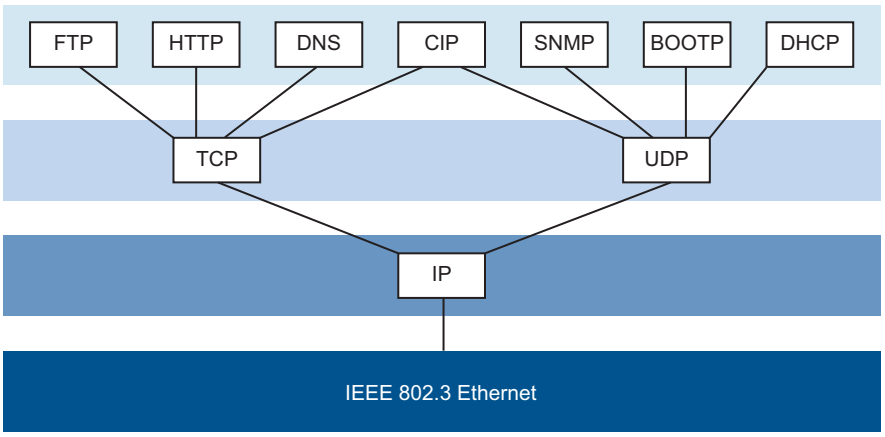


Figura 81: IEEE802.3 EtherNet/IP

Para obtener información detallada sobre *EtherNet/IP*, consulte el sitio web de ODVA en www.odva.org.

16.3.1 Integración en un sistema de control

Lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Switching > IGMP Snooping > Global*.
  Verifique que la función *IGMP Snooping* está activada.
- ☐ Abra el cuadro de diálogo *Advanced > Industrial Protocols > EtherNet/IP*.
  Verifique que la función *EtherNet/IP* está activada.
- ☐ Abra el cuadro de diálogo *Advanced > Industrial Protocols > EtherNet/IP*.
- ☐ Para guardar la EDS como archivo ZIP en su ordenador, haga clic en *Download*.
  El archivo ZIP contiene el archivo de configuración de *EtherNet/IP* y el icono utilizado para configurar el controlador a fin de conectarlo al dispositivo.

16.3.2 Parámetros de la entidad EtherNet/IP

Los siguientes párrafos identifican los objetos y las operaciones que el dispositivo admite.

Operaciones admitidas

Tabla 63: Descripción de las solicitudes de Ethernet/IP admitidas para las instancias de objetos

Service Code	Identity Object	TCP/IP Interface Object	Ethernet Link Object	Switch Agent Object	Base Switch Object
0x01 Get Attribute All	All attributes	All attributes	All attributes	All attributes	All attributes
0x02 Set Attribute All	–	Settable attributes (0x3, 0x5, 0x6, 0x8, 0x9, 0xA)	Settable attributes (0x6, 0x9)	–	–
0x0e Get Attribute Single	All attributes	All attributes	All attributes	All attributes	All attributes
0x10 Set Attribute Single	–	Settable attributes (0x3, 0x5, 0x6, 0x8, 0x9, 0xA, 0x64)	Settable attributes (0x6, 0x9, 0x65, 0x67, 0x68, 0x69, 0x6C)	Settable attributes (0x5, 0x7)	–
0x05 Reset	Parameter (0x0, 0x1)	–	–	–	–
0x35 Save Configuration Vendor specific	–	–	–	Save switch configuration	–
0x36 Mac Filter Vendor specific	–	–	–	Add MAC filter STRUCT of: USINT VlanId ARRAY of: 6 USINT Mac DWORD PortMask	–

Objeto de identidad

El dispositivo admite el objeto de identidad (Class Code 0x01) de *EtherNet/IP*. La identificación del fabricante Schneider Electric es 634. Schneider Electric utiliza el ID 44 (0x2C) para indicar el tipo de producto "Managed Ethernet Switch".

Tabla 64: Atributos de instancia (solo hay 1 instancia disponible)

Id	Attribute	Access Rule	Data type	Description
0x1	Vendor ID	Get	UINT	Schneider Electric634
0x2	Device Type	Get	UINT	Managed Ethernet Switch 44 (0x2C) (0x2C)
0x3	Product Code	Get	UINT	Product Code: mapping is defined for every device type
0x4	Revision	Get	STRUCT of:	Revision of the EtherNet/IP implementation, 2.1.
			USINT Major	
			USINT Minor	
0x5	Status	Get	WORD	Support for the following Bit status only:
				0: Owned (always 1)
				2: Configured (always 1)
				4: Extend Device Status
				5: 0x3: No I/O connection established 0x7: At least one I/O connection established, all in idle mode.
				6:
				7:
0x6	Serial number	Get	UDINT	Serial number of the device (contains last 3 Bytes of MAC address).
0x7	Product name	Get	SHORT-STRING	Displayed as "Schneider Electric" + product family + product ID + software variant.

TCP/IP Interface Object

El dispositivo admite únicamente la Instancia 1 de TCP/IP Interface Object (Class Code 0xF5) de *EtherNet/IP*.

En función del estado de acceso de escritura, el dispositivo almacena la configuración completa en su memoria flash. La grabación del archivo de configuración puede tardar hasta 10 segundos. Si, por ejemplo, el proceso de grabación se interrumpe por una alimentación de corriente no operativa, el funcionamiento del dispositivo podría resultar imposible.

Nota: El dispositivo responde al cambio de configuración `Get Request` con una `Response` aunque la configuración aún no se haya guardado por completo.

Tabla 65: Atributos de clase

Id	Attribute	Access Rule	Data type	Description
0x1	Revision	Get	UINT	Revision of this object: 3
0x2	Max Instance	Get	UINT	Maximum instance number: 1
0x3	Number of instance	Get	UINT	Number of object instances currently created: 1

Tabla 66: Atributos de la Instancia 1

Id	Attribute	Access Rule	Data type	Description
0x1	Status	Get	DWORD	0: Interface Status (0=Interface not configured, 1=Interface contains valid config)
				6: ACD status (default 0)
				7: ACD fault (default 0)
0x2	Interface Capability flags	Get	DWORD	0: BOOTP Client
				1: DNS Client
				2: DHCP Client
				3: DHCP-DNS Update
				4: Configuration setable (within CIP) Other bits reserved (0)
				7: ACD capable (0=not capable, 1=capable)
0x3	Config Control	Set/Get	DWORD	0: 0x0=using stored config 1: 0x1=using BOOTP 2: 0x2=using DHCP 3:
				4: One device uses DNS for name lookup (always 0 because it is not supported) Other bits reserved (0)
0x4	Physical Link Object	Get	STRUCT of:	Path to the Physical Link Object, always {0x20, 0xF6, 0x24, 0x01} describing instance 1 of the Ethernet Link Object.
			UINT PathSize	
			EPATH Path	
0x5	Interface Configuration	Set/Get	STRUCT of:	IP Stack Configuration (IP-Address, Netmask, Gateway, 2 Name servers (DNS, if supported) and the domain name).
			UDINT IpAddress	
			UDINT Netmask	
			UDINT GatewayAddress	
			UDINT NameServer1	
			UDINT NameServer2	
			STRING DomainName	
0x6	Host Name	Set/Get	STRING	Host Name (for DHCP DNS Update)
0x7	Safety Network Number			Not supported
0x8	TTL Value	Get/Set	USINT	Time to live value for IP multicast packets Range 1..255 (default = 1)

Tabla 66: Atributos de la Instancia 1 (cont

Id	Attribute	Access Rule	Data type	Description
0x9	Mcast Config	Get/Set	STRUCT of: USINT AllocControl USINT reserved UINT NumMcast UDINT McastStartAddr	Alloc Control = 0 Number of IP multicast addresses = 32 Multicast start address = 239.192.1.0
0xA	Selected Acd	Get/Set	BOOL	0=ACD disable 1=ACD enable (default)
0xB	Last Conflict Detected	Get	STRUCT of: USINT AcdActivity ARRAY of: 6 USINT RemoteMac ARRAY of: 28 USINT ArpPdu	ACD Diagnostic Parameters

Tabla 67: Schneider Electric extensiones a TCP/IP Interface Object

Id	Attribute	Access Rule	Data type	Description
0x64	Cable Test	Set/Get	STRUCT of: USINT Interface USINT Status	Interface Status (1=Active, 2=Success, 3=Failure, 4=Uninitialized)
0x65	Cable Pair Size	Get	USINT	Size of the Cable Test Result STRUCT of: 2 Pair for 100BASE 4 Pair for 1000BASE

Tabla 67: Schneider Electric extensiones a TCP/IP Interface Object (cont

Id	Attribute	Access Rule	Data type	Description

0x66	Cable Test Result	Get	STRUCT of:
			USINT Interface
			USINT CablePair
			USINT CableStatus
			USINT CableMinLength
			USINT CableMaxLength
			USINTCableFailureLocation
				100BASE:{
				{Interface, CablePair1, CableStatus, CableMinLength, CableMaxLength, CableFailureLocation}
				{Interface, CablePair2, CableStatus, CableMinLength, CableMaxLength, CableFailureLocation}
				}
				1000BASE:{
				{Interface, CablePair1, CableStatus, CableMinLength, CableMaxLength, CableFailureLocation}
				{Interface, CablePair2, CableStatus, CableMinLength, CableMaxLength, CableFailureLocation}
				{Interface, CablePair3, CableStatus, CableMinLength, CableMaxLength, CableFailureLocation}
				{Interface, CablePair4, CableStatus, CableMinLength, CableMaxLength, CableFailureLocation}
				}

Ethernet Link Object

La información en las siguientes dos tablas forma parte de Ethernet Link Object. Para acceder a la información, use los siguientes valores:

- Class(####)
- Instance(###)
- Attribute(#)

Por ejemplo, los valores *class*, *instance* y *attribute* son valores para el acceso de informacion para la utilizacion de la alarma, usando los siguientes mensajes explícitos:

- Class = 0xF6
- Instance = 1
- Attribute = 6

Tabla 68: Atributos de la instancia y Schneider Electric extensiones para Ethernet Link Object

Id	Attribute	Access Rule	Data type	Description
Atributos de la instancia				
0x1	Interface Speed	Get	UDINT	Used interface speed in MBit/s (10, 100, 1000, …). 0 is used when the speed has not been determined or is invalid because of detected errors.
0x2	Interface Flags	Get	DWORD	Interface Status Flags: 0: Link State (0=No link, 1=Link) 1: Duplex mode (0=Half, 1=Full) 2: Auto-Negotiation Status 3: 0x0=Auto-Negotiation in progress 4: 0x1=Auto-Negotiation failed 0x2=Failed but speed detected 0x3=Auto-Negotiation success 0x4=No Auto-Negotiation 5: Manual configuration require reset (always 0 because it is not needed) 6: Hardware error
0x3	Physical Address	Get	ARRAY of: 6 USINT	MAC address of physical interface
0x4	Interface Counters	Get	STRUCT of: UDINT MibIICounter1 UDINT MibIICounter2 …	InOctets, InUcastPackets, InNUcastPackets, InDiscards, InErrors, InUnknownProtos, OutOctets, OutUcastPackets, OutNUcastPackets, OutDiscards, OutErrors
0x5	Media Counters	Get	STRUCT of: UDINT EthernetMib Counter1 UDINT EthernetMib Counter2 …	Errores detectados: Alignment, FCS, single collision, multiple collision, SQE Test, deferred transmissions, late collisions, excessive collisions, MAC TX, carrier sense, frame too long, MAC RX

Tabla 68: Atributos de la instancia y Schneider Electric extensiones para Ethernet Link Object (cont

Id	Attribute	Access Rule	Data type	Description
0x6	Interface Control	Get/Set	STRUCT of:	Control Bits:
			WORD ControlBits	0: Auto-negotiation enable/disable (0=disable, 1=enable)
				1: Duplex mode (0=Half, 1=Full), if Auto-negotiation disabled
			UINT ForcedInterface Speed	Interface speed in MBits/s: 10,100,…, if Auto-negotiation disabled
0x7	Interface type	Get	USINT	Type of interface: 0: Unknown interface type 1: The interface is internal 2: Twisted-pair 3: Optical fiber
0x8	Interface state	Get	USINT	Current state of the interface: 0: Unknown interface state 1: The interface is enabled 2: The interface is disabled 3: The interface is testing
0x9	Admin State	Set/Get	USINT	Administrative state: 1: Enable the interface 2: Disable the interface
0xA	Interface label	Get	SHORT-STRING	Human readable ID
Schneider Electric extensiones a Ethernet Link Object				
0x64	Ethernet Interface Index	Get	USINT	Interface/Port Index (ifIndex out of MIBII)
0x65	Port Control	Get/Set	DWORD	0: Link state (0=link down, 1=link up)
				1: Link admin state (0=disabled, 1=enabled)
				8: Access violation alarm (read-only)
				9: Utilization alarm (read-only)
0x66	Interface Utilization	Get	USINT	The existing Counter out of the private MIB hm2IDiagfaceUtilization is used. Utilization in percentage (Unit 1%=100, %/100). RX Interface Utilization.
0x67	Interface Utilization Alarm Upper Threshold	Get/Set	USINT	Within this parameter the variable hm2DiagIfaceUtilizationAlarmUpperThreshold can be accessed. Utilization in percentage (Unit 1%=100). RX Interface Utilization Upper Limit.
0x68	Interface Utilization Alarm Lower Threshold	Get/Set	USINT	Within this parameter the variable hm2DiagIfaceUtilizationAlarmLowerThreshold can be accessed. Utilization in percentage (Unit 1%=100). RX Interface Utilization Lower Limit.
0x69	Broadcast limit	Get/Set	USINT	Broadcast limiter Service (Egress BC-Frames limitation, 0=disabled), Frames/second

Tabla 68: Atributos de la instancia y Schneider Electric extensiones para Ethernet Link Object (cont

Id	Attribute	Access Rule	Data type	Description
0x6A	Ethernet Interface Description	Get/Set	STRING	Interface/Port Description (from MIB II ifDescr), for example "Unit: 1 Slot: 2 Port: 1 - 10/100 Mbit TX" or "unavailable", max. 64 Bytes.
0x6B	Port Monitor	Get/Set	DWORD	0: Link Flap (0=Off, 1=On)
				1: CRC/Fragment (0=Off, 1=On)
				2: Duplex Mismatch (0=Off, 1=On)
				3: Overload-Detection (0=Off, 1=On)
				4: Link-Speed/ Duplex Mode (0=Off, 1=On)
				5: Deactivate port action (0=Off, 1=On)
				6: Send trap action (0=Off, 1=On)
				7: Active Condition (displays which condition caused an action to occur) 8: 9: 10: 11: 00001_B: Link Flap 00010_B: CRC/Fragments 00100_B: Duplex Mismatch 01000_B: Overload-Detection 10000_B: Link-Speed/ Duplex mode
				12: Reserved (always 0)
				13: Reserved (always 0)
				14: Reserved (always 0)
				15: Reserved (always 0)
0x6C	Quick Connect	Get/Set	USINT	Quick Connect on the interface (0=Off, 1=On) If you enable Quick Connect, then the device sets the port speed to 100FD, disables Auto-Negotiation, and Spanning Tree on the interface.
0x6D	SFP Diagnostics	Get	STRUCT of:	
			STRING ModuleType	
			SHORT-STRING SerialNumber	
			USINT Connector	
			USINT Supported	
			DINT Temperature	in °C
			DINT TxPower	in mW
			DINT RxPower	in mW
			DINT RxPower	in dBm
			DINT TxPower	in dBm

Tabla 69: Asignación de los puertos a Instancias de Ethernet Link Object

Ethernet Port	Ethernet Link Object Instance
CPU	1
1	2
2	3
3	4
4	5
…	…

Nota: El número de puertos depende del tipo de hardware utilizado. Ethernet Link Object solo existe si el puerto está conectado.

Switch Agent Object

El dispositivo es compatible con el Ethernet Switch Agent Object de Schneider Electric (Class Code 0x95) para la configuración del dispositivo y los parámetros de información con la Instancia 1.

Tabla 70: Atributos de clase

Id	Attribute	Access Rule	Data type	Description	
0x1	Switch Status	Get	DWORD	0:	Like the signal contact, the value indicates the Device Overall state (0=ok, 1=failed)
				1:	Device Security Status (0=ok, 1=failed)
				2:	Power Supply 1 (0=ok, 1=failed)
				3:	Power Supply 2 (0=ok, 1=failed or not existing)
				4:	Reserved
				5:	Reserved
				6:	Signal Contact 1 (0=closed, 1=open)
				7:	Signal Contact 2 (0=closed, 1=open or not existing)
				8:	Reserved
				9:	Temperature (0=ok, 1=failure)
				10:	Module removed (1=removed)
				11:	EAM removed (1=removed)
				12:	EAM-SD removed (1=removed)
				13:	Reserved
				14:	Reserved
				15:	Reserved
				16:	Reserved
				17:	Reserved
				18:	Reserved
				19:	Reserved
				20:	Reserved
				21:	Reserved
				22:	Reserved
				23:	MRP (0=disabled, 1=enabled)
				24:	Reserved
				25:	Reserved
				26:	RSTP (0=disabled, 1=enabled)
				27:	LAG (0=disabled, 1=enabled)
				28:	Reserved
				29:	Reserved
				30:	Reserved
				31:	Connection Error (1=failure)

Tabla 70: Atributos de clase (cont

Id	Attribute	Access Rule	Data type	Description
0x2	Switch Temperature	Get	STRUCT of:	
			INT TemperatureF	in °F
			INT TemperatureC	in °C
0x3	Reserved	Get	UDINT	Reserved for future use (always 0)
0x4	Switch Max Ports	Get	UINT	Maximum number of Ethernet Switch Ports
0x5	Multicast Settings (IGMP Snooping)	Get/Set	WORD	0: IGMP Snooping (0=disabled, 1=enabled) 1: IGMP Querier (0=disabled, 1=enabled) 2: IGMP Querier Mode (read-only) (0=Non-Querier, 1=Querier) 3: 4: 5: 6: 7: IGMP Querier Packet Version Off=0 IGMP Querier disabled V1=1 V2=2 V3=3 8: 9: 10: Treatment of Unknown Multicasts: 0=Send To All Ports 2=Discard
0x6	Switch Existing Ports	Get	ARRAY of: DWORD	Bitmask of existing switch ports Per bit starting with Bit 0 (=Port 1) (0=Port not available, 1=Port existing) Array (bit mask) size is adjusted to the size of maximum number of switch ports (for max. 28 Ports 1 DWORD is used)
0x7	Switch Port Control	Get/Set	ARRAY of: DWORD	Bitmask Link Admin Status switch ports Per bit starting with Bit 0 (=Port 1) (0=Port enabled, 1=Port disabled) Array (bit mask) size is adjusted to the size of maximum number of Switch ports (for max. 28 Ports 1 DWORD is used)
0x8	Switch Ports Mapping	Get	ARRAY of: USINT	Instance number of the Ethernet-Link-Object Starting with Index 0 (=Port 1) All Ethernet Link Object Instances for the existing Ethernet Switch Ports (1..N, maximum number of ports). When the entry is 0, the Ethernet Link Object for this port does not exist

Tabla 70: Atributos de clase (cont

Id	Attribute	Access Rule	Data type	Description
0x9	Switch Action Status	Get	DWORD	Status of the last executed action (for example config save, software update, etc.)
				0: Flash Save Configuration In Progress/Flash Write In Progress
				1: Flash Save Configuration Failed/Flash Write Failed
				4: Configuration changed (configuration not in sync. between running configuration

El Ethernet Switch Agent Object específico de Schneider Electric le proporciona el servicio específico adicional del proveedor, con el Service Code 0x35 para guardar la configuración del switch. Si envía una solicitud desde su ordenador para guardar una configuración del dispositivo, el dispositivo envía una respuesta después de guardar la configuración en la memoria flash.

Base Switch Object

Base Switch Object proporciona la interfaz a nivel de aplicación del CIP a la información de estado básica para un switch Ethernet administrado (revisión 1).

Solo la Instancia 1 de Base Switch (Class Code 0x51) está disponible.

Tabla 71: Atributos de la instancia

Id	Attribute	Access Rule	Data type	Description
0x1	Device Up Time	Get	UDINT	Time since the device powered up
0x2	Total port count	Get	UDINT	Number of physical ports
0x3	System Firmware Version	Get	SHORT-STRING	Human readable representation of System Firmware Version
0x4	Power source	Get	WORD	Status of switch power source
0x5	Port Mask Size	Get	UINT	Number of DWORD in port array attributes
0x6	Existing ports	Get	ARRAY of:	Port Mask
			DWORD	
0x7	Global Port Admin State	Get	ARRAY of:	Port Admin Status
			DWORD	
0x8	Global Port link Status	Get	ARRAY of:	Port Link Status
			DWORD	
0x9	System Boot Loader Version	Get	SHORT-STRING	Readable System Firmware Version
0xA	Contact Status	Get	UDINT	Switch Contact Closure

Tabla 71: Atributos de la instancia (cont

Id	Attribute	Access Rule	Data type	Description
0xB	Aging Time	Get	UDINT	Range 10..1000000 · 1/10 seconds (default=300) 0=Learning off
0xC	Temperature C	Get	UINT	Switch temperature in degrees Celsius
0xD	Temperature F	Get	UINT	Switch temperature in degrees Fahrenheit

RSTP Bridge Object (MCSESM-E)

RSTP es un protocolo Layer 2 que permite el uso de una topología de Ethernet redundante (por ejemplo de un anillo). El RSTP está especificado en el capítulo 17 de la IEEE 802.1D-2004.

El dispositivo es compatible con el RSTP Bridge Object específico de Schneider Electric (Class Code 64_H, 100) para la configuración y los parámetros de información del dispositivo.

El dispositivo admite 2 instancias:
- La instancia 1 representa la instancia RSTP primaria del puente y
- la instancia 2 representa la instancias RSTP secundaria (Dual).

Encontrará más información acerca de estos parámetros y del modo de configurarlos en el manual de referencia "Interfaz gráfica de usuario".

Tabla 72: Schneider Electric RSTP Bridge Object

Id	Attribute	Access rule	Data type	Description
1	Bridge Identifier Priority	Set	UDINT	Range: 0 to 61,440 in steps of 4,096, default: 32,768 (refer to IEEE, 802.1D-2004, § 17.13.7)
2	Transmit Hold Count	Set	UINT	Range: 1 to 40, default: 10 (refer to IEEE 802.1D-2004, §17.13.12)
3	Force Protocol Version	Set	UINT	Default:2 (refer to IEEE 802.1D-2004, §17.13.4 and dot1dStpVersion in RFC 4318)
4	Bridge Hello Time	Set	UDINT	Range: 100 to 200, unit: centi-seconds (1/100 of a second), default: 200 (refer to IEEE 802.1D-2004, §17.13.6 and dot1dStpHoldTime in RFC 4188)
5	Bridge Forward Delay	Set	UDINT	Range: 400 to 3000, unit: centi-seconds, default: 2100 (refer to IEEE 802.1D-2004, §17.13.5 and dot1dStpForwardDelay in RFC 4188)
6	Bridge Max. Age	Set	UINT	Range: 600 to 4000, unit: centi-seconds, default: 4000 (refer to IEEE 802.1D-2004, §17.13.8 and dot1dStpBridgeMaxAge in RFC 4188)
7	Time Since Topology Change	Get	UDINT	Unit: centi-seconds (refer to dot1dStpTimeSinceTopologyChange in RFC 4188)

Tabla 72: Schneider Electric RSTP Bridge Object (cont

Id	Attribute	Access rule	Data type	Description
8	Topology Change	Get	UDINT	Refer to dot1dStpTopChanges in RFC 4188
100	InnerPort	Get	UINT	Schneider Electric-specific object. ▶ For instance 1, it holds the port number of the DRSTP Primary instance‘s inner port. ▶ For instance 2, it holds the port number of the DRSTP Secondary instance‘s inner port.
101	OuterPort	Get	UINT	Schneider Electric-specific object. ▶ For instance 1, it holds the port number of the DRSTP Primary instance‘s outer port. ▶ For instance 2, it holds the port number of the DRSTP Secondary instance‘s outer port.

RSTP Port Object (MCSESM-E)

El dispositivo es compatible con el RSTP Port Object específico de Schneider Electric (Class Code 65_H, 101) para la configuración y los parámetros de información del RSTP con al menos una instancia (Instance 1).

La instancia 1 representa la interfaz de Ethernet de la CPU; la instancia 2 representa el primer puerto físico; la instancia 3 el segundo puerto físico, etc.

Encontrará más información acerca de estos parámetros y del modo de configurarlos en el manual de referencia "Interfaz gráfica de usuario".

Tabla 73: Schneider Electric RSTP Port Object

Id	Attribute	Access rule	Data type	Description
1	Port Identifier Priority	Set	UDINT	Range: 0 to 240 in steps of 16, default: 128 (refer to IEEE, 802.1D-2004, § 17.13.10).
2	mcheck	Set	BOOL	True (1), False (2) (refer to IEEE 802.1D-2004, §17.19.13 and dot1dStpPortProtocolMigration in RFC 4318).
3	Port Path Cost	Set	UDINT	Range: 1 to 200,00,000, default:auto (0) (refer to IEEE 802.1D-2004, §17.13.11 and dot1dStpPortAdminPathCost in RFC 4318).
4	Port Admin Edge Port	Set	BOOL	True (1), False (2) (refer to IEEE 802.1D-2004, §17.13.1 and dot1dS-tpPortAdminEdgePort in RFC 4318).
5	Port Oper Edge Port	Get	BOOL	True (1), False (2) (refer to dot1dStpPortOperEdgePort in RFC 4318).
6	Port Admin PointToPoint	Set	UINT	forceTrue (0), forceFalse (1), auto (2) (refer to dot1dStpPortAdminPointToPoint in RFC 4318).
7	Port Oper PointToPoint	Get	UINT	True (1), False (2) (refer to dot1dStpPortOperPointToPoint in RFC 4318).

Tabla 73: Schneider Electric RSTP Port Object (cont

Id	Attribute	Access rule	Data type	Description
8	Port Enable	Set	UINT	Enabled (1), Disabled (2) (Refer to dot1dStpPortEnable in RFC 4188).
9	Port State	Get	UINT	Disabled (1), Blocking (2), Listening (3), Learning (4), Forwarding (5), Broken (6) (refer to dot1dStpPortState in RFC 4188).
10	Port Role	Get	UNT	Unknown (0), Alternate/Backup (1), Root (2), Designated (3) (refer to dot1dStpTopChanges in RFC 4188).
100	DRSTP	Get	UINT	Schneider Electric-specific object. True (1), False (2).

Servicios, conexiones y datos de E/S

El dispositivo admite los siguientes tipos de conexiones y parámetros.

Tabla 74: Configuración para integrar un nuevo módulo

Setting	I/O connection	Input only	Listen only
Comm Format:	Data - DINT	Data - DINT	Input Data - DINT - Run/Program
IP Address	IP address of the device	IP address of the device	IP address of the device
Input Assembly Instance	100	100	100
Input Size	32	32	32
Output Assembly Instance	150	152	153
Output Size	32	0	0
Configuration Assembly Instance	151	151	151
Data Size	10	10	10

Tabla 75: Estructura de datos de E/S del dispositivo

I/O Data	Value (data types and sizes to be defined)	Direction	Size[1]
Device Status	Bitmask (see Switch Agent Attribute 0x1)	Input	DWORD
Link Status	Bitmask, 1 Bit per port (0=No link, 1=Link up)	Input	DWORD
Output Links Admin State applied	Bitmask (1 Bit per port) to acknowledge output. Link state change can be denied, for example for controller access port. (0=Port enabled, 1=Port disabled)	Input	DWORD
Utilization Alarm[2]	Bitmask, 1 Bit per port (0=No alarm, 1=Alarm on port)	Input	DWORD
Access Violation Alarm[3]	Bitmask, 1 Bit per port (0=No alarm, 1=Alarm on port)	Input	DWORD
Multicast Connections	Integer, number of connections	Input	DINT

Tabla 75: Estructura de datos de E/S del dispositivo (cont

I/O Data	Value (data types and sizes to be defined)	Direction	Size[1]
TCP/IP Connections	Integer, number of connections	Input	DINT
Quick Connect Mask	Bitmask (1 Bit per port) (0=Quick Connect disabled, 1=Quick Connec enabled)	Input	DINT
Link Admin State	Bitmask, 1 Bit per port (0=Port enabled, 1=Port disabled)	Output	DWORD

1. El tamaño predeterminado de las máscaras de bits del puerto es de 32 bits (DWORD). Para dispositivos con más de 28 puertos, las máscaras de bits del puerto se han ampliado a n * DWORD.
2. Especifique la configuración de la alarma de uso en el cuadro de diálogo *Basic Settings > Port*, pestaña *Utilization*. El umbral superior es el límite en el que se activa la condición de la alarma. El umbral inferior es el límite en el que se desactiva la condición de la alarma.
3. Especifique la configuración de Access Violation Alarm en el cuadro de diálogo *Network Security > Port Security*. El umbral superior es el límite en el que se activa la condición de la alarma. El umbral inferior es el límite en el que se desactiva la condición de la alarma.

Tabla 76: Mapeo de los tipos de datos a tamaños de bits

Tipo de objeto	Tamaño de bits
BOOL	1 bit
DINT	32 bit
DWORD	32 bit
SHORT-STRING	max. 32 bytes
STRING	max. 64 bytes
UDINT	32 bit
UINT	16 bit
USINT	8 bit
WORD	16 bit

A Ajuste del entorno de configuración

A.1 Ajuste de un servidor DHCP/BOOTP

El siguiente ejemplo describe la configuración de un servidor DHCP mediante el software haneWIN DHCP Server. El software shareware es un producto de IT-Consulting Dr. Herbert Hanewinkel. Puede descargar el software en www.hanewin.net. Puede utilizar el software en modo de prueba durante 30 días naturales desde la fecha de la primera instalación y, a continuación, decidir si desea adquirir una licencia.

Lleve a cabo los siguientes pasos:
- ☐ Instale el servidor DHCP en su PC.
  Para llevar a cabo la instalación, siga los pasos del asistente de instalación.
- ☐ Inicie el programa *haneWIN DHCP Server*.

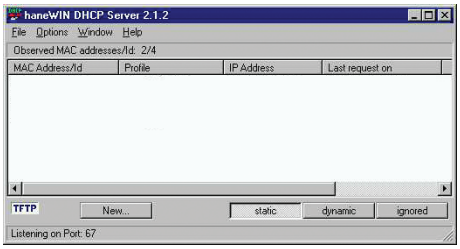


Figura 82: Ventana de bienvenida del programa haneWIN DHCP Server

Nota: Al activar Windows, el procedimiento de instalación incluye un servicio que se inicia automáticamente en la configuración básica. Este servicio también se activa aunque el programa en sí no se haya iniciado. El servicio iniciado responde consultas DHCP.

- ☐ En la barra de menú, haga clic en los elementos *Options > Preferences* para abrir la ventana de la configuración del programa.
- ☐ Seleccione la pestaña *DHCP*.
- ☐ Especifique la configuración que se muestra en la figura.

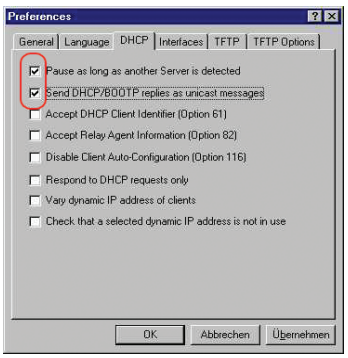


Figura 83: Configuración DHCP

- ☐ Haga clic en el botón *OK*.
- ☐ Para introducir los perfiles de configuración, seleccione los elementos *Options > Configuration Profiles* en la barra de menú.

☐ Especifique el nombre del nuevo perfil de configuración.

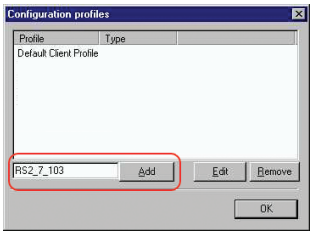


Figura 84: Agregar perfiles de configuración

☐ Haga clic en el botón *Add*.
☐ Especifique la máscara de red.

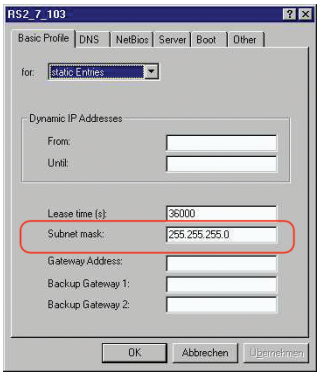


Figura 85: Máscara de red en el perfil de configuración

☐ Haga clic en el botón *Apply*.
☐ Seleccione la pestaña *Boot*.
☐ Escriba la dirección IP del servidor tftp.
☐ Escriba la ruta y el nombre del archivo de configuración.

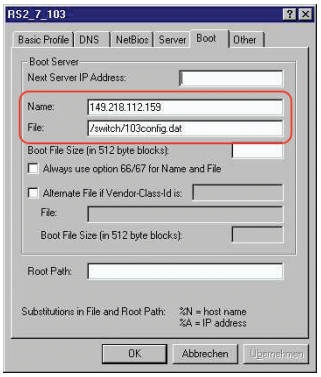


Figura 86: Archivo de configuración en el servidor tftp

☐ Haga clic en el botón *Apply* y, a continuación, en el botón *OK*.

☐ Agregue un perfil por cada tipo de dispositivo.
Si varios dispositivos del mismo tipo tienen configuraciones distintas, añada un perfil para cada configuración.

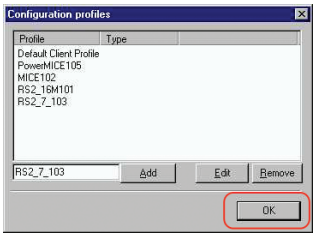


Figura 87: Administración de perfiles de configuración

☐ Para terminar de añadir los perfiles de configuración, haga clic en el botón *OK*.
☐ Para introducir las direcciones estáticas, haga clic en el botón *Static* de la ventana principal.

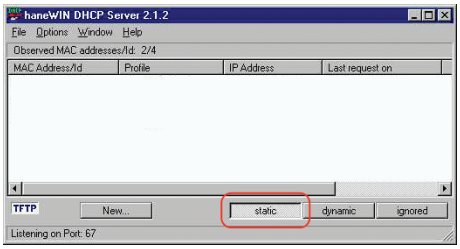


Figura 88: Especificación de direcciones estáticas

☐ Haga clic en el botón *Add*.

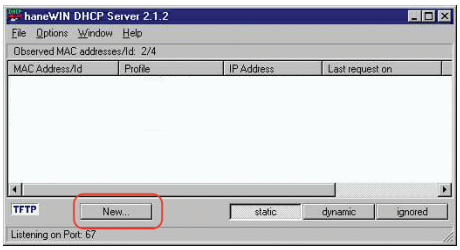


Figura 89: Agregar direcciones estáticas

☐ Escriba la dirección MAC del dispositivo.
☐ Escriba la dirección IP del dispositivo.

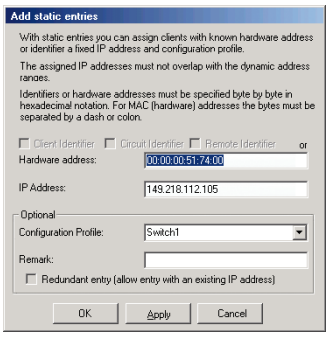


Figura 90: Entradas de direcciones estáticas

☐ Seleccione el perfil de configuración del dispositivo.

- ☐ Haga clic en el botón *Apply* y, a continuación, en el botón *OK*.
- ☐ Agregue una entrada por cada dispositivo que deba recibir sus parámetros del servidor DHCP.

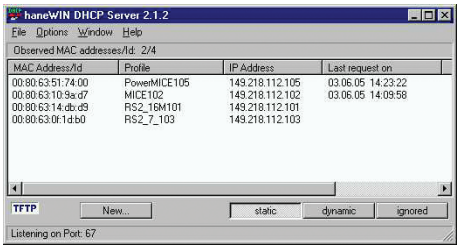


Figura 91: Servidor DHCP con entradas

A.2 Ajuste de un servidor DHCP con la Opción 82

El siguiente ejemplo describe la configuración de un servidor DHCP mediante el software haneWIN DHCP Server. El software shareware es un producto de IT-Consulting Dr. Herbert Hanewinkel. Puede descargar el software en www.hanewin.net. Puede utilizar el software en modo de prueba durante 30 días naturales desde la fecha de la primera instalación y, a continuación, decidir si desea adquirir una licencia.

Lleve a cabo los siguientes pasos:

- ☐ Instale el servidor DHCP en su PC.
  Para llevar a cabo la instalación, siga los pasos del asistente de instalación.
- ☐ Inicie el programa *haneWIN DHCP Server*.

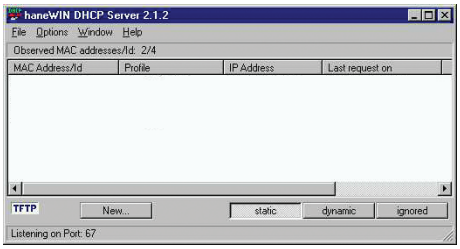


Figura 92: Ventana de bienvenida del programa haneWIN DHCP Server

Nota: Al activar Windows, el procedimiento de instalación incluye un servicio que se inicia automáticamente en la configuración básica. Este servicio también se activa aunque el programa en sí no se haya iniciado. El servicio iniciado responde consultas DHCP.

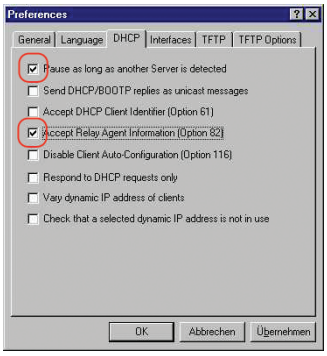


Figura 93: Configuración DHCP

☐ Para introducir las direcciones estáticas, haga clic en el botón *Add*.

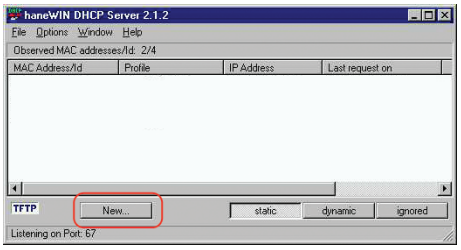


Figura 94: Agregar direcciones estáticas

☐ Marque la casilla *Circuit Identifier*.
☐ Marque la casilla *Remote Identifier*.

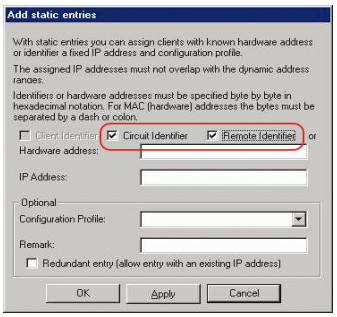


Figura 95: Configuración por defecto para la asignación permanente de direcciones

☐ En el campo *Hardware address*, especifique el valor *Circuit Identifier* y el valor *Remote Identifier* para el switch y el puerto.
El servidor DHCP asigna la dirección IP especificada en el campo *IP address* al dispositivo que conecte al puerto especificado en el campo *Hardware address*.
La dirección de hardware se muestra de la siguiente forma:
`ciclvvvvssmmpprirlxxxxxxxxxxxx`

- `ci`
  Identificador secundario para el tipo de ID de circuito
- `cl`
  Longitud de ID de circuito.
- Schneider Electric identificador:
  `01` cuando se conecta un dispositivo Schneider Electric al puerto; de lo contrario, `00`.
- `vvvv`
  ID VLAN de la solicitud DHCP.
  Configuración por defecto: `0001` = VLAN 1
- `ss`
  Conector del dispositivo en el que se encuentra el módulo con el puerto al que está conec-

tado el dispositivo. Especifique el valor `00`.

- `mm`
  Módulo con el puerto al que está conectado el dispositivo.
- `pp`
  Puerto al que está conectado el dispositivo.
- `ri`
  Identificador secundario para el tipo de ID remoto
- `rl`
  Longitud de ID remoto.
- `xxxxxxxxxxxx`
  ID remoto del dispositivo (por ejemplo, dirección MAC) al que está conectado un dispositivo.

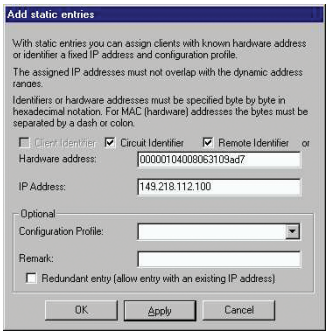


Figura 96: Especificación de las direcciones

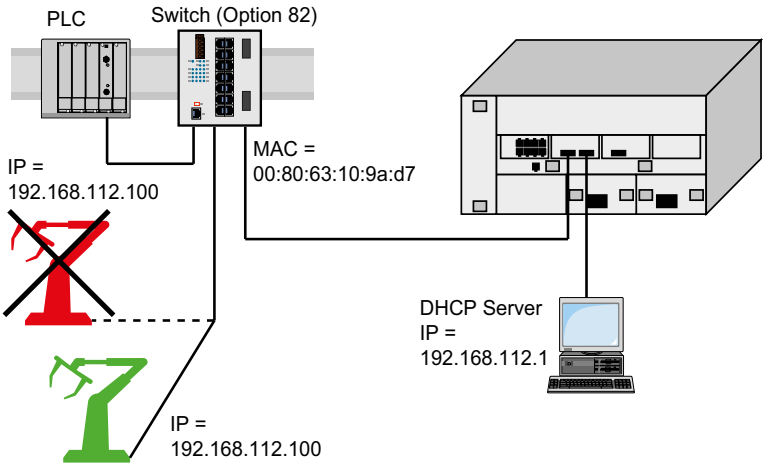


Figura 97: Ejemplo de aplicación con la Opción 82

A.3 Preparación del acceso a través de SSH

Puede conectarse al dispositivo mediante SSH. Para ello, siga los siguientes pasos:
- Genere una clave en el dispositivo.
  o bien
- Transfiera su propia clave al dispositivo.
- Prepare el acceso al dispositivo en el programa cliente SSH.

Nota: En la configuración por defecto, la clave ya existe y el acceso mediante SSH está habilitado.

A.3.1 Generación de una clave en el dispositivo

Es posible generar una clave directamente en el dispositivo. Para ello, siga los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Device Security > Management Access > Server*, pestaña *SSH*.
- ☐ Para desactivar el servidor SSH, seleccione el botón de opción `Off` en el cuadro *Operation*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✓.
- ☐ Para crear una clave RSA, en el cuadro *Signature*, haga clic en el botón *Create*.
- ☐ Para activar el servidor SSH, seleccione el botón de opción `On` en el cuadro *Operation*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✓.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`ssh key rsa generate`	Generar una nueva clave RSA.

A.3.2 Carga de una clave propia en el dispositivo

OpenSSH le ofrece a los administradores de red experimentados la opción de generar una clave propia. Para generar la clave, escriba los siguientes comandos en su PC:

```
ssh-keygen(.exe) -q -t rsa -f rsa.key -C '' -N ''
rsaparam -out rsaparam.pem 2048
```

Es posible transferir su propia clave SSH al dispositivo. Para ello, siga los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Device Security > Management Access > Server*, pestaña *SSH*.
- ☐ Para desactivar el servidor SSH, seleccione el botón de opción `Off` en el cuadro *Operation*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✓.
- ☐ Si la clave de host se encuentra en su PC o en una unidad de red, arrastre y suelte el archivo que contenga la clave en el área . También puede hacer clic en el área para seleccionar el archivo.

- ☐ Haga clic en el botón *Start* del cuadro *Key import* para cargar la clave en el dispositivo.
- ☐ Para activar el servidor SSH, seleccione el botón de opción `On` en el cuadro *Operation*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón ✓.

Lleve a cabo los siguientes pasos:
- ☐ Copie la clave generada automáticamente en la memoria externa desde el PC.
- ☐ Copie la clave en el dispositivo desde la memoria externa.

`enable`	Cambiar al modo Privileged EXEC.
`copy sshkey envm <file name>`	Cargar su propia clave en el dispositivo desde la memoria externa.

A.3.3 Preparación del programa cliente SSH

El programa *PuTTY* le permite acceder al dispositivo mediante SSH. Puede descargar el software en www.putty.org.

Lleve a cabo los siguientes pasos:
- ☐ Inicie el programa haciendo doble clic.

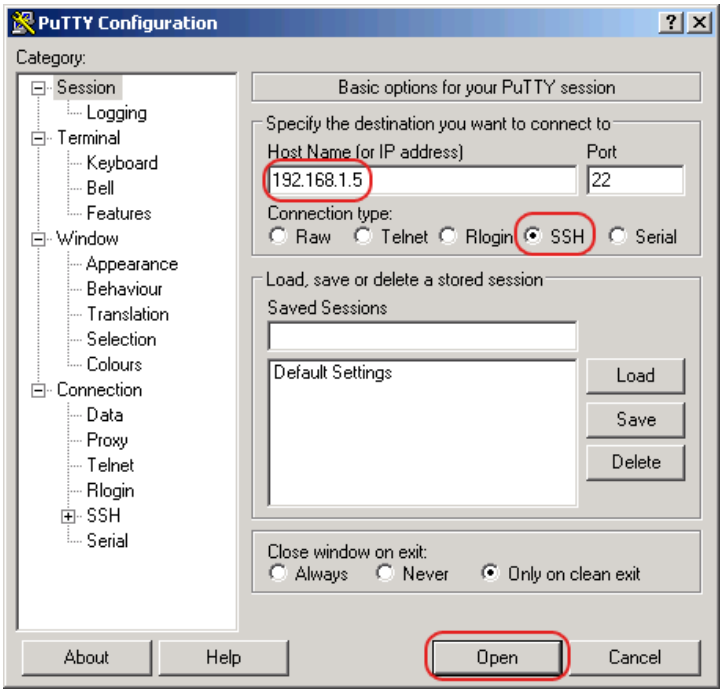


Figura 98: Pantalla de entrada de PuTTY

- ☐ En el campo *Host Name (or IP address)*, introduzca la dirección IP de su dispositivo.
  La dirección IP (a.b.c.d) se compone de 4 números decimales con valores de entre `0` y `255`. Los 4 números decimales están separados por puntos.
- ☐ Para seleccionar el tipo de conexión, seleccione el botón de opción *SSH* en la lista de opciones *Connection type*.
- ☐ Haga clic en el botón *Open* para establecer la conexión de datos con su dispositivo.

Antes de establecer la conexión, el programa *PuTTY* muestra un mensaje de alarma de seguridad y le permite comprobar la huella digital de la clave.

Figura 99: Pregunta de seguridad sobre la huella digital

Antes de establecer la conexión, el programa *PuTTY* muestra un mensaje de alarma de seguridad y le permite comprobar la huella digital de la clave.

- ☐ Compruebe la huella digital de la clave para garantizar que se ha conectado realmente al dispositivo deseado.
- ☐ Si la huella digital coincide con su clave, haga clic en el botón *Yes*.

Para los administradores de red experimentados, un modo alternativo de acceder a su dispositivo mediante SSH consiste en utilizar la suite OpenSSH. Para establecer la conexión de datos, escriba el siguiente comando:

```
ssh admin@10.0.112.53
```

`admin` es el nombre de usuario.

`10.0.112.53` es la dirección IP de su dispositivo.

A.4 Certificado HTTPS

Su navegador web establece la conexión al dispositivo con el protocolo HTTPS. Como requisito previo, debe activar la función *HTTPS server* en el cuadro de diálogo *Device Security > Management Access > Server*, pestaña *HTTPS*.

Nota: Los softwares de terceros, como los navegadores web, validan los certificados basados en criterios como la fecha de caducidad y las recomendaciones actuales de parámetros criptográficos. Los certificados obsoletos pueden ocasionar problemas por información no válida o no actualizada. Ejemplo: Un certificado caducado o un cambio de recomendaciones criptográficas. Para resolver los conflictos de validación con un software de terceros, transfiera su propio certificado al día al dispositivo o vuelva a generar el certificado con el firmware más reciente.

A.4.1 Administración de certificados HTTPS

Se requiere un certificado estándar de acuerdo con el sistema X.509/PEM (infraestructura de clave pública) para la encriptación. En la configuración por defecto, ya existe un certificado generado automáticamente en el dispositivo. Para ello, siga los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Device Security > Management Access > Server*, pestaña *HTTPS*.
- ☐ Para crear un certificado X509/PEM, en el cuadro *Certificate*, haga clic en el botón *Create*.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón  .
- ☐ Reinicie el servidor HTTPS para activar la clave. Reinicie el servidor con la interfaz de línea de comando.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`https certificate generate`	Generar un certificado https X.509/PEM.
`no https server`	Desactivar la función *HTTPS*.
`https server`	Activar la función *HTTPS*.

- ☐ El dispositivo también le permite transferir un certificado X.509/PEM generado de manera externa al dispositivo:

- ☐ Abra el cuadro de diálogo *Device Security > Management Access > Server*, pestaña *HTTPS*.
- ☐ Si el certificado se encuentra en su PC o en una unidad de red, arrastre y suelte el certificado en el área  . También puede hacer clic en el área para seleccionar el certificado.
- ☐ Haga clic en el botón *Start* para copiar el certificado en el dispositivo.
- ☐ Guarde los cambios provisionalmente. Para hacer esto, haga clic en el botón  .

`enable`	Cambiar al modo Privileged EXEC.
`copy httpscert envm <file name>`	Copiar el certificado HTTPS desde un dispositivo de memoria no volátil externo.

`configure`	Cambiar al modo de configuración.
`no https server`	Desactivar la función *HTTPS*.
`https server`	Activar la función *HTTPS*.

Nota: Para activar el certificado después de haberlo creado o transferido, reinicie el dispositivo o el servidor HTTPS. Reinicie el servidor HTTPS con la interfaz de línea de comando.

A.4.2 Acceso a través de HTTPS

La configuración por defecto para la conexión de datos HTTPS es el puerto TCP `443`. Si cambia el número del puerto HTTPS, deberá reiniciar el dispositivo o el servidor HTTPS. De este modo, el cambio se hará efectivo. Para ello, siga los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Device Security > Management Access > Server*, pestaña *HTTPS*.
- ☐ Para activar la función, seleccione el botón de opción `On` en el cuadro *Operation*.
- ☐ Para acceder al dispositivo por HTTPS, escriba HTTPS en lugar de HTTP en su navegador, seguido de la dirección IP del dispositivo.

`enable`	Cambiar al modo Privileged EXEC.
`configure`	Cambiar al modo de configuración.
`https port 443`	Especificar el número del puerto TCP en el que el servidor web recibe las solicitudes HTTPS de los clientes.
`https server`	Activar la función *HTTPS*.
`show https`	Mostrar el estado del servidor *HTTPS* y el número de puerto.

Si realiza cambios en el número de puerto HTTPS, desactive el servidor HTTPS y actívelo de nuevo para que los cambios se hagan efectivos.

El dispositivo utiliza el protocolo HTTPS y establece una nueva conexión de datos. Cuando cierre la sesión al terminar, el dispositivo finaliza la conexión de datos.

B Apéndice

B.1 Base de información de administración (MIB)

La Base de información de administración (MIB, Management Information Base) ha sido diseñada como estructura de árbol abstracta.

Las ramificaciones son clases de objeto. Las "hojas" de la MIB se denominan clases de objetos genéricas.

Cuando se necesitan para una identificación exclusiva, se crea una instancia para las clases de objetos genéricas, lo cual significa que la estructura abstracta se asigna a la realidad, especificando el puerto o la dirección de origen.

Estas instancias están subordinadas a valores (Integer, TimeTicks, Counter u Octet String) que se pueden leer y, en parte, también se pueden modificar. La descripción de objeto o el ID de objeto (OID) designan la clase de objeto. Se utiliza el identificador secundario (SID) a fin de crear una instancia para ellos.

Por ejemplo:

La clase de objeto genérica `sa2PSState` (`OID` = `1.3.6.1.4.1.3833.1.1.11.11.1.1.2.1`) es la descripción de la información abstracta `power supply status`. No obstante, no es posible leer ningún valor a partir de esto, ya que el sistema no sabe a qué alimentación eléctrica hace referencia.

Al especificar el identificador secundario `2`, se asigna esta información abstracta a la realidad (crea una instancia para ella), identificándola de este modo como el estado de funcionamiento de la alimentación eléctrica `2`. Se asigna un valor a esta instancia y puede leerse. La instancia `get 1.3.6.1.4.1.3833.1.1.11.11.1.1.2.1` devuelve la respuesta `1`, lo cual significa que la alimentación eléctrica está lista para funcionar.

Definición de los conceptos de sintaxis usados:	
Integer	Número entero en el rango -2^{31} - 2^{31}-1
IP address ‹Dirección IP›	`xxx.xxx.xxx.xxx` (`xxx` = número entero en el rango `0..255`)
Dirección MAC	Número hexadecimal de 12 dígitos según la norma ISO/IEC 8802-3
Object Identifier	x.x.x.x… (por ejemplo 1.3.6.1.1.4.1.3833...)
Octet String	Cadena de caracteres ASCII
PSID	Identificador de la alimentación eléctrica (número de la fuente de alimentación)
TimeTicks	Cronómetro, tiempo transcurrido = valor numérico / 100 (en segundos) valor numérico = número entero en el rango 0-2^{32}-1

Definición de los conceptos de sintaxis usados:	
Timeout	Valor de tiempo en centésimas de segundo valor de tiempo = número entero en el rango $0\text{-}2^{32}\text{-}1$
Campo de tipo	Número hexadecimal de 4 dígitos según la norma ISO/IEC 8802-3
Contador	Número entero ($0\text{-}2^{32\text{-}1}$); cuando se producen determinados eventos, el valor aumenta en 1.

B.2 Lista de RFC

RFC 768	UDP
RFC 783	TFTP
RFC 791	IP
RFC 792	ICMP
RFC 793	TCP
RFC 826	ARP
RFC 854	Telnet
RFC 855	Telnet Option
RFC 951	BOOTP
RFC 1112	IGMPv1
RFC 1157	SNMPv1
RFC 1155	SMIv1
RFC 1212	Concise MIB Definitions
RFC 1213	MIB2
RFC 1493	Dot1d
RFC 1542	BOOTP-Extensions
RFC 1643	Ethernet-like -MIB
RFC 1757	RMON
RFC 1867	Form-Based File Upload in HTML
RFC 1901	Community based SNMP v2
RFC 1905	Protocol Operations for SNMP v2
RFC 1906	Transport Mappings for SNMP v2
RFC 1945	HTTP/1.0
RFC 2068	HTTP/1.1 protocol as updated by draft-ietf-http-v11-spec-rev-03
RFC 2131	DHCP
RFC 2132	DHCP-Options
RFC 2233	The Interfaces Group MIB using SMI v2
RFC 2236	IGMPv2
RFC 2246	The TLS Protocol, Version 1.0
RFC 2346	AES Ciphersuites for Transport Layer Security
RFC 2365	Administratively Scoped IP Multicast
RFC 2578	SMIv2
RFC 2579	Textual Conventions for SMI v2
RFC 2580	Conformance statements for SMI v2
RFC 2613	SMON
RFC 2618	RADIUS Authentication Client MIB
RFC 2620	RADIUS Accounting MIB
RFC 2674	Dot1p/Q
RFC 2818	HTTP over TLS
RFC 2851	Internet Addresses MIB
RFC 2863	The Interfaces Group MIB
RFC 2865	RADIUS Client
RFC 2866	RADIUS Accounting

RFC 2868	RADIUS Attributes for Tunnel Protocol Support
RFC 2869	RADIUS Extensions
RFC 2869bis	RADIUS support for EAP
RFC 2933	IGMP MIB
RFC 3164	The BSD Syslog Protocol
RFC 3376	IGMPv3
RFC 3410	Introduction and Applicability Statements for Internet Standard Management Framework
RFC 3411	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
RFC 3412	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC 3413	Simple Network Management Protocol (SNMP) Applications
RFC 3414	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
RFC 3415	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
RFC 3418	Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)
RFC 3580	802.1X RADIUS Usage Guidelines
RFC 3584	Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework
RFC 3621	Power Ethernet MIB
RFC 4022	Management Information Base for the Transmission Control Protocol (TCP)
RFC 4113	Management Information Base for the User Datagram Protocol (UDP)
RFC 4188	Definitions of Managed Objects for Bridges
RFC 4251	SSH protocol architecture
RFC 4291	IPv6 Addressing Architecture
RFC 4252	SSH authentication protocol
RFC 4253	SSH transport layer protocol
RFC 4254	SSH connection protocol
RFC 4293	Management Information Base for the Internet Protocol (IP)
RFC 4318	Definitions of Managed Objects for Bridges with Rapid Spanning Tree Protocol
RFC 4330	Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI
RFC 4363	Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual LAN Extensions
RFC 4541	Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches
RFC 4836	Definitions of Managed Objects for IEEE 802.3 Medium Attachment Units (MAUs)
RFC 4861	Neighbor Discovery for IPv6
RFC 5321	Simple Mail Transfer Protocol
RFC 6221	Leightweight DHCPv6 Relay Agent
RFC 8200	IPv6 Specification
RFC 8415	DHCPv6

B.3 Normas IEEE aplicadas

IEEE 802.1AB	Station and Media Access Control Connectivity Discovery
IEEE 802.1D	MAC Bridges (switching function)
IEEE 802.1Q	Virtual LANs (VLANs, MRP, Spanning Tree)
IEEE 802.1X	Port Authentication
IEEE 802.3	Ethernet
IEEE 802.3ac	VLAN Tagging
IEEE 802.3x	Flow Control
IEEE 802.3af	Power over Ethernet

B.4 Normas IEC aplicadas

IEC 62439	High availability automation networks MRP – Media Redundancy Protocol based on a ring topology

B.5 Normas ANSI aplicadas

ANSI/TIA-1057	Link Layer Discovery Protocol for Media Endpoint Devices, April 2006

B.6 Datos técnicos

16.3.3 Conmutación

Tamaño de la tabla de direcciones MAC (incluido filtros estáticos)	16384
Número máx. de filtros de direcciones MAC configurados de forma estática	100
Número máx. de filtros de direcciones MAC que se pueden aprender mediante el IGMP Snooping	1024
Número máx. de entradas de direcciones MAC (MMRP)	64
Número de colas con prioridad	8 Colas
Prioridades del puerto configurables	0..7
MTU (longitud máxima permitida de los paquetes que un puerto puede recibir o transmitir).	9720 Bytes

16.3.4 VLAN

Rango de ID de VLAN	1..4042
Número de VLAN	Máximo 128 simultáneos por dispositivo Máximo 128 simultáneos por puerto

16.3.5 Listas de control de acceso (ACL)

Número máximo de ACL	50
Número máximo de reglas por ACL	256
Número máximo de reglas por puerto	256
Número de reglas configurables totales	2048 (8 × 256)
Número máximo de asignaciones de VLAN	12
Número máximo de reglas que registran un evento	128
Número máximo de reglas de entrada	514

B.7 Copyright del software integrado

El producto contiene, entre otras cosas, archivos de software de código abierto desarrollados por terceros y con licencia de software de código abierto.

Puede consultar las condiciones de la licencia en la interfaz gráfica de usuario en el cuadro de diálogo *Help > Licenses*.

B.8 Abreviaturas usadas

ACL	Access Control List
BOOTP	Bootstrap Protocol
CLI	Command Line Interface
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol for IPv6
DUID	DHCP Unique Identifier
EUI	Extended Unique Identifier
FDB	Forwarding Database
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPv6	Internet Protocol version 6
LDRA	Lightweight DHCPv6 Relay Agent
LED	Light Emitting Diode
LLDP	Link Layer Discovery Protocol
MAC	Media Access Control
MIB	Management Information Base
MRP	Media Redundancy Protocol
NDP	Neighbor Discovery Protocol
NMS	Network Management System
PC	Personal Computer
PTP	Precision Time Protocol
QoS	Quality of Service
RFC	Request For Comment
RM	Redundancy Manager
RSTP	Rapid Spanning Tree Protocol
SCP	Secure Copy
SFP	Small Form-factor Pluggable
SFTP	SSH File Transfer Protocol
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TP	Twisted Pair
UDP	User Datagram Protocol

URL	Uniform Resource Locator
UTC	Coordinated Universal Time
VLAN	Virtual Local Area Network

C Índice

S

T

U

V

W