# Modicon

## Switch MCSESM, MCSESM-E, MCSESP con administración
## Manual de referencia de la GUI

QGH59088.02

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

# Indicaciones sobre la interfaz gráfica de usuario

El dispositivo es compatible con los siguientes sistemas operativos:
- Windows 10
- Linux

La interfaz gráfica de usuario del dispositivo se divide de la siguiente manera:
- Área de navegación
- Área de diálogo
- Botones

### Área de navegación

El área de navegación se encuentra en el lateral izquierdo de la interfaz gráfica de usuario.

El área de navegación contiene los siguientes elementos:
- Barra de herramientas
- Filtro
- Menú

Tiene la opción de ocultar toda el área de navegación, por ejemplo, al mostrar la interfaz gráfica de usuario en pantallas pequeñas. Para ocultarla o desplegarla, haga clic en la flecha pequeña de la parte superior del área de navegación.

### Barra de herramientas

La barra de herramientas situada en la parte superior del área de navegación contiene varios botones.
- Al colocar el puntero sobre un botón, aparecerá un cuadro con más información sobre este.
- Si se pierde la conexión con el dispositivo, la barra de herramientas aparecerá en gris.

El dispositivo actualiza automáticamente la información de la barra de herramientas cada 5 segundos.

Al hacer clic en este botón, se actualizará la barra de herramientas de forma manual.

Al colocar el puntero sobre este botón, aparecerá un cuadro con la siguiente información:
- *User:*
  Nombre del usuario conectado
- *Device name:*
  Nombre del dispositivo

Al hacer clic en este botón, se abrirá el cuadro de diálogo *Device Security > User Management*.

Al colocar el puntero sobre este botón, aparecerá un cuadro con el resumen del cuadro de diálogo *Diagnostics > System > Configuration Check*.

Al hacer clic en este botón, se abrirá el cuadro de diálogo *Diagnostics > System > Configuration Check*.

Al hacer clic en el botón se cierra la sesión del usuario y se muestra el cuadro de diálogo de inicio de sesión.

Si el perfil de configuración en la memoria volátil (*RAM*) y el perfil de configuración "Seleccionado" en la memoria no volátil (*NVM*) son iguales, el dispositivo muestra el cuadro de diálogo *Warning*.

- Para guardar los cambios de forma permanente, haga clic en el botón *Yes* del cuadro de diálogo *Warning*.
- Para descartar los cambios, haga clic en el botón *No* del cuadro de diálogo *Warning*.


Muestra el tiempo restante en segundos hasta que el dispositivo cierre automáticamente la sesión del usuario inactivo.

Al hacer clic en este botón, se abrirá el cuadro de diálogo *Device Security > Management Access > Web*. Aquí puede especificar el límite de tiempo.

Si el perfil de configuración en la memoria volátil (*RAM*) es diferente del perfil de configuración "Seleccionado" en la memoria no volátil (*NVM*), aparecerá este botón. De lo contrario, el botón permanecerá oculto.

Al hacer clic en este botón, se abrirá el cuadro de diálogo *Basic Settings > Load/Save*.

Al hacer clic con el botón derecho en este botón, podrá guardar la configuración en la memoria no volátil (*NVM*).

Al colocar el puntero sobre este botón, aparecerá un cuadro con la siguiente información:

- *Device Status:* Esta sección muestra una vista comprimida del cuadro *Device status* en el cuadro de diálogo *Basic Settings > System*. La sección muestra la alarma activa en este momento y la primera alarma registrada.
- *Security Status:* Esta sección muestra una vista comprimida del cuadro *Security status* en el cuadro de diálogo *Basic Settings > System*. La sección muestra la alarma activa en este momento y la primera alarma registrada.
- *Boot Parameter:* Si guarda los cambios en la configuración de forma permanente y al menos un parámetro de arranque es diferente del perfil de configuración utilizado durante el último reinicio, esta sección mostrará una nota.
  Los siguientes ajustes cambiarán los parámetros de arranque:
  - Cuadro de diálogo *Basic Settings > External Memory*, parámetro *Software auto update*
  - Cuadro de diálogo *Basic Settings > External Memory*, parámetro *Config priority*
  - Cuadro de diálogo *Device Security > Management Access > Server*, pestaña *SNMP*, parámetro *UDP port*
  - Cuadro de diálogo *Diagnostics > System > Selftest*, parámetro *RAM test*
  - Cuadro de diálogo *Diagnostics > System > Selftest*, parámetro *SysMon1 is available*
  - Cuadro de diálogo *Diagnostics > System > Selftest*, parámetro *Load default config on error*

Al hacer clic en este botón, se abrirá el cuadro de diálogo *Diagnostics > Status Configuration > Device Status*.

### Filtro

El filtro le permite reducir el número de elementos en el menú. Al filtrar, el menú solo mostrará los elementos que encajen con la secuencia de búsqueda introducida en el campo de filtro.

### Menú

El menú muestra los elementos del menú.

Puede filtrar los elementos del menú. Consulte la sección “Filtro”.

Para mostrar el cuadro de diálogo correspondiente en el área de diálogo, haga clic en el elemento del menú deseado. Si el elemento del menú seleccionado es un nodo que contiene subelementos, el nodo se desplegará o se ocultará al hacer clic. El área de diálogo mantiene el cuadro de diálogo mostrado anteriormente.

Puede desplegar u ocultar todos los nodos del menú a la vez. Al hacer clic con el botón derecho en cualquier parte del menú, se mostrará un menú contextual con las siguientes entradas:

- *Expand*
  Despliega todos los nodos del menú a la vez. El menú muestra los elementos de cada nivel.
- *Collapse*
  Oculta todos los nodos del menú a la vez. El menú muestra los elementos del nivel superior.

### Área de diálogo

El área de diálogo se encuentra en el lateral derecho de la interfaz gráfica de usuario. Al hacer clic en un elemento del menú del área de navegación, el área de diálogo mostrará el cuadro de diálogo correspondiente.

### Actualización de la pantalla

Si un cuadro de diálogo permanece abierto durante mucho tiempo, es posible que los valores del dispositivo hayan cambiado.

- ☐ Para actualizar los datos mostrados en el cuadro de diálogo, haga clic en el botón . La información en el cuadro de diálogo sin guardar se perderá.

### Cómo guardar la configuración

El almacenamiento transfiere las configuraciones cambiadas a la memoria volátil (*RAM*) del dispositivo. Lleve a cabo el paso siguiente:

- ☐ Haga clic en el botón .

Para mantener los ajustes cambiados, incluso después de reiniciar el dispositivo, lleve a cabo los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Basic Settings > Load/Save*.
- ☐ En la tabla, marque el perfil de configuración que desee.
- ☐ Si en la columna *Selected*, la casilla aparece `unmarked`, haga clic en el botón y, a continuación, en el elemento *Select*.
- ☐ Haga clic en el botón y, a continuación, en el elemento *Save*.

**Nota:** Cambios accidentales en la configuración pueden cortar la conexión entre el PC y el dispositivo. Para asegurar su acceso al dispositivo, active la función *Undo configuration modifications* en el cuadro de diálogo *Basic Settings > Load/Save* antes de cambiar la configuración. Usando esta función, el dispositivo comprueba de forma continua si todavía es accesible desde la dirección IP de su PC. Si se pierde la conexión, el dispositivo cargará el perfil de configuración guardado en la memoria no volátil (*NVM*) tras el tiempo especificado. Después, se podrá acceder otra vez al dispositivo.

### Trabajo con tablas

Los cuadros de diálogos muestran varias configuraciones en forma de tabla.

Cuando modifique una celda de la tabla, aparecerá una marca roja en la esquina superior izquierda de esa celda. La marca roja indica que las modificaciones no se han transferido todavía a la memoria volátil (*RAM*) del dispositivo.

Puede personalizar la apariencia de las tablas según sus necesidades. Al colocar el puntero sobre el encabezado de una columna, aparecerá un botón de lista desplegable en este. Al hacer clic en este botón, la lista desplegable mostrará las siguientes entradas:

- ▶ Orden ascendente
  Ordena las entradas de la tabla en orden ascendente según las entradas de la columna seleccionada.
  Podrá identificar las entradas ordenadas de una tabla mediante una flecha en la cabecera de la columna.
- ▶ Orden descendente
  Ordena las entradas de la tabla en orden descendente según las entradas de la columna seleccionada.
  Podrá identificar las entradas ordenadas de una tabla mediante una flecha en la cabecera de la columna.

- Columnas
  Muestra u oculta columnas.
  Podrá identificar las columnas ocultas mediante una casilla sin marcar en la lista desplegable.
- Filtros
  La tabla solo muestra las entradas cuyo contenido encaja con los criterios de filtrado especificados para la columna seleccionada.
  Podrá identificar las entradas filtradas de una tabla mediante la cabecera resaltada de la columna.

Puede seleccionar varias entradas de la tabla a la vez y aplicar una acción a todas. Esto resulta útil cuando necesita eliminar varias entradas de la tabla a la vez.

- Seleccionar varias entradas consecutivas de la tabla:
  - ☐ Haga clic en la primera entrada de la tabla que desee para resaltarla.
  - ☐ Mantenga presionada la tecla <MAYÚS>.
  - ☐ Haga clic en la última entrada de la tabla para resaltar todas las entradas deseadas.
- Seleccionar varias entradas individuales de la tabla:
  - ☐ Haga clic en la primera entrada de la tabla que desee para resaltarla.
  - ☐ Mantenga presionada la tecla <CTRL>.
  - ☐ Haga clic en la siguiente entrada de la tabla que desee para resaltarla.
    Repita el proceso hasta que haya resaltado todas las entradas que desee.

### Botones

Aquí encontrará la descripción de los botones estándar. Los botones especiales específicos de cuadros de diálogo se describen en el texto de ayuda del cuadro de diálogo correspondiente.

Transfiere los cambios a la memoria volátil (*RAM*) del dispositivo y los aplica al dispositivo. Para guardar los cambios en la memoria no volátil, siga los siguientes pasos:

- ☐ Abra el cuadro de diálogo *Basic Settings > Load/Save*.
- ☐ En la tabla, marque el perfil de configuración que desee.
- ☐ Si en la columna *Selected*, la casilla aparece `unmarked`, haga clic en el botón  y, a continuación, en el elemento *Select*.
- ☐ Haga clic en el botón  para guardar los cambios actuales.

Actualiza los campos con los valores guardados en la memoria volátil (*RAM*) del dispositivo.

Transfiere la configuración de la memoria volátil (*RAM*) al perfil de configuración designado como "Seleccionado" en la memoria no volátil (*NVM*).

Cuando la casilla en la columna *Backup config when saving* del cuadro de diálogo *Basic Settings > External Memory* aparece marcada, el dispositivo genera una copia del perfil de configuración en la memoria externa.

Muestra un submenú con los elementos correspondientes al cuadro de diálogo en cuestión.

Abre el cuadro de diálogo *Wizard*.

Añade una nueva entrada a la tabla.

Elimina la entrada de la tabla seleccionada.

Abre la ayuda en línea.

# 1 Basic Settings

El menú contiene los siguientes cuadros de diálogo:
- System
- Network
- Out of Band over USB
- Software
- Load/Save
- External Memory
- Port
- Power over Ethernet (MCSESP)
- Restart

## 1.1 System

[Basic Settings > System]

En este cuadro de diálogo, podrá supervisar estados de funcionamiento individuales.

### Device status

Los campos en este cuadro muestran el estado del dispositivo y le informan de todas las alarmas que se hayan producido. Si existe una alarma en este momento, el cuadro aparecerá resaltado.

Especifique los parámetros que el dispositivo supervisará en el cuadro de diálogo *Diagnostics* > Status Configuration > *Device Status*.

**Nota:** Si conecta solo una fuente de alimentación para la tensión de alimentación a un dispositivo con una fuente de alimentación redundante, el dispositivo informará de una alarma. Para evitar esta alarma, desactive el control de fuentes de alimentación ausentes en el cuadro de diálogo *Diagnostics > Status Configuration > Device Status*.

Alarm counter

Muestra el número de alarmas existentes actualmente.

Si hay al menos una alarma activa en este momento, este icono será visible.

Al colocar el puntero sobre este icono, un cuadro de ayuda mostrará la causa de la alarma activa y el momento en el que el dispositivo activó la alarma.

Si un parámetro bajo supervisión no se encuentra en el estado deseado, el dispositivo activará una alarma. El cuadro de diálogo *Diagnostics > Status Configuration > Device Status*, pestaña *Status*, muestra una vista general de las alarmas.

### Security status

Los campos en este cuadro muestran el estado de seguridad y le informan de todas las alarmas que se hayan producido. Si existe una alarma en este momento, el cuadro aparecerá resaltado.

Especifique los parámetros que el dispositivo supervisará en el cuadro de diálogo *Diagnostics* > Status Configuration > *Security Status*.

Alarm counter

Muestra el número de alarmas existentes actualmente.

Si hay al menos una alarma activa en este momento, este icono será visible.

Al colocar el puntero sobre este icono, un cuadro de ayuda mostrará la causa de la alarma activa y el momento en el que el dispositivo activó la alarma.

Si un parámetro bajo supervisión no se encuentra en el estado deseado, el dispositivo activará una alarma. El cuadro de diálogo *Diagnostics > Status Configuration > Security Status*, pestaña *Status*, muestra una vista general de las alarmas.

### Signal contact status

Los campos en este cuadro muestran el estado del contacto de señalización y le informan de todas las alarmas que se hayan producido. Si existe una alarma en este momento, el cuadro aparecerá resaltado.

Especifique los parámetros que el dispositivo supervisará en el cuadro de diálogo *Diagnostics* > Status Configuration > *Signal Contact* > *Signal Contact 1*/*Signal Contact 2*.

Alarm counter

Muestra el número de alarmas existentes actualmente.

Si hay al menos una alarma activa en este momento, este icono será visible.

Al colocar el puntero sobre este icono, un cuadro de ayuda mostrará la causa de la alarma activa y el momento en el que el dispositivo activó la alarma.

Si un parámetro bajo supervisión no se encuentra en el estado deseado, el dispositivo activará una alarma. El cuadro de diálogo *Diagnostics > Status Configuration > Signal Contact > Signal Contact 1*/ *Signal Contact 2*, pestaña *Status*, muestra una vista general de las alarmas.

### System data

Los campos en este cuadro muestran los datos de funcionamiento e información sobre la localización del dispositivo.

System name

Especifica el nombre con el que se identificará al dispositivo en la red.

Valores posibles:

- Cadena de caracteres ASCII alfanuméricos con entre 0 y 255 caracteres
  Solo se permiten los siguientes caracteres:
  - `0..9`
  - `a..z`
  - `A..Z`
  - `!#$%&'()*+,-./:;<=>?@[\\]^_`{}~`
  - `<device name>-<MAC address>` (configuración por defecto)

Al crear certificados HTTPS X.509, la aplicación que genera el certificado utiliza el valor especificado como el nombre de dominio y nombre común.

Las siguientes funciones utilizan el valor especificado como nombre del host o FQDN (Fully Qualified Domain Name). Por cuestiones de compatibilidad, se recomienda utilizar solo minúsculas, puesto que no todos los sistemas distinguen entre mayúsculas y minúsculas en el FQDN. Compruebe que el nombre sea único en toda la red.

- Cliente DHCP
- *Syslog*
- *IEC61850-MMS*

Location

Especifica la ubicación del dispositivo.

Valores posibles:

- Cadena de caracteres ASCII alfanuméricos con entre 0 y 255 caracteres

Contact person

Especifica la persona de contacto para este dispositivo.

Valores posibles:

- Cadena de caracteres ASCII alfanuméricos con entre 0 y 255 caracteres

Device type

Muestra el nombre de producto del dispositivo.

Power supply 1
Power supply 2

Muestra el estado de la fuente de alimentación en la conexión de alimentación relevante.

Valores posibles:

- *present*
- *defective*

- *not installed*
- *unknown*

Uptime

Muestra el tiempo transcurrido desde la última vez que se reinició este dispositivo.

Valores posibles:

- Hora en el formato `day(s), ...h ...m ...s`

Temperature [°C]

Muestra la temperatura actual en el dispositivo en °C.

Active el control de los límites de temperatura en el cuadro de diálogo *Diagnostics > Status Configuration > Device Status*.

Upper temp. limit [°C]

Especifica el límite superior de temperatura en °C.

Valores posibles:

- `-99..99` (número entero)
  Si la temperatura del dispositivo sobrepasa este valor, el dispositivo creará una alarma.

Lower temp. limit [°C]

Especifica el límite inferior de temperatura en °C.

Valores posibles:

- `-99..99` (número entero)
  Si la temperatura del dispositivo se encuentra por debajo este valor, el dispositivo creará una alarma.

### LED status

Este cuadro muestra el estado de las LED de estado del dispositivo en el momento de la última actualización. El manual de usuario "Instalación" contiene información detallada sobre las LED de estado del dispositivo.

| Parámetros | Color | Significado |
|---|---|---|
| *Status* | ● | Actualmente no hay alarmas de estado del dispositivo. El estado del dispositivo es correcto. |
| | ● | Actualmente hay al menos una alarma de estado del dispositivo. Consulte el cuadro de *Device status* anterior. |
| *Power* | ● | En la variante del dispositivo con 2 fuentes de alimentación: Solo está activa la tensión de alimentación. |
| | ● | En la variante del dispositivo con 1 fuente de alimentación: La tensión de alimentación está activa. En la variante del dispositivo con 2 fuentes de alimentación: Las dos tensiones de alimentación están activas. |

| Parámetros | Color | Significado |
|---|---|---|
| *EAM* | ● | No hay una memoria externa conectada. |
| | ● | La memoria externa está conectada, pero no lista para funcionar. |
| | ● | La memoria externa está conectada y lista para funcionar. |

### Port status

Este cuadro muestra una vista simplificada de los puertos del dispositivo en el momento de la última actualización.

Los iconos representan el estado de los puertos individuales. En algunas situaciones, los siguientes iconos interfieren entre sí. Al colocar el puntero sobre el icono de puerto adecuado, aparecerá un cuadro con información detallada sobre el estado del puerto.

| Parámetros | Estado: | Significado |
|---|---|---|
| `<Port number>` | | El puerto está inactivo.<br>El puerto no envía o recibe datos. |
| | | El puerto está inactivo.<br>El cable está conectado. Enlace activo. |
| | | El puerto está activo.<br>No hay ningún cable conectado o ninguna conexión activa. |
| | | El puerto está activo.<br>El cable está conectado. Conexión en perfecto estado. Enlace activo.<br>Modo Full-Dúplex |
| | | El modo Half-Dúplex está activado.<br>Compruebe la configuración en el cuadro de diálogo *Basic Settings* > Ports, pestaña *Configuration*. |
| | | El puerto está bloqueado debido a un mecanismo de redundancia. |
| | | El puerto opera como interfaz del enrutador. |

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## 1.2 Network

[Basic Settings > Network]

El menú contiene los siguientes cuadros de diálogo:

- Global
- IPv4
- IPv6

# 1.2.1 Global

[Basic Settings > Network > Global]

Este cuadro de diálogo le permite especificar la VLAN y la configuración de Ethernet Switch Configurator necesarias para el acceso a la gestión del dispositivo a través de la red.

### Management interface

Este cuadro le permite especificar la VLAN en la que se puede acceder a la gestión del dispositivo.

VLAN ID

Especifica la VLAN en la cual se puede acceder a la gestión del dispositivo mediante la red. Se puede acceder a la gestión del dispositivo mediante puertos que sean miembros de esta VLAN.

Valores posibles:

- `1..4042` (configuración por defecto: `1`)
  El requisito previo es que la VLAN ya esté configurada. Consulte el cuadro de diálogo *Switching > VLAN > Configuration*.

Si hace clic en el botón ✓ después de cambiar el valor, se abrirá la ventana *Information*. Seleccione el puerto mediante el cual va a conectarse al dispositivo en el futuro. Tras hacer clic en el botón *Ok*, la nueva configuración de la VLAN de administración del dispositivo se asigna al puerto.

- Después de esto, el puerto será miembro de la VLAN y transmitirá los paquetes de datos sin una etiqueta VLAN (sin etiquetar). Consulte el cuadro de diálogo *Switching > VLAN > Configuration*.
- El dispositivo asigna el ID de VLAN del puerto de la VLAN de administración del dispositivo al puerto. Consulte el cuadro de diálogo *Switching > VLAN > Port*.

Tras un momento, se podrá acceder al dispositivo mediante el nuevo puerto en la nueva VLAN de administración del dispositivo.

MAC address

Muestra la dirección MAC del dispositivo. Se puede acceder a la gestión del dispositivo mediante la red usando la dirección MAC.

### Ethernet Switch Configurator protocol v1/v2

Este cuadro le permite especificar la configuración del acceso al dispositivo utilizando el protocolo Ethernet Switch Configurator.

En un PC, el software Ethernet Switch Configurator muestra los dispositivos Schneider Electric a los que se puede acceder en la red en la que está activada la función Ethernet Switch Configurator. Puede acceder a estos dispositivos aunque no tengan parámetros IP asignados o estos no sean válidos. El software Ethernet Switch Configurator le permite asignar o cambiar los parámetros IP en el dispositivo.

**Nota:** Con el software Ethernet Switch Configurator, puede acceder al dispositivo solo mediante puertos que sean miembros de la misma VLAN que la gestión del dispositivo. Puede especificar a cuál VLAN se asigna un puerto en concreto en el cuadro de diálogo *Switching > VLAN > Configuration*.

Operation

Activa/desactiva la función Ethernet Switch Configurator en el dispositivo.

Valores posibles:

- `On` (configuración por defecto)
  Ethernet Switch Configurator está activado.
  Puede utilizar el software Ethernet Switch Configurator para acceder al dispositivo desde su PC.
- `Off`
  Ethernet Switch Configurator está desactivado.

Access

Activa/desactiva el acceso de escritura en el dispositivo mediante Ethernet Switch Configurator.

Valores posibles:

- `readWrite` (configuración por defecto)
  El software Ethernet Switch Configurator recibe acceso de escritura en el dispositivo.
  Esta configuración le permite cambiar los parámetros IP en el dispositivo.
- `readOnly`
  El software Ethernet Switch Configurator recibe acceso de solo lectura en el dispositivo.
  Esta configuración le permite ver los parámetros IP en el dispositivo.

Recomendación: cambie la configuración al valor `readOnly` solo después de poner en funcionamiento el dispositivo.

Signal

Activa/desactiva el parpadeo de los LED del puerto al igual que hace la función con el mismo nombre en el software Ethernet Switch Configurator. La función le permite identificar el dispositivo en el campo.

Valores posibles:

- `marked`
  El parpadeo de los LED del puerto está activo.
  Los LED del puerto parpadean hasta que vuelva a desactivar la función.
- `unmarked` (configuración por defecto)
  El parpadeo de los LED del puerto está desactivado.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

# 1.2.2 IPv4

[ Basic Settings > Network > IPv4 ]

Este cuadro de diálogo le permite especificar la configuración IPv4 necesaria para el acceso a la gestión del dispositivo a través de la red.

### Management interface

IP address assignment

Especifica la fuente desde la que la gestión del dispositivo recibe sus parámetros IP.

Valores posibles:

- `Local`
  El dispositivo utiliza parámetros IP de la memoria interna. Especifique los ajustes correspondientes en el cuadro *IP parameter*.
- `BOOTP`
  El dispositivo recibe los parámetros IP de un servidor BOOTP o DHCP.
  El servidor evalúa la dirección MAC del dispositivo y, a continuación, asigna los parámetros IP.
- `DHCP` (configuración por defecto)
  El dispositivo recibe sus parámetros IP de un servidor DHCP.
  El servidor evalúa la dirección MAC del dispositivo, el nombre DHCP y otros parámetros del dispositivo y, a continuación, asigna los parámetros IP.
  Cuando el servidor también facilita las direcciones de los servidores DNS, el dispositivo muestra estas direcciones en el cuadro de diálogo *Advanced > DNS > Cache > Current*.

**Nota:** Si no hay respuesta desde el servidor BOOTP o DHCP, el dispositivo selecciona la dirección IP `0.0.0.0` y vuelve a intentar obtener una dirección IP válida.

### BOOTP/DHCP

Client ID

Muestra el ID de cliente DHCP que el dispositivo envía al servidor BOOTP o DHCP. Si el servidor está configurado adecuadamente, reservará una dirección IP para este ID de cliente DHCP. Por lo tanto, el dispositivo recibe la misma IP del servidor cada ver que la solicite.

El ID de cliente DHCP que el dispositivo envía es el nombre del dispositivo especificado en el campo *System name*, en el cuadro de diálogo *Basic Settings > System*.

DHCP option 66/67/4/42

Activa/desactiva la función *DHCP option 66/67/4/42* en el dispositivo.

Valores posibles:

- *On* (configuración por defecto)
  La función *DHCP option 66/67/4/42* está activada.
  El dispositivo carga el perfil de configuración y recibe la información del servidor de hora utilizando las siguientes opciones de DHCP:
  - `Option 66: TFTP server name`
    `Option 67: Boot file name`
    El dispositivo carga automáticamente el perfil de configuración del servidor DHCP en la memoria volátil (*RAM*) utilizando el protocolo TFTP. El dispositivo utiliza los ajustes del perfil de configuración importado en `running-config`.
  - `Option 4: Time Server`
    `Option 42: Network Time Protocol Servers`
    El dispositivo recibe la información del servidor de hora del servidor DHCP.
- *Off*
  La función *DHCP option 66/67/4/42* está desactivada.
  - El dispositivo no carga un perfil de configuración mediante las opciones 66/67 de DHCP.
  - El dispositivo no recibe información del servidor de hora utilizando las opciones 4/42 de DHCP.

### IP parameter

Este cuadro le permite asignar los parámetros de ID manualmente. Si ha seleccionado el botón de opción `Local` en el cuadro *Management interface*, lista de opciones *IP address assignment*, podrá editar estos campos.

IP address

Especifica la dirección IP bajo la cual se puede acceder a la gestión del dispositivo mediante la red.

Valores posibles:

- Dirección IPv4 válida

Netmask

Especifica la máscara de red.

Valores posibles:

- Máscara de red IPv4 válida

Gateway address

Especifica la dirección IP de un enrutador mediante el cual el dispositivo accede a otros dispositivos fuera de su propia red.

Valores posibles:

- Dirección IPv4 válida

### Remaining lease time

Lease time [s]

Muestra el tiempo restante en segundos durante el cual la dirección IP que el servidor DHCP asignó a la gestión del dispositivo sigue siendo válida.

Para actualizar la pantalla, haga clic en el botón  .

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

# 1.2.3 IPv6

[Basic Settings > Network > IPv6]

Este cuadro de diálogo le permite especificar la configuración IPv6 requerida para acceder a la gestión del dispositivo a través de la red.

### Operation

Operation

Activa/desactiva el protocolo IPv6 en el dispositivo.

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.

Valores posibles:

- *On* (configuración por defecto)
  El protocolo IPv6 está activado.
- *Off*
  El protocolo IPv6 está desactivado.
  Si desea que el dispositivo funcione solo utilizando el protocolo IPv4, desactive el protocolo IPv6 en el dispositivo.

### Configuration

Dynamic IP address assignment

Especifica la fuente desde la que la gestión del dispositivo recibe sus parámetros IPv6.

Valores posibles:

- *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.
- *Auto* (configuración por defecto)
  El dispositivo recibe sus parámetros IPv6 dinámicamente. El dispositivo recibe un máximo de 2 direcciones IPv6.
  Como ejemplo aquí tenemos el Router Advertisement Daemon (radvd). El radvd utiliza mensajes *Router Solicitation* y *Router Advertisement* para configurar automáticamente una dirección IPv6. Los mensajes *Router Solicitation* y *Router Advertisement* se describen en RFC 4861.
- *DHCPv6*
  El dispositivo recibe sus parámetros IPv6 de un servidor DHCPv6.
- *All*
  Si se selecciona el botón de opción *All*, el dispositivo recibirá sus parámetros IPv6 utilizando cada alternativa para asignaciones dinámicas y manuales.

### DHCP

Client ID

Muestra el ID de cliente DHCPv6 que el dispositivo envía al servidor DHCPv6. Si el servidor está configurado adecuadamente, recibirá una dirección IPv6 para este ID de cliente DHCPv6.

La dirección IPv6 recibida del servidor DHCPv6 tiene un *PrefixLength* de `128`. De acuerdo con RFC 8415, en este momento un servidor DHCPv6 no se puede utilizar para suministrar información de *Gateway address* o *PrefixLength*.

El dispositivo solo puede recibir una dirección IPv6 del servidor DHCPv6.

### IP parameter

Gateway address

Especifica la dirección IPv6 de un enrutador mediante el cual el dispositivo accede a otros dispositivos fuera de su propia red.

Valores posibles:

- Dirección IPv6 válida (excepto direcciones de loopback y *Multicast*)

**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.

### Duplicate Address Detection

En este campo puede especificar el número de mensajes *Neighbor Solicitation* consecutivos que envía el dispositivo para la función *Duplicate Address Detection*. Esta función se utiliza para determinar la singularidad de una dirección Unicast IPv6 en la interfaz.

Number of neighbor solicitants

Especifica el número de mensajes *Neighbor Solicitation* que el dispositivo envía para la función *Duplicate Address Detection*.

Valores posibles:

- `0`
  La función está desactivada.
- `1..5` (configuración por defecto: `1`)

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).

### Tabla

Esta tabla muestra una lista de las direcciones IPv6 configuradas para la gestión del dispositivo.

Prefix

Muestra el prefijo de la dirección IPv6 en formato comprimido. El prefijo muestra los bits de la izquierda de una dirección IPv6, también conocido como la parte de red de la dirección.

PrefixLength

Muestra la longitud del prefijo de la dirección IPv6.

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.

Valores posibles:

- `0..128`

IP address

Muestra la dirección IPv6 completa en formato comprimido.

El formato comprimido se aplica automáticamente a cada dirección IPv6, independientemente del origen desde el que la gestión del dispositivo recibe sus parámetros de IPv6.

Valores posibles:

- Dirección IPv6 válida
  Para utilizar una dirección IPv6 en una URL, utilice la siguiente sintaxis de URL: `https://[ipv6_address]`.

Si desea obtener más información sobre las reglas de compresión de IPv6 y los tipos de direcciones, consulte el manual "Configuración".

EUI option

Especifica si la función *EUI option* se ha aplicado a la dirección IPv6.

Al marcar esta casilla de verificación, el ID de interfaz de la dirección IPv6 se configura automáticamente. 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`.

Valores posibles:

- `marked`
  La función *EUI option* está activa.
- `unmarked` (configuración por defecto)
  La función *EUI option* está inactiva.

Origin

Especifica la manera en que el dispositivo ha recibido sus parámetros IPv6.

Valores posibles:

- *Autoconf*
  El dispositivo recibió la dirección IPv6 dinámicamente al seleccionar el botón de opción *Auto*.
- *Manual*
  El dispositivo recibió la dirección IPv6 manualmente.
- *DHCP*
  El dispositivo recibió la dirección IPv6 de un servidor DHCPv6.
- *Linklayer*
  El dispositivo configura automáticamente una dirección IPv6 de tipo enlace-local. La dirección de enlace-local no se puede cambiar.

Status

Muestra el estado actual de la dirección IPv6.

Valores posibles:

- *active*
  La dirección IPv6 está activa.
- *notInService*
  La dirección IPv6 está inactiva.
- *notReady*
  La dirección IPv6 se ha especificado, pero actualmente no es *active* debido a que hay algunos parámetros de configuración que faltan.

**Nota:** Al especificar manualmente la dirección IPv6, puede cambiar entre los estados *active* y *notInService*. Para realizar este cambio, en la columna *Status*, seleccione el estado necesario en la lista desplegable relacionada con su entrada.

### Botones

Encontrará una descripción de los botones estándar en la sección “Botones” en página 17.

## 1.3 Out of Band over USB

[ Basic Settings > Out of Band over USB ]

El dispositivo cuenta con una interfaz de red USB 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 esta interfaz de red USB para acceder a la gestión del dispositivo.

El dispositivo le permite acceder a la gestión del dispositivo a través de la interfaz de red USB con los siguientes protocolos:

- HTTP
- HTTPS
- SSH

- Telnet
- SNMP
- FTP
- TFTP
- SFTP
- SCP

Si accede a la gestión del dispositivo, existen las siguientes limitaciones:
- La estación de administración se conecta directamente al puerto USB.
- La interfaz de red USB no admite las siguientes funciones:
  - Paquetes con etiquetas de prioridad
  - Paquetes que incluyen una etiqueta *VLAN*
  - *DHCP L2 Relay*
  - *LLDP*
  - *DiffServ*
  - *ACL*
  - *Industrial Protocols*

En este cuadro de diálogo, el dispositivo le permite cambiar los parámetros de IP y desactivar la interfaz de red USB, en caso necesario.

### Operation

Operation

Activa/desactiva la interfaz de red USB.

Valores posibles:
- `On` (configuración por defecto)
  El dispositivo le permite acceder a la gestión del dispositivo a través de la interfaz de red USB.
- `Off`
  El dispositivo prohíbe el acceso a la gestión del dispositivo mediante la interfaz de red USB.

### Management interface

Device MAC address

Muestra la dirección MAC de la interfaz de red USB.

Host MAC address

Muestra la dirección MAC de la estación de administración conectada.

### IP parameter

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

IP address

Especifica la dirección IP de la gestión del dispositivo para acceder a través de la interfaz de red USB.

Valores posibles:

▶ Dirección IPv4 válida
(configuración por defecto: `91.0.0.100`)
El dispositivo asigna esta dirección IP, más 1, a la estación de administración de red que está conectada al dispositivo.
Ejemplo: `91.0.0.100` para la interfaz de red USB, `91.0.0.101` para la estación de administración de red.

Netmask

Especifica la máscara de red.

Valores posibles:

▶ Máscara de red IPv4 válida
(configuración por defecto: `255.255.255.0`)

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

# 1.4 Software

[ Basic Settings > Software ]

Este cuadro de diálogo le permite actualizar el software del dispositivo y mostrar información sobre el software del dispositivo.

También tiene la opción de restaurar una copia de seguridad del software del dispositivo guardada en el dispositivo.

**Nota:** Antes de actualizar el software del dispositivo, siga las instrucciones específicas para su versión en el archivo de texto `Readme`.

### Version

Stored version

Muestra el número de la versión y la fecha de creación del software del dispositivo guardada en la memoria flash. El dispositivo cargará el software del dispositivo durante el siguiente reinicio.

Running version

Muestra el número de la versión y la fecha de creación del software del dispositivo cargada por el dispositivo durante el último reinicio y que se está ejecutando actualmente.

Backup version

Muestra el número de la versión y la fecha de creación del software del dispositivo guardada como copia de seguridad en la memoria flash. El dispositivo ha copiado el software de este dispositivo en la memoria de la copia de seguridad durante la última actualización de software o después de que haya pulsado el botón *Restore*.

Restore

Restaura el software del dispositivo guardado como copia de seguridad. En el proceso, el dispositivo cambia la *Stored version* y la *Backup version* del software del dispositivo.

Tras reiniciar el dispositivo, este cargará la *Stored version*.

Bootcode

Muestra el número de la versión y la fecha de creación del código de arranque.

### Software update

Además, si el archivo de imagen se encuentra en la memoria externa, el dispositivo le permite actualizar el software del dispositivo haciendo clic con el botón derecho en la tabla.

URL

Especifica la ruta y el nombre de archivo del archivo de imagen con el que va a actualizar el software del dispositivo.

El dispositivo le ofrece las siguientes opciones para actualizar el software del dispositivo:

- Actualización del software desde el PC
  Si el archivo se encuentra en su PC o en una unidad de red, arrastre y suelte el archivo en el área  . También puede hacer clic en el área para seleccionar el archivo.
- Actualización de software desde un servidor FTP
  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>`
- Actualización de software desde un servidor TFTP
  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>`
- Actualización de software desde un servidor SCP o SFTP
  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://<user>:<password>@<IP address>/<path>/<file name>`

Start

Actualiza el software del dispositivo.

El dispositivo instala el archivo seleccionado en la memoria flash, reemplazando el software de dispositivo almacenado anteriormente. Tras reiniciar el dispositivo, este cargará el software instalado.

El dispositivo copia el software existente en la memoria de la copia de seguridad.

Para permanecer conectado al dispositivo durante la actualización de software, mueva el puntero de vez en cuando. Como alternativa, especifique un valor lo suficientemente alto en el cuadro de diálogo *Device Security > Management Access > Web*, campo *Web interface session timeout [min]*, antes de la actualización del software.

### Tabla

File location

Muestra la ubicación de almacenamiento del software del dispositivo.

Valores posibles:

- *ram*
  Memoria volátil del dispositivo

- *flash*
  Memoria no volátil (*NVM*) del dispositivo
- *usb*
  Memoria USB externa (EAM)

Index

Muestra el índice del software del dispositivo.

Para el software del dispositivo en la memoria flash, el índice significa lo siguiente:

- 1
  Tras reiniciar el dispositivo, este cargará el software de este dispositivo.
- 2
  El dispositivo ha copiado el software de este dispositivo en la zona de la copia de seguridad durante la última actualización de software.

File name

Muestra el nombre del archivo interno del software del dispositivo.

Firmware

Muestra el número de la versión y la fecha de creación del software del dispositivo.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

# 1.5 Load/Save

[ Basic Settings > Load/Save ]

El cuadro de diálogo le permite guardar de forma permanente los ajustes del dispositivo en un perfil de configuración.

El dispositivo puede contener varios perfiles de configuración. Cuando activa un perfil de configuración alternativo, cambia a otra configuración del dispositivo. Tiene la opción de exportar los perfiles de configuración a su PC o a un servidor. También tiene la opción de importar los perfiles de configuración desde su PC o desde un servidor al dispositivo.

En la configuración por defecto, el dispositivo guarda los perfiles de configuración sin encriptar. Si introduce una contraseña en el cuadro *Configuration encryption*, el dispositivo guarda los perfiles de configuración, tanto el presente como los futuros, en un formato encriptado.

Cambios accidentales en la configuración pueden cortar la conexión entre el PC y el dispositivo. Para asegurar su acceso al dispositivo, active la función *Undo configuration modifications* antes de cambiar la configuración. Si se pierde la conexión, el dispositivo cargará el perfil de configuración guardado en la memoria no volátil (*NVM*) tras el tiempo especificado.

### External memory

Selected external memory

Muestra el tipo de memoria externa.

Valores posibles:

- *usb*
  Memoria USB externa (EAM)

Status

Muestra el modo de funcionamiento de la memoria externa.

Valores posibles:

- *notPresent*
  No hay una memoria externa conectada.
- *removed*
  Alguien ha extraído la memoria externa del dispositivo durante su funcionamiento.
- *ok*
  La memoria externa está conectada y lista para funcionar.
- *outOfMemory*
  El espacio de memoria de la memoria externa está ocupado.
- *genericErr*
  El dispositivo ha detectado un error.

### Configuration encryption

Active

Muestra si la encriptación está activa/inactiva en el dispositivo.

Valores posibles:

- `marked`
  La encriptación está activa.
  Si el perfil de configuración está encriptado y la contraseña coincide con la contraseña almacenada en el dispositivo, el dispositivo cargará un perfil de configuración de la memoria no volátil (*NVM*).
- `unmarked`
  La encriptación está inactiva.
  Si el perfil de configuración no está encriptado, el dispositivo cargará un perfil de configuración de la memoria no volátil (*NVM*).

Si en el cuadro de diálogo *Basic Settings > External Memory*, la columna *Config priority* tiene el valor `first` y el perfil de configuración no está encriptado, el cuadro *Security status* en el cuadro de diálogo *Basic Settings > System* mostrará una alarma.

En el cuadro de diálogo *Diagnostics > Status Configuration > Security Status*, pestaña *Global*, columna *Monitor*, puede especificar si el dispositivo supervisará el parámetro *Load unencrypted config from external memory*.

Set password

Abre la ventana *Set password* que le ayudará a introducir la contraseña necesaria para la encriptación del perfil de configuración. Encriptar los perfiles de configuración dificulta los accesos no autorizados. Para ello, siga los siguientes pasos:

- ☐ Para cambiar una contraseña existente, introduzca la contraseña existente en el campo *Old password*. Para mostrar la contraseña en texto no cifrado en lugar de ***** (asteriscos), marque la casilla *Display content*.
- ☐ Introduzca la contraseña en el campo *New password*.
  Para mostrar la contraseña en texto no cifrado en lugar de ***** (asteriscos), marque la casilla *Display content*.
- ☐ Marque la casilla *Save configuration afterwards* para utilizar encriptación también en el perfil de configuración seleccionado en la memoria no volátil (*NVM*) y en la memoria externa.

**Nota:** Si hay un máximo de un perfil de configuración almacenado en la memoria no volátil (*NVM*) del dispositivo, utilice solo esta función. Antes de crear perfiles de configuración adicionales, decida si va a activar permanentemente la encriptación en el dispositivo. Guarde perfiles de configuración adicionales con o sin encriptación con la misma contraseña.

Si va a reemplazar un dispositivo con un perfil de configuración encriptado, por ejemplo, debido a un dispositivo no operativo, proceda de la siguiente manera:

- ☐ Reinicie el nuevo dispositivo y asigne los parámetros IP.
- ☐ Abra el cuadro de diálogo *Basic Settings > Load/Save* en el nuevo dispositivo.
- ☐ Encripte el perfil de configuración en el nuevo dispositivo. Véase instrucciones anteriores. Introduzca la misma contraseña que en el dispositivo no operativo.
- ☐ Instale la memoria externa desde el dispositivo no operativo al nuevo dispositivo.
- ☐ Reinicie el nuevo dispositivo.
  Cuando reinicie el dispositivo, el dispositivo cargará el perfil de configuración con los ajustes del dispositivo no operativo desde la memoria externa. El dispositivo copia la configuración en la memoria volátil (*RAM*) y en la memoria no volátil (*NVM*).

Delete

Abre la ventana *Delete*, la cual le ayudará a cancelar la encriptación en el dispositivo. Para cancelar el cifrado de configuración, lleve a cabo los siguientes pasos:

- ☐ Introduzca la contraseña existente en el campo *Old password*.
  Para mostrar la contraseña en texto no cifrado en lugar de ***** (asteriscos), marque la casilla *Display content*.
- ☐ Marque la casilla *Save configuration afterwards* para eliminar la encriptación también en el perfil de configuración seleccionado en la memoria no volátil (*NVM*) y en la memoria externa.

**Nota:** Si tiene perfiles de configuración encriptados adicionales en la memoria, el dispositivo le ayudará a evitar activar o designar estos perfiles de configuración como "Seleccionados".

## Information

NVM in sync with running config

Muestra si el perfil de configuración en la memoria volátil (*RAM*) y el perfil de configuración "Seleccionado" en la memoria no volátil (*NVM*) son iguales.

Valores posibles:

- `marked`
  Los perfiles de configuración son iguales.
- `unmarked`
  Los perfiles de configuración son diferentes.

External memory in sync with NVM

Muestra si el perfil de configuración "Seleccionado" en la memoria externa y el perfil de configuración "Seleccionado" en la memoria no volátil (*NVM*) son iguales.

Valores posibles:

- `marked`
  Los perfiles de configuración son iguales.
- `unmarked`
  Los perfiles de configuración son diferentes.
  Causas posibles:
  - No hay una memoria externa conectada al dispositivo.
  - La función *Backup config when saving* está desactivada en el cuadro de diálogo *Basic Settings* > External Memory.

### Backup config on a remote server when saving

Operation

Activa/desactiva la función *Backup config on a remote server when saving*.

Valores posibles:

- *Enabled*
  La función *Backup config on a remote server when saving* está activada.
  Al guardar el perfil de configuración en la memoria no volátil (*NVM*), el dispositivo hace automáticamente una copia de seguridad del perfil de configuración en el servidor remoto especificado en el campo *URL*.
- *Disabled* (configuración por defecto)
  La función *Backup config on a remote server when saving* está desactivada.

URL

Especifica la ruta y el nombre del archivo del perfil de configuración del que ha hecho una copia de seguridad en el servidor remoto.

Valores posibles:

- Cadena de caracteres ASCII alfanuméricos con entre 0 y 128 caracteres
  Por ejemplo: `tftp://192.9.200.1/cfg/config.xml`
  El dispositivo es compatible con los siguientes comodines:
  - `%d`
    Fecha del sistema con el formato `YYYY-mm-dd`
  - `%t`
    Hora del sistema con el formato `HH_MM_SS`
  - `%i`
    Dirección IP del dispositivo
  - `%m`
    Dirección MAC del dispositivo con el formato `AA-BB-CC-DD-EE-FF`
  - `%p`
    Nombre de producto del dispositivo

Set credentials

Abre la ventana *Credentials*, la cual le ayudará a introducir las credenciales de inicio de sesión necesarias para autenticarse en el servidor remoto. Para ello, siga los siguientes pasos:

- ☐ Introduzca el nombre de usuario en el campo *User name*.
  Para mostrar el nombre de usuario en texto no cifrado en lugar de ***** (asteriscos), marque la casilla *Display content*.
  Valores posibles:
  - Cadena de caracteres ASCII alfanuméricos con entre 1 y 32 caracteres
- ☐ Introduzca la contraseña en el campo *Password*.
  Para mostrar la contraseña en texto no cifrado en lugar de ***** (asteriscos), marque la casilla *Display content*.
  Valores posibles:
  - Cadena de caracteres ASCII alfanuméricos con entre 6 y 64 caracteres
    Solo se permiten los siguientes caracteres:

```
a..z
A..Z
0..9
!#$%&'()*+,-./:;<=>?@[\\]^_`{}~
```

### Undo configuration modifications

Operation

Activa/desactiva la función *Undo configuration modifications*. Usando esta función, el dispositivo comprueba de forma continua si todavía es accesible desde la dirección IP de su PC. Si se pierde la conexión, el dispositivo cargará el perfil de configuración "Seleccionado" en la memoria no volátil (*NVM*) tras el tiempo especificado. Después, se podrá acceder otra vez al dispositivo.

Valores posibles:

- *On*
  La función está activada.
  - Especifique el período de tiempo entre la interrupción de la conexión y la carga del perfil de configuración en el campo *Timeout [s] to recover after connection loss*.
  - Cuando la memoria no volátil (*NVM*) contiene varios perfiles de configuración, el dispositivo carga el perfil de configuración designado como "Seleccionado".
- *Off* (configuración por defecto)
  La función está desactivada.
  Desactive la función otra vez antes de cerrar la Interfaz gráfica de usuario. De esta manera evitará que el dispositivo restaure el perfil de configuración designado como "Seleccionado".

**Nota:** Antes de activar la función, guarde la configuración en el perfil de configuración. De esta manera, lo cambios actuales, almacenados de forma temporal, permanecerán en el dispositivo.

Timeout [s] to recover after connection loss

Especifica el tiempo en segundos que el dispositivo esperará antes de cargar el perfil de configuración "Seleccionado" desde la memoria no volátil (*NVM*) si se pierde la conexión.

Valores posibles:

- 30..600 (configuración por defecto: 600)

Especifique un valor lo suficientemente grande. Tenga en cuenta el tiempo en el que estará viendo cuadros de diálogo de la Interfaz gráfica de usuario sin cambiar o actualizarlos.

Watchdog IP address

Muestra la dirección IP del PC en el cual ha activado la función.

Valores posibles:

- Dirección IPv4 (configuración por defecto: 0.0.0.0)

### Tabla

Storage type

Muestra la ubicación de almacenamiento del perfil de configuración.

Valores posibles:

- *RAM* (memoria volátil del dispositivo)
  El dispositivo almacena la configuración de la operación actual en la memoria volátil.

- `NVM` (memoria no volátil del dispositivo)
  Al aplicar la función *Undo configuration modifications* o durante un reinicio, el dispositivo carga el perfil de configuración "Seleccionado" desde la memoria no volátil.
  La memoria no volátil proporciona espacio para varios perfiles de configuración, dependiendo del número de ajustes almacenados en el perfil de configuración. El dispositivo gestiona un máximo de 20 perfiles de configuración en la memoria no volátil.
  Puede cargar un perfil de configuración en la memoria volátil (`RAM`). Para ello, siga los siguientes pasos:
  - ☐ En la tabla, marque el perfil de configuración.
  - ☐ Haga clic en el botón ☰ y, a continuación, en el elemento *Activate*.
- `ENVM` (memoria externa)
  El dispositivo guarda una copia de seguridad del perfil de configuración "Seleccionado" en la memoria externa.
  El requisito previo es que marque la casilla *Backup config when saving* en el cuadro de diálogo *Basic Settings > External Memory*.

Profile name

Muestra el nombre del perfil de configuración.

Valores posibles:

- `running-config`
  Nombre del perfil de configuración en la memoria volátil (`RAM`).
- `config`
  Nombre del perfil de configuración de la configuración de fábrica en la memoria no volátil (`NVM`).
- Nombre definido por el usuario
  El dispositivo le permite guardar un perfil de configuración con un nombre especificado por el usuario marcando un perfil de configuración existente en la tabla, haciendo clic en el botón ☰ y, a continuación, en el elemento *Save as...*.

Para exportar el perfil de configuración como archivo XML en su PC, haga clic en el enlace. A continuación, seleccione la ubicación de almacenamiento y especifique el nombre del archivo.

Para guardar el archivo en un servidor remoto, haga clic en el botón ☰ y, a continuación, en el elemento *Export...*.

Modification date (UTC)

Muestra la hora (UTC) a la que el usuario guardó por última vez el perfil de configuración.

Selected

Muestra si el perfil de configuración se ha designado con el nombre "Seleccionado".

Para designar a otro perfil de configuración como "Seleccionado", señale el perfil de configuración que desee en la tabla, haga clic en el botón ☰ y, a continuación, en el elemento *Activate*.

Valores posibles:

- `marked`
  El perfil de configuración se ha designado con el nombre "Seleccionado".
  - Al aplicar la función *Undo configuration modifications* o durante un reinicio, el dispositivo carga el perfil de configuración en la memoria volátil (`RAM`).
  - Al hacer clic en el botón  , el dispositivo guardará la configuración guardada temporalmente en este perfil de configuración.
- `unmarked`
  Otro perfil de configuración se ha designado con el nombre "Seleccionado".

Encrypted

Muestra si el perfil de configuración está encriptado.

Valores posibles:

- `marked`
  El perfil de configuración está encriptado.
- `unmarked`
  El perfil de configuración no está encriptado.

Active/desactive la encriptación del perfil de configuración en el cuadro *Configuration encryption*.

Encryption verified

Muestra si la contraseña del perfil de configuración encriptado coincide con la contraseña almacenada en el dispositivo.

Valores posibles:

- `marked`
  Las contraseñas coinciden. El dispositivo podrá encriptar el perfil de configuración.
- `unmarked`
  Las contraseñas son diferentes. El dispositivo no podrá encriptar el perfil de configuración.

Software version

Muestra el número de la versión del software del dispositivo que el dispositivo ejecutó al guardar el perfil de configuración.

Fingerprint

Muestra la suma de comprobación guardada en el perfil de configuración.

Al guardar la configuración, el dispositivo calcula la suma de comprobación y la inserta en el perfil de configuración.

Fingerprint verified

Muestra si la suma de comprobación guardada en el perfil de configuración es válida.

El dispositivo calcula la suma de comprobación del perfil de configuración marcado como "Seleccionado" y la compara con la suma de comprobación almacenada en este perfil de configuración.

Valores posibles:

- `marked`
  La suma de comprobación calculada y la almacenada coinciden.
  La configuración guardada es consistente.
- `unmarked`
  En el perfil de configuración marcado como "Seleccionado":
  La suma de comprobación calculada y la almacenada son diferentes.
  El perfil de configuración contiene ajustes modificados.
  Causas posibles:
  - El archivo está dañado.
  - El sistema de archivos de la memoria externa es inconsistente.
  - Un usuario ha exportado el perfil de configuración y ha cambiado el archivo XML fuera del dispositivo.

  El dispositivo no ha calculado la suma de comprobación para otros perfiles de configuración.

El dispositivo solo podrá comprobar correctamente la suma de comprobación si el perfil de configuración se ha guardado de la siguiente manera:

- en un dispositivo idéntico
- con la misma versión de software que el dispositivo está ejecutando

**Nota:** Esta función identifica los cambios en la configuración en el perfil de configuración. La función no proporciona protección frente al funcionamiento del dispositivo con ajustes modificados.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

Elimina el perfil de configuración señalado en la tabla de la memoria no volátil (*NVM*) o de la memoria externa.

Si el perfil de configuración se ha designado con el nombre "Seleccionado", el dispositivo ayudará a evitar que elimine el perfil de configuración.

Save as..

Copia el perfil de configuración señalado en la tabla y lo guarda con un nombre especificado por el usuario en la memoria no volátil (*NVM*). El dispositivo designa el perfil de configuración nuevo con el nombre "Seleccionado".

**Nota:** Antes de crear perfiles de configuración adicionales, decida si va a activar permanentemente la encriptación en el dispositivo. Guarde perfiles de configuración adicionales con o sin encriptación con la misma contraseña.

Si la casilla en la columna *Backup config when saving* del cuadro de diálogo *Basic Settings > External Memory* aparece marcada, el dispositivo designa al perfil de configuración del mismo nombre en la memoria externa como "Seleccionado".

Activate

Carga la configuración del perfil de configuración marcado en la tabla a la memoria no volátil (*RAM*).

- El dispositivo interrumpe la conexión a la Interfaz gráfica de usuario. Para acceder a la gestión del dispositivo otra vez, lleve a cabo los siguientes pasos:
  - ☐ Vuelva a cargar la Interfaz gráfica de usuario.
  - ☐ Inicie sesión de nuevo.
- El dispositivo utiliza inmediatamente la configuración del perfil de configuración al momento.

Active la función *Undo configuration modifications* antes de activar otro perfil de configuración. Si la conexión se pierde más adelante, el dispositivo cargará el último perfil de configuración designado como "Seleccionado" desde la memoria no volátil (*NVM*). Ahora podrá acceder otra vez al dispositivo.

Si la encriptación está inactiva, el dispositivo cargará un perfil de configuración sin encriptar. Si la encriptación está activa y la contraseña coincide con la contraseña almacenada en el dispositivo, el dispositivo cargará un perfil de configuración encriptado.

Al activar un perfil de configuración antiguo, el dispositivo asume la configuración de las funciones contenidas en esta versión de software. El dispositivo devuelve los valores de las funciones a sus valores por defecto.

Select

Designa el perfil de configuración marcado en la tabla como "Seleccionado". En la columna *Selected*, la casilla estará `marked`.

Al aplicar la función *Undo configuration modifications* o durante un reinicio, el dispositivo carga la configuración de este perfil en la memoria volátil (*RAM*).

- Si la encriptación del dispositivo está inactiva, designe como "Seleccionado" solo a un perfil de configuración sin encriptar.
- Si la encriptación del dispositivo está activa y la contraseña del perfil de configuración coincide con la contraseña almacenada en el dispositivo, designe solo como "Seleccionado" un perfil de configuración encriptado.

De lo contrario, el dispositivo no podrá cargar y encriptar la configuración en el perfil de configuración la próxima vez que reinicie. En este caso, especifique en el cuadro de diálogo *Diagnostics* > System > *Selftest* si el dispositivo se iniciará con la configuración por defecto o interrumpirá el reinicio y parará.

**Nota:** Marque solo los perfiles de configuración almacenados en la memoria no volátil (*NVM*).

Si la casilla en la columna *Backup config when saving* del cuadro de diálogo *Basic Settings* > *External Memory* aparece marcada, el dispositivo designa al perfil de configuración del mismo nombre en la memoria externa como "Seleccionado".

Import...

Abre la ventana *Import...* para importar un perfil de configuración.

El requisito previo es que debe haber exportado el perfil de configuración mediante el botón *Export...* o mediante el enlace de la columna *Profile name*.

- ☐ En la lista desplegable de *Select source*, seleccione desde donde el dispositivo importará el perfil 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.
- ☐ Si *PC/URL* aparece seleccionada, especifique en el cuadro *Import profile from PC/URL* el archivo del perfil de configuración a importar.
  - – Importar desde el PC
    Si el archivo se encuentra en su PC o en una unidad de red, arrastre y suelte el archivo en el área  . También puede hacer clic en el área para seleccionar el archivo.
  - – Importar desde un servidor FTP
    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>`
  - – Importar desde un servidor TFTP
    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>`
  - – Importar desde un servidor SCP o SFTP
    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://<user>:<password>@<IP address>/<path>/<file name>`
- ☐ Si *External memory* aparece seleccionada, especifique en el cuadro *Import profile from external memory* el archivo del perfil de configuración a importar.
  En la lista desplegable *Profile name*, seleccione el nombre del perfil de configuración que desee importar.
- ☐ 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. El requisito previo es seleccionar el elemento *PC/URL* en la lista desplegable *Select source*.
  - ▶ *RAM*
    El dispositivo guarda el perfil de configuración en la memoria volátil (*RAM*) del dispositivo. Este reemplazará el `running-config`, el dispositivo utilizará inmediatamente el perfil de configuración importado. El dispositivo interrumpe la conexión a la Interfaz gráfica de usuario. Vuelva a cargar la Interfaz gráfica de usuario. Inicie sesión de nuevo.
  - ▶ *NVM*
    El dispositivo guarda el perfil de configuración en la memoria no volátil (*NVM*) del dispositivo.

Al importar un perfil de configuración, el dispositivo asume la configuración de la siguiente manera:

- Si el perfil de configuración se exportó al mismo dispositivo o a un dispositivo del mismo tipo con el mismo equipamiento, entonces:
  El dispositivo asume la configuración completamente.
- Si el perfil de configuración se exportó a otro dispositivo, entonces:
  El dispositivo asume la configuración que puede interpretar basándose en su hardware y nivel de software.
  El dispositivo tomará el resto de ajustes de su perfil de configuración `running-config`.

En cuando a la encriptación de perfiles de configuración, consulte también el texto de ayuda del cuadro *Configuration encryption*. El dispositivo importa un perfil de configuración bajo las siguientes condiciones:

- La encriptación del dispositivo está inactiva. El perfil de configuración no está encriptado.
- La encriptación del dispositivo está activa. El perfil de configuración está encriptado con la misma contraseña que el dispositivo utiliza actualmente.

Export...

Exporta el perfil de configuración señalado en la tabla y lo guarda como archivo XML en un servidor remoto.

Para guardar el archivo en su PC, haga clic en el enlace de la columna *Profile name* para seleccionar la ubicación de almacenamiento y especificar el nombre del archivo.

El dispositivo le ofrece las opciones siguientes para exportar el perfil de configuración:

- Exportar a un servidor FTP
  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>`
- Exportar a un servidor TFTP
  Para guardar el archivo en un servidor TFTP, especifique la URL correspondiente al archivo en el formato siguiente:
  `tftp://<dirección IP>/<ruta>/<nombre archivo>`
- Exportar a un servidor SCP o SFTP
  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://<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.
  - `scp://` o `sftp://<user>:<password>@<IP address>/<path>/<file name>`

Load running-config as script

Importa un archivo de script que modifique el perfil de configuración `running config` actual.

El dispositivo le ofrece las opciones siguientes para importar un archivo de script:

- Importar desde el PC
  Si el archivo se encuentra en su PC o en una unidad de red, arrastre y suelte el archivo en el área  . También puede hacer clic en el área para seleccionar el archivo.
- Importar desde un servidor FTP
  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>`

- Importar desde un servidor TFTP
  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>`
- Importar desde un servidor SCP o SFTP
  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>`

**Nota:** El dispositivo aplica los archivos de script adicionalmente a los ajustes actuales. Verifique que el archivo de script no incluya ninguna parte que presente un conflicto con los ajustes actuales.

Save running-config as script

Guarda el perfil de configuración `running config` como archivo de script en el PC local. Esto le permite hacer una copia de seguridad de la configuración actual del dispositivo o utilizarla en varios dispositivos.

Back to factory...

Restablece los ajustes por defecto en el dispositivo.

- El dispositivo elimina los perfiles de configuración guardados de la memoria volátil (*RAM*) y de la memoria no volátil (*NVM*).
- El dispositivo elimina el certificado HTTPS que el servidor web utiliza en el dispositivo.
- El dispositivo elimina la clave RSA (clave de host) que el servidor SSH utiliza en el dispositivo.
- Al conectar una memoria externa, el dispositivo elimina los perfiles de configuración guardados en la memoria externa.
- Tras un breve período, el dispositivo se reinicia y carga los valores por defecto.

Back to default

Elimina la configuración actual (`running config`) de la memoria volátil (*RAM*).

# 1.6 External Memory

[Basic Settings > External Memory]

Este diálogo le permite activar funciones que el dispositivo ejecutará automáticamente en combinación con la memoria externa. El cuadro de diálogo también muestra el modo de funcionamiento e identifica las características de la memoria externa.

### Tabla

Type

Muestra el tipo de memoria externa.

Valores posibles:

- *usb*
  Memoria USB externa (EAM)

Status

Muestra el modo de funcionamiento de la memoria externa.

Valores posibles:

- *notPresent*
  No hay una memoria externa conectada.
- *removed*
  Alguien ha extraído la memoria externa del dispositivo durante su funcionamiento.
- *ok*
  La memoria externa está conectada y lista para funcionar.
- *outOfMemory*
  El espacio de memoria de la memoria externa está ocupado.
- *genericErr*
  El dispositivo ha detectado un error.

Writable

Muestra si el dispositivo tiene permiso de escritura en la memoria externa.

Valores posibles:

- marked
  El dispositivo tiene permiso de escritura en la memoria externa.
- unmarked
  El dispositivo solo tiene permiso de lectura en la memoria externa. Es posible que la protección contra escritura esté activada en la memoria externa.

Software auto update

Activa/desactiva la actualización de software automática del dispositivo durante el reinicio.

Valores posibles:

- `marked` (configuración por defecto)
  La actualización de software automática del dispositivo durante el reinicio está activada. El dispositivo actualiza el software del dispositivo cuando los archivos siguientes se encuentran en la memoria externa:
  - el archivo de imagen del software del dispositivo
  - un archivo de texto `startup.txt` con el contenido `autoUpdate=<image_file_name>.bin`
- `unmarked`
  La actualización de software automática del dispositivo durante el reinicio está desactivada.

SSH key auto upload

Activa/desactiva la carga de la clave RSA desde una memoria externa al reiniciar.

Valores posibles:

- `marked` (configuración por defecto)
  La carga de la clave RSA está activada.
  Durante un reinicio, el dispositivo carga la clave RSA desde la memoria externa cuando los archivos siguientes se encuentran en la memoria externa:
  - Archivo de clave SSH RSA
  - un archivo de texto `startup.txt` con el contenido `autoUpdateRSA=<nombre_archivo_de_clave_SSH_RSA>`

  El dispositivo muestra mensajes en la consola del sistema de la interfaz serie.
- `unmarked`
  La carga de la clave RSA está desactivada.

**Nota:** Al cargar la clave RSA desde la memoria externa (*ENVM*), el dispositivo sobrescribe las claves existentes en la memoria no volátil (*NVM*).

Config priority

Especifica la memoria desde la cual el dispositivo cargará el perfil de configuración después del reinicio.

Valores posibles:

- `disable`
  El dispositivo carga el perfil de configuración desde la memoria no volátil (*NVM*).
- `first`
  El dispositivo carga el perfil de configuración desde la memoria externa.
  Si el dispositivo no encuentra un perfil de configuración en la memoria externa, cargará el perfil de configuración desde la memoria no volátil (*NVM*).

**Nota:** Al cargar el perfil de configuración desde la memoria externa (*ENVM*), el dispositivo sobrescribe los ajustes del perfil de configuración seleccionado en la memoria no volátil (*NVM*).

Si la columna *Config priority* tiene el valor `first` y el perfil de configuración no está encriptado, el cuadro *Security status* en el cuadro de diálogo *Basic Settings > System* mostrará una alarma.

En el cuadro de diálogo *Diagnostics > Status Configuration > Security Status*, pestaña *Global*, columna *Monitor*, puede especificar si el dispositivo supervisará el parámetro *Load unencrypted config from external memory*.

Backup config when saving

Activa/desactiva la creación de una copia del perfil de configuración en la memoria externa.

Valores posibles:

- `marked` (configuración por defecto)
  La creación de copia está activada. Al hacer clic en el botón *Save* del cuadro de diálogo *Basic Settings > Load/Save*, el dispositivo genera una copia del perfil de configuración en la memoria externa activa.
- `unmarked`
  La creación de copia está desactivada. El dispositivo no genera una copia del perfil de configuración.

Manufacturer ID

Muestra el nombre del fabricante de la memoria.

Revision

Muestra el número de revisión especificado por el fabricante de la memoria.

Version

Muestra el número de versión especificado por el fabricante de la memoria.

Name

Muestra el nombre del producto especificado por el fabricante de la memoria.

Serial number

Muestra el número de serie especificado por el fabricante de la memoria.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

# 1.7 Port

[Basic Settings > Port]

Este cuadro de diálogo le permite especificar la configuración de los puertos individuales: El cuadro de diálogo también muestra el modo de funcionamiento, el estado de conexión, la velocidad de bits y el modo dúplex de cada puerto.

El cuadro de diálogo contiene las siguientes pestañas:
- [Configuration]
- [Statistics]
- [Utilization]

## [Configuration]

### Tabla

Port

Muestra el número de puerto.

Name

Nombre del puerto.

Valores posibles:
- Cadena de caracteres ASCII alfanuméricos con entre 0 y 64 caracteres
  Solo se permiten los siguientes caracteres:
  - `<space>`
  - `0..9`
  - `a..z`
  - `A..Z`
  - `!#$%&'()*+,-./:;<=>?@[\\]^_`{}~`

Port on

Activa/desactiva el puerto.

Valores posibles:
- `marked` (configuración por defecto)
  El puerto está activo.
- `unmarked`
  El puerto está inactivo. El puerto no envía o recibe datos.

State

Muestra si el puerto se encuentra activado o desactivado físicamente en este momento.

Valores posibles:

- `marked`
  El puerto se encuentra físicamente activado.
- `unmarked`
  El puerto se encuentra físicamente desactivado.
  Si la función *Port on* está activa, la función *Auto-Disable* habrá desactivado el puerto.
  Especifique los ajustes de la función *Auto-Disable* en el cuadro de diálogo *Diagnostics > Ports >* Auto-Disable.

Power state (port off)

Especifica si el puerto se encuentra encendido o apagado físicamente al desactivar el puerto con la función *Port on*.

Valores posibles:

- `marked`
  El puerto permanece físicamente activado. Un dispositivo conectado recibe un enlace activo.
- `unmarked` (configuración por defecto)
  El puerto se encuentra físicamente desactivado.

Auto power down

Especifica el comportamiento del puerto cuando no haya cables conectados.

Valores posibles:

- *`no-power-save`* (configuración por defecto)
  El puerto permanece activado.
- *`auto-power-down`*
  El puerto cambia al modo de ahorro de energía.
- *`unsupported`*
  El puerto no es compatible con esta función y permanece activado.

Automatic configuration

Activa/desactiva la selección automática del modo de funcionamiento para el puerto.

Valores posibles:

- `marked` (configuración por defecto)
  La selección automática del modo de funcionamiento está activa.
  El puerto configura el modo de funcionamiento de manera independiente mediante la configuración automática y detecta los dispositivos conectados al puerto TP automáticamente (Auto Cable Crossing). Esta configuración tiene prioridad sobre la configuración manual del puerto.
  Trascurrirán varios segundos hasta que el puerto ajuste el modo de funcionamiento.
- `unmarked`
  La selección automática del modo de funcionamiento está inactiva.
  El puerto funciona con los valores que haya especificado en la columna *Manual configuration* y en la columna *Manual cable crossing (Auto. conf. off)*.
- Pantalla sombreada
  No hay selección automática del modo de funcionamiento.

Manual configuration

Especifica el modo de funcionamiento de los puertos cuando la función *Automatic configuration* está desactivada.

Valores posibles:

- `10 Mbit/s HDX`
  Conexión Half-Dúplex
- `10 Mbit/s FDX`
  Conexión Full-Dúplex
- `100 Mbit/s HDX`
  Conexión Half-Dúplex
- `100 Mbit/s FDX`
  Conexión Full-Dúplex
- `1000 Mbit/s FDX`
  Conexión Full-Dúplex
- `2500 Mbit/s FDX`
  Conexión Full-Dúplex

**Nota:** Los modos de funcionamiento del puerto que están realmente disponibles dependen de la configuración del dispositivo.

Link/Current settings

Muestra el modo de funcionamiento que el puerto utiliza actualmente.

Valores posibles:

- `-`
  No hay cable conectado, no hay enlace
- `10 Mbit/s HDX`
  Conexión Half-Dúplex
- `10 Mbit/s FDX`
  Conexión Full-Dúplex
- `100 Mbit/s HDX`
  Conexión Half-Dúplex
- `100 Mbit/s FDX`
  Conexión Full-Dúplex
- `1000 Mbit/s FDX`
  Conexión Full-Dúplex
- `2500 Mbit/s FDX`
  Conexión Full-Dúplex

**Nota:** Los modos de funcionamiento del puerto que están realmente disponibles dependen de la configuración del dispositivo.

Manual cable crossing (Auto. conf. off)

Especifica los dispositivos conectados a un puerto TP.

El requisito previo es que la función *Automatic configuration* esté inactiva.

Valores posibles:

- *mdi*
  El dispositivo intercambia los pares de líneas de envío y de recepción en el puerto.

- `mdix` (configuración por defecto en puertos TP)
  El dispositivo ayuda a prevenir el intercambio de los pares de líneas de envío y de recepción en el puerto.
- `auto-mdix`
  El dispositivo detecta los pares de líneas de envío y de recepción en el dispositivo conectado y se adapta automáticamente a ellos.
  Por ejemplo: al conectar el dispositivo terminal con un cable cruzado, el dispositivo reinicia automáticamente el puerto de `mdix` a `mdi`.
- `unsupported` (configuración por defecto en puertos ópticos o en puertos TP-SFP)
  El puerto no es compatible con esta función.

Flow control

Activa/desactiva el control del flujo en el puerto.

Valores posibles:

- `marked` (configuración por defecto)
  El control del flujo en el puerto está activo.
  El envío y evaluación de paquetes de pausa (funcionamiento Full-Dúplex) o colisiones (funcionamiento Half-Dúplex) está activado en el puerto.
  - ☐ Para activar el control del flujo en el dispositivo, active también la función *Flow control* en el cuadro de diálogo *Switching > Global*.
  - ☐ Active el control de flujo en el puerto del dispositivo conectado a este puerto.

  En un puerto Uplink, activar el control de flujo puede provocar la aparición de pausas no deseadas en el envío en el segmento de red de nivel superior ("contrapresión de ralentización").
- `unmarked`
  El control del flujo en el puerto está inactivo.

Si está utilizando un mecanismo 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.

Send trap (Link up/down)

Activa/desactiva el envío de trampas SNMP cuando el dispositivo detecta un cambio en el estado de vínculo activo/inactivo para este puerto.

Valores posibles:

- `marked` (configuración por defecto)
  El envío de trampas SNMP está activo.
  Cuando el dispositivo detecta un cambio de estado de enlace activo/inactivo, el dispositivo envía una trampa SNMP.
- `unmarked`
  El envío de trampas SNMP está inactivo.

Como requisito previo para enviar trampas SNMP, debe activar la función en el cuadro de diálogo *Diagnostics > Status Configuration > Alarms (Traps)* y especificar al menos un destino de la trampa.

MTU

Especifica el tamaño máximo permitido de paquetes de Ethernet en el puerto en bytes.

Valores posibles:

- `1518..9720` (configuración por defecto: `1518`)
  Con la configuración `1518`, el puerto transmite paquetes de Ethernet con el tamaño máximo siguiente:
  - 1518 bytes sin etiqueta VLAN
    (1514 bytes + CRC de 4 bytes)
  - 1522 bytes con etiqueta VLAN
    (1518 bytes + CRC de 4 bytes)

Esta configuración le permite aumentar el tamaño máximo permitido de los paquetes de Ethernet que este puerto puede recibir o transmitir.

La lista siguiente contiene las aplicaciones posibles:

- Al usar el dispositivo en la red de transferencia con etiquetado VLAN doble, es posible que necesite un *MTU* mayor de 4 bytes.

En otras interfaces, especifique el tamaño máximo admisible de los paquetes de Ethernet de la siguiente manera:

- Interfaces *Link Aggregation*
  Cuadro de diálogo *Switching > L2-Redundancy > Link Aggregation*, columna *MTU*

Signal

Activa/desactiva el parpadeo de la LED del puerto. Esta función le permite identificar el puerto en el campo.

Valores posibles:

- `marked`
  El parpadeo de la LED del puerto está activo.
  La LED del puerto parpadea hasta que vuelva a desactivar la función.
- `unmarked` (configuración por defecto)
  El parpadeo del LED del puerto está desactivado.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

Clear port statistics

Reinicia el contador de estadísticas de puertos a `0`.

## [Statistics]

Esta pestaña muestra la siguiente vista general por puerto:

- Número de paquetes de datos/bytes recibidos en el dispositivo
  - *Received packets*
  - *Received octets*
  - *Received unicast packets*
  - *Received multicast packets*
  - *Received broadcast packets*
- Número de paquetes de datos/bytes enviados desde el dispositivo
  - *Transmitted packets*
  - *Transmitted octets*
  - *Transmitted unicast packets*
  - *Transmitted multicast packets*
  - *Transmitted broadcast packets*
- Número de errores detectados por el dispositivo
  - *Received fragments*
  - *Detected CRC errors*
  - *Detected collisions*
- Número de paquetes de datos por categoría de tamaño recibidos en el dispositivo
  - *Packets 64 bytes*
  - *Packets 65 to 127 bytes*
  - *Packets 128 to 255 bytes*
  - *Packets 256 to 511 bytes*
  - *Packets 512 to 1023 bytes*
  - *Packets 1024 to 1518 bytes*
- Número de paquete de datos descartados por el dispositivo
  - *Received discards*
  - *Transmitted discards*

Para ordenar la tabla según un criterio específico, haga clic en la cabecera de la fila correspondiente.

Por ejemplo, para ordenar la tabla según el número de bytes recibidos en orden ascendente, haga clic en la cabecera de la columna *Received octets* una vez. Para ordenarla en orden descendente, vuelva a hacer clic en la cabecera.

Para reiniciar el contador de estadísticas de puertos en la tabla a `0`, lleve a cabo los siguientes pasos:

- ☐ En el cuadro de diálogo *Basic Settings > Port*, haga clic en el botón ☰ y, a continuación, en el elemento *Clear port statistics*.
  o bien
- ☐ En el cuadro de diálogo *Basic Settings > Restart*, haga clic en el botón *Clear port statistics*.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

Clear port statistics

Reinicia el contador de estadísticas de puertos a `0`.

## [Utilization]

Esta pestaña muestra el uso (carga de red) de cada puerto individual.

### Tabla

Port

Muestra el número de puerto.

Utilization [%]

Muestra el porcentaje de uso actual en relación con el intervalo de tiempo especificado en la columna *Control interval [s]*.

El uso es la relación entre la cantidad de datos recibidos y la mayor cantidad de datos posible con la velocidad de transferencia actualmente configurada.

Lower threshold [%]

Especifica un umbral inferior para el uso. Si el uso del puerto se encuentra por debajo este valor, la columna *Alarm* mostrará una alarma.

Valores posibles:

- `0.00..100.00` (configuración por defecto: `0.00`)

El valor `0` desactiva el umbral inferior.

Upper threshold [%]

Especifica un umbral superior para el uso. Si el uso del puerto sobrepasa este valor, la columna *Alarm* mostrará una alarma.

Valores posibles:

- `0.00..100.00` (configuración por defecto: `0.00`)

El valor `0` desactiva el umbral superior.

Control interval [s]

Especifica el intervalo en segundos.

Valores posibles:

- `1..3600` (configuración por defecto: `30`)

Alarm

Muestra el estado de la alarma de uso.

Valores posibles:

- `marked`
  El uso del puerto se encuentra por debajo del valor especificado en la columna *Lower threshold [%]* o por encima del valor especificado en la columna *Upper threshold [%]*. El dispositivo envía una trampa SNMP.
- `unmarked`
  El uso del puerto se encuentra por encima del valor especificado en la columna *Lower threshold [%]* o por debajo del valor especificado en la columna *Upper threshold [%]*.
  Como requisito previo para enviar trampas SNMP, debe activar la función en el cuadro de diálogo *Diagnostics > Status Configuration > Alarms (Traps)* y especificar al menos un destino de la trampa.

**Botones**

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

Clear port statistics

Reinicia el contador de estadísticas de puertos a `0`.

## 1.8 Power over Ethernet (MCSESP)

[Basic Settings > Power over Ethernet]

En Power over Ethernet (PoE), el equipo de potencia (PSE) suministra corriente a los dispositivos alimentados (PD), como los teléfonos IP, a través del cable de par trenzado.

El código de producto y el etiquetado específico de PoE en el alojamiento del dispositivo PSE indica si el dispositivo admite *Power over Ethernet*. Los puertos PoE del dispositivo admiten Power over Ethernet de acuerdo con el estándar IEEE 802.3at.

El sistema proporciona un balance de potencia máximo interno para los puertos. Los puertos reservan potencia según la clase detectada de un dispositivo alimentado conectado. La potencia real suministrada es igual o inferior a la potencia reservada.

Puede gestionar la potencia de salida con el parámetro *Priority*. Cuando la suma de la potencia requerida por los dispositivos conectados supera la potencia disponible, el dispositivo desactiva la potencia suministrada a los puertos de acuerdo con la prioridad configurada. El dispositivo desactiva la potencia suministrada a los puertos comenzando en primer lugar por los puertos configurados como de baja prioridad. Si varios puertos tienen una prioridad baja, el dispositivo desactiva la potencia empezando por los puertos con una numeración superior.

El menú contiene los siguientes cuadros de diálogo:

- PoE Global
- PoE Port

# 1.8.1 PoE Global

[ Basic Settings > Power over Ethernet > Global ]

En función de la configuración especificada en este cuadro de diálogo, el dispositivo proporciona potencia a los dispositivos de usuario final. Si el consumo de potencia alcanza el umbral especificado por el usuario, el dispositivo envía una trampa SNMP.

### Operation

Operation

Activa/desactiva la función *Power over Ethernet*.

Valores posibles:

- `On` (configuración por defecto)
  La función *Power over Ethernet* está activada.
- `Off`
  La función *Power over Ethernet* está desactivada.

### Configuration

Send trap

Activa/desactiva el envío de trampas SNMP.

Si el consumo de potencia supera el umbral especificado por el usuario, el dispositivo envía una trampa SNMP.

Valores posibles:

- `marked` (configuración por defecto)
  El dispositivo envía trampas SNMP.
- `unmarked`
  El dispositivo no envía ninguna trampa SNMP.

Como requisito previo para enviar trampas SNMP, debe activar la función en el cuadro de diálogo *Diagnostics > Status Configuration > Alarms (Traps)* y especificar al menos un destino de la trampa.

Threshold [%]

Especifica el valor límite del consumo de potencia en forma de porcentaje.

Si la potencia de salida supera este umbral, el dispositivo mide la potencia de salida total y envía una trampa SNMP.

Valores posibles:

- `0..99` (configuración por defecto: `90`)

### System power

Budget [W]

Muestra la suma de potencia disponible para el balance global.

Reserved [W]

Muestra la potencia reservada global. El dispositivo reserva potencia conforme a las clases detectadas de los dispositivos alimentados conectados. La potencia reservada es igual o inferior a la potencia real suministrada.

Delivered [W]

Muestra la potencia real suministrada a los módulos en vatios.

Delivered [mA]

Muestra la corriente real suministrada a los módulos en miliamperios.

### Tabla

Module

Módulo del dispositivo al que se refieren las entradas de la tabla.

Configured power budget [W]

Especifica la potencia de los módulos para la distribución en los puertos.

Valores posibles:

- `0..n` (configuración por defecto: n)
  En este caso, `n` corresponde al valor de la columna *Max. power budget [W]*.

Max. power budget [W]

Muestra la potencia máxima disponible para este módulo.

Reserved power [W]

Muestra la potencia reservada para el módulo conforme a las clases detectadas de los dispositivos alimentados conectados.

Delivered power [W]

Muestra la potencia real en vatios suministrada a los dispositivos alimentados que están conectados a este puerto.

Delivered current [mA]

Muestra la corriente real en miliamperios suministrada a los dispositivos alimentados que están conectados a este puerto.

Power source

Muestra el equipo de potencia del dispositivo.

Valores posibles:

- *internal*
  Fuente de potencia interna
- *external*
  Fuente de potencia externa

Threshold [%]

Especifica el valor límite del consumo de potencia del módulo en forma de porcentaje. Si la potencia de salida supera este umbral, el dispositivo mide la potencia de salida total y envía una trampa SNMP.

Valores posibles:

- `0..99` (configuración por defecto: `90`)

Send trap

Activa/desactiva el envío de trampas SNMP si el dispositivo detecta que se supera el valor límite del consumo de potencia.

Valores posibles:

- `marked`
  El envío de trampas SNMP está activo.
  Si el consumo de potencia del módulo supera el umbral definido por el usuario, el dispositivo envía una trampa SNMP.
- `unmarked` (configuración por defecto)
  El envío de trampas SNMP está inactivo.

Como requisito previo para enviar trampas SNMP, debe activar la función en el cuadro de diálogo *Diagnostics > Status Configuration > Alarms (Traps)* y especificar al menos un destino de la trampa.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## 1.8.2 PoE Port

[ Basic Settings > Power over Ethernet > Port ]

Si el consumo de potencia es superior a la potencia suministrable, el dispositivo desactiva la alimentación a los dispositivos alimentados conforme a los niveles de prioridad y los números de puerto. Si los dispositivos alimentados requieren más potencia eléctrica que la facilitada por el dispositivo, el dispositivo desactiva la función *Power over Ethernet* en los puertos. El dispositivo desactiva en primer lugar la función *Power over Ethernet* en los puertos con la prioridad más baja. Si varios puertos tienen la misma prioridad, el dispositivo desconecta primero la función *Power over Ethernet* en los puertos con el número de puerto más alto. El dispositivo también desactiva la potencia en los dispositivos alimentados (PD) durante un período de tiempo específico.

**Tabla**

Port

Muestra el número de puerto.

PoE enable

Activa/desactiva la potencia PoE suministrada al puerto.

Cuando la función se activa o desactiva, el dispositivo registra un evento en el archivo de registro (System Log).

Valores posibles:

- `marked` (configuración por defecto)
  El suministro de potencia PoE al puerto está activo.
- `unmarked`
  El suministro de potencia PoE al puerto está inactivo.

Fast startup

Activa/desactiva la función de inicio rápido de Power over Ethernet en el puerto.

Como requisito previo, la casilla de verificación de la columna *PoE enable* debe estar marcada.

Valores posibles:

- `marked`
  La función de inicio rápido está activa. El dispositivo envía potencia a los dispositivos alimentados (PD) inmediatamente después de activar la potencia del dispositivo.
- `unmarked` (configuración por defecto)
  La función de inicio rápido está inactiva. El dispositivo envía potencia a los dispositivos alimentados (PD) tras cargar su propia configuración.

Priority

Especifica la prioridad del puerto.

Para ayudar a evitar sobrecargas de corriente, el dispositivo desactiva en primer lugar los puertos con baja prioridad. Para ayudar a evitar que el dispositivo desactive los puertos que suministran potencia a los dispositivos necesarios, especifique una prioridad alta para esos puertos.

Valores posibles:

- *critical*
- *high*
- *low* (configuración por defecto)

Status

Muestra el estado de la detección del dispositivo alimentado (PD) mediante puerto.

Valores posibles:

- *disabled*
  El dispositivo está en estado DISABLED y no suministra potencia a los dispositivos alimentados.
- *deliveringPower*
  El dispositivo identificó la clase del dispositivo alimentado conectado y está en estado POWER ON.
- *fault*
  El dispositivo está en estado TEST ERROR.
- *otherFault*
  El dispositivo está en estado IDLE.
- *searching*
  El dispositivo está en un estado distinto a los enumerados.
- *test*
  El dispositivo está en TEST MODE.

Detected class

Muestra la clase de potencia del dispositivo alimentado conectado al puerto.

Valores posibles:

- *Class 0*
- *Class 1*
- *Class 2*
- *Class 3*
- *Class 4*

Class 0
Class 1
Class 2
Class 3
Class 4

Activa/desactiva la corriente de las clases 0 a 4 en el puerto.

Valores posibles:

- marked (configuración por defecto)
- unmarked

Consumption [W]

Muestra el consumo de potencia actual del puerto en vatios.

Valores posibles:

▶ `0,0..30,0`

Consumption [mA]

Muestra la corriente suministrada al puerto en miliamperios.

Valores posibles:

▶ `0..600`

Power limit [W]

Especifica la potencia máxima en vatios emitida por el puerto.

Esta función le permite distribuir el balance de potencia disponible entre los puertos PoE según sea necesario.

Por ejemplo, para un dispositivo conectado que no proporcione una "clase de potencia", el puerto reserva una cantidad fija de 15,4 W (clase 0) aunque el dispositivo requiera menos potencia. El excedente de potencia no está disponible en ningún otro puerto.

Mediante la especificación del límite de potencia, reduce la potencia reservada al requisito actual del dispositivo conectado. La potencia no utilizada está disponible para otros puertos.

Si no se conoce el consumo de potencia exacto del dispositivo alimentado, el dispositivo muestra el valor en la columna *Max. consumption [W]*. Compruebe que el límite de potencia sea superior al valor de la columna *Max. consumption [W]*.

Si la potencia máxima observada es superior al límite de potencia establecido, el dispositivo considera el límite de potencia como no válido. En este caso, el dispositivo utiliza la clase PoE para el cálculo.

Valores posibles:

▶ `0,0..30,0` (configuración por defecto: `0`)

Max. consumption [W]

Muestra la potencia máxima en vatios que ha consumido el dispositivo hasta el momento.

El valor se restablece al desactivar PoE en el puerto o al finalizar la conexión al dispositivo conectado.

Name

Especifica el nombre del puerto.

Especifique el nombre que desee.

Valores posibles:

- Cadena de caracteres ASCII alfanuméricos con entre 0 y 32 caracteres

Auto-shutdown power

Activa/desactiva la función *Auto-shutdown power* de acuerdo con la configuración.

Valores posibles:

- `marked`
- `unmarked` (configuración por defecto)

Disable power at [hh:mm]

Especifica el tiempo tras el cual el dispositivo desactiva la potencia del puerto después de la activación de la función *Auto-shutdown power*.

Valores posibles:

- `00:00..23:59` (configuración por defecto: `00:00`)

Re-enable power at [hh:mm]

Especifica el tiempo tras el cual el dispositivo activa la potencia del puerto después de la activación de la función *Auto-shutdown power*.

Valores posibles:

- `00:00..23:59` (configuración por defecto: `00:00`)

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## 1.9 Restart

[ Basic Settings > Restart ]

Este cuadro de diálogo le permite reiniciar el dispositivo, reiniciar los contadores del puerto y tablas de direcciones, y eliminar los archivos de registro.

### Restart

Restart in

Muestra el tiempo restante hasta que el dispositivo se reinicie.

Para actualizar los datos mostrados del tiempo restante, haga clic en el botón .

Cancel

Cancela un reinicio aplazado.

Cold start...

Abre el cuadro de diálogo *Restart* para iniciar un reinicio inmediato o aplazado del dispositivo.

Si el perfil de configuración en la memoria volátil (*RAM*) y el perfil de configuración "Seleccionado" en la memoria no volátil (*NVM*) son iguales, el dispositivo muestra el cuadro de diálogo *Warning*.

- Para guardar los cambios de forma permanente, haga clic en el botón *Yes* del cuadro de diálogo *Warning*.
- Para descartar los cambios, haga clic en el botón *No* del cuadro de diálogo *Warning*.
- En el campo *Restart in*, especifique el tiempo de retraso para el reinicio aplazado.
  Valores posibles:
  – `00:00:00..596:31:23` (configuración por defecto: `00:00:00`)

Una vez haya transcurrido el tiempo de retraso, el dispositivo se reiniciará y pasará por las siguientes fases:

- Si activa la función en el cuadro de diálogo *Diagnostics > System > Selftest*, el dispositivo llevará a cabo una prueba de RAM.
- El dispositivo inicia el software del dispositivo mostrado en el campo *Stored version*, en el cuadro de diálogo *Basic Settings > Software*.
- El dispositivo carga la configuración del perfil de configuración "seleccionado". Consulte el cuadro de diálogo *Basic Settings > Load/Save*.

**Nota:** Durante el reinicio, el dispositivo no transmite datos. Durante este tiempo, no se puede acceder al dispositivo mediante la Interfaz gráfica de usuario y otros sistemas de gestión.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

Reset MAC address table

Elimina las direcciones MAC de la tabla de reenvíos que tienen el valor *Switching > Filter for MAC Addresses* en el cuadro de diálogo `learned`, en la columna *Status*.

Reset ARP table

Elimina las direcciones configuradas dinámicamente de la tabla ARP.

Consulte el cuadro de diálogo *Diagnostics > System > ARP*.

Clear port statistics

Reinicia el contador de estadísticas de puertos a `0`.

Consulte el cuadro de diálogo *Basic Settings > Port*, pestaña *Statistics*.

Clear management access statistics

Restablece los contadores para obtener estadísticas sobre el acceso de la gestión del dispositivo a `0`.

Consulte el cuadro de diálogo *Diagnostics > System > System Information*, tabla `Used Management Ports`.

Reset IGMP snooping data

Elimina las entradas de IGMP Snooping y restablece el contador en el cuadro *Information* a `0`.

Consulte el cuadro de diálogo *Switching > IGMP Snooping > Global*.

Delete log file

Elimina los eventos registrados del archivo de registro.

Consulte el cuadro de diálogo *Diagnostics > Report > System Log*.

Delete persistent log file

Elimina los archivos de registro de la memoria externa.

Consulte el cuadro de diálogo *Diagnostics > Report > Persistent Logging*.

Clear email notification statistics

Restablece los contadores en el cuadro *Information* a `0`.

Consulte el cuadro de diálogo *Diagnostics > Email Notification > Global*.

# 2 Time

El menú contiene los siguientes cuadros de diálogo:
- Basic Settings
- SNTP
- PTP
- 802.1AS

## 2.1 Basic Settings

[Time > Basic Settings]

El dispositivo está equipado con un reloj de hardware almacenado en búfer. Este reloj mantiene la hora correcta en caso de que el suministro de corriente se vuelva inoperativo o si desconecta el dispositivo de este. Una vez iniciado el dispositivo, tendrá disponible la hora actual, por ejemplo, para las entradas de registro.

El reloj de hardware soporta cortes del suministro de corriente de 3 horas. El requisito previo es que el suministro de corriente del dispositivo haya estado conectado previamente y de manera continua durante al menos 5 minutos.

En este cuadro de diálogo, se especifican los ajustes relacionados con la hora independientemente del protocolo de sincronización de la hora especificado.

El cuadro de diálogo contiene las siguientes pestañas:
- [Global]
- [Daylight saving time]

### [Global]

En esta pestaña, especifique la hora del sistema en el dispositivo y la zona horaria.

#### Configuration

System time (UTC)

Muestra la fecha y hora actuales en relación con el tiempo universal coordinado (UTC).

Set time from PC

El dispositivo utiliza la hora del PC como hora del sistema.

System time

Muestra la fecha y hora actuales en relación con la hora local: *System time* = *System time (UTC)* + *Local offset [min]* + *Daylight saving time*

Time source

Muestra la fuente de la que el dispositivo obtiene la información de la hora.

El dispositivo selecciona automáticamente la fuente de la hora disponible con la mayor precisión.

Valores posibles:

- *local*
  Reloj del sistema del dispositivo.
- *sntp*
  El cliente *SNTP* está activado y el dispositivo es sincronizado por un servidor *SNTP*.
- *ptp*
  Se activa PTP y el reloj del dispositivo se sincroniza con un reloj *PTP* maestro.

Local offset [min]

Especifica la diferencia entre la hora local y *System time (UTC)* en minutos: *Local offset [min]* = *System time* − *System time (UTC)*

Valores posibles:

- `-780..840` (configuración por defecto: `60`)

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## [Daylight saving time]

En esta pestaña, active la función de horario de verano automático. Especifique el inicio y el final del horario de verano con un perfil predefinido o especifique estos ajustes individualmente. Durante el horario de verano, el dispositivo adelanta la hora local 1 hora.

### Operation

Daylight saving time

Activa/desactiva el modo *Daylight saving time*.

Valores posibles:

- *On*
  El modo *Daylight saving time* se activa.
  El dispositivo cambia automáticamente entre el horario de verano y el de invierno.
- *Off* (configuración por defecto)
  El modo *Daylight saving time* se desactiva.

Las horas a las que el dispositivo cambia entre el horario de verano y el de invierno se especifican en los cuadros *Summertime begin* y *Summertime end*.

Profile...

Muestra el cuadro de diálogo *Profile...*. Allí podrá seleccionar un perfil predefinido para el inicio y finalización del horario de verano. Este perfil sobrescribe los ajustes de los cuadros *Summertime begin* y *Summertime end*.

### Summertime begin

En los 3 primeros campos, puede especificar el día en que desea que se inicie el horario de verano y en el último campo, la hora.

Cuando la hora del campo *System time* alcance el valor introducido aquí, el dispositivo cambiará al horario de verano.

Week

Especifica la semana en el mes actual.

Valores posibles:

- *none* (configuración por defecto)
- *first*
- *second*
- *third*
- *fourth*
- *last*

Day

Especifica el día de la semana.

Valores posibles:

- *none* (configuración por defecto)
- *Sunday*
- *Monday*
- *Tuesday*
- *Wednesday*
- *Thursday*
- *Friday*
- *Saturday*

Month

Especifica el mes.

Valores posibles:

- *none* (configuración por defecto)
- *January*
- *February*
- *March*
- *April*
- *May*

- *June*
- *July*
- *August*
- *September*
- *October*
- *November*
- *December*

System time

Especifica la hora.

Valores posibles:

- `<HH:MM>` (configuración por defecto: `00:00`)

### Summertime end

En los 3 primeros campos, puede especificar el día en que desea que finalice el horario de verano y en el último campo, la hora.

Cuando la hora del campo *System time* alcance el valor introducido aquí, el dispositivo cambiará al horario de invierno.

Week

Especifica la semana en el mes actual.

Valores posibles:

- *none* (configuración por defecto)
- *first*
- *second*
- *third*
- *fourth*
- *last*

Day

Especifica el día de la semana.

Valores posibles:

- *none* (configuración por defecto)
- *Sunday*
- *Monday*
- *Tuesday*
- *Wednesday*
- *Thursday*
- *Friday*
- *Saturday*

Month

Especifica el mes.

Valores posibles:
- *none* (configuración por defecto)
- *January*
- *February*
- *March*
- *April*
- *May*
- *June*
- *July*
- *August*
- *September*
- *October*
- *November*
- *December*

System time

Especifica la hora.

Valores posibles:
- <HH:MM> (configuración por defecto: 00:00)

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## 2.2 SNTP

[ Time > SNTP ]

El Simple Network Time Protocol (SNTP) es un procedimiento descrito en RFC 4330 para la sincronización de la hora en la red.

El dispositivo le permite sincronizar la hora del sistema en el dispositivo como cliente *SNTP*. Como servidor *SNTP*, el dispositivo facilita la información de la hora a otros dispositivos.

El menú contiene los siguientes cuadros de diálogo:
- SNTP Client
- SNTP Server

## 2.2.1 SNTP Client

[ Time > SNTP > Client ]

En este cuadro de diálogo, especifique la configuración con la que desea que actúe el dispositivo como cliente *SNTP*.

Como cliente *SNTP*, el dispositivo obtiene la información de la hora de los servidores *SNTP* y *NTP*, y sincroniza el reloj local con la hora del servidor de hora.

### Operation

Operation

Activa/desactiva la función *SNTP Client* del dispositivo.

Valores posibles:

- `On`
  La función *SNTP Client* está activada.
  El dispositivo actúa como cliente *SNTP*.
- `Off` (configuración por defecto)
  La función *SNTP Client* está desactivada.

### Configuration

Mode

Especifica si el dispositivo solicita de manera activa la información de la hora de un servidor *SNTP* conocido y configurado en la red (modo Unicast) o espera de manera pasiva la información de la hora de un servidor *SNTP* aleatorio (modo Broadcast).

Valores posibles:

- `unicast` (configuración por defecto)
  El dispositivo toma la información de la hora solamente del servidor *SNTP* configurado. El dispositivo envía solicitudes Unicast al servidor *SNTP* y evalúa sus respuestas.
- `broadcast`
  El dispositivo obtiene la información de la hora de uno o más servidores *SNTP* o *NTP*. El dispositivo evalúa las respuestas Broadcast o Multicast procedentes únicamente de estos servidores.

Request interval [s]

Especifica en segundos el intervalo con el que el dispositivo solicita información de la hora del servidor *SNTP*.

Valores posibles:

- `5..3600` (configuración por defecto: `30`)

Broadcast recv timeout [s]

Especifica en segundos el tiempo que un cliente en modo de cliente Broadcast debe esperar antes de cambiar el valor del campo de `syncToRemoteServer` a `notSynchronized` cuando el cliente no recibe ningún paquete Broadcast.

Valores posibles:

- `128..2048` (configuración por defecto: `320`)

Disable client after successful sync

Activa/desactiva la inhabilitación del cliente *SNTP* una vez que el dispositivo ha sincronizado la hora correctamente.

Valores posibles:

- `marked`
  La desactivación del cliente *SNTP* está activa.
  El dispositivo desactiva el cliente *SNTP* tras la sincronización correcta de la hora.
- `unmarked` (configuración por defecto)
  La desactivación del cliente *SNTP* está inactiva.
  El cliente *SNTP* permanece activo tras la sincronización correcta de la hora.

### State

State

Muestra el estado del cliente *SNTP*.

Valores posibles:

- `disabled`
  El cliente *SNTP* se desactiva.
- `notSynchronized`
  El cliente *SNTP* no se sincroniza con ningún servidor *SNTP* o *NTP*.
- `synchronizedToRemoteServer`
  El cliente *SNTP* se sincroniza con un servidor *SNTP* o *NTP*.

### Tabla

En la tabla, especifica los ajustes de hasta 4 servidores *SNTP*.

Index

Muestra el número de índice al que la entrada de la tabla hace referencia.

Valores posibles:

- `1..4`

El dispositivo asigna este número automáticamente.

Cuando elimine una entrada de la tabla, quedará un hueco en la numeración. Al crear una nueva entrada en la tabla, el dispositivo introduce el primer número que falta.

Tras el inicio, el dispositivo envía solicitudes al servidor *SNTP* configurado en la primera entrada de la tabla. Cuando el servidor no responda, el dispositivo enviará sus solicitudes al servidor *SNTP* configurado en la siguiente entrada de la tabla.

Si ninguno de los servidores *SNTP* configurados responde mientras tanto, el cliente *SNTP* interrumpirá su sincronización. El dispositivo envía solicitudes cíclicamente a cada servidor *SNTP* hasta que uno envía una hora válida. El dispositivo se sincroniza con este servidor *SNTP*, aunque se pueda poner en contacto con los demás servidores de nuevo más tarde.

Name

Especifica el nombre del servidor *SNTP*.

Valores posibles:

- Cadena de caracteres ASCII alfanuméricos con entre 1 y 32 caracteres

Address

Especifica la dirección IP del servidor *SNTP*.

Valores posibles:

- Dirección IPv4 válida (configuración por defecto: `0.0.0.0`)
- Dirección IPv6 válida
- Nombre de host

Destination UDP port

Especifica el puerto UDP en el que el servidor *SNTP* espera la información de la hora.

Valores posibles:

- `1..65535` (configuración por defecto: `123`)
  Excepción: el puerto `2222` está reservado para funciones internas.

Status

Muestra el estado de conexión entre el cliente *SNTP* y el servidor *SNTP*.

Valores posibles:

- *success*
  El dispositivo ha sincronizado la hora con el servidor *SNTP* correctamente.

- `badDateEncoded`
  La información de la hora recibida contiene errores de protocolo (sincronización incorrecta).
- `other`
  - Se introduce el valor `0.0.0.0` para la dirección IP del servidor *SNTP* (sincronización incorrecta).
    o bien
  - El cliente *SNTP* está utilizando un servidor *SNTP* diferente.
- `requestTimedOut`
  El dispositivo no ha recibido una respuesta del servidor *SNTP* (sincronización incorrecta).
- `serverKissOfDeath`
  El servidor *SNTP* está sobrecargado. Se solicita al dispositivo que se sincronice con otro servidor *SNTP*. Si no hay ningún otro servidor *SNTP* disponible, el dispositivo comprueba a intervalos superiores a los indicados en el ajuste del campo *Request interval [s]* si el servidor continúa sobrecargado.
- `serverUnsychronized`
  El servidor *SNTP* no está sincronizado con una fuente de la hora de referencia local o externo (sincronización incorrecta).
- `versionNotSupported`
  Las versiones *SNTP* del cliente y del servidor no son compatibles entre sí (sincronización incorrecta).

Active

Activa/desactiva la conexión con el servidor *SNTP*.

Valores posibles:

- `marked`
  La conexión con el servidor *SNTP* está activada.
  El cliente *SNTP* tiene acceso al servidor *SNTP*.
- `unmarked` (configuración por defecto)
  La conexión con el servidor *SNTP* está desactivada.
  El cliente *SNTP* no tiene acceso al servidor *SNTP*.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## 2.2.2 SNTP Server

[Time > SNTP > Server]

En este cuadro de diálogo, especifique la configuración con la que desea que actúe el dispositivo como servidor *SNTP*.

El servidor *SNTP* proporciona la hora UTC (tiempo universal coordinado) sin tener en cuenta las diferencias de hora locales.

Si el ajuste es el adecuado, el servidor *SNTP* funciona en modo Broadcast. En modo Broadcast, el servidor *SNTP* envía mensajes Broadcast o Multicast automáticamente en función del intervalo de envío Broadcast.

### Operation

Operation

Activa/desactiva la función *SNTP Server* del dispositivo.

Valores posibles:

- *On*
  La función *SNTP Server* está activada.
  El dispositivo actúa como servidor *SNTP*.
- *Off* (configuración por defecto)
  La función *SNTP Server* está desactivada.

Tenga en cuenta el ajuste de la casilla *Disable server at local time source* en el cuadro *Configuration*.

### Configuration

UDP port

Especifica el número del puerto UDP en el que el servidor *SNTP* del dispositivo recibe solicitudes de otros clientes.

Valores posibles:

- `1..65535` (configuración por defecto: `123`)
  Excepción: el puerto `2222` está reservado para funciones internas.

Broadcast admin mode

Activa/desactiva el modo Broadcast.

- `marked`
  El servidor *SNTP* responde a solicitudes de clientes *SNTP* en modo Unicast y también envía paquetes *SNTP* en modo Broadcast como Broadcast o Multicast.
- `unmarked` (configuración por defecto)
  El servidor *SNTP* responde a solicitudes de clientes *SNTP* en modo Unicast.

Broadcast destination address

Especifica la dirección IP a la que el servidor *SNTP* del dispositivo envía los paquetes *SNTP* en modo Broadcast.

Valores posibles:

- Dirección IPv4 válida (configuración por defecto: `0.0.0.0`)

Se permiten direcciones Broadcast y Multicast.

Broadcast UDP port

Especifica el número del puerto UDP en el que el servidor *SNTP* envía los paquetes *SNTP* en modo Broadcast.

Valores posibles:

- `1..65535` (configuración por defecto: `123`)
  Excepción: el puerto `2222` está reservado para funciones internas.

Broadcast VLAN ID

Especifica el ID de VLAN en el que el servidor *SNTP* del dispositivo envía los paquetes *SNTP* en modo Broadcast.

Valores posibles:

- `0`
  El servidor *SNTP* envía los paquetes *SNTP* de la misma VLAN en la que es posible acceder a la administración del dispositivo. Consulte el cuadro de diálogo *Basic Settings > Network*.
- `1..4042` (configuración por defecto: `1`)

Broadcast send interval [s]

Especifica el intervalo de tiempo después del cual el servidor *SNTP* del dispositivo envía paquetes Broadcast *SNTP*.

Valores posibles:

- `64..1024` (configuración por defecto: `128`)

Disable server at local time source

Activa/desactiva la inhabilitación del servidor *SNTP* cuando el dispositivo está sincronizado con el reloj local.

Valores posibles:

- `marked`
  La desactivación del servidor *SNTP* está activa.
  Si el dispositivo está sincronizado con el reloj local, el dispositivo desactiva el servidor *SNTP*. El servidor *SNTP* continúa respondiendo a solicitudes de clientes *SNTP*. En el paquete *SNTP*, el servidor *SNTP* informa a los clientes de que está sincronizado localmente.
- `unmarked` (configuración por defecto)
  La desactivación del servidor *SNTP* está inactiva.
  Si el dispositivo está sincronizado con el reloj local, el servidor *SNTP* permanece activo.

### State

State

Muestra el estado del servidor *SNTP*.

Valores posibles:

- `disabled`
  El servidor *SNTP* está desactivado.
- `notSynchronized`
  El servidor *SNTP* no está sincronizado con una fuente de la hora de referencia local o externo.
- `syncToLocal`
  El servidor *SNTP* está sincronizado con el reloj de hardware del dispositivo.
- `syncToRefclock`
  El servidor *SNTP* está sincronizado con una fuente de la hora de referencia externa, por ejemplo PTP.
- `syncToRemoteServer`
  El servidor *SNTP* está sincronizado con un servidor *SNTP* situado en una posición más alta que el dispositivo en una cascada.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## 2.3 PTP

[ Time > PTP ]

El menú contiene los siguientes cuadros de diálogo:

- PTP Global
- PTP Boundary Clock
- PTP Transparent Clock

## 2.3.1 PTP Global

[ Time > PTP > Global ]

En este cuadro de diálogo , especifique la configuración básica para el protocolo *PTP*.

El Precision Time Protocol (PTP) es un procedimiento descrito en el estándar IEEE 1588-2008 que suministra a los dispositivos de la red la hora precisa. El método sincroniza los relojes de la red con una precisión de unos pocos 100 ns. El protocolo utiliza comunicación Multicast, por lo que la carga en la red debido a los mensajes de sincronización de *PTP* es insignificante.

PTP es notablemente más preciso que SNTP. Si las funciones *SNTP* y *PTP* están activadas en el dispositivo al mismo tiempo, la función *PTP* tendrá prioridad.

Con el *Best Master Clock Algorithm*, los dispositivos de la red determinan qué dispositivo tiene la hora más precisa. Los dispositivos utilizan el dispositivo con la hora más precisa como origen de hora de referencia (*Grandmaster*). Posteriormente, los dispositivos participantes se sincronizan a sí mismos con este origen de hora de referencia.

Si desea transportar la hora PTP de manera precisa a través de la red, utilice únicamente dispositivos con compatibilidad de hardware PTP en las rutas de transporte.

El protocolo diferencia entre los siguientes relojes:

- *Boundary Clock (BC)*
  Este reloj tiene un número indefinido de puertos PTP y funciona como *PTP* maestro y *PTP* esclavo. En su segmento de red correspondiente, el reloj funciona como un reloj normal.
  - Como *PTP* esclavo, el reloj se sincroniza solo con un *PTP* maestro situado en una posición superior a la del dispositivo en la cascada.
  - Como *PTP* maestro, el reloj reenvía la información de la hora a través de la red a los *PTP* esclavos situados en una posición superior a la del dispositivo en la cascada.
- *Transparent Clock (TC)*
  Este reloj tiene un número indefinido de puertos PTP. En contraste con el *Boundary Clock*, este reloj corrige la información de la hora antes de reenviarla, sin sincronizarse a sí mismo.

### Operation IEEE1588/PTP

Operation IEEE1588/PTP

Activa/desactiva la función *PTP*.

En el dispositivo, la función *802.1AS* o *PTP* pueden activarse a la vez.

Valores posibles:

- `On`
  La función *PTP* está activada.
  El dispositivo sincroniza su reloj con PTP.
  Si las funciones *SNTP* y *PTP* están activadas en el dispositivo al mismo tiempo, la función *PTP* tendrá prioridad.
- `Off` (configuración por defecto)
  La función *PTP* está desactivada.
  El dispositivo transmite los mensajes de sincronización de *PTP* sin ninguna corrección en cada puerto.

### Configuration IEEE1588/PTP

PTP mode

Especifica la versión PTP y el modo del reloj local.

Valores posibles:

- *v2-transparent-clock* (configuración por defecto)
- *v2-boundary-clock*

Sync lower bound [ns]

Especifica el valor límite inferior en nanosegundos para la diferencia de ruta entre el reloj local y el origen de la hora de referencia (*Grandmaster*). Si la diferencia de ruta cae por debajo de este valor una vez, el reloj local se clasifica como sincronizado.

Valores posibles:

- `0..999999999` (configuración por defecto: `30`)

Sync upper bound [ns]

Especifica el valor límite superior en nanosegundos para la diferencia de ruta entre el reloj local y el origen de la hora de referencia (*Grandmaster*). Si la diferencia de ruta supera este valor una vez, el reloj local se clasifica como no sincronizado.

Valores posibles:

- `31..1000000000` (configuración por defecto: `5000`)

PTP management

Activa/desactiva la gestión de PTP definida en el estándar PTP.

Valores posibles:

- `marked`
  La gestión de PTP está activada.
- `unmarked` (configuración por defecto)
  La gestión de PTP está desactivada.

### Status

Is synchronized

Muestra si el reloj local está sincronizado con el origen de hora de referencia (*Grandmaster*).

Si la diferencia de ruta entre el reloj local y el origen de hora de referencia (*Grandmaster*) cae por debajo del umbral inferior de sincronización una vez, se sincronizará el reloj local. Este estado se mantiene hasta que la diferencia de ruta supera el límite superior de sincronización una vez.

Especifique los límites de sincronización en el cuadro *Configuration IEEE1588/PTP*.

Max. offset absolute [ns]

Muestra la diferencia de ruta máxima en nanosegundos producida desde la sincronización del reloj local con el origen de hora de referencia (*Grandmaster*).

PTP time

Muestra la fecha y la hora de la escala de hora PTP cuando el reloj local está sincronizado con el origen de hora de referencia (*Grandmaster*). `Month Day, Year hh:mm:ss AM/PM`

**Botones**

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## 2.3.2 PTP Boundary Clock

[ Time > PTP > Boundary Clock ]

Con este menú puede configurar el modo Reloj delimitador para el reloj local.

El menú contiene los siguientes cuadros de diálogo:
- PTP Boundary Clock Global
- PTP Boundary Clock Port

# 2.3.2.1 PTP Boundary Clock Global

[ Time > PTP > Boundary Clock > Global ]

En este cuadro de diálogo puede introducir la configuración general multipuertos del modo *Boundary Clock* para el reloj local. El *Boundary Clock (BC)* funciona conforme a PTP versión 2 (IEEE 1588-2008).

La configuración es efectiva cuando el reloj local funciona como *Boundary Clock (BC)*. Para esto, seleccione en el cuadro de diálogo *Time > PTP > Global* del campo *PTP mode* el valor `v2-boundary-clock`.

### Operation IEEE1588/PTPv2 BC

Priority 1

Especifica *priority 1* para el dispositivo.

Valores posibles:

- `0..255` (configuración por defecto: `128`)

El *Best Master Clock Algorithm* evalúa en primer lugar *priority 1* entre los dispositivos participantes para determinar el origen de la hora de referencia (*Grandmaster*).

Cuanto más bajo establezca este valor, más probabilidades hay de que el dispositivo se convierta en el origen de hora de referencia (*Grandmaster*). Consulte el cuadro *Grandmaster*.

Priority 2

Especifica *priority 2* para el dispositivo.

Valores posibles:

- `0..255` (configuración por defecto: `128`)

Si los criterios evaluados anteriormente son los mismos para varios dispositivos, el *Best Master Clock Algorithm* evalúa *priority 2* de los dispositivos participantes.

Cuanto más bajo establezca este valor, más probabilidades hay de que el dispositivo se convierta en el origen de hora de referencia (*Grandmaster*). Consulte el cuadro *Grandmaster*.

Domain number

Asigna el dispositivo a un dominio *PTP*.

Valores posibles:

- `0..255` (configuración por defecto: `0`)

El dispositivo transmite la información de la hora de y a dispositivos del mismo dominio únicamente.

### Status IEEE1588/PTPv2 BC

Two step

Muestra que el reloj está funcionando en modo Two-Step.

Steps removed

Muestra el número de rutas de comunicación pasadas entre el reloj local del dispositivo y el origen de hora de referencia (*Grandmaster*).

Para un *PTP* esclavo, el valor `1` significa que el reloj está conectado con el origen de hora de referencia (*Grandmaster*) directamente a través de 1 ruta de comunicación.

Offset to master [ns]

Muestra la diferencia medida (desviación) entre el reloj local y el origen de hora de referencia (*Grandmaster*) en nanosegundos. El *PTP* esclavo calcula la diferencia respecto a la información de hora recibida.

En el modo Two-Step la información de hora está compuesta por 2 mensajes de sincronización de *PTP* cada uno, que el *PTP* maestro envía de manera cíclica:

- El primer mensaje de sincronización contiene un valor estimado de la hora de envío del mensaje exacta.
- El segundo mensaje de sincronización (mensaje de seguimiento) contiene la hora de envío exacta del primer mensaje.

El *PTP* esclavo utiliza los dos mensajes de sincronización de *PTP* para calcular la diferencia (desviación) respecto al maestro y corrige su reloj teniendo en cuenta esta diferencia. En este caso el *PTP* esclavo también considera el valor *Delay to master [ns]*.

Delay to master [ns]

Muestra el tiempo que tardan en transmitirse los mensajes de sincronización de *PTP* del *PTP* maestro al *PTP* esclavo en nanosegundos.

El *PTP* esclavo envía un paquete de "Delay Request" (Solicitud de retardo) al *PTP* maestro y determina la hora de envío exacta del paquete. Cuando recibe el paquete, el *PTP* maestro genera una marca de hora y la envía en un paquete de "Delay Response" (Respuesta de retardo) al *PTP* esclavo. El *PTP* esclavo utiliza los dos paquetes para calcular el retardo y lo calcula empezando desde la siguiente medición de la desviación.

Como requisito previo, el valor del mecanismo de retardo de los puertos esclavos se especifica como `e2e`.

### Grandmaster

Este cuadro muestra los criterios que utiliza el *Best Master Clock Algorithm* al evaluar el origen de la hora de referencia (*Grandmaster*).

En primer lugar el algoritmo evalúa la *priority 1* de los dispositivos participantes. El dispositivo con el valor más bajo de *priority 1* se designará como origen de hora de referencia (*Grandmaster*). Si el valor es el mismo para varios dispositivos, el algoritmo toma el siguiente criterio y, cuando este también coincide, el algoritmo toma el siguiente criterio a este. Cuando todos los valores coinciden para varios dispositivos, el valor más bajo del campo *Clock identity* decide qué dispositivo se designa como origen de hora de referencia (*Grandmaster*).

El dispositivo le permite tener influencia sobre qué dispositivo de la red se designa como origen de hora de referencia (*Grandmaster*). Para ello, modifique el valor en el campo *Priority 1* o *Priority 2* en el cuadro *Operation IEEE1588/PTPv2 BC*.

Priority 1

Muestra *priority 1* para el dispositivo que actualmente es el origen de hora de referencia (*Grandmaster*).

Clock class

Muestra la clase de origen de hora de referencia (*Grandmaster*). Parámetro del *Best Master Clock Algorithm*.

Clock accuracy

Muestra la precisión estimada del origen de hora de referencia (*Grandmaster*). Parámetro del *Best Master Clock Algorithm*.

Clock variance

Muestra la desviación del origen de hora de referencia (*Grandmaster*), también denominada *variación de registro escalado de desviación*. Parámetro del *Best Master Clock Algorithm*.

Priority 2

Muestra *priority 2* para el dispositivo que actualmente es el origen de hora de referencia (*Grandmaster*).

### Local time properties

Time source

Especifica el origen de hora del que el reloj local obtiene la información de la hora.

Valores posibles:

- `atomicClock`
- `gps`
- `terrestrialRadio`
- `ptp`
- `ntp`
- `handSet`

- *other*
- *internalOscillator* (configuración por defecto)

UTC offset [s]

Especifica la diferencia entre la escala de tiempo *PTP* y UTC.

Consulte la casilla de verificación *PTP timescale*.

Valores posibles:

- -32768..32767

**Nota:** El ajuste predeterminado es el valor válido en la fecha de creación del software del dispositivo. Puede obtener información adicional en el "Boletín C" del Servicio Internacional de Rotación de la Tierra y Sistemas de Referencia (IERS):http://www.iers.org/IERS/EN/Publications/Bulletins/bulletins.html

UTC offset valid

Especifica si el valor especificado en el campo *UTC offset [s]* es correcto.

Valores posibles:

- marked
- unmarked (configuración por defecto)

Time traceable

Muestra si el dispositivo obtiene la hora de una referencia UTC primaria, p. ej., de un servidor NTP.

Valores posibles:

- marked
- unmarked

Frequency traceable

Muestra si el dispositivo obtiene frecuencia de una referencia UTC primaria, por ejemplo, de un servidor NTP.

Valores posibles:

- marked
- unmarked

PTP timescale

Muestra si el dispositivo utiliza la escala horaria PTP.

Valores posibles:

- marked
- unmarked

La escala horaria PTP, según el estándar IEEE 1588, es el tiempo atómico TAI que se inició el 01/01/1970.

Al contrario que UTC, TAI no tiene segundos intercalares.

Desde el 1 de julio de 2020, la hora TAI se encuentra 37 segundos por delante de la hora UTC.

### Identities

El dispositivo muestra las identidades como secuencias de bytes en notación hexadecimal.

Los números de identificación (UUID) están compuestos de la manera siguiente:
- El número de identificación del dispositivo de la dirección MAC de este, con los valores `ff` y `fe` añadidos entre byte 3 y byte 4.
- El UUID del puerto está compuesto por el número de identificación del dispositivo seguido de un ID de puerto de 16 bits.

Clock identity

Muestra el propio número de identificación del dispositivo (UUID).

Parent port identity

Muestra el número de identificación del puerto (UUID) del dispositivo maestro directamente superior.

Grandmaster identity

Muestra el número de identificación (UUID) del dispositivo de origen de hora de referencia (*Grandmaster*).

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## 2.3.2.2 PTP Boundary Clock Port

[ Time > PTP > Boundary Clock > Port ]

En este cuadro de diálogo , especifique la configuración de *Boundary Clock (BC)* en cada puerto individual.

La configuración es efectiva cuando el reloj local funciona como *Boundary Clock (BC)*. Para esto, seleccione en el cuadro de diálogo *Time > PTP > Global* del campo *PTP mode* el valor `v2-boundary-clock`.

### Tabla

Port

Muestra el número de puerto.

PTP enable

Activa/desactiva la transmisión de mensajes de sincronización de *PTP* en el puerto.

Valores posibles:

- `marked` (configuración por defecto)
  La transmisión está activada. El puerto reenvía y recibe mensajes de sincronización *PTP*.
- `unmarked`
  La transmisión está desactivada. El puerto bloquea los mensajes de sincronización *PTP*.

PTP status

Muestra el estado actual del puerto.

Valores posibles:

- *initializing*
  Fase de inicialización
- *faulty*
  Modo de error: error en el protocolo PTP.
- *disabled*
  PTP está desactivado en el puerto.
- *listening*
  El puerto del dispositivo está esperando mensajes de sincronización *PTP*.
- *pre-master*
  Modo *PTP* premaestro
- *master*
  Modo *PTP* maestro
- *passive*
  Modo *PTP* pasivo
- *uncalibrated*
  Modo *PTP* no calibrado
- *slave*
  Modo *PTP* esclavo

Sync interval

Especifica en segundos el intervalo tras el que el puerto transmite mensajes de sincronización *PTP*.

Valores posibles:

- `0.25`
- `0.5`
- `1` (configuración por defecto)
- `2`

Delay mechanism

Especifica el mecanismo con el que el dispositivo mide el retardo en la transmisión de mensajes de sincronización *PTP*.

Valores posibles:

- *`disabled`*
  La medición del retardo de los mensajes de sincronización *PTP* para los dispositivos PTP conectados está inactiva.
- *`e2e`* (configuración por defecto)
  De extremo a extremo: como *PTP* esclavo, el puerto mide el retardo de los mensajes de sincronización *PTP* hasta el *PTP* maestro.
  El dispositivo muestra el valor medido en el cuadro de diálogo *Time > PTP > Boundary Clock >* Global.
- *`p2p`*
  De igual a igual: el dispositivo mide el tiempo que tardan los mensajes de sincronización *PTP* para los dispositivos PTP conectados, siempre que dichos dispositivos admitan P2P.
  Este mecanismo evita que el dispositivo tenga que determinar el retardo de nuevo en caso de reconfiguración.

P2P delay

Muestra el retardo Peer-to-Peer medido de los mensajes de sincronización *PTP*.

Como requisito previo debe seleccionar el valor *`p2p`* en la columna *Delay mechanism*.

P2P delay interval [s]

Especifica en segundos el intervalo tras el que el puerto mide el retardo Peer-to-Peer.

Como requisito previo debe haber especificado el valor *`p2p`* en este puerto y en el puerto del dispositivo remoto.

Valores posibles:

- `1` (configuración por defecto)
- `2`
- `4`
- `8`
- `16`
- `32`

Network protocol

Especifica qué protocolo utiliza el puerto para transmitir los mensajes de sincronización *PTP*.

Valores posibles:

- *IEEE 802.3* (configuración por defecto)
- *UDP/IPv4*

Announce interval [s]

Especifica en segundos el intervalo con el que el puerto transmite mensajes para la detección de la topología PTP.

Asigne el mismo valor a cada dispositivo de un dominio *PTP*.

Valores posibles:

- 1
- 2 (configuración por defecto)
- 4
- 8
- 16

Announce timeout

Especifica el número de intervalos de anuncio.

Por ejemplo:

En la configuración por defecto (*Announce interval [s]* = 2 y *Announce timeout* = 3), el tiempo de espera es de 3 × 2 s = 6 s.

Valores posibles:

- 2..10 (configuración por defecto: 3)
  Asigne el mismo valor a cada dispositivo de un dominio *PTP*.

E2E delay interval [s]

Muestra en segundos el intervalo tras el que el puerto mide el retardo End-to-End:

- Si el puerto está funcionando como *PTP* maestro, el dispositivo asigna el valor 8 al puerto.
- Si el puerto está funcionando como *PTP* esclavo, el valor es especificado por el *PTP* maestro conectado al puerto.

V1 hardware compatibility

Especifica si el puerto ajusta la longitud de los mensajes de sincronización *PTP* si ha establecido el valor *udpIpv4* en la columna *Network protocol*.

Es posible que los demás dispositivos de la red esperen que los mensajes de sincronización *PTP* tengan la misma longitud que los mensajes PTPv1.

Valores posibles:

- *auto* (configuración por defecto)
  El dispositivo detecta automáticamente si otros dispositivos de la red esperan que los mensajes de sincronización *PTP* tengan la misma longitud que los mensajes PTPv1. En tal caso, el dispositivo amplía la longitud de los mensajes de sincronización *PTP* antes de transmitirlos.

- *on*
  El dispositivo amplía la longitud de los mensajes de sincronización *PTP* antes de transmitirlos.
- *off*
  El dispositivo transmite los mensajes de sincronización *PTP* sin cambiar la longitud.

Asymmetry

Corrige el valor medido del retardo dañado por rutas de transmisión asimétricas.

Valores posibles:

- `-2000000000..2000000000` (configuración por defecto: `0`)

El valor representa la simetría del retardo en nanosegundos.

Un valor de retardo medido de y ns se corresponde con una asimetría de y × 2 ns.

El valor es positivo si el retardo desde el *PTP* maestro hasta el *PTP* esclavo es superior que en dirección opuesta.

VLAN

Especifica el ID de la VLAN con el que el dispositivo marca los mensajes de sincronización *PTP* en este puerto.

Valores posibles:

- *none* (configuración por defecto)
  El dispositivo transmite los mensajes de sincronización *PTP* sin una etiqueta VLAN.
- `0..4042`
  Especifique las VLAN que ya tenga configuradas en el dispositivo de la lista.

Compruebe que el puerto sea miembro de la VLAN.

Consulte el cuadro de diálogo *Switching > VLAN > Configuration*.

VLAN priority

Especifica la prioridad con la que el dispositivo transmite los mensajes de sincronización *PTP* marcados con un ID de VLAN (capa 2, IEEE 802.1D).

Valores posibles:

- `0..7` (configuración por defecto: `6`)

Si ha especificado en la columna *VLAN* el valor *none*, el dispositivo ignora la prioridad de la VLAN.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## 2.3.3 PTP Transparent Clock

[ Time > PTP > Transparent Clock ]

Con este menú puede configurar el modo *Transparent Clock* para el reloj local.

El menú contiene los siguientes cuadros de diálogo:
- PTP Transparent Clock Global
- PTP Transparent Clock Port

# 2.3.3.1 PTP Transparent Clock Global

[ Time > PTP > Transparent Clock > Global ]

En este cuadro de diálogo puede introducir la configuración general multipuertos del modo *Transparent Clock* para el reloj local. El *Transparent Clock (TC)* funciona conforme a PTP versión 2 (IEEE 1588-2008).

La configuración es efectiva cuando el reloj local funciona como *Transparent Clock (TC)*. Para esto, seleccione en el cuadro de diálogo *Time > PTP > Global* del campo *PTP mode* el valor `v2-transparent-clock`.

### Operation IEEE1588/PTPv2 TC

Delay mechanism

Especifica el mecanismo con el que el dispositivo mide el retardo en la transmisión de mensajes de sincronización *PTP*.

Valores posibles:

- `e2e` (configuración por defecto)
  Como *PTP* esclavo, el puerto mide el retardo de los mensajes de sincronización *PTP* hasta el *PTP* maestro.
  El dispositivo muestra el valor medido en el cuadro de diálogo *Time > PTP > Transparent Clock >* Global.
- `p2p`
  El dispositivo mide el tiempo que tardan los mensajes de sincronización *PTP* para todos los dispositivos PTP conectados, siempre que el dispositivo admita P2P.
  Este mecanismo evita que el dispositivo tenga que determinar el retardo de nuevo en caso de reconfiguración.
  Si especifica este valor, el valor `IEEE 802.3` solamente estará disponible en el campo *Network protocol*.
- `e2e-optimized`
  Igual que `e2e`, con las siguientes características especiales:
  - El dispositivo transmite las solicitudes de retardo de los *PTP* esclavos solamente al *PTP* maestro, aunque estas solicitudes sean mensajes Multicast. Por tanto, el dispositivo evita el envío de solicitudes Multicast innecesarias a los demás dispositivos.
  - Si cambia la topología maestro-esclavo, el dispositivo vuelve a aprender el puerto para el *PTP* maestro en cuanto recibe un mensaje de sincronización de otro *PTP* maestro.
  - Si el dispositivo no conoce a un *PTP* maestro, el dispositivo transmite solicitudes de retardo a los puertos.
- `disabled`
  La medición del retardo se desactiva en el puerto. El dispositivo descarta mensajes para la medición del retardo.

Primary domain

Asigna el dispositivo a un dominio *PTP*.

Valores posibles:

- `0..255` (configuración por defecto: `0`)

El dispositivo transmite la información de la hora de y a dispositivos del mismo dominio únicamente.

Network protocol

Especifica qué protocolo utiliza el puerto para transmitir los mensajes de sincronización *PTP*.

Valores posibles:

- `ieee8023` (configuración por defecto)
- `udpIpv4`

Multi domain mode

Activa/desactiva la corrección de mensajes de sincronización *PTP* en cada dominio *PTP*.

Valores posibles:

- `marked`
  El dispositivo corrige los mensajes de sincronización *PTP* en cada dominio *PTP*.
- `unmarked` (configuración por defecto)
  El dispositivo corrige mensajes de sincronización *PTP* solamente en el dominio *PTP* primario. Consulte el campo *Primary domain*.

VLAN ID

Especifica el ID de la VLAN con el que el dispositivo marca los mensajes de sincronización *PTP* en este puerto.

Valores posibles:

- `none` (configuración por defecto)
  El dispositivo transmite los mensajes de sincronización *PTP* sin una etiqueta VLAN.
- `0..4042`
  Especifique las VLAN que ya tenga configuradas en el dispositivo de la lista.

VLAN priority

Especifica la prioridad con la que el dispositivo transmite los mensajes de sincronización *PTP* marcados con un ID de VLAN (capa 2, IEEE 802.1D).

Valores posibles:

- `0..7` (configuración por defecto: `6`)

Si ha especificado el valor `none` en el campo *VLAN ID*, el dispositivo ignorará el valor especificado.

### Local synchronization

Syntonize

Activa/desactiva la sincronización de la frecuencia del *Transparent Clock* con el *PTP* maestro.

Valores posibles:

- `marked` (configuración por defecto)
  La sincronización de la frecuencia está activa.
  El dispositivo sincroniza la frecuencia.
- `unmarked`
  La sincronización de la frecuencia está inactiva.
  La frecuencia permanece constante.

Synchronize local clock

Activa/desactiva la sincronización de la hora local del sistema.

Valores posibles:

- `marked`
  La sincronización está activa.
  El dispositivo sincroniza la hora local del sistema con la hora recibida a través de PTP. Como requisito previo, la casilla de verificación *Syntonize* debe estar marcada.
- `unmarked` (configuración por defecto)
  La sincronización está inactiva.
  La hora local del sistema permanece constante.

Current master

Muestra el número de identificación del puerto (UUID) del dispositivo maestro directamente superior en el que el dispositivo sincroniza su frecuencia.

Si el valor contiene solamente ceros, esto se debe a lo siguiente:

- La función *Syntonize* está desactivada.
  o bien
- El dispositivo no puede encontrar un *PTP* maestro.

Offset to master [ns]

Muestra la diferencia medida (desviación) entre el reloj local y el *PTP* maestro en nanosegundos. El dispositivo calcula la diferencia respecto a la información de hora recibida.

Como requisito previo, la función *Synchronize local clock* debe estar activada.

Delay to master [ns]

Muestra el tiempo que tardan en transmitirse los mensajes de sincronización de *PTP* del *PTP* maestro al *PTP* esclavo en nanosegundos.

Requisito previo:

- La función *Synchronize local clock* está activada.
- En el campo *Delay mechanism*, el valor `e2e` está seleccionado.

### Status IEEE1588/PTPv2 TC

Clock identity

Muestra el propio número de identificación del dispositivo (UUID).

El dispositivo muestra las identidades como secuencias de bytes en notación hexadecimal.

El número de identificación del dispositivo de la dirección MAC de este, con los valores `ff` y `fe` añadidos entre byte 3 y byte 4.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## 2.3.3.2 PTP Transparent Clock Port

[ Time > PTP > Transparent Clock > Port ]

En este cuadro de diálogo , especifique la configuración de *Transparent Clock (TC)* en cada puerto individual.

La configuración es efectiva cuando el reloj local funciona como *Transparent Clock (TC)*. Para esto, seleccione en el cuadro de diálogo *Time > PTP > Global* del campo *PTP mode* el valor `v2-transparent-clock`.

### Tabla

Port

Muestra el número de puerto.

PTP enable

Activa/desactiva la transmisión de mensajes de sincronización *PTP* en el puerto.

Valores posibles:

- `marked` (configuración por defecto)
  La transmisión está activa.
  El puerto reenvía y recibe mensajes de sincronización *PTP*.
- `unmarked`
  La transmisión está inactiva.
  El puerto bloquea los mensajes de sincronización *PTP*.

P2P delay interval [s]

Especifica en segundos el intervalo tras el que el puerto mide el retardo Peer-to-Peer.

Como requisito previo debe haber especificado el valor `p2p` en este puerto y en el puerto del terminal remoto. Consulte la lista de opciones *Delay mechanism* del cuadro de diálogo *Time > PTP > Transparent Clock > Global*.

Valores posibles:

- `1` (configuración por defecto)
- `2`
- `4`
- `8`
- `16`
- `32`

P2P delay

Muestra el retardo Peer-to-Peer medido de los mensajes de sincronización *PTP*.

Como requisito previo, debe seleccionar el botón de opción `p2p` en la lista de opciones *Delay mechanism*. Consulte el campo *Delay mechanism* del cuadro de diálogo *Time > PTP > Transparent Clock > Global*.

Asymmetry

Corrige el valor medido del retardo dañado por rutas de transmisión asimétricas.

Valores posibles:

- `-2000000000..2000000000` (configuración por defecto: `0`)

El valor representa la simetría del retardo en nanosegundos.

Un valor de retardo medido de y ns se corresponde con una asimetría de y × 2 ns.

El valor es positivo si el retardo desde el *PTP* maestro hasta el *PTP* esclavo es superior que en dirección opuesta.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## 2.4 802.1AS

[ Time > 802.1AS ]

El protocolo *802.1AS* es un procedimiento descrito en el estándar IEEE 802.1AS-2011 que define cómo sincronizar la hora con precisión entre dispositivos en la red. Cuando utiliza el protocolo *802.1AS* a través de Ethernet, puede considerar el protocolo como un perfil del estándar IEEE 1588-2008.

Con el *Best Master Clock Algorithm*, los dispositivos de la red determinan qué dispositivo tiene la hora más precisa. Los dispositivos utilizan el dispositivo con la hora más precisa como origen de hora de referencia (*Grandmaster*). Posteriormente, los dispositivos participantes se sincronizan a sí mismos con este origen de hora de referencia.

El protocolo *802.1AS* cuenta con las siguientes especificaciones:

- En el dispositivo, la función *802.1AS* o *PTP* pueden activarse.
- Si las funciones *SNTP* y *802.1AS* están activadas en el dispositivo al mismo tiempo, la función *802.1AS* tendrá prioridad.
- La función *802.1AS* solo admite un dominio.

El menú contiene los siguientes cuadros de diálogo:

- 802.1AS Global
- 802.1AS Port
- 802.1AS Statistics

# 2.4.1 802.1AS Global

[ Time > 802.1AS > Global ]

En este cuadro de diálogo , especifique la configuración básica para el protocolo *802.1AS*.

### Operation

Operation

Activa/desactiva la función *802.1AS*.

Valores posibles:

- *On*
  La función *802.1AS* está activada.
  El dispositivo sincroniza su reloj utilizando el protocolo *802.1AS*.
  Considere activar el protocolo *802.1AS* en los puertos individuales.

- *Off* (configuración por defecto)
  La función *802.1AS* está desactivada.

### Configuration

Priority 1

Especifica *priority 1* para el dispositivo.

Valores posibles:

- `0..255` (configuración por defecto: `246`)

El *Best Master Clock Algorithm* evalúa en primer lugar *priority 1* entre los dispositivos participantes para determinar el origen de la hora de referencia (*Grandmaster*).

Cuanto más bajo establezca este valor, más probabilidades hay de que el dispositivo se designe como el origen de hora de referencia (*Grandmaster*).

Si especifica el valor `255`, el dispositivo no se designará como origen de hora de referencia (*Grandmaster*). Consulte el cuadro *Grandmaster*.

Priority 2

Especifica *priority 2* para el dispositivo.

Valores posibles:

- `0..255` (configuración por defecto: `248`)

Si los criterios evaluados anteriormente son los mismos para varios dispositivos, el *Best Master Clock Algorithm* evalúa *priority 2* de los dispositivos participantes.

Cuanto más bajo establezca este valor, más probabilidades hay de que el dispositivo se designe como el origen de hora de referencia (*Grandmaster*). Consulte el cuadro *Grandmaster*.

Sync lower bound [ns]

Especifica el valor límite inferior en nanosegundos para la diferencia de hora medida entre el reloj local y el origen de la hora de referencia (*Grandmaster*). Si la diferencia de hora medida cae por debajo de este valor una vez, el reloj local se clasifica como sincronizado.

Valores posibles:

- `0..999999999` (configuración por defecto: `30`)

Sync upper bound [ns]

Especifica el valor límite superior en nanosegundos para la diferencia de hora medida entre el reloj local y el origen de la hora de referencia (*Grandmaster*). Si la diferencia de hora medida supera este valor una vez, el reloj local se clasifica como no sincronizado.

Valores posibles:

- `31..1000000000` (configuración por defecto: `5000`)

UTC offset [s]

Muestra la diferencia entre la escala de tiempo *802.1AS* y UTC.

UTC offset valid

Muestra si el valor mostrado en el campo *UTC offset [s]* es correcto.

Valores posibles:

- `marked`
- `unmarked`

### Status

Offset to master [ns]

Muestra la diferencia medida (desviación) entre el reloj local y el origen de hora de referencia (*Grandmaster*) en nanosegundos. El dispositivo calcula la diferencia respecto a la información de hora recibida.

Max. offset absolute [ns]

Muestra la diferencia de hora medida máxima en nanosegundos producida desde la sincronización del reloj local con el origen de hora de referencia (*Grandmaster*).

Is synchronized

Muestra si el reloj local está sincronizado con el origen de hora de referencia (*Grandmaster*).

Si la diferencia de hora medida entre el reloj local y el origen de hora de referencia (*Grandmaster*) cae por debajo del umbral inferior de sincronización, se sincronizará el reloj local. Este estado se mantiene hasta que la diferencia de hora medida supera el límite superior de sincronización.

Especifique los límites de sincronización en el cuadro *Configuration*.

Steps removed

Muestra el número de rutas de comunicación pasadas entre el reloj local del dispositivo y el origen de hora de referencia (*Grandmaster*).

Para un *802.1AS* esclavo, el valor `1` significa que el reloj está conectado con el origen de hora de referencia (*Grandmaster*) directamente a través de 1 ruta de comunicación.

Clock identity

Muestra el número de identificación del reloj del dispositivo.

El dispositivo muestra el número de identificación como secuencias de bytes en notación hexadecimal.

El número de identificación del dispositivo de la dirección MAC de este, con los valores `ff` y `fe` añadidos entre byte 3 y byte 4.

### Grandmaster

Este cuadro muestra los criterios que utiliza el *Best Master Clock Algorithm* al evaluar el origen de la hora de referencia (*Grandmaster*).

En primer lugar el algoritmo evalúa la *priority 1* de los dispositivos participantes. El dispositivo con el valor más bajo de *priority 1* se designará como origen de hora de referencia (*Grandmaster*). Si el valor es el mismo para varios dispositivos, el algoritmo toma el siguiente criterio y, cuando este también coincide, el algoritmo toma el siguiente criterio a este. Cuando todos los valores coinciden para varios dispositivos, el valor más bajo del campo *Clock identity* decide qué dispositivo se designa como origen de hora de referencia (*Grandmaster*).

El dispositivo le permite tener influencia sobre qué dispositivo de la red se designa como origen de hora de referencia (*Grandmaster*). Para ello, modifique el valor en el campo *Priority 1* o *Priority 2* en el cuadro *Configuration*.

Priority 1

Muestra *priority 1* para el dispositivo que actualmente es el origen de hora de referencia (*Grandmaster*).

Clock class

Muestra la clase de origen de hora de referencia (*Grandmaster*). Parámetro del *Best Master Clock Algorithm*.

Clock accuracy

Muestra la precisión estimada del origen de hora de referencia (*Grandmaster*). Parámetro del *Best Master Clock Algorithm*.

Clock variance

Muestra la desviación del origen de hora de referencia (*Grandmaster*), también denominada *variación de registro escalado de desviación*. Parámetro del *Best Master Clock Algorithm*.

Priority 2

Muestra *priority 2* para el dispositivo que actualmente es el origen de hora de referencia (*Grandmaster*).

Clock identity

Muestra el número de identificación del dispositivo de origen de hora de referencia (*Grandmaster*). El dispositivo muestra el número de identificación como secuencias de bytes en notación hexadecimal.

### Parent

Clock identity

Muestra el número de identificación del puerto del dispositivo maestro directamente superior. El dispositivo muestra el número de identificación como secuencias de bytes en notación hexadecimal.

Port

Muestra el número de puerto del dispositivo maestro directamente superior.

Cumulative rate ratio [ppm]

Muestra la diferencia de frecuencia medida del reloj local en partes por millón relativas al origen de hora de referencia (*Grandmaster*).

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## 2.4.2 802.1AS Port

[ Time > 802.1AS > Port ]

En este cuadro de diálogo , especifique la configuración de *802.1AS* en cada puerto individual.

### Tabla

Port

Muestra el número de puerto.

Active

Activa/desactiva el protocolo *802.1AS* en el puerto.

Valores posibles:

- `marked` (configuración por defecto)
  El protocolo está activo en el puerto.
  En el puerto, el dispositivo sincroniza su reloj utilizando el protocolo *802.1AS*.
- `unmarked`
  El protocolo está inactivo en el puerto.

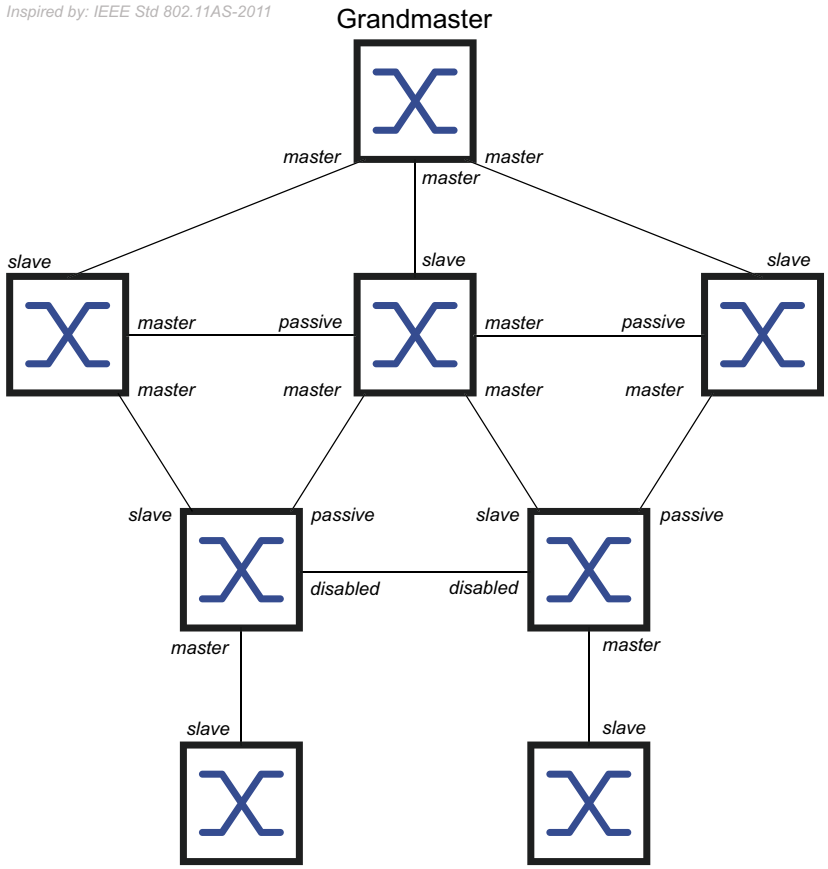
Role

Muestra el rol actual del puerto, considerando el protocolo *802.1AS*.

Valores posibles:

- *`disabled`*
  El puerto funciona en el rol *Disabled Port*. El puerto no es compatible con *802.1AS*.
- *`master`*
  El puerto funciona en el rol *Master Port*.

- `passive`
  El puerto funciona en el rol *Passive Port*.
- `slave`
  El puerto funciona en el rol *Slave Port*.




AS capable

Muestra si el protocolo *802.1AS* está activo en el puerto.

Valores posibles:

- `marked`
  El protocolo *802.1AS* está activo en el puerto. Los requisitos previos son:
  - El puerto mide un *Peer delay*, la casilla de verificación de la columna *Measuring delay* está marcada.
  - El valor de la columna *Peer delay [ns]* es inferior al valor de la columna *Peer delay threshold [ns]*.
- `unmarked`
  El protocolo *802.1AS* está inactivo en el puerto.

Announce interval [s]

Especifica en segundos el intervalo con el que el puerto (en el rol de *Master Port*) transmite mensajes *Announce* para la detección de la topología *802.1AS*.

Valores posibles:

- `1..2` (configuración por defecto: `1`)
  Asigne el mismo valor a cada dispositivo de un dominio *802.1AS*.
- `-`
  El puerto no transmite mensajes *Announce*.

Announce timeout

Especifica el número de *Announce interval [s]* en el que el puerto (en el rol de *Slave Port*) espera mensajes *Announce*.

Cuando transcurre el número de intervalos sin recibir un mensaje *Announce*, el dispositivo intenta encontrar una ruta nueva al origen de hora de referencia mediante el *Best Master Clock Algorithm*. Si el dispositivo encuentra un origen de hora de referencia (*Grandmaster*), le asigna el rol *Slave Port* al puerto a través del cual guía la nueva ruta. De lo contrario, el dispositivo se convierte en el origen de hora de referencia (*Grandmaster*) y le asigna el rol *Master Port* a sus puertos.

Ejemplo: con la configuración por defecto (*Announce interval [s]* = 1, *Announce timeout* = 3), el tiempo de espera es de 3 × 1 s = 3 s.

Valores posibles:

- 2..10 (configuración por defecto: 3)
  Asigne el mismo valor a cada puerto que pertenezca al mismo dominio *802.1AS*.

Sync interval [s]

Especifica en segundos el intervalo con el que el puerto (en el rol de *Master Port*) transmite mensajes *Sync* para la sincronización de la hora.

Valores posibles:

- 0.125 (configuración por defecto)
- 0.250
- 0.5
- 1
- –
  El puerto no transmite mensajes *Sync*.

Sync timeout

Especifica el número de *Sync interval [s]* en el que el puerto (en el rol de *Slave Port*) espera mensajes *Sync*.

Cuando transcurre el número de intervalos sin recibir un mensaje *Sync*, el dispositivo intenta encontrar una ruta nueva al origen de hora de referencia mediante el *Best Master Clock Algorithm*. Si el dispositivo encuentra un origen de hora de referencia (*Grandmaster*), le asigna el rol *Slave Port* al puerto a través del cual guía la nueva ruta. De lo contrario, el dispositivo se convierte en el origen de hora de referencia (*Grandmaster*) y le asigna el rol *Master Port* a sus puertos.

Ejemplo: con la configuración por defecto (*Sync interval [s]* = 0.125, *Sync timeout* = 3), el tiempo de espera es de 3 × 0.125 s = 0.375 s.

Valores posibles:

- 2..10 (configuración por defecto: 3)
  Asigne el mismo valor a cada puerto que pertenezca al mismo dominio *802.1AS*.

Peer delay interval [s]

Especifica en segundos el intervalo con el que el puerto (en el rol de *Master Port*, *Passive Port* o *Slave Port*) transmite un mensaje *Peer delay request* para medir el *Peer delay*.

Valores posibles:

- `1` (configuración por defecto)
- `2`
- `4`
- `8`
- `-`
  El puerto no transmite mensajes *Peer delay request*.

Peer delay timeout

Especifica el número de *Peer delay interval [s]* en el que el puerto (en el rol *Master Port*, *Passive Port* o *Slave Port*) espera mensajes *Delay response*.

Cuando transcurre el número de intervalos sin recibir un mensaje *Delay response*, el dispositivo asigna el rol *Disabled Port* al puerto. El puerto ya no es compatible con *802.1AS*.

Valores posibles:

- `2..10` (configuración por defecto: `3`)

Peer delay threshold [ns]

Especifica el valor límite superior de *Peer delay* en nanosegundos. Si el valor de la columna *Peer delay [ns]* es superior a este valor, el dispositivo asigna el rol *Disabled Port* al puerto. El puerto ya no es compatible con *802.1AS*.

Valores posibles:

- `0..1000000000` (configuración por defecto: `10000`)

Measuring delay

Muestra si el puerto mide un *Peer delay*.

Valores posibles:

- `marked`
  El puerto mide un *Peer delay*. El valor medido se encuentra en la columna *Peer delay [ns]*.
- `unmarked`
  El puerto no mide un *Peer delay*.

Peer delay [ns]

Muestra el valor de *Peer delay* en nanosegundos. Como requisito previo, la casilla de verificación de la columna *Measuring delay* debe estar marcada.

Neighbor rate ratio [ppm]

Muestra la diferencia de frecuencia medida del reloj local en partes por millón relativas al reloj en el dispositivo adyacente.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## 2.4.3 802.1AS Statistics

[ Time > 802.1AS > Statistics ]

Este cuadro de diálogo muestra información acerca del número de mensajes recibidos, enviados o descartados en los puertos. El cuadro de diálogo muestra contadores que van aumentando cada vez que se produce un evento de tiempo de espera.

### Tabla

Port

Muestra el número de puerto.

Received messages

Muestra los contadores de mensajes recibidos en los puertos:

Sync messages

Muestra el número de mensajes *Sync*.

Sync follow-up messages

Muestra el número de mensajes *Sync follow-up*.

Delay request messages

Muestra el número de mensajes *Peer delay request*.

Delay response messages

Muestra el número de mensajes *Peer delay response*.

Delay response follow-up messages

Muestra el número de mensajes *Peer delay response follow-up*.

Announce messages

Muestra el número de mensajes *Announce*.

Discarded messages

Muestra el número de mensajes *Sync* descartados por el dispositivo en este puerto. El dispositivo descarta un mensaje *Sync* por ejemplo, en casos en los que el puerto no recibe un mensaje *Sync follow-up* para un mensaje *Sync* correspondiente.

Sync timeout

Muestra el número de veces que se ha producido un evento *Sync timeout* en el puerto. Consulte la columna *Sync timeout* del cuadro de diálogo *Time > 802.1AS > Port*.

Announce timeout

Muestra el número de veces que se ha producido un evento *Announce timeout* en este puerto. Consulte la columna *Announce timeout* del cuadro de diálogo *Time > 802.1AS > Port*.

Delay timeout

Muestra el número de veces que se produjo un evento *Peer delay timeout* en este puerto. Consulte la columna *Peer delay timeout* del cuadro de diálogo *Time > 802.1AS > Port*.

Transmitted messages

Muestra los contadores de mensajes transmitidos en los puertos:

Sync messages

Muestra el número de mensajes *Sync*.

Sync follow-up messages

Muestra el número de mensajes *Sync follow-up*.

Delay request messages

Muestra el número de mensajes *Peer delay request*.

Delay response messages

Muestra el número de mensajes *Peer delay response*.

Delay response follow-up messages

Muestra el número de mensajes *Peer delay response follow-up*.

Announce messages

Muestra el número de mensajes *Announce*.

## Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

# 3 Device Security

El menú contiene los siguientes cuadros de diálogo:
- User Management
- Authentication List
- LDAP
- Management Access
- Pre-login Banner

## 3.1 User Management

[Device Security > User Management]

Si el usuario inicia sesión con datos de acceso válidos, el dispositivo le permitirá tener acceso a sus funciones de gestión.

En este cuadro de diálogo puede administrar la gestión de usuarios locales. También puede especificar los siguientes ajustes aquí:
- Configuración para el inicio de sesión
- Configuración para el almacenamiento de contraseñas
- Especificar la política para contraseñas válidas

Puede especificar los métodos que el dispositivo utiliza para la autenticación en el cuadro de diálogo *Device Security > Authentication List*.

### Configuration

Este cuadro le permite especificar la configuración para el inicio de sesión.

Login attempts

Especifica el número de intentos de inicio de sesión posibles cuando el usuario accede a la gestión del dispositivo mediante la interfaz gráfica de usuario y la interfaz de línea de comando.

**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.

Valores posibles:
- `0..5` (configuración por defecto: `0`)

Si el usuario hace un intento fallido más de iniciar sesión, el dispositivo bloqueará el acceso al usuario.

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

El valor `0` desactiva el bloqueo. El usuario tiene un número ilimitado de intentos para iniciar sesión.

Login attempts period (min.)

Muestra el período de tiempo hasta que el dispositivo reinicie el contador en el campo *Login attempts*.

Valores posibles:

- `0..60` (configuración por defecto: `0`)

Min. password length

El dispositivo acepta la contraseña si contiene al menos el número de caracteres especificado aquí.

El dispositivo comprueba la contraseña según este ajuste, independientemente de la configuración de la casilla *Policy check*.

Valores posibles:

- `1..64` (configuración por defecto: `6`)

### Password policy

Este cuadro le permite especificar la política para una contraseña válida. El dispositivo comprueba cada nueva contraseña y cambio de contraseña según esta política.

Los cambios afectan a la columna *Password*. El requisito previo es que marque la casilla de la columna *Policy check*.

Upper-case characters (min.)

El dispositivo acepta la contraseña si contiene al menos el número de letras mayúsculas especificado aquí.

Valores posibles:

- `0..16` (configuración por defecto: `1`)

El valor `0` desactiva este ajuste.

Lower-case characters (min.)

El dispositivo acepta la contraseña si contiene al menos el número de letras minúsculas especificado aquí.

Valores posibles:

- `0..16` (configuración por defecto: `1`)

El valor `0` desactiva este ajuste.

Digits (min.)

El dispositivo acepta la contraseña si contiene al menos la cantidad de números especificada aquí.

Valores posibles:

- `0..16` (configuración por defecto: `1`)

El valor `0` desactiva este ajuste.

Special characters (min.)

El dispositivo acepta la contraseña si contiene al menos el número de caracteres especiales especificado aquí.

Valores posibles:

- `0..16` (configuración por defecto: `1`)

El valor `0` desactiva este ajuste.

### Tabla

Cada usuario necesita una cuenta de usuario activa para tener acceso a la gestión del dispositivo. La tabla le permite crear y gestionar cuentas de usuario.

Para cambiar la configuración, haga clic en el parámetro deseado en la tabla y modifique su valor.

User name

Muestra el nombre de la cuenta de usuario.

Para crear una nueva cuenta de usuario, haga clic en el botón  .

Active

Activa/desactiva la cuenta de usuario.

Valores posibles:

- `marked`
  La cuenta de usuario está activa. El dispositivo acepta el inicio de sesión de un usuario con este nombre de usuario.
- `unmarked` (configuración por defecto)
  La cuenta de usuario está inactiva. El dispositivo rechaza el inicio de sesión de un usuario con este nombre de usuario.

Cuando existe una cuenta de usuario con el rol de acceso *`administrator`*, esta cuenta de usuario estará constantemente activa.

Password

Especifica la contraseña que el usuario utiliza para acceder a la gestión del dispositivo mediante la interfaz gráfica de usuario o la interfaz de línea de comando.

Muestra ***** (asteriscos) en lugar de la contraseña con la que el usuario va a iniciar sesión. Para cambiar una contraseña, haga clic en el campo correspondiente.

Cuando especifique la contraseña por primera vez, el dispositivo utilizará la misma contraseña en las columnas *SNMP auth password* y *SNMP encryption password*.

- El dispositivo le permite especificar contraseñas diferentes en las columnas *SNMP auth password* y *SNMP encryption password*.
- Si cambia la contraseña en la columna actual, el dispositivo también cambiará las contraseñas para las columnas *SNMP auth password* y *SNMP encryption password*, pero solo si no se han especificado anteriormente de forma individual.

Valores posibles:

- Cadena de caracteres ASCII alfanuméricos con entre 6 y 64 caracteres
  Solo se permiten los siguientes caracteres:
  - `a..z`
  - `A..Z`
  - `0..9`
  - `!#$%&'()*+,-./:;<=>?@[\]^_`{}~`

La longitud mínima de la contraseña se especifica en el cuadro *Configuration*. El dispositivo distingue entre mayúsculas y minúsculas.

Si la casilla en la columna *Policy check* aparece marcada, el dispositivo comprueba la contraseña conforme a la política especificada en el cuadro *Password policy*.

El dispositivo comprueba constantemente la longitud mínima de la contraseña, incluso aunque la casilla de la columna *Policy check* aparezca como `unmarked`.

Role

Especifica el rol del usuario que regula el acceso del usuario a las funciones individuales del dispositivo.

Valores posibles:

- *unauthorized*
  El usuario está bloqueado y el dispositivo rechaza su inicio de sesión.
  Asigne este valor para bloquear temporalmente la cuenta de usuario. Si el dispositivo detecta un error al asignar otra función, el dispositivo asignará esta función a la cuenta de usuario.
- *guest* (configuración por defecto)
  El usuario tiene autorización para supervisar el dispositivo.
- *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*.
- *operator*
  El usuario tiene autorización para supervisar el dispositivo y cambiar la configuración, a excepción de los ajustes de seguridad para el acceso al dispositivo.
- *administrator*
  El usuario tiene autorización para supervisar el dispositivo y cambiar la configuración.

El dispositivo asigna a una función de usuario el Tipo de servicio transferido en respuesta a un servidor RADIUS de la siguiente manera:

- `Administrative-User`: *administrator*
- `Login-User`: *operator*
- `NAS-Prompt-User`: *guest*

User locked

Desbloquea la cuenta de usuario.

Valores posibles:

- `marked`
  La cuenta de usuario está bloqueada. El usuario no tiene acceso a la gestión del dispositivo. Si el usuario hace demasiados intentos fallidos de iniciar sesión, el dispositivo bloqueará automáticamente al usuario.
- `unmarked` (sombreado) (configuración por defecto)
  La cuenta de usuario está desbloqueada. El usuario tiene acceso a la gestión del dispositivo.

Policy check

Activa/desactiva la comprobación de la contraseña.

Valores posibles:

- `marked`
  La comprobación de la contraseña está activa.
  Al crear o cambiar la contraseña, el dispositivo comprueba la contraseña conforme a la política especificada en el cuadro *Password policy*.
- `unmarked` (configuración por defecto)
  La comprobación de la contraseña está desactivada.

SNMP auth type

Especifica el protocolo de autenticación que el dispositivo aplicará para el acceso de usuario mediante SNMPv3.

Valores posibles:

- *hmacmd5* (valor por defecto)
  Para esta cuenta de usuario, el dispositivo utiliza el protocolo HMACMD5.
- *hmacsha*
  Para esta cuenta de usuario, el dispositivo utiliza el protocolo HMACSHA

SNMP auth password

Especifica la contraseña que el dispositivo aplicará para el acceso de usuario mediante SNMPv3.

Muestra ***** (asteriscos) en lugar de la contraseña con la que el usuario va a iniciar sesión. Para cambiar una contraseña, haga clic en el campo correspondiente.

Por defecto, el dispositivo utiliza la misma contraseña que especifique en la columna *Password*.

- Para la columna actual, el dispositivo le permite especificar una contraseña distinta de la contraseña en la columna *Password*.
- Si cambia la contraseña en la columna *Password*, el dispositivo también cambiará la contraseña para la columna actual, pero solo si no se ha especificado de forma individual.

Valores posibles:

- Cadena de caracteres ASCII alfanuméricos con entre 6 y 64 caracteres
  Solo se permiten los siguientes caracteres:
  - `a..z`
  - `A..Z`
  - `0..9`
  - `!#$%&'()*+,-./:;<=>?@[\]^_`{}~`

SNMP encryption type

Especifica el protocolo de encriptación que el dispositivo aplicará para el acceso de usuario mediante SNMPv3.

Valores posibles:

- `none`
  Sin encriptación.
- `des` (valor por defecto)
  Encriptación DES
- `aesCfb128`
  Encriptación AES128

SNMP encryption password

Especifica la contraseña que el dispositivo aplicará para encriptar el acceso de usuario mediante SNMPv3.

Muestra ***** (asteriscos) en lugar de la contraseña con la que el usuario va a iniciar sesión. Para cambiar una contraseña, haga clic en el campo correspondiente.

Por defecto, el dispositivo utiliza la misma contraseña que especifique en la columna *Password*.

- Para la columna actual, el dispositivo le permite especificar una contraseña distinta de la contraseña en la columna *Password*.
- Si cambia la contraseña en la columna *Password*, el dispositivo también cambiará la contraseña para la columna actual, pero solo si no se ha especificado de forma individual.

Valores posibles:

- Cadena de caracteres ASCII alfanuméricos con entre 6 y 64 caracteres
  Solo se permiten los siguientes caracteres:
  - `a..z`
  - `A..Z`
  - `0..9`
  - `!#$%&'()*+,-./:;<=>?@[\]^_`{}~`

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

Abre la ventana *Create* para añadir una entrada nueva a la tabla.

- En el campo *User name*, especifique el nombre de la cuenta de usuario.
  Valores posibles:
  - Cadena de caracteres ASCII alfanuméricos con entre 1 y 32 caracteres

# 3.2 Authentication List

[ Device Security > Authentication List ]

En este cuadro de diálogo, administre las listas de autenticación. En la lista de autenticación, puede especificar el método que el dispositivo utiliza para la autenticación. También tiene la opción de asignar aplicaciones predefinidas a las listas de autenticación.

Si el usuario inicia sesión con datos de acceso válidos, el dispositivo le permitirá tener acceso a sus funciones de gestión. El dispositivo autentica a los usuarios mediante los siguientes métodos:
- Gestión del dispositivo por parte del usuario
- LDAP
- RADIUS

Mediante el control de acceso basado en puerto conforme al estándar IEEE 802.1X., si los dispositivos terminales conectados inician sesión con datos de acceso válidos, el dispositivo les permitirá tener acceso a la red. El dispositivo autentica los dispositivos terminales mediante los siguientes métodos:
- RADIUS
- IAS (Servidor de autenticación integrada)

En la configuración por defecto, se encuentran disponibles las siguientes listas de autenticación
- `defaultDot1x8021AuthList`
- `defaultLoginAuthList`
- `defaultV24AuthList`

### Tabla

**Nota:** Si la tabla no contiene una lista, el acceso a la gestión del dispositivo solo será posible utilizando la interfaz de línea de comando a través de la interfaz serie del dispositivo. En este caso, el dispositivo autentica a los usuarios mediante la gestión local de usuarios. Consulte el cuadro de diálogo *Device Security > User Management*.

Name

Muestra el nombre de la lista.

Para crear una nueva lista, haga clic en el botón  .

Valores posibles:
- Cadena de caracteres ASCII alfanuméricos con entre 1 y 32 caracteres

Policy 1
Policy 2
Policy 3
Policy 4
Policy 5

Especifica la política de autenticación que el dispositivo utilizará para el acceso mediante la aplicación especificada en la columna *Dedicated applications*.

El dispositivo le brinda la posibilidad de recurrir a una solución alternativa. Para ello, especifique una política diferente en cada campo de política. Si la autenticación con la política especificada no es correcta, el dispositivo podrá utilizar la siguiente política, en función del orden de los valores introducidos en cada política.

Valores posibles:

- `local` (configuración por defecto)
  El dispositivo autentica a los usuarios mediante la gestión local de usuarios. Consulte el cuadro de diálogo *Device Security > User Management*.
  No puede asignar este valor a la lista de autenticación `defaultDot1x8021AuthList`.
- `radius`
  El dispositivo autentica a los usuarios mediante un servidor RADIUS en la red. Especifique el servidor RADIUS en el cuadro de diálogo *Network Security > RADIUS > Authentication Server*.
- `reject`
  El dispositivo aceptará o rechazará la autenticación según la política que pruebe primero. La lista siguiente contiene casos de autenticación:
  - Si la primera política en la lista de autenticación es `local` y el dispositivo acepta las credenciales de inicio de sesión, se iniciará la sesión del usuario sin probar otras políticas.
  - Si la primera política en la lista de autenticación es `local` y el dispositivo rechaza las credenciales de inicio de sesión, este intentará iniciar la sesión del usuario mediante otras políticas en el orden especificado.
  - Si la primera política en la lista de autenticación es `radius` or `ldap` y el dispositivo acepta las credenciales de inicio de sesión, se iniciará la sesión del usuario sin probar otras políticas.
    Si no hay respuesta del servidor RADIUS o LDAP, el dispositivo intentará autenticar al usuario con la siguiente política.
  - Si la primera política en la lista de autenticación es `reject`, el dispositivo rechazará inmediatamente el inicio de sesión del usuario sin probar otra política.
  - Compruebe que la lista de autenticación `defaultV24AuthList` contiene al menos una política diferente a `reject`.
- `ias`
  El dispositivo autentica el inicio de sesión de los dispositivos terminales mediante 802.1X con el servidor de autenticación integrado (IAS). El servidor de autenticación integrado gestiona los datos de inicio de sesión en una base de datos independiente. Consulte el cuadro de diálogo *Network Security > 802.1X Port Authentication > Integrated Authentication Server*.
  Solo puede asignar este valor a la lista de autenticación `defaultDot1x8021AuthList`.
- `ldap`
  El dispositivo autentica a los usuarios mediante datos de autenticación y un rol de acceso guardado en una ubicación central. Especifique el servidor de Active Directory que el dispositivo supervisará en el cuadro de diálogo *Network Security > LDAP > Configuration*.

Dedicated applications

Muestra las aplicaciones dedicadas. Cuando los usuarios acceden al dispositivo con la aplicación correspondiente, el dispositivo utiliza las políticas especificadas para la autenticación.

Para asignar otra aplicación a la lista o eliminar la asignación, haga clic en el botón  y, a continuación, en el elemento *Allocate applications*. El dispositivo le permite asignar cada aplicación a una sola lista.

Active

Activa/desactiva la lista.

Valores posibles:

- `marked`
  La lista está activada. El dispositivo utiliza las políticas de esta lista cuando los usuarios acceden al dispositivo con la aplicación correspondiente.
- `unmarked` (configuración por defecto)
  La lista está desactivada.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

Allocate applications

Abre la ventana *Allocate applications*.

- El campo izquierdo muestra las aplicaciones que se pueden asignar a la lista señalada.
- El campo derecho muestra las aplicaciones que se han asignado a la lista señalada.
- Botones:
  - Mueve todas las entradas al campo derecho.
  - Mueve las entradas señaladas del campo izquierdo al campo derecho.
  - Mueve las entradas señaladas del campo derecho al campo izquierdo.
  - Mueve todas las entradas al campo izquierdo.

**Nota:** Si mueve la entrada `WebInterface` al campo izquierdo, se pierde la conexión con el dispositivo y después haga clic en el botón *Ok*.

## 3.3 LDAP

[ Device Security > LDAP ]

El Lightweight Directory Access Protocol (LDAP) le permite autenticar y autorizar los usuarios en un punto central de la red. Un servicio de directorio ampliamente utilizado a través del LDAP es Active Directory®.

El dispositivo desvía los datos de inicio de sesión del usuario al servidor de autenticación mediante el protocolo LDAP. El servidor de autenticación decide si los datos de acceso son válidos y transfiere las autorizaciones del usuario al dispositivo.

Tras iniciar sesión correctamente, el dispositivo guarda los datos de inicio de sesión temporalmente en la caché. Esto acelera el proceso de inicio de sesión cuando los usuarios inician sesión de nuevo. En este caso, no es necesario realizar ninguna operación de búsqueda de LDAP compleja.

El menú contiene los siguientes cuadros de diálogo:

- LDAP Configuration
- LDAP Role Mapping

# 3.3.1 LDAP Configuration

[Device Security > LDAP > Configuration]

Este cuadro de diálogo le permite hasta 4 servidores de autenticación. Un servidor de autenticación autentica y autoriza a los usuarios cuando el dispositivo reenvía los datos de acceso al servidor.

El dispositivo envía los datos de acceso al primer servidor de autenticación. Si no se recibe respuesta de este servidor, el dispositivo se dirige al siguiente servidor de la tabla.

### Operation

Operation

Activa/desactiva el cliente *LDAP*.

Si en el cuadro de diálogo *Device Security > Authentication List* especifica el valor `ldap` en una de las filas *Policy 1* en *Policy 5*, el dispositivo utiliza el cliente *LDAP*. Antes de esto, especifique en el cuadro de diálogo *Device Security > LDAP > Role Mapping* al menos una asignación para este rol *`administrator`*. Esto le proporciona acceso al dispositivo como administrador después de iniciar sesión a través de LDAP.

Valores posibles:

- *`On`*
  El cliente *LDAP* se activa.
- *`Off`* (configuración por defecto)
  El cliente *LDAP* se desactiva.

### Configuration

Client cache timeout [min]

Especifica durante cuántos minutos después de iniciar sesión correctamente continúan siendo válidos los datos de acceso de un usuario. Si un usuario inicia sesión de nuevo durante este período, no deberá realizarse ninguna operación de búsqueda LDAP compleja. El proceso de inicio de sesión es mucho más rápido.

Valores posibles:

- `1..1440` (configuración por defecto: `10`)

Bind user

Especifica el ID de usuario en forma de "Nombre distintivo" (DN) con el que el dispositivo inicia sesión en el servidor LDAP.

Si el servidor LDAP requiere un ID de usuario en forma de "Nombre distintivo" (DN) para el inicio de sesión, esta información será necesaria. En entornos de Active Directory, esta información es innecesaria.

El dispositivo inicia sesión en el servidor LDAP con el ID de usuario para encontrar el "Nombre distintivo" (DN) para los usuarios que inician sesión. El dispositivo realiza la búsqueda conforme a la configuración de los campos *Base DN* y *User name attribute*.

Valores posibles:

- Cadena de caracteres ASCII alfanuméricos con entre 0 y 64 caracteres

Bind user password

Especifica la contraseña que utiliza el dispositivo junto con el ID de usuario especificado en el campo *Bind user* al iniciar sesión en el servidor LDAP.

Valores posibles:

- Cadena de caracteres ASCII alfanuméricos con entre 0 y 64 caracteres

Base DN

Especifica el punto de partida de la búsqueda en el árbol del directorio en forma de "Nombre distintivo" (DN).

Valores posibles:

- Cadena de caracteres ASCII alfanuméricos con entre 0 y 255 caracteres

User name attribute

Especifica el atributo LDAP que contiene un nombre de usuario biúnico. Posteriormente, el usuario utiliza el nombre de usuario contenido en este atributo para iniciar sesión.

A menudo los atributos LDAP `userPrincipalName`, `mail`, `sAMAccountName` y `uid` contienen un nombre de usuario único.

El dispositivo añade la cadena de caracteres especificada en el campo *Default domain* al nombre de usuario bajo la siguiente condición:

- El nombre de usuario contenido en el atributo no incluye el carácter @.
- En el campo *Default domain* se especifica un nombre de dominio.

Valores posibles:

- Cadena de caracteres ASCII alfanuméricos con entre 0 y 64 caracteres (configuración por defecto: `userPrincipalName`)

Default domain

Especifica la cadena de caracteres que añade el dispositivo al nombre de usuario de los usuarios que inician sesión si el nombre de usuario no contiene el carácter @.

Valores posibles:

- Cadena de caracteres ASCII alfanuméricos con entre 0 y 64 caracteres

## CA certificate

URL

Especifica la ruta y el nombre de archivo del certificado.

El dispositivo acepta certificados con las siguientes propiedades:

- Formato X.509
- Extensión de nombre de archivo `.PEM`
- Codificación con Base64, acompañado por
  `-----BEGIN CERTIFICATE-----`
  y
  `-----END CERTIFICATE-----`

Por motivos de seguridad, es recomendable utilizar constantemente un certificado firmado por una autoridad de certificación.

El dispositivo le ofrece las opciones siguientes para copiar el certificado al dispositivo:

- Importar desde el PC
  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.
- Importar desde un servidor FTP
  Cuando el certificado se encuentre en un servidor FTP, especifique la URL correspondiente al archivo en el formato siguiente:
  `ftp://<usuario>:<contraseña>@<dirección IP>:<puerto>/<ruta>/<nombre archivo>`
- Importar desde un servidor TFTP
  Cuando el certificado se encuentre en un servidor TFTP, especifique la URL correspondiente al archivo en el formato siguiente:
  `tftp://<dirección IP>/<ruta>/<nombre archivo>`
- Importar desde un servidor SCP o SFTP
  Cuando el certificado se encuentre en un servidor SCP o SFTP, especifique la URL correspondiente al archivo en el formato siguiente:
  - `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://<user>:<password>@<IP address>/<path>/<file name>`

Start

Copia el certificado especificado en el campo *URL* del dispositivo.

### Tabla

Index

Muestra el número de índice al que la entrada de la tabla hace referencia.

Description

Especifica la descripción.

Tiene la opción de describir aquí el servidor de autenticación o anotar información adicional.

Valores posibles:

- Cadena de caracteres ASCII alfanuméricos con entre 0 y 255 caracteres

Address

Especifica la dirección IP o el nombre de DNS del servidor.

Valores posibles:

- Dirección IPv4 (configuración por defecto: `0.0.0.0`)
- Dirección IPv6
- Nombre de DNS en formato `<domain>.<tld>` o `<host>.<domain>.<tld>`
- `_ldap._tcp.<domain>.<tld>`
  Utilizando este nombre de DNS, el dispositivo consulta la lista de servidores LDAP (registro de recursos SRV) del servidor DNS.

Si en la fila *Connection security* se especifica un valor distinto de *none* y el certificado solamente contiene nombres de DNS del servidor, utilice un nombre de DNS. Active la función *Client* en el cuadro de diálogo *Advanced > DNS > Client > Global*.

Destination TCP port

Especifica el puerto TCP en el que el servidor espera las solicitudes.

Si ha especificado el valor `_ldap._tcp.domain.tld` en la columna *Address*, el dispositivo ignora este valor.

Valores posibles:

- `0..65535` (configuración por defecto: `389`)
  Excepción: el puerto `2222` está reservado para funciones internas.

Puertos TCP utilizados con frecuencia:

- `LDAP: 389`
- `LDAP over SSL: 636`
- `Active Directory Global Catalogue: 3268`
- `Active Directory Global Catalogue SSL: 3269`

Connection security

Especifica el protocolo que encripta la comunicación entre el dispositivo y el servidor de autenticación.

Valores posibles:

- *none*
  Sin encriptación.
  El dispositivo establece una conexión LDAP con el servidor y transmite la comunicación, incluidas las contraseñas, en texto no cifrado.
- *ssl*
  Encriptación con SSL.
  El dispositivo establece una conexión TLS con el servidor y transmite la comunicación LDAP sobre ella.
- *startTLS* (configuración por defecto)
  Encriptación con extensión startTLS.
  El dispositivo establece una conexión LDAP con el servidor y encripta la comunicación.

El requisito previo de la comunicación encriptada es que el dispositivo utilice la hora correcta. Si el certificado solo contiene los nombres de DNS, especifique el nombre de DNS del servidor en la fila *Address*. Active la función *Client* en el cuadro de diálogo *Advanced > DNS > Client > Global*.

Si el certificado contiene la dirección IP del servidor en el campo "Nombre alternativo del sujeto", el dispositivo podrá verificar la identidad del servidor sin la configuración de DNS.

Server status

Muestra el estado de conexión y la autenticación con el servidor de autenticación.

Valores posibles:

- *ok*
  Se puede acceder al servidor.
  Si en la fila *Connection security* se especifica un valor distinto de *none*, el dispositivo ha verificado el certificado del servidor.
- *unreachable*
  No se puede acceder al servidor.
- *other*
  El dispositivo todavía no ha establecido una conexión con el servidor.

Active

Activa/desactiva el uso del servidor.

Valores posibles:

- marked
  El dispositivo utiliza el servidor.
- unmarked (configuración por defecto)
  El dispositivo no utiliza el servidor.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

Flush cache

Elimina los datos de inicio de sesión almacenados en la caché de los usuarios que han iniciado sesión correctamente.

## 3.3.2 LDAP Role Mapping

[Device Security > LDAP > Role Mapping]

Este cuadro de diálogo le permite crear hasta 64 asignaciones para asignar un rol a los usuarios.

En la tabla debe especificar si el dispositivo asigna un rol al usuario en función de un atributo con un valor específico o según la suscripción al grupo.
- El dispositivo busca el atributo y el valor del atributo en el objeto del usuario.
- Mediante la evaluación del "Nombre distintivo" (DN) contenido en los atributos de los miembros, el dispositivo comprueba la pertenencia al grupo.

Si un usuario inicia sesión, el dispositivo busca la siguiente información en el servidor LDAP:
- En el proyecto de usuario relacionado, el dispositivo busca los atributos especificados en las asignaciones.
- En los objetos de los grupos especificados en las asignaciones, el dispositivo busca los atributos de los miembros.

Basándose en ello, el dispositivo comprueba si hay alguna asignación.
- ¿Contiene el objeto del usuario el atributo requerido?
  o bien
- ¿Es el usuario miembro del grupo?

Si el dispositivo no encuentra una coincidencia, el usuario no obtiene acceso al dispositivo.

Si el dispositivo encuentra más de una asignación que se aplique a un usuario, el ajuste del campo *Matching policy* será el que decida. El usuario obtiene el rol con las autorizaciones más amplias o el primer rol de la tabla que se aplique.

### Configuration

Matching policy

Especifica qué rol aplica el dispositivo si se aplica más de una asignación a un usuario.

Valores posibles:
- `highest` (configuración por defecto)
  El dispositivo aplica el rol con autorizaciones más amplias.
- `first`
  El dispositivo aplica la regla con un menor valor en la columna *Index* al usuario.

### Tabla

Index

Muestra el número de índice al que la entrada de la tabla hace referencia.

Role

Especifica el rol del usuario que regula el acceso del usuario a las funciones individuales del dispositivo.

Valores posibles:

- `unauthorized`
  El usuario está bloqueado y el dispositivo rechaza su inicio de sesión.
  Asigne este valor para bloquear temporalmente la cuenta de usuario. Si se detecta un error durante la asignación de otro rol, el dispositivo asignará este rol a la cuenta de usuario.
- `guest` (configuración por defecto)
  El usuario tiene autorización para supervisar el dispositivo.
- `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*.
- `operator`
  El usuario tiene autorización para supervisar el dispositivo y cambiar la configuración, a excepción de los ajustes de seguridad para el acceso al dispositivo.
- `administrator`
  El usuario tiene autorización para supervisar el dispositivo y cambiar la configuración.

Type

Especifica si se ha establecido en la columna *Parameter* un grupo o un atributo con un valor de atributo.

Valores posibles:

- `attribute` (configuración por defecto)
  La columna *Parameter* contiene un atributo con un valor de atributo.
- `group`
  La columna *Parameter* contiene el "Nombre distintivo" (DN) de un grupo.

Parameter

Especifica un grupo o un atributo con un valor de atributo, en función del ajuste de la columna *Type*.

Valores posibles:

- Cadena de caracteres ASCII alfanuméricos con entre 0 y 255 caracteres
  El dispositivo distingue entre mayúsculas y minúsculas.
  - Si se ha especificado en la columna *Type* el valor `attribute`, especifique el atributo en forma de `Attribute_name=Attribute_value`.
    Por ejemplo: `l=Germany`
  - Si se ha especificado en la columna *Type* el valor `group`, especifique el "Nombre distintivo" (DN) de un grupo.
    Por ejemplo: `CN=admin-users,OU=Groups,DC=example,DC=com`

Active

Activa/desactiva la asignación de roles.

Valores posibles:

- `marked` (configuración por defecto)
  La asignación de roles está activa.
- `unmarked`
  La asignación de roles está inactiva.

**Botones**

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

Abre la ventana *Create* para añadir una entrada nueva a la tabla.

- En el campo *Index*, especifique el número de índice.
  Valores posibles:
  - `1..64`

## 3.4 Management Access

[ Device Security > Management Access ]

El menú contiene los siguientes cuadros de diálogo:

- Server
- IP Access Restriction
- Web
- Command Line Interface
- SNMPv1/v2 Community

## 3.4.1 Server

[Device Security > Management Access > Server]

Este cuadro de diálogo le permite configurar los servicios del servidor que permitan a usuarios y aplicaciones el acceso a las funciones de administración del dispositivo.

El cuadro de diálogo contiene las siguientes pestañas:
- [Information]
- [SNMP]
- [Telnet]
- [SSH]
- [HTTP]
- [HTTPS]

### [Information]

Esta pestaña muestra una vista general de los servicios del servidor que están activados.

#### Tabla

SNMPv1

Muestra si el servicio del servidor está activo o inactivo. Este autoriza el acceso al dispositivo mediante SNMP versión 1. Consulte la pestaña *SNMP*.

Valores posibles:
- `marked`
  El servicio del servidor está activo.
- `unmarked`
  El servicio del servidor está inactivo.

SNMPv2

Muestra si el servicio del servidor está activo o inactivo. Este autoriza el acceso al dispositivo mediante SNMP versión 2. Consulte la pestaña *SNMP*.

Valores posibles:
- `marked`
  El servicio del servidor está activo.
- `unmarked`
  El servicio del servidor está inactivo.

SNMPv3

Muestra si el servicio del servidor está activo o inactivo. Este autoriza el acceso al dispositivo mediante SNMP versión 3. Consulte la pestaña *SNMP*.

Valores posibles:

- `marked`
  El servicio del servidor está activo.
- `unmarked`
  El servicio del servidor está inactivo.

Telnet server

Muestra si el servicio del servidor está activo o inactivo. Este autoriza el acceso al dispositivo mediante Telnet. Consulte la pestaña *Telnet*.

Valores posibles:

- `marked`
  El servicio del servidor está activo.
- `unmarked`
  El servicio del servidor está inactivo.

SSH server

Muestra si el servicio del servidor está activo o inactivo. Este autoriza el acceso al dispositivo mediante Secure Shell. Consulte la pestaña *SSH*.

Valores posibles:

- `marked`
  El servicio del servidor está activo.
- `unmarked`
  El servicio del servidor está inactivo.

HTTP server

Muestra si el servicio del servidor está activo o inactivo. Este autoriza el acceso al dispositivo usando la interfaz gráfica de usuario mediante HTTP. Consulte la pestaña *HTTP*.

Valores posibles:

- `marked`
  El servicio del servidor está activo.
- `unmarked`
  El servicio del servidor está inactivo.

HTTPS server

Muestra si el servicio del servidor está activo o inactivo. Este autoriza el acceso al dispositivo usando la interfaz gráfica de usuario mediante HTTPS. Consulte la pestaña *HTTPS*.

Valores posibles:

- `marked`
  El servicio del servidor está activo.
- `unmarked`
  El servicio del servidor está inactivo.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## [SNMP]

Esta pestaña le permite especificar la configuración del agente SNMP del dispositivo y activar/desactivar el acceso al dispositivo con una versión de SNMP diferente.

El agente SNMP permite el acceso a la gestión del dispositivo con aplicaciones basadas en SNMP.

### Configuration

SNMPv1

Activa/desactiva el acceso al dispositivo con SNMP versión 1.

Valores posibles:

- `marked` (configuración por defecto)
  El acceso está activado.
- `unmarked`
  El acceso está desactivado.

Especifique los nombres de la comunidad en el cuadro de diálogo *Device Security > Management Access > SNMPv1/v2 Community*.

SNMPv2

Activa/desactiva el acceso al dispositivo con SNMP versión 2.

Valores posibles:

- `marked` (configuración por defecto)
  El acceso está activado.
- `unmarked`
  El acceso está desactivado.

Especifique los nombres de la comunidad en el cuadro de diálogo *Device Security > Management Access > SNMPv1/v2 Community*.

SNMPv3

Activa/desactiva el acceso al dispositivo con SNMP versión 3.

Valores posibles:

- `marked` (configuración por defecto)
  El acceso está activado.
- `unmarked`
  El acceso está desactivado.

Los sistemas de gestión de red como ConneXium Network Manager emplean este protocolo para comunicarse con el dispositivo.

UDP port

Especifica el número del puerto UDP en el que el agente SNMP recibe las solicitudes de los clientes.

Valores posibles:

- `1..65535` (configuración por defecto: `161`)
  Excepción: el puerto `2222` está reservado para funciones internas.

Para permitir al agente SNMP utilizar el nuevo puerto tras un cambio, proceda de la siguiente manera:

- ☐ Haga clic en el botón ✔.
- ☐ Seleccione el perfil de configuración activo en el cuadro de diálogo *Basic Settings > Load/Save*.
- ☐ Haga clic en el botón para guardar los cambios actuales.
- ☐ Reinicie el dispositivo.

SNMPover802

Activa/desactiva el acceso al dispositivo mediante SNMP a través del estándar IEEE-802.

Valores posibles:

- `marked`
  El acceso está activado.
- `unmarked` (configuración por defecto)
  El acceso está desactivado.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## [Telnet]

Esta pestaña le permite activar/desactivar el servidor Telnet en el dispositivo y especificar su configuración.

El servidor Telnet activa el acceso a la gestión del dispositivo de manera remota mediante la interfaz de línea de comando. Las conexiones Telnet no están encriptadas.

### Operation

Telnet server

Activa/desactiva el servidor Telnet.

Valores posibles:

- El servidor Telnet está activado.
  El acceso a la gestión del dispositivo es posible mediante la interfaz de línea de comando, usando una conexión Telnet sin encriptar.
- El servidor Telnet está desactivado.

**Nota:** Si se desactiva el servidor *SSH* y también el *Telnet*, el acceso a la interfaz de la línea de comandos solo será posible con la interfaz serie del dispositivo.

### Configuration

TCP port

Especifica el número del puerto TCP en el que el dispositivo recibe las solicitudes Telnet de los clientes.

Valores posibles:

- `1..65535` (configuración por defecto: `23`)
  Excepción: el puerto `2222` está reservado para funciones internas.

El servidor reinicia automáticamente después de cambiar el puerto. Las conexiones existentes se mantienen.

Connections

Muestra cuántas conexiones Telnet están establecidas en ese momento en el dispositivo.

Connections (max.)

Especifica el número máximo de conexiones Telnet al dispositivo que se pueden establecer simultáneamente.

Valores posibles:

- `1..5` (configuración por defecto: `5`)

Session timeout [min]

Especifica el tiempo de espera en minutos. Después de que el dispositivo haya estado inactivo durante este tiempo, se finaliza la sesión del usuario conectado.

Los cambios de este valor tendrán efecto la siguiente vez que un usuario inicie sesión.

Valores posibles:

- `0`
  Desactiva la función. La conexión continúa en caso de inactividad.
- `1..160` (configuración por defecto: `5`)

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## [SSH]

Esta pestaña le permite activar/desactivar el servidor SSH en el dispositivo y especificar la configuración necesaria para SSH. El servidor funciona con la versión 2 de SSH.

El servidor SSH activa el acceso a la gestión del dispositivo de manera remota mediante la interfaz de línea de comando. Las conexiones SSH están encriptadas.

El servidor SSH se identifica ante los clientes mediante su clave RSA pública. Al establecer la conexión por primera vez, el programa cliente muestra al usuario la huella digital de esta clave. La huella digital contiene una secuencia de caracteres con codificación Base64 fácil de comprobar. Al poner esta secuencia de caracteres a disposición de los usuarios mediante un canal fiable, estos tienen la opción de comparar las huellas digitales. Si la secuencia de caracteres coincide, el cliente está conectado al servidor correcto.

Es posible crear las claves privadas y públicas (claves de host) necesarias para RSA directamente en el dispositivo. De lo contrario, tendrá la opción de copiar sus propias claves al dispositivo en formato PEM.

Como alternativa, el dispositivo le permite cargar la clave RSA (clave de host) desde una memoria externa al reiniciar. Puede activar esta función en el cuadro de diálogo *Basic Settings > External Memory*, columna *SSH key auto upload*.

### Operation

SSH server

Activa/desactiva el servidor SSH.

Valores posibles:

- `On` (configuración por defecto)
  El servidor SSH está activado.
  El acceso a la gestión del dispositivo es posible mediante la interfaz de línea de comando, usando una conexión SSH encriptada.
  Solo podrá iniciar el servidor si existe una firma RSA en el dispositivo.
- `Off`
  El servidor SSH está desactivado.
  Cuando desactive el servidor SSH, las conexiones existentes permanecerán establecidas. Sin embargo, el dispositivo ayuda a prevenir que se establezcan nuevas conexiones.

**Nota:** Si se desactiva el servidor *Telnet* y también el *SSH*, el acceso a la interfaz de la línea de comandos solo será posible con la interfaz serie del dispositivo.

### Configuration

TCP port

Especifica el número del puerto TCP en el que el dispositivo recibe las solicitudes SSH de los clientes.

Valores posibles:

- `1..65535` (configuración por defecto: `22`)
  Excepción: el puerto `2222` está reservado para funciones internas.

El servidor reinicia automáticamente después de cambiar el puerto. Las conexiones existentes se mantienen.

Sessions

Muestra cuantas conexiones SSH están establecidas en ese momento en el dispositivo.

Sessions (max.)

Especifica el número máximo de conexiones SSH al dispositivo que se pueden establecer simultáneamente.

Valores posibles:

- `1..5` (configuración por defecto: `5`)

Session timeout [min]

Especifica el tiempo de espera en minutos. Después de que el usuario conectado haya estado inactivo durante este tiempo, el dispositivo finaliza la conexión.

Los cambios de este valor tendrán efecto la siguiente vez que un usuario inicie sesión.

Valores posibles:

- `0`
  Desactiva la función. La conexión continúa en caso de inactividad.
- `1..160` (configuración por defecto: `5`)

### Fingerprint

La huella digital es una secuencia fácil de verificar que identifica claramente la clave de host del servidor SSH.

Después de importar una nueva clave de host, el dispositivo continuará mostrando la huella digital existente hasta que reinicie el servidor.

Fingerprint type

Especifica qué huella digital mostrará el campo *RSA fingerprint*.

Valores posibles:

- `md5`
  El campo *RSA fingerprint* muestra la huella digital como hash MD5 hexadecimal.
- `sha256`
  El campo *RSA fingerprint* muestra la huella digital como hash SHA256 codificado en Base64.

RSA fingerprint

Muestra la huella digital de la clave de host pública del servidor SSH.

Cuando cambie la configuración del campo *Fingerprint type*, haga clic en el botón y, a continuación, en el botón para actualizar la visualización.

### Signature

RSA present

Muestra si hay una clave de host RSA presente en el dispositivo.

Valores posibles:

- `marked`
  Hay una clave presente.
- `unmarked`
  No hay una clave presente.

Create

Genera una clave de host en el dispositivo. El requisito previo es que el servidor *SSH* esté inactivo.

Longitud de la clave creada:

- 2048 bits (RSA)

Para que el servidor SSH utilice la clave de host generada, vuelva a activar el servidor SSH.

También tiene la opción de copiar su propia clave de host al dispositivo en formato PEM. Consulte el cuadro *Key import*.

Delete

Elimina la clave de host del dispositivo. El requisito previo es que el servidor SSH esté inactivo.

Oper status

Muestra si el dispositivo está generando una clave de host en este momento.

Es posible que otro usuario haya activado esta acción.

Valores posibles:

- *rsa*
  El dispositivo está generando una clave de host RSA en este momento.
- *none*
  El dispositivo no está generando una clave de host.

### Key import

URL

Especifica la ruta y el nombre de archivo de su clave de host RSA propia.

El dispositivo acepta la clave RSA si tiene la siguiente longitud:

- 2048 bit (RSA)

El dispositivo le ofrece las opciones siguientes para copiar la clave al dispositivo:

- Importar desde el PC
  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.
- Importar desde un servidor FTP
  Cuando la clave se encuentre en un servidor FTP, especifique la URL correspondiente al archivo en el formato siguiente:
  `ftp://<usuario>:<contraseña>@<dirección IP>:<puerto>/<nombre archivo>`
- Importar desde un servidor TFTP
  Cuando la clave se encuentre en un servidor TFTP, especifique la URL correspondiente al archivo en el formato siguiente:
  `tftp://<dirección IP>/<ruta>/<nombre archivo>`
- Importar desde un servidor SCP o SFTP
  Cuando la clave se encuentre en un servidor SCP o SFTP, especifique la URL correspondiente al archivo en el formato siguiente:
  - `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://<user>:<password>@<IP address>/<path>/<file name>`

Start

Copia la clave especificada en el campo *URL* del dispositivo.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## [HTTP]

Esta pestaña le permite activar/desactivar el protocolo HTTP para el servidor web y especificar la configuración necesaria para HTTP.

El servidor web proporciona una interfaz gráfica de usuario mediante una conexión HTTP sin encriptar. Por razones de seguridad, desactive el protocolo HTTP y utilice en su lugar el protocolo HTTPS.

El dispositivo admite hasta 10 conexiones simultáneas mediante HTTP o HTTPS.

**Nota:** Si cambia la configuración en esta pestaña y hace clic en el botón ✓, el dispositivo finaliza la sesión y desconecta todas las conexiones abiertas. Para continuar trabajando con la interfaz gráfica de usuario, vuelva a iniciar sesión.

### Operation

HTTP server

Activa/desactiva el protocolo *HTTP* para el servidor web.

Valores posibles:

- *On* (configuración por defecto)
  El protocolo *HTTP* está activado.
  El acceso a la gestión del dispositivo es posible mediante una conexión *HTTP* sin encriptar.
  Si el protocolo *HTTPS* también está activado, el dispositivo redirige automáticamente la petición de conexión *HTTPS* a una conexión *HTTP* encriptada.
- *Off*
  El protocolo *HTTP* está desactivado.
  Si el protocolo *HTTPS* está activado, el acceso a la gestión del dispositivo es posible mediante una conexión *HTTPS* encriptada.

**Nota:** Si los protocolos *HTTP* y *HTTPS* están desactivados, podrá activar el protocolo *HTTP* mediante el comando de la interfaz de línea de comando `http server` para acceder a la interfaz gráfica de usuario.

### Configuration

TCP port

Especifica el número del puerto TCP en el que el servidor web recibe las solicitudes HTTP de los clientes.

Valores posibles:

- `1..65535` (configuración por defecto: `80`)
  Excepción: el puerto `2222` está reservado para funciones internas.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## [HTTPS]

Esta pestaña le permite activar/desactivar el protocolo HTTPS para el servidor web y especificar la configuración necesaria para HTTPS.

El servidor web proporciona una interfaz gráfica de usuario mediante una conexión HTTP encriptada.

Se necesita un certificado digital para la encriptación de la conexión HTTP. El dispositivo le permite crear este certificado usted mismo o cargar un certificado existente al dispositivo.

El dispositivo admite hasta 10 conexiones simultáneas mediante HTTP o HTTPS.

**Nota:** Si cambia la configuración en esta pestaña y hace clic en el botón , el dispositivo finaliza la sesión y desconecta todas las conexiones abiertas. Para continuar trabajando con la interfaz gráfica de usuario, vuelva a iniciar sesión.

### Operation

HTTPS server

Activa/desactiva el protocolo *HTTPS* para el servidor web.

Valores posibles:

- *On* (configuración por defecto)
  El protocolo *HTTPS* está activado.
  El acceso a la gestión del dispositivo es posible mediante una conexión *HTTPS* encriptada.
  Si no hay un certificado digital presente, el dispositivo genera un certificado digital antes de activar el protocolo *HTTPS*.
- *Off*
  El protocolo *HTTPS* está desactivado.
  Si el protocolo *HTTP* está activado, el acceso a la administración del dispositivo es posible mediante una conexión *HTTP* sin encriptar.

**Nota:** Si los protocolos *HTTP* y *HTTPS* están desactivados, podrá activar el protocolo *HTTPS* mediante el comando de la interfaz de línea de comando `https server` para acceder a la interfaz gráfica de usuario.

### Configuration

TCP port

Especificar el número del puerto TCP en el que el servidor web recibe las solicitudes HTTPS de los clientes.

Valores posibles:

- `1..65535` (configuración por defecto: `443`)
  Excepción: el puerto `2222` está reservado para funciones internas.

### Fingerprint

La huella digital es una secuencia de números hexadecimales fácil de verificar que identifica claramente al certificado digital del servidor HTTPS.

Después de importar un nuevo certificado digital, el dispositivo mostrará la huella digital actual hasta que reinicie el servidor.

Fingerprint type

Especifica qué huella digital mostrará el campo *Fingerprint*.

Valores posibles:

- *sha1*
  El campo *Fingerprint* muestra la huella SHA1 del certificado.
- *sha256*
  El campo *Fingerprint* muestra la huella SHA256 del certificado.

Fingerprint

Secuencia de caracteres del certificado digital utilizada por el servidor.

Cuando cambie la configuración del campo *Fingerprint type*, haga clic en el botón y, a continuación, en el botón para actualizar la visualización.

### Certificate

**Nota:** Si el dispositivo utiliza un certificado que no está firmado por una autoridad de certificación, el navegador web mostrará un mensaje mientras carga la interfaz gráfica de usuario. Para continuar, añada una excepción para el certificado en el navegador web.

Present

Muestra si hay un certificado digital presente en el dispositivo.

Valores posibles:

- `marked`
  El certificado está presente.
- `unmarked`
  El certificado se ha eliminado.

Create

Genera un certificado digital en el dispositivo.

Hasta que se reinicie, el servidor web utilizará el certificado anterior.

Para que el servidor web utilice el nuevo certificado, reinicie el servidor web. Es posible reiniciar el servidor web mediante la interfaz de línea de comando.

También tiene la opción de copiar su propio certificado al dispositivo. Consulte el cuadro *Certificate import*.

Delete

Elimina el certificado digital.

Hasta que se reinicie, el servidor web utilizará el certificado anterior.

Oper status

Muestra si el dispositivo está generando o eliminando un certificado digital en este momento.

Es posible que otro usuario haya activado la acción.

Valores posibles:

- *none*
  El dispositivo no está generando o eliminando un certificado en este momento.
- *delete*
  El dispositivo está eliminando un certificado en este momento.
- *generate*
  El dispositivo está generando un certificado en este momento.

### Certificate import

URL

Especifica la ruta y el nombre de archivo del certificado.

El dispositivo acepta certificados con las siguientes propiedades:

- Formato X.509
- Extensión de nombre de archivo `.PEM`
- Codificación con Base64, acompañado por
  - `-----BEGIN PRIVATE KEY-----`
    y
    `-----END PRIVATE KEY-----`
    así como
  - `-----BEGIN CERTIFICATE-----`
    y
    `-----END CERTIFICATE-----`
- Clave RSA con longitud de 2048 bits

El dispositivo le ofrece las opciones siguientes para copiar el certificado al dispositivo:

- Importar desde el PC
  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.
- Importar desde un servidor FTP
  Cuando el certificado se encuentre en un servidor FTP, especifique la URL correspondiente al archivo en el formato siguiente:
  `ftp://<usuario>:<contraseña>@<dirección IP>:<puerto>/<ruta>/<nombre archivo>`
- Importar desde un servidor TFTP
  Cuando el certificado se encuentre en un servidor TFTP, especifique la URL correspondiente al archivo en el formato siguiente:
  `tftp://<dirección IP>/<ruta>/<nombre archivo>`
- Importar desde un servidor SCP o SFTP
  Cuando el certificado se encuentre en un servidor SCP o SFTP, especifique la URL correspondiente al archivo en el formato siguiente:
  - `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://<user>:<password>@<IP address>/<path>/<file name>`

Start

Copia el certificado especificado en el campo *URL* del dispositivo.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

# 3.4.2 IP Access Restriction

[Device Security > Management Access > IP Access Restriction]

El cuadro de diálogo le permite restringir el acceso a la gestión del dispositivo a rangos de direcciones IP específicos y a aplicaciones basadas en IP seleccionadas.

- Si la función está desactivada, el acceso a la gestión del dispositivo es posible desde cualquier dirección IP y mediante cualquier aplicación.
- Si la función está activada, el acceso está restringido. Solo tendrá acceso a la gestión del dispositivo bajo las siguientes condiciones:
  - Al menos una entrada de la tabla está activada.
    y
  - Está accediendo al dispositivo mediante una aplicación permitida y desde un rango de direcciones IP permitido.

### Operation

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

Operation

Activa/desactiva la función *IP Access Restriction*.

Valores posibles:

- `On`
  La función *IP Access Restriction* está activada.
  El acceso a la gestión del dispositivo está restringido.
- `Off` (configuración por defecto)
  La función *IP Access Restriction* está desactivada.

### Tabla

Tiene la opción de definir hasta 16 entradas de tabla y activarlas de forma independiente.

Index

Muestra el número de índice al que la entrada de la tabla hace referencia.

Cuando elimine una entrada de la tabla, quedará un hueco en la numeración. Al crear una nueva entrada en la tabla, el dispositivo introduce el primer número que falta.

Valores posibles:

- `1..16`

Address

Especifica la dirección IP de la red desde la cual permitirá el acceso a la gestión del dispositivo. Especifique el rango de red en la columna *Netmask*.

Valores posibles:

- Dirección IPv4 válida (configuración por defecto: `0.0.0.0`)

Netmask

Especifica el rango de la red especificada en la columna *Address*.

Valores posibles:

- Máscara de red válida (configuración por defecto: `0.0.0.0`)

HTTP

Activa/desactiva el acceso HTTP.

Valores posibles:

- `marked` (configuración por defecto)
  El acceso está activado para el rango de direcciones IP adyacente.
- `unmarked`
  El acceso está desactivado.

HTTPS

Activa/desactiva el acceso HTTPS.

Valores posibles:

- `marked` (configuración por defecto)
  El acceso está activado para el rango de direcciones IP adyacente.
- `unmarked`
  El acceso está desactivado.

SNMP

Activa/desactiva el acceso SNMP.

Valores posibles:

- `marked` (configuración por defecto)
  El acceso está activado para el rango de direcciones IP adyacente.
- `unmarked`
  El acceso está desactivado.

Telnet

Activa/desactiva el acceso Telnet.

Valores posibles:

- `marked` (configuración por defecto)
  El acceso está activado para el rango de direcciones IP adyacente.
- `unmarked`
  El acceso está desactivado.

SSH

Activa/desactiva el acceso SSH.

Valores posibles:

- `marked` (configuración por defecto)
  El acceso está activado para el rango de direcciones IP adyacente.
- `unmarked`
  El acceso está desactivado.

IEC61850-MMS

Activa/desactiva el acceso al servidor MMS.

Valores posibles:

- `marked` (configuración por defecto)
  El acceso está activado para el rango de direcciones IP adyacente.
- `unmarked`
  El acceso está desactivado.

Modbus TCP

Activa/desactiva el acceso al servidor *Modbus TCP*.

Valores posibles:

- `marked` (configuración por defecto)
  El acceso está activado para el rango de direcciones IP adyacente.
- `unmarked`
  El acceso está desactivado.

EtherNet/IP

Activa/desactiva el acceso al servidor *EtherNet/IP*.

Valores posibles:

- `marked` (configuración por defecto)
  El acceso está activado para el rango de direcciones IP adyacente.
- `unmarked`
  El acceso está desactivado.

Active

Activa/desactiva la entrada de la tabla.

Valores posibles:

- `marked` (configuración por defecto)
  La entrada de la tabla está activada. El dispositivo restringe el acceso a la gestión del dispositivo a rangos de direcciones IP adyacentes y a las aplicaciones basadas en IP seleccionadas.
- `unmarked`
  La entrada de la tabla está desactivada.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## 3.4.3 Web

[Device Security > Management Access > Web]

En este cuadro de diálogo, podrá especificar la configuración de la interfaz gráfica de usuario.

### Configuration

Web interface session timeout [min]

Especifica el tiempo de espera en minutos. Después de que el dispositivo haya estado inactivo durante este tiempo, se finaliza la sesión del usuario conectado.

Valores posibles:

- `0..160` (configuración por defecto: `5`)

El valor `0` desactiva la función y el usuario permanece conectado cuando esté inactivo.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## 3.4.4 Command Line Interface

[Device Security > Management Access > CLI]

En este cuadro de diálogo podrá especificar la configuración de la interfaz de línea de comando. En el manual de referencia "Interfaz de línea de comando", encontrará información detallada de la interfaz de línea de comando.

El cuadro de diálogo contiene las siguientes pestañas:
- [Global]
- [Login banner]

### [Global]

Esta pestaña le permite cambiar el símbolo de la interfaz de línea de comando y especificar el cierre automático de sesiones mediante la interfaz serie cuando estén inactivas.

El dispositivo tiene las siguientes interfaces serie.
- Interfaz USB-C

#### Configuration

Login prompt

Especifica la cadena de caracteres que el dispositivo muestra en la interfaz de línea de comando al inicio de cada línea de comando.

Valores posibles:
- Cadena de caracteres ASCII alfanuméricos con entre 0 y 128 caracteres (`0x20..0x7E`) incluyendo caracteres de espacio
  Comodines
  - `%d` fecha
  - `%i` dirección IP
  - `%m` dirección MAC
  - `%p` nombre del producto
  - `%t` hora

  Configuración por defecto: `(MCSESM-E)`

Los cambios de estos ajustes entrarán en efecto inmediatamente en la sesión activa de la interfaz de línea de comando.

Serial interface timeout [min]

Especifica el tiempo en minutos tras el cual el dispositivo cerrará automáticamente la sesión de un usuario inactivo conectado a la interfaz de línea de comando mediante la interfaz serie.

Valores posibles:
- `0..160` (configuración por defecto: `5`)
  El valor `0` desactiva la función y el usuario permanece conectado cuando esté inactivo.

Los cambios de este valor tendrán efecto la siguiente vez que un usuario inicie sesión.

Para los servidores e *Telnet* y *SSH* , especifique el tiempo de espera en el cuadro de diálogo *Device Security > Management Access > Server*.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## [Login banner]

En esta pestaña podrá sustituir la pantalla de inicio de la interfaz de línea de comando por su propio texto.

En la configuración por defecto, la pantalla de inicio muestra información sobre el dispositivo, por ejemplo, la versión del software y la configuración del dispositivo. Con la función de esta pestaña, podrá desactivar esta información y reemplazarla con un texto personalizado.

Para mostrar su propio texto en la interfaz de línea de comando y en la interfaz gráfica de usuario antes de iniciar sesión, utilice el cuadro de diálogo *Device Security > Pre-login Banner*.

### Operation

Operation

Activa/desactiva la función *Login banner*.

Valores posibles:

- `On`
  La función *Login banner* está activada.
  El dispositivo muestra la información de texto especificada en el campo *Banner text* a los usuarios que inicien sesión mediante la interfaz de línea de comando.
- `Off` (configuración por defecto)
  La función *Login banner* está desactivada.
  La pantalla de inicio de muestra información sobre el dispositivo. Se mantiene la información de texto del campo *Banner text*.

### Banner text

Banner text

Especifica la secuencia de caracteres que el dispositivo muestra en la interfaz de línea de comando al inicio de cada sesión.

Valores posibles:

- Cadena de caracteres ASCII alfanuméricos con entre 0 y 1024 caracteres (`0x20..0x7E`) incluyendo caracteres de espacio

- `<Pestaña>`
- `<Line break>`

Remaining characters

Muestra los caracteres restantes en el campo *Banner text* para información de texto.

Valores posibles:

- `1024..0`

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

# 3.4.5 SNMPv1/v2 Community

[Device Security > Management Access > SNMPv1/v2 Community]

En este cuadro de diálogo, especifique el nombre de la comunidad para las aplicaciones SNMPv1/v2.

Las aplicaciones envían solicitudes mediante SNMPv1/v2 con un nombre de comunidad en el encabezado del paquete de datos SNMP. En función del nombre de la comunidad, la aplicación recibirá permisos de lectura o permisos de lectura y escritura para el dispositivo.

Active el acceso al dispositivo mediante SNMPv1/v2 en el cuadro de diálogo *Device Security > Management Access > Server*.

### Tabla

Community

Muestra la autorización de las aplicaciones SNMPv1/v2 para el dispositivo:

- `Write`
  En solicitudes con el nombre de la comunidad, la aplicación recibirá permisos de lectura y escritura para el dispositivo.
- `Read`
  En solicitudes con el nombre de la comunidad, la aplicación recibirá permisos de lectura para el dispositivo.

Name

Especifica el nombre de la comunidad para la autorización adyacente.

Valores posibles:

- Cadena de caracteres ASCII alfanuméricos con entre 0 y 32 caracteres
  `admin` (configuración por defecto para permisos de lectura y escritura)
  `user` (configuración por defecto para permisos de lectura)

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

# 3.5 Pre-login Banner

[Device Security > Pre-login Banner]

Este cuadro de diálogo le permitirá mostrar un saludo o información de texto a los usuarios antes de que inicien sesión.

Los usuarios verán este texto en el cuadro de diálogo de inicio de sesión de la interfaz gráfica de usuario y de la interfaz de línea de comando. Los usuarios que inicien sesión con SSH verán el texto (independientemente del cliente utilizado) antes o durante el inicio de sesión.

Para mostrar el texto solo en la interfaz de línea de comando, utilice los ajustes del cuadro de diálogo *Device Security > Management Access > CLI*.

### Operation

Operation

Activa/desactiva la función *Pre-login Banner*.

Mediante la función *Pre-login Banner*, el dispositivo muestra un saludo o información de texto en el cuadro de diálogo de inicio de sesión de la interfaz gráfica de usuario (GUI) y de la interfaz de línea de comando (CLI).

Valores posibles:

- *On*
  La función *Pre-login Banner* está activada.
  El dispositivo muestra el texto especificado en el campo *Banner text* en el cuadro de diálogo de inicio de sesión.
- *Off* (configuración por defecto)
  La función *Pre-login Banner* está desactivada.
  El dispositivo no muestra un texto en el cuadro de diálogo de inicio de sesión. Cuando introduzca un texto en el campo *Banner text*, este texto se guardará en el dispositivo.

### Banner text

Banner text

Especifica la información de texto que el dispositivo mostrará en el cuadro de diálogo de inicio de sesión de la interfaz gráfica de usuario y de la interfaz de línea de comando.

Valores posibles:

- Cadena de caracteres ASCII alfanuméricos con entre 0 y 512 caracteres (`0x20..0x7E`) incluyendo caracteres de espacio
- `<Pestaña>`
- `<Line break>`

Remaining characters

Muestra los caracteres restantes en el campo *Banner text*.

Valores posibles:

- 512..0

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

# 4 Network Security

El menú contiene los siguientes cuadros de diálogo:

- Network Security Overview
- Port Security
- 802.1X Port Authentication
- RADIUS
- DoS
- DHCP Snooping
- IP Source Guard
- Dynamic ARP Inspection
- ACL

## 4.1 Network Security Overview

[ Network Security > Overview ]

Este diálogo muestra las normas de seguridad utilizadas en el dispositivo.

### Parámetro

Port/VLAN

Especifica si el dispositivo muestra reglas basadas en VLAN y/o puerto.

Valores posibles:

- `All` (configuración por defecto)
  El dispositivo muestra las reglas basadas en VLAN y puerto que haya especificado.
- `Puerto: <Número de puerto>`
  El dispositivo muestra las reglas basadas en puerto para un puerto específico. Esta selección estará disponible si ha especificado una o más reglas para este puerto.
- `VLAN: <ID de VLAN>`
  El dispositivo muestra las reglas basadas en VLAN para una VLAN específica. Esta selección estará disponible si ha especificado una o más reglas para esta VLAN.

ACL

Muestra las reglas *ACL* en la vista general.

Puede editar las reglas *ACL* en el cuadro de diálogo *Network Security > ACL*.

All

Marca las casillas adyacentes. El dispositivo muestra las reglas relacionadas en la vista general.

None

Desmarca las casillas adyacentes. El dispositivo no muestra ninguna regla en la vista general.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

# 4.2 Port Security

[ Network Security > Port Security ]

El dispositivo solo le permite transmitir paquetes de datos desde los emisores deseados en un puerto. Cuando esta función está activada, el dispositivo comprueba el ID de VLAN y la dirección MAC o el ID de VLAN y la dirección IP del emisor antes de que este transmita un paquete de datos. El dispositivo descarta los paquetes de datos de otros emisores y registra este evento.

El dispositivo también ofrece la función de comprobar la dirección IP del remitente antes de transmitir un paquete de datos.

**Nota:** Si en el cuadro *Mode* se encuentra seleccionado el botón de opción *IP*, la función *Port Security* opera indirectamente en la capa 2. Al configurar una dirección IP permitida, el dispositivo recupera la dirección MAC asociada actualmente con la dirección IP. El dispositivo utiliza una solicitud ARP y guarda internamente la dirección MAC asociada. El requisito previo para la especificación de una dirección IP permitida es que el dispositivo conectado sea accesible y responda a solicitudes ARP.

Si un dispositivo conectado envía paquetes de datos con una dirección IP permitida, pero con una dirección MAC distinta de la asociada, el dispositivo descarta los paquetes de datos relacionados. Si sustituye el dispositivo conectado y utiliza la misma dirección IP que antes, vuelva a especificar la dirección IP de la forma permitida. Tras este paso, el dispositivo utiliza la dirección MAC asociada.

Si la función *Auto-Disable* está activada, el dispositivo desactiva el puerto. Esta restricción dificulta los ataques de suplantación de direcciones MAC. La función *Auto-Disable* vuelve a activar el puerto correspondiente automáticamente cuando no se excedan los parámetros.

En este cuadro de diálogo, una ventana *Wizard* le ayudará a conectar los puertos con una o más fuentes deseadas. En el dispositivo, a estas direcciones se las conoce como *Static entries (x/y)*. Para visualizar las direcciones estáticas especificadas, señale los puertos correspondientes y haga clic en el botón  .

Para simplificar el proceso de configuración, el dispositivo le permite registrar los emisores que desee automáticamente. El dispositivo "aprende" los emisores mediante la evaluación de los paquetes de datos recibidos. En el dispositivo, a estas direcciones se las conoce como *Dynamic entries*. Si se alcanza el límite superior definido por el usuario (*Dynamic limit*), el dispositivo detiene el "aprendizaje" en el puerto correspondiente y solo transmite paquetes de datos de los emisores ya registrados. Al adaptar el límite superior de emisores previstos, dificulta los ataques de desbordamiento de direcciones MAC.

**Nota:** Con el registro automático de las *Dynamic entries*, el dispositivo siempre descartará el primer paquete de datos que venga de un emisor desconocido. Mediante este primer paquete de datos, el dispositivo comprueba si se ha alcanzado el límite superior. El dispositivo registrará el emisor hasta que se alcance el límite superior. Después, el dispositivo transmitirá los paquetes de datos que reciba de este emisor en el puerto correspondiente.

### Operation

Operation

Activa/desactiva la función *Port Security*.

Valores posibles:

- `On`
  La función *Port Security* está activada.
  El dispositivo comprueba el ID de VLAN y la dirección MAC de la fuente antes de que esta transmita un paquete de datos.
  El dispositivo transmite un paquete de datos recibido solamente si el ID de VLAN y la dirección MAC de origen del paquete de datos se permiten en el puerto correspondiente. Para que esta configuración tenga efecto, active también la comprobación de la dirección de origen en los puertos relevantes.
- `Off` (configuración por defecto)
  La función *Port Security* está desactivada.
  El dispositivo transmite todos los paquetes de datos sin comprobar la dirección de origen.

**Nota:** Si en el cuadro *Mode* se encuentra seleccionado el botón de opción *MAC*, el dispositivo comprueba la dirección MAC de origen con las direcciones MAC de origen permitidas. Si el botón de opción *IP* está seleccionado, el dispositivo comprobará la dirección MAC de origen con las direcciones MAC asociadas a las direcciones IP de origen permitidas.

### Configuration

Auto-disable

Activa/desactiva la función *Auto-Disable* para la *Port Security*.

Valores posibles:

- `marked`
  La función *Auto-Disable* de *Port Security* está activa.
  Marque también la casilla de la columna *Auto-disable* para los puertos correspondientes.
- `unmarked` (configuración por defecto)
  La función *Auto-Disable* de *Port Security* está inactiva.

### Mode

Mode

Especifica si la función *Port Security* utiliza las direcciones MAC o IP permitidas para comprobar un paquete recibido.

Valores posibles:

- *MAC* (configuración por defecto)
  La función *Port Security* utiliza las direcciones MAC de origen permitidas.
  El dispositivo comprueba el ID de VLAN y la dirección MAC de origen con las direcciones MAC de origen permitidas antes de que esta transmita un paquete de datos.
- *IP*
  La función *Port Security* utiliza las direcciones IP de origen permitidas.
  El dispositivo comprueba el ID de VLAN y la dirección MAC de origen con las direcciones MAC asociadas con las direcciones IP de origen permitidas antes de transmitir un paquete de datos.

### Tabla

Port

Muestra el número de puerto.

Active

Activa/desactiva la comprobación de la dirección de origen en el puerto.

Valores posibles:

- `marked`
  El dispositivo comprueba todos los paquetes de datos recibidos en el puerto y solo los transmite si la dirección de origen del paquete de datos está permitida. Active también la función *Port Security* en el cuadro *Operation*.
- `unmarked` (configuración por defecto)
  El dispositivo transmite todos los paquetes de datos recibidos en el puerto sin comprobar la dirección de origen.

**Nota:** Al utilizar el dispositivo como participante activo dentro de un anillo *MRP* o *HIPER Ring*, le recomendamos que desmarque la casilla de verificación correspondiente a los puertos de anillos.

**Nota:** Al utilizar el dispositivo como suscriptor activo dentro de un *Ring/Network Coupling* o *RCP*, le recomendamos desmarcar la casilla de verificación de los puertos de acoplamiento correspondientes.

Auto-disable

Activa/desactiva la función *Auto-Disable* para los parámetros que la función *Port Security* está supervisando en el puerto.

Valores posibles:

- `marked` (configuración por defecto)
  La función *Auto-Disable* está activa en el puerto.
  El requisito previo es que marque la casilla *Auto-disable* del cuadro *Configuration*.
  - Si el puerto registra direcciones MAC de origen que no están permitidas o más direcciones MAC de origen de las especificadas en la columna *Dynamic limit*, el dispositivo desactivará el puerto. El LED de "Estado de enlace" del puerto parpadea 3 veces por período.
  - El cuadro de diálogo *Diagnostics > Ports > Auto-Disable* muestra qué puertos están desactivados actualmente debido a que se han superado los parámetros.
  - La función *Auto-Disable* reactiva el puerto automáticamente. Para esto, vaya al cuadro de diálogo *Diagnostics > Ports > Auto-Disable* y especifique un período de espera para el puerto correspondiente en la columna *Reset timer [s]*.
- `unmarked`
  La función *Auto-Disable* en el puerto está inactiva.

Send trap

Activa/desactiva el envío de trampas SNMP cuando el dispositivo descarta un paquete de datos de un emisor no deseado en el puerto.

Valores posibles:

- `marked`
  El envío de trampas SNMP está activo.
  Si el dispositivo descarta paquetes de datos de un emisor no permitido en el puerto, el dispositivo envía una trampa SNMP.
- `unmarked` (configuración por defecto)
  El envío de trampas SNMP está inactivo.

Como requisito previo para enviar trampas SNMP, debe activar la función en el cuadro de diálogo *Diagnostics > Status Configuration > Alarms (Traps)* y especificar al menos un destino de la trampa.

Trap interval [s]

Especifica en segundos el tiempo que desea que espere el dispositivo después de enviar una trampa SNMP y antes de enviar la siguiente trampa SNMP.

Valores posibles:

- `0..3600` (configuración por defecto: `0`)

El valor `0` desactiva el tiempo de retardo.

Dynamic limit

Especifica el límite superior para la cantidad de fuentes registradas automáticamente (*Dynamic entries*). Cuando se alcance el límite superior, el dispositivo dejará de "aprender" en este puerto.

Ajuste el valor a la cantidad de fuentes previstas.

Si el puerto registra más emisores de los especificados aquí, el puerto desactivará la función *Auto-Disable*. El requisito previo es que marque la casilla en la columna *Configuration* y la casilla *Auto-disable* en el cuadro *Auto-disable*.

Valores posibles:

- `0`
  Desactiva el registro automático de fuentes en este puerto.
- `1..600` (configuración por defecto: `600`)

Static limit

Especifica el límite superior para la cantidad de fuentes conectadas al puerto (*Static entries (x/y)*). La ventana *Wizard*, cuadro de diálogo *MAC addresses*, le ayudará a conectar el puerto con una o más fuentes deseadas.

Valores posibles:

- `0..64` (configuración por defecto: `64`)

El valor `0` le ayuda a evitar conectar a una fuente con el puerto.

Dynamic entries

Muestra el número de emisores que el dispositivo ha establecido automáticamente.

Consulte la ventana *Wizard*, cuadro de diálogo *MAC addresses*, campo *Dynamic entries*.

Si selecciona el valor *IP* en el cuadro *Mode*, la columna *Dynamic entries* muestra el valor `0`.

Static MAC entries

Muestra el número de emisores conectados con el puerto.

Consulte la ventana *Wizard*, cuadro de diálogo *MAC addresses*, campo *Static entries (x/y)*.

Static IP entries

Muestra el número de direcciones IP permitidas en el puerto.

Consulte la ventana *Wizard*, cuadro de diálogo *IP addresses*, campo *Static entries (x/y)*.

Last violating VLAN ID/MAC

Muestra el ID de VLAN y la dirección MAC de un emisor no deseado de los últimos paquetes de datos que el dispositivo haya descartado en este puerto.

Sent traps

Muestra la cantidad de paquetes de datos descartados en este puerto que hayan provocado el envío de una trampa SNMP.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## [Port security (Wizard)]

La ventana *Wizard* le ayudará a conectar los puertos con una o más fuentes deseadas. Después de especificar los ajustas, haga clic en el botón *Finish*.

**Nota:** El dispositivo guarda las fuentes conectadas con el puerto hasta que desactive la comprobación de fuente en el puerto relevante o en el cuadro *Operation*.

Tras cerrar la ventana *Wizard*, haga clic en el botón ☑ para guardar su configuración.

## [Port security (Wizard) – Select port]

Port

Especifica el puerto que va a asignar al emisor en el siguiente paso.

## [Port security (Wizard) – MAC addresses]

VLAN ID

Especifica el ID de VLAN de la fuente deseada.

Valores posibles:

- `1..4042`

Para transferir el ID de VLAN y la dirección MAC al campo *Static entries (x/y)*, haga clic en el botón *Add*.

MAC address

Especifica la dirección MAC de la fuente deseada.

Valores posibles:

- Dirección MAC Unicast válida
  Especifique el valor separándolo con dos puntos, por ejemplo `00:11:22:33:44:55`.

Para transferir el ID de VLAN y la dirección MAC al campo *Static entries (x/y)*, haga clic en el botón *Add*.

Add

Transfiere los valores especificados en los campos *VLAN ID* y *MAC address* al campo *Static entries (x/y)*.

Static entries (x/y)

Muestra el ID de VLAN y la dirección MAC de un emisor deseado conectado al puerto.

El dispositivo utiliza este campo para mostrar la cantidad de emisores conectados al puerto y el límite superior. Especifique el límite superior para la cantidad de entradas en la tabla, campo *Static limit*.

**Nota:** No puede asignar la dirección MAC que ha asignado a este puerto a otro puerto.

Remove

Elimina las entradas señaladas en el campo *Static entries (x/y)*.

Mueve las entradas señaladas en el campo *Static entries (x/y)* al campo *Dynamic entries*.

Mueve todas las entradas del campo *Static entries (x/y)* al campo *Dynamic entries*.

Cuando el campo *Dynamic entries* contiene más entradas de las permitidas en el campo *Static entries (x/y)*, el dispositivo mueve las entradas principales hasta que se alcance el límite superior.

Dynamic entries

Muestra en orden ascendente el ID de VLAN y la dirección MAC de los emisores registrados automáticamente en este puerto. El dispositivo transmite paquetes de datos desde estos emisores al recibir los paquetes de datos en este puerto.

Los requisitos previos del dispositivo para mostrar direcciones MAC son los siguientes:

- La función *Port Security* está activada. Consulte el cuadro *Operation*.
- El dispositivo comprueba todos los paquetes de datos recibidos en el puerto. La casilla de la columna *Active* está marcada.

Especifique el límite superior para la cantidad de entradas en la tabla, campo *Dynamic limit*.

Los botones  y  le permiten transferir entradas desde este campo al campo *Static entries (x/y)*. De esta manera, podrá conectar los emisores correspondientes con el puerto.

## [Port security (Wizard) – IP addresses]

VLAN ID

Especifica el ID de VLAN de la fuente deseada.

Valores posibles:

▶ `1..4042`

**Nota:** Asigna el ID de VLAN de la VLAN de administración.

Para transferir el *VLAN ID* y la *IP address* al campo *Static entries (x/y)*, haga clic en el botón *Add*.

IP address

Especifica la dirección IP de la fuente deseada.

Valores posibles:
- Dirección IPv4 válida

Para transferir el *VLAN ID* y la *IP address* al campo *Static entries (x/y)*, haga clic en el botón *Add*.

Add

Transfiere los valores especificados en los campos *VLAN ID* y *IP address* al campo *Static entries (x/y)*.

Static entries (x/y)

Muestra el ID de VLAN y la dirección IP de emisores deseados conectados al puerto.

El dispositivo utiliza este campo para mostrar la cantidad de emisores conectados al puerto y el límite superior. Puede especificar un número máximo de `10` direcciones IP.

Remove

Elimina las entradas señaladas en el campo *Static entries (x/y)*.

## 4.3 802.1X Port Authentication

[Network Security > 802.1X Port Authentication]

Según la norma IEEE 802.1X, con el control de acceso basado en puerto, el dispositivo monitoriza el acceso a la red desde dispositivos terminales conectados. El dispositivo (autenticador) permite a un dispositivo terminal (solicitante) tener acceso a la red si inicia sesión con datos de acceso válidos. El autenticador y los dispositivos terminales se comunican mediante el protocolo de autenticación EAPoL (Protocolo de autenticación extensible sobre LAN).

El dispositivo es compatible con los siguientes métodos de autenticación de dispositivos terminales:
- `radius`
  Un servidor RADIUS en la red autentica los dispositivos terminales.
- `ias`
  El Servidor de autenticación integrada (IAS) implementado en el dispositivo autentica los dispositivos terminales. Comparado con RADIUS, IAS solo proporciona funciones básicas.

El menú contiene los siguientes cuadros de diálogo:
- 802.1X Global
- 802.1X Port Configuration
- 802.1X Port Clients
- 802.1X EAPOL Port Statistics
- 802.1X Port Authentication History
- 802.1X Integrated Authentication Server

# 4.3.1 802.1X Global

[Network Security > 802.1X Port Authentication > Global]

Este cuadro de diálogo le permite especificar la configuración básica del control de acceso basado en puerto.

### Operation

Operation

Activa/desactiva la función *802.1X Port Authentication*.

Valores posibles:

- `On`
  La función *802.1X Port Authentication* está activada.
  El dispositivo comprueba el acceso a la red desde dispositivos terminales conectados.
  El control de acceso basado en puerto está activado.
- `Off` (configuración por defecto)
  La función *802.1X Port Authentication* está desactivada.
  El control de acceso basado en puerto está desactivado.

### Configuration

VLAN assignment

Activa/desactiva la asignación del puerto correspondiente a la VLAN. Esta función le permite proporcionar determinados servicios al dispositivo terminal conectado en esta VLAN.

Valores posibles:

- `marked`
  La asignación está activa.
  Si el dispositivo terminal se autentica correctamente, el dispositivo terminal asignará al puerto correspondiente el ID de VLAN transferido por el servidor de autenticación RADIUS.
- `unmarked` (configuración por defecto)
  La asignación está inactiva.
  Se asigna el puerto correspondiente a la VLAN especificada en el cuadro de diálogo *Network Security > 802.1X Port Authentication > Port Configuration*, fila *Assigned VLAN ID*.

Dynamic VLAN creation

Activa/desactiva la creación automática de la VLAN asignada por el servidor de autenticación RADIUS si la VLAN no existe.

Valores posibles:

- `marked`
  La creación automática de la VLAN está activa.
  El dispositivo creará la VLAN si esta no existe.
- `unmarked` (configuración por defecto)
  La creación automática de la VLAN está inactiva.
  Si la VLAN asignada no existe, el puerto permanecerá asignado a la VLAN original.

Monitor mode

Activa/desactiva el modo de supervisión.

Valores posibles:

- `marked`
  El modo de supervisión está activo.
  El dispositivo monitoriza la autenticación y ayuda con el diagnóstico de errores reconocidos. Si un dispositivo terminal no ha iniciado sesión correctamente, el dispositivo dará al dispositivo terminal acceso a la red.
- `unmarked` (configuración por defecto)
  El modo de supervisión está inactivo.

### MAC authentication bypass format options

Group size

Especifica el tamaño de los grupos de direcciones MAC. El dispositivo divide la dirección MAC para la autenticación en grupos. El tamaño de los grupos se especifica en medios bytes, cada uno de los cuales se representa como un carácter.

Valores posibles:

- *1*
  El dispositivo divide la dirección MAC en 12 grupos de un carácter.
  Por ejemplo: `A:A:B:B:C:C:D:D:E:E:F:F`
- *2*
  El dispositivo divide la dirección MAC en 6 grupos de 2 caracteres.
  Por ejemplo: `AA:BB:CC:DD:EE:FF`
- *4*
  El dispositivo divide la dirección MAC en 3 grupos de 4 caracteres.
  Por ejemplo: `AABB:CCDD:EEFF`
- *12* (configuración por defecto)
  El dispositivo formatea la dirección MAC como un grupo de 12 caracteres.
  Por ejemplo: `AABBCCDDEEFF`

Group separator

Especifica el carácter que separa los grupos.

Valores posibles:

- *-*
  barra inclinada
- *:*
  dos puntos
- *.*
  punto

Upper or lower case

Especifica si el dispositivo formatea los datos de autenticación en minúsculas o mayúsculas.

Valores posibles:

- `lower-case`
- `upper-case`

Password

Especifica la contraseña opcional de los clientes que utilizan la omisión de autenticación.

Valores posibles:

- Cadena de caracteres ASCII alfanuméricos con entre 0 y 64 caracteres
  Al introducirla, el campo muestra ***** (asteriscos) en lugar de la contraseña.
- `<empty>`
  El dispositivo utiliza el nombre de usuario del cliente como contraseña.

### Information

Monitor mode clients

Muestra a cuántos dispositivos terminales ha dado acceso de red el dispositivo a pesar de no haber iniciado sesión correctamente.

Como requisito previo, debe activar la función *Monitor mode*. Consulte el cuadro *Configuration*.

Non monitor mode clients

Muestra el número de dispositivos terminales a los que el dispositivo ha dado acceso de red tras iniciar sesión correctamente.

Policy 1

Muestra el método que el dispositivo está usando actualmente para autenticar los dispositivos terminales, usando IEEE 802.1X.

Especifique el método utilizado en el cuadro de diálogo *Device Security > Authentication List*.

- ☐ Para autenticar los dispositivos terminales mediante un servidor RADIUS, asigne la política `radius` a la lista `8021x`.
- ☐ Para autenticar los dispositivos terminales mediante Servidor de autenticación integrada (IAS), asigne la política `ias` a la lista `8021x`.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

# 4.3.2 802.1X Port Configuration

[Network Security > 802.1X Port Authentication > Port Configuration]

Este cuadro de diálogo le permite especificar la configuración de acceso de cada puerto.

Si hay varios dispositivos terminales conectados a un puerto, el dispositivo le permite autenticarlos de forma individual (autenticación de clientes múltiples). En este caso, el dispositivo deja que los dispositivos terminales con sesión iniciada tengan acceso a la red. En cambio, el dispositivo bloquea el acceso para los dispositivos terminales no autenticados o para los dispositivos terminales cuya autenticación haya transcurrido.

### Tabla

Port

Muestra el número de puerto.

Port initialization

Activa/desactiva la inicialización del puerto para activar el control de acceso en el puerto o restaurarlo a su estado inicial. Utilice esta función solamente en puertos en los que la columna *Port control* contenga el valor `auto` o `multiClient`.

Valores posibles:

- `marked`
  La inicialización de puerto está activa.
  Cuando la inicialización finalice, el dispositivo volverá a cambiar el valor a `unmarked`.
- `unmarked` (configuración por defecto)
  La inicialización de puerto está inactiva.
  El dispositivo mantiene el estado del puerto actual.

Port reauthentication

Activa/desactiva la solicitud de reautenticación de un solo uso.

Utilice esta función solamente en puertos en los que la columna *Port control* contenga el valor `auto` o `multiClient`.

El dispositivo también le permite solicitar periódicamente al dispositivo terminal volver a iniciar sesión. Consulte la columna *Periodic reauthentication*.

Valores posibles:

- `marked`
  La solicitud de reautenticación de un solo uso está activa.
  El dispositivo solicita al dispositivo terminal volver a iniciar sesión. Después, el dispositivo volverá a cambiar el valor a `unmarked`.
- `unmarked` (configuración por defecto)
  La solicitud de reautenticación de un solo uso está inactiva.
  El dispositivo mantiene activa la sesión del dispositivo terminal.

Authentication activity

Muestra el estado actual del Autenticador (`Authenticator PAE state`).

Valores posibles:

- *initialize*
- *disconnected*
- *connecting*
- *authenticating*
- *authenticated*
- *aborting*
- *held*
- *forceAuth*
- *forceUnauth*

Backend authentication state

Muestra el estado actual de la conexión al servidor de autenticación (`Backend Authentication state`).

Valores posibles:

- *request*
- *response*
- *success*
- *fail*
- *timeout*
- *idle*
- *initialize*

Authentication state

Muestra el estado actual de la autenticación en el puerto (`Controlled Port Status`).

Valores posibles:

- *authorized*
  El dispositivo terminal ha iniciado sesión correctamente.
- *unauthorized*
  El dispositivo terminal no ha iniciado sesión.

Users (max.)

Especifica el límite superior para el número de dispositivos terminales que el dispositivo autentica en este puerto al mismo tiempo. Este límite superior se aplica únicamente en puertos en los que la columna *Port control* contenga el valor `multiClient`.

Valores posibles:

- `1..16` (configuración por defecto: `16`)

Port control

Especifica cómo el dispositivo concede acceso a la red (`Port control mode`).

Valores posibles:

- *`forceUnauthorized`*
  El dispositivo bloquea el acceso a la red. Utilice esta configuración si hay un dispositivo terminal conectado al puerto que no reciba acceso a la red.
- *`auto`*
  El dispositivo concede acceso a la red si el dispositivo terminal ha iniciado sesión correctamente. Utilice esta configuración si hay un dispositivo terminal conectado al puerto que inicie sesión en el autenticador.

**Nota:** Si hay otros dispositivos terminales conectados mediante el mismo puerto, estos tendrán acceso a la red sin ninguna autenticación adicional.

- *`forceAuthorized`* (configuración por defecto)
  Si los dispositivos terminales no son compatibles con el estándar IEEE 802.1X, el dispositivo les dará acceso a la red. Utilice esta configuración si hay un dispositivo terminal conectado al puerto que reciba acceso a la red sin iniciar sesión.
- *`multiClient`*
  El dispositivo concede acceso a la red si el dispositivo terminal ha iniciado sesión correctamente.
  Si el dispositivo final no envía ningún paquete de datos de EAPOL, el dispositivo otorga o niega el acceso a la red individualmente en función de la dirección MAC del dispositivo terminal. Consulte la columna *MAC authorized bypass*.
  Utilice esta configuración si hay múltiples dispositivos terminales conectados al puerto o si se requiere la función *MAC authorized bypass*.

Quiet period [s]

Especifica el período de tiempo en segundos durante el cual el autenticador no aceptará más inicios de sesión del dispositivo terminal después de un intento fallido de iniciar sesión (*Quiet period [s]*).

Valores posibles:

- `0..65535` (configuración por defecto: `60`)

Transmit period [s]

Especifica el período en segundos tras el cual el autenticador solicita al dispositivo terminal volver a iniciar sesión. Después de este período de espera, el dispositivo envía un paquete de datos de solicitud/identidad EAP al dispositivo terminal.

Valores posibles:

- `1..65535` (configuración por defecto: `30`)

Supplicant timeout period [s]

Especifica el período en segundos durante el cual el autenticador espera el inicio de sesión del dispositivo terminal.

Valores posibles:

- `1..65535` (configuración por defecto: `30`)

Server timeout [s]

Especifica el período en segundos durante el cual el autenticador espera la respuesta del servidor de autenticación (RADIUS o IAS).

Valores posibles:

- `1..65535` (configuración por defecto: `30`)

Requests (max.)

Especifica cuántas veces el autenticador va a solicitar que el dispositivo terminal inicie sesión hasta que haya transcurrido el tiempo especificado en la columna *Supplicant timeout period [s]*. El dispositivo envía un paquete de datos de solicitud/identidad EAP al dispositivo terminal con la frecuencia especificada aquí.

Valores posibles:

- `0..10` (configuración por defecto: `2`)

Assigned VLAN ID

Muestra el ID de la VLAN que el autenticador ha asignado al puerto. Este valor se aplica únicamente en puertos en los que la columna *Port control* contenga el valor `auto`.

Valores posibles:

- `0..4042` (configuración por defecto: `0`)

Encontrará el ID de VLAN que el autenticador ha asignado al puerto en el cuadro de diálogo *Network Security > 802.1X Port Authentication > Port Clients*.

Para los puertos en los que la columna *Port control* contiene el valor `multiClient`, el dispositivo asigna la etiqueta VLAN según la dirección MAC del dispositivo terminal al recibir paquetes de

datos sin una etiqueta VLAN.

Assignment reason

Muestra el motivo de la asignación de el ID de VLAN. Este valor se aplica únicamente en puertos en los que la columna *Port control* contenga el valor `auto`.

Valores posibles:

- `notAssigned` (configuración por defecto)
- `radius`
- `guestVlan`
- `unauthenticatedVlan`

Encontrará el ID de VLAN que el autenticador ha asignado al puerto para un solicitante en el cuadro de diálogo *Network Security > 802.1X Port Authentication > Port Clients*.

Reauthentication period [s]

Especifica el período en segundos tras el cual el autenticador solicita periódicamente al dispositivo terminal volver a iniciar sesión.

Valores posibles:

- `1..65535` (configuración por defecto: `3600`)

Periodic reauthentication

Activa/desactiva las solicitudes de reautenticación periódica.

Valores posibles:

- `marked`
  Las solicitudes de reautenticación periódica están activas.
  El dispositivo solicita periódicamente al dispositivo terminal volver a iniciar sesión. Especifique este período de tiempo en la columna *Reauthentication period [s]*.
  Si el autenticador ha asignado el ID de una Voice VLAN, Unauthenticated VLAN o Guest VLAN al dispositivo terminal, esta configuración dejará de tener efecto.
- `unmarked` (configuración por defecto)
  Las solicitudes de reautenticación periódica están inactivas.
  El dispositivo mantiene activa la sesión del dispositivo terminal.

Guest VLAN ID

Especifica el ID de la VLAN que el autenticador asignará al puerto si el dispositivo terminal no inicia sesión durante el período de tiempo especificado en la columna *Guest VLAN period*. Este valor se aplica solamente en puertos en los que la columna *Port control* contenga el valor `auto` o `multi-Client`.

Esta función le permite conceder acceso a determinados servicios de la red a dispositivos terminales no compatibles con el estándar IEEE 802.1X.

Valores posibles:

- `0` (configuración por defecto)
  El autenticador no asigna una Guest VLAN al puerto.
  Cuando activa la autenticación basada en MAC en la columna *MAC authorized bypass*, el dispositivo establece automáticamente el valor en `0`.
- `1..4042`

**Nota:** La función *MAC authorized bypass* y la función *Guest VLAN ID* no pueden utilizarse simultáneamente.

Guest VLAN period

Especifica el período en segundos durante el cual el autenticador espera los paquetes de datos EAPOL después de que el dispositivo terminal esté conectado. Si finaliza este período, el autenticador concede acceso al dispositivo terminal a la red y asigna el puerto a la Guest VLAN especificada en la columna *Guest VLAN ID*.

Valores posibles:

- `1..300` (configuración por defecto: `90`)

Unauthenticated VLAN ID

Especifica el ID de la VLAN que el autenticador asignará al puerto si el dispositivo terminal no inicia sesión correctamente. Este valor se aplica únicamente en puertos en los que la columna *Port control* contenga el valor `auto`.

Esta función le permite conceder acceso a determinados servicios de la red a dispositivos terminales sin datos de acceso válidos.

Valores posibles:

- `0..4042` (configuración por defecto: `0`)

El efecto del valor `0` es que el autenticador no asignará una Unauthenticated VLAN al puerto.

**Nota:** Asigna al puerto una VLAN configurada estáticamente en el dispositivo.

MAC authorized bypass

Activa/desactiva la autenticación basada en MAC.

Esta función le permite autenticar dispositivos terminales no compatibles con el estándar IEEE 802.1X de acuerdo con sus direcciones MAC.

Valores posibles:

- `marked`
  La autenticación basada en MAC está activa.
  El dispositivo envía la dirección MAC del dispositivo terminal al servidor de autenticación RADIUS. El dispositivo asigna al solicitante según su dirección MAC al VLAN correspondiente como si la autenticación se realizara a través de IEEE 802.1X directamente.
- `unmarked` (configuración por defecto)
  La autenticación basada en MAC está inactiva.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## 4.3.3 802.1X Port Clients

[Network Security > 802.1X Port Authentication > Port Clients]

Este cuadro de diálogo muestra información de los dispositivos terminales conectados.

**Tabla**

Port

Muestra el número de puerto.

User name

Muestra el nombre de usuario con el que el dispositivo terminal inició sesión.

MAC address

Muestra la dirección MAC del dispositivo terminal.

Assigned VLAN ID

Muestra el ID de VLAN que el autenticador ha asignado al puerto después de la autenticación correcta del dispositivo terminal.

Si para el puerto en el cuadro de diálogo *Network Security > 802.1X Port Authentication > Port Configuration* columna *Port control*, se especifica el valor `multiClient`, el dispositivo asigna la etiqueta VLAN según la dirección MAC del dispositivo terminal al recibir paquetes de datos sin una etiqueta VLAN.

Assignment reason

Muestra el motivo de la asignación de la VLAN.

Valores posibles:

- `default`
- `radius`
- `unauthenticatedVlan`
- `guestVlan`
- `monitorVlan`
- `invalid`

El campo solo muestra un valor válido mientras el cliente esté autenticado.

Session timeout

Muestra el tiempo restante en segundos hasta que la sesión del dispositivo terminal expire. Este valor solo es válido si para el puerto en el cuadro de diálogo *Network Security > 802.1X Port Authentication > Port Configuration*, columna *Port control*, se especifica el valor `auto` o `multiClient`.

El servidor de autenticación asigna el período de tiempo de espera al dispositivo mediante RADIUS. El valor `0` indica que el servidor de autenticación no ha asignado un período de espera.

Termination action

Muestra la acción que el dispositivo lleva a cabo cuando haya finalizado la sesión.

Valores posibles:

- *default*
- *reauthenticate*

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## 4.3.4 802.1X EAPOL Port Statistics

[Network Security > 802.1X Port Authentication > Statistics]

Este cuadro de diálogo muestra qué paquetes de datos EAPOL ha enviado y recibido el dispositivo terminal para la autenticación de los dispositivos terminales.

### Tabla

Port

Muestra el número de puerto.

Received packets

Muestra el número total de paquetes de datos EAPOL recibidos por el dispositivo en el puerto.

Transmitted packets

Muestra el número total de paquetes de datos EAPOL enviados por el dispositivo en el puerto.

Start packets

Muestra el número de paquetes de datos iniciales EAPOL recibidos por el dispositivo en el puerto.

Logoff packets

Muestra el número de paquetes de datos de fin de sesión EAPOL recibidos por el dispositivo en el puerto.

Response/ID packets

Muestra el número de paquetes de datos de respuesta/identidad EAP recibidos por el dispositivo en el puerto.

Response packets

Muestra el número de paquetes de datos de respuesta EAP válidos recibidos por el dispositivo en el puerto (paquetes de datos sin respuesta/identidad EAP).

Request/ID packets

Muestra el número de paquetes de datos de solicitud/identidad EAP recibidos por el dispositivo en el puerto.

Request packets

Muestra el número de paquetes de datos de solicitud EAP válidos recibidos por el dispositivo en el puerto (paquetes de datos sin respuesta/identidad EAP).

Invalid packets

Muestra el número de paquetes de datos EAPOL con un tipo de trama desconocido recibidos por el dispositivo en el puerto.

Received error packets

Muestra el número de paquetes de datos EAPOL con Packet Body Length-Feld no válido recibidos por el dispositivo en el puerto.

Packet version

Muestra el número de versión del protocolo del paquete de datos EAPOL recibido por el dispositivo en el puerto.

Source of last received packet

Muestra la dirección MAC del emisor del paquete de datos EAPOL recibido por el dispositivo en el puerto.

El valor `00:00:00:00:00:00` indica que el puerto aún no ha recibido paquetes de datos EAPOL.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## 4.3.5 802.1X Port Authentication History

[Network Security > 802.1X Port Authentication > Port Authentication History]

El dispositivo registra el proceso de autenticación de los dispositivos terminales conectados a sus puertos. Este cuadro de diálogo muestra la información registrada durante la autenticación.

### Tabla

Port

Muestra el número de puerto.

Authentification time stamp

Muestra la hora a la que el autenticador ha autenticado el dispositivo terminal.

Result age

Muestra el tiempo que esta entrada lleva en la tabla.

MAC address

Muestra la dirección MAC del dispositivo terminal.

VLAN ID

Muestra el ID de la VLAN asignada al dispositivo terminal antes de iniciar sesión.

Authentication status

Muestra el estado del autenticador en el puerto.

Valores posibles:

- *success*
  La autenticación se ha realizado correctamente.
- *failure*
  La autenticación no se ha realizado correctamente.

Access status

Muestra si el dispositivo concede acceso a la red al dispositivo terminal.

Valores posibles:

- *granted*
  El dispositivo concede acceso a la red al dispositivo terminal.
- *denied*
  El dispositivo deniega el acceso a la red al dispositivo terminal.

Assigned VLAN ID

Muestra el ID de la VLAN que el autenticador ha asignado al puerto.

Assignment type

Muestra el tipo de VLAN que el autenticador ha asignado al puerto.

Valores posibles:

- *default*
- *radius*
- *unauthenticatedVlan*
- *guestVlan*
- *monitorVlan*
- *notAssigned*

Assignment reason

Muestra el motivo de la asignación del ID de VLAN y del tipo de VLAN.

### 802.1X Port Authentication History

Port

Simplifica la tabla y muestra solo las entradas relacionadas con el puerto seleccionado aquí. Esto facilita el registro de la tabla y ordenarla como desee.

Valores posibles:

- `all`
  La tabla muestra las entradas de cada puerto.
- `<Port number>`
  La tabla muestra las entradas relacionadas con el puerto seleccionado aquí.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## 4.3.6 802.1X Integrated Authentication Server

[Network Security > 802.1X Port Authentication > Integrated Authentication Server]

El servidor de autenticación integrado (IAS) le permite autenticar dispositivos terminales mediante el estándar IEEE 802.1X. En comparación con RADIUS, el IAS tiene una variedad de funciones muy limitada. La autenticación se basa únicamente en el nombre de usuario y la contraseña.

En este cuadro de diálogo, puede administrar los datos de acceso de los dispositivos terminales. El dispositivo le permite configurar hasta 100 conjuntos de datos de acceso.

Para autenticar los dispositivos terminales mediante Servidor de autenticación integrada, asigne la política *Device Security > Authentication List* a la lista 8021x en el cuadro de diálogo `ias`.

### Tabla

User name

Muestra el nombre de usuario del dispositivo terminal.

Para crear un nuevo usuario, haga clic en el botón .

Password

Especifica la contraseña con la que el usuario se autenticará.

Valores posibles:

- Cadena de caracteres ASCII alfanuméricos con entre 0 y 64 caracteres

El dispositivo distingue entre mayúsculas y minúsculas.

Active

Activa/desactiva los datos de acceso.

Valores posibles:

- `marked`
  Los datos de acceso están activos. Un dispositivo terminal tiene la opción de iniciar sesión mediante IEEE 802.1X utilizando estos datos de acceso.
- `unmarked` (configuración por defecto)
  Los datos de acceso están inactivos.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

# 4.4 RADIUS

[Network Security > RADIUS]

Con la configuración de fábrica, el dispositivo autentica a los usuarios basándose en la gestión local de usuarios. Sin embargo, al aumentar el tamaño de red, se hace más difícil que los datos de acceso de los usuarios sean consistentes en todos los dispositivos.

RADIUS (Servicio de autenticación remota de llamadas de usuarios) le permite autenticar y autorizar los usuarios en un punto central de la red. Un servidor RADIUS realiza las siguientes tareas:

- Autenticación
  Un servidor de autenticación autentica a los usuarios cuando el cliente RADIUS del punto de acceso reenvía los datos de acceso de los usuarios al servidor.
- Autorización
  El servidor de autenticación autoriza a los usuarios que hayan iniciado sesión a utilizar determinados servicios mediante la asignación de varios parámetros para el dispositivo terminal correspondiente al cliente RADIUS del punto de acceso.
- Administración
  El servidor de administración registra los datos de tráfico producido durante la autenticación del puerto según el estándar IEEE 802.1X. Esto le permitirá determinar posteriormente qué servicios han utilizado los usuarios y en qué medida.

Si asigna la política `radius` a una aplicación en el cuadro de diálogo *Device Security > Authentication List*, el dispositivo operará en la función de cliente RADIUS. El dispositivo reenvía los datos de acceso de los usuarios al servidor de autenticación primario. El servidor de autenticación decide si los datos de acceso son válidos y transfiere las autorizaciones del usuario al dispositivo.

El dispositivo asigna a un rol de usuario existente en el dispositivo el Tipo de Servicio transferido en respuesta a un servidor RADIUS de la siguiente manera:

- `Administrative-User`: *`administrator`*
- `Login-User`: *`operator`*
- `NAS-Prompt-User`: *`guest`*

El dispositivo también le permite autenticar dispositivos terminales con el estándar IEEE 802.1X mediante un servidor de autenticación. Para ello, asigne la política `radius` a la lista `8021x` en el cuadro de diálogo *Device Security > Authentication List*.

El menú contiene los siguientes cuadros de diálogo:

- RADIUS Global
- RADIUS Authentication Server
- RADIUS Accounting Server
- RADIUS Authentication Statistics
- RADIUS Accounting Statistics

# 4.4.1 RADIUS Global

[ Network Security > RADIUS > Global ]

Este cuadro de diálogo le permite especificar la configuración básica para RADIUS.

### RADIUS configuration

Retransmits (max.)

Especifica cuántas veces retransmitirá el dispositivo una petición sin respuesta al servidor de autenticación antes de que el dispositivo envíe la solicitud a un servidor de autenticación alternativo.

Valores posibles:

- `1..15` (configuración por defecto: `4`)

Timeout [s]

Especifica durante cuántos segundos el dispositivo esperará una respuesta después de enviar una solicitud al servidor de autenticación antes de retransmitir la petición.

Valores posibles:

- `1..30` (configuración por defecto: `5`)

Accounting

Activa/desactiva la administración.

Valores posibles:

- `marked`
  La administración está activa.
  El dispositivo envía los datos de tráfico a un servidor de administración especificado en el cuadro de diálogo *Network Security > RADIUS > Accounting Server*.
- `unmarked` (configuración por defecto)
  La administración está inactiva.

NAS IP address (attribute 4)

Especifica la dirección IP que el dispositivo transfiere al servidor de autenticación como atributo 4. Escriba la dirección IP del dispositivo u otra dirección disponible.

**Nota:** El dispositivo solo incluye el atributo 4 si el paquete ha sido desencadenado por la solicitud de autenticación *802.1X* de un dispositivo final (solicitante).

Valores posibles:

- Dirección IPv4 válida (configuración por defecto: `0.0.0.0`)

En muchos casos, hay un cortafuegos entre el dispositivo y el servidor de autenticación. La Traducción de direcciones de red (NAT, Network Address Translation) del cortafuegos cambia la dirección IP original y el servidor de autenticación recibe la dirección IP traducida del dispositivo.

El dispositivo transfiere la dirección IP de este campo sin cambiar a lo largo de la Traducción de direcciones de red (NAT).

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

Reset

Elimina las estadísticas del cuadro de diálogo *Network Security > RADIUS > Authentication Statistics* y del cuadro de diálogo *Network Security > RADIUS > Accounting Statistics*.

## 4.4.2 RADIUS Authentication Server

[Network Security > RADIUS > Authentication Server]

Este cuadro de diálogo le permite hasta 8 servidores de autenticación. Un servidor de autenticación autentica y autoriza a los usuarios cuando el dispositivo reenvía los datos de acceso al servidor.

El dispositivo envía los datos de acceso al servidor de autenticación primario especificado. Cuando el servidor no responde, el dispositivo se pone en contacto con el servidor de autenticación especificado en la posición más alta de la tabla. Si no se recibe respuesta tampoco de este servidor, el dispositivo se dirige al siguiente servidor de la tabla.

### Tabla

Index

Muestra el número de índice al que la entrada de la tabla hace referencia.

Name

Muestra el nombre del servidor.

Para cambiar el valor, haga clic en el campo correspondiente.

Valores posibles:

- Cadena de caracteres ASCII alfanuméricos con entre 1 y 32 caracteres (configuración por defecto: `Default-RADIUS-Server`)

Address

Especifica la dirección IP del servidor.

Valores posibles:

- Dirección IPv4 válida

Destination UDP port

Especifica el número del puerto UDP en el que el servidor recibe solicitudes.

Valores posibles:

- `0..65535` (configuración por defecto: `1812`)
  Excepción: el puerto `2222` está reservado para funciones internas.

Secret

Muestra ****** (asteriscos) al especificar una contraseña con la que el dispositivo iniciará sesión en el servidor. Para cambiar una contraseña, haga clic en el campo correspondiente.

Valores posibles:

- Cadena de caracteres ASCII alfanuméricos con entre 1 y 64 caracteres

Recibirá la contraseña del administrador del servidor de autenticación.

Primary server

Establece el servidor de autenticación como primario o secundario.

Valores posibles:

- `marked`
  El servidor aparece establecido como servidor de autenticación primario. El dispositivo envía los datos de acceso para la autenticación de los usuarios a este servidor de autenticación.
  Al activar varios servidores, el dispositivo establece el último servidor activo como el servidor de autenticación primario.
- `unmarked` (configuración por defecto)
  El servidor es el servidor de autenticación secundario. Si el dispositivo no recibe una respuesta del servidor de autenticación primario, el dispositivo envía los datos de acceso al servidor de autenticación secundario.

Active

Activa/desactiva la conexión con el servidor.

El dispositivo utiliza el servidor, si especifica el valor *Device Security > Authentication List* en el cuadro de diálogo `radius`, en una de las filas de *Policy 1* a *Policy 5*.

Valores posibles:

- `marked` (configuración por defecto)
  La conexión está activa. El dispositivo envía los datos de acceso para la autenticación de los usuarios a este servidor si se cumplen las condiciones previas mencionadas anteriormente.
- `unmarked`
  La conexión está inactiva. El dispositivo no envía datos de acceso a este servidor.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

Abre la ventana *Create* para añadir una entrada nueva a la tabla.

- En el campo *Index*, especifique el número de índice.
- En el campo *Address*, especifique la dirección IP del servidor.

## 4.4.3 RADIUS Accounting Server

[Network Security > RADIUS > Accounting Server]

Este cuadro de diálogo le permite hasta 8 servidores de administración. Un servidor de administración registra los datos de tráfico producidos durante la autenticación del puerto según el estándar IEEE 802.1X. Como requisito previo, debe activar la función *Accounting* en el menú *Network Security > RADIUS > Global*.

El dispositivo envía los datos de tráfico al primer servidor de administración accesible. Cuando el servidor de administración no responde, el dispositivo se pone en contacto con el siguiente servidor de la tabla.

### Tabla

Index

Muestra el número de índice al que la entrada de la tabla hace referencia.

Valores posibles:

- `1..8`

Name

Muestra el nombre del servidor.

Para cambiar el valor, haga clic en el campo correspondiente.

Valores posibles:

- Cadena de caracteres ASCII alfanuméricos con entre 1 y 32 caracteres (configuración por defecto: `Default-RADIUS-Server`)

Address

Especifica la dirección IP del servidor.

Valores posibles:

- Dirección IPv4 válida

Destination UDP port

Especifica el número del puerto UDP en el que el servidor recibe solicitudes.

Valores posibles:

- `0..65535` (configuración por defecto: `1813`)
  Excepción: el puerto `2222` está reservado para funciones internas.

Secret

Muestra ****** (asteriscos) al especificar una contraseña con la que el dispositivo iniciará sesión en el servidor. Para cambiar una contraseña, haga clic en el campo correspondiente.

Valores posibles:

- Cadena de caracteres ASCII alfanuméricos con entre 1 y 16 caracteres

Recibirá la contraseña del administrador del servidor de autenticación.

Active

Activa/desactiva la conexión con el servidor.

Valores posibles:

- `marked` (configuración por defecto)
  La conexión está activa. El dispositivo envía los datos de tráfico a este servidor si se cumplen las condiciones previas mencionadas anteriormente.
- `unmarked`
  La conexión está inactiva. El dispositivo no envía datos de tráfico a este servidor.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

Abre la ventana *Create* para añadir una entrada nueva a la tabla.

- En el campo *Index*, especifique el número de índice.
- En el campo *Address*, especifique la dirección IP del servidor.

# 4.4.4 RADIUS Authentication Statistics

[Network Security > RADIUS > Authentication Statistics]

Este cuadro de diálogo muestra información sobre la comunicación entre el dispositivo y el servidor de autenticación. La tabla muestra la información de cada servidor en una fila individual.

Para eliminar las estadísticas, haga clic en el cuadro de diálogo *Network Security > RADIUS > Global* en el botón ☰ y, a continuación, en el elemento *Reset*.

### Tabla

Name

Muestra el nombre del servidor.

Address

Muestra la dirección IP del servidor.

Round trip time

Muestra el intervalo de tiempo en centésimas de segundo transcurrido entre la última respuesta recibida del servidor (Respuesta al acceso/desafío de acceso) y el envío del paquete de datos correspondiente (Petición de acceso).

Access requests

Muestra el número de paquetes de datos de acceso enviados por el dispositivo al servidor. Este valor no tiene en cuenta repeticiones.

Retransmitted access-request packets

Muestra el número de paquetes de datos de acceso retransmitidos por el dispositivo al servidor.

Access accepts

Muestra el número de paquetes de datos de aceptación de acceso que el dispositivo ha recibido del servidor.

Access rejects

Muestra el número de paquetes de datos de rechazo de acceso que el dispositivo ha recibido del servidor.

Access challenges

Muestra el número de paquetes de datos de desafío de acceso que el dispositivo ha recibido del servidor.

Malformed access responses

Muestra el número de paquetes de datos de respuesta de acceso malformados que el dispositivo ha recibido del servidor (incluyendo paquetes de datos con una longitud no válida).

Bad authenticators

Muestra el número de paquetes de datos de respuesta de acceso con un autenticador no válido que el dispositivo ha recibido del servidor.

Pending requests

Muestra el número de paquetes de datos de petición de acceso enviados por el dispositivo al servidor que aún no han recibido respuesta del servidor.

Timeouts

Muestra cuántas veces no se ha recibido respuesta del servidor antes de que haya transcurrido el tiempo de espera especificado.

Unknown types

Muestra el número de paquetes de datos con un tipo de datos desconocido que el dispositivo ha recibido del servidor en el puerto de autenticación.

Packets dropped

Muestra el número de paquetes de datos que el dispositivo ha recibido del servidor en el puerto de autenticación y, a continuación, ha descartado.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

# 4.4.5 RADIUS Accounting Statistics

[ Network Security > RADIUS > Accounting Statistics ]

Este cuadro de diálogo muestra información sobre la comunicación entre el dispositivo y el servidor de administración. La tabla muestra la información de cada servidor en una fila individual.

Para eliminar las estadísticas, haga clic en el cuadro de diálogo *Network Security > RADIUS > Global* en el botón ☰ y, a continuación, en el elemento *Reset*.

### Tabla

Name

Muestra el nombre del servidor.

Address

Muestra la dirección IP del servidor.

Round trip time

Muestra el intervalo de tiempo en centésimas de segundo transcurrido entre la última respuesta recibida del servidor (Respuesta de administración) y el envío del paquete de datos correspondiente (Petición de administración).

Accounting-request packets

Muestra el número de paquetes de datos de petición de administración enviados por el dispositivo al servidor. Este valor no tiene en cuenta repeticiones.

Retransmitted accounting-request packets

Muestra el número de paquetes de datos de petición de administración retransmitidos por el dispositivo al servidor.

Received packets

Muestra el número de paquetes de datos de respuesta de administración que el dispositivo ha recibido del servidor.

Malformed packets

Muestra el número de paquetes de datos de respuesta de administración malformados que el dispositivo ha recibido del servidor (incluyendo paquetes de datos con una longitud no válida).

Bad authenticators

Muestra el número de paquetes de datos de respuesta de administración con un autenticador no válido que el dispositivo ha recibido del servidor.

Pending requests

Muestra el número de paquetes de datos de petición de administración enviados por el dispositivo al servidor que aún no han recibido respuesta del servidor.

Timeouts

Muestra cuántas veces no se ha recibido respuesta del servidor antes de que haya transcurrido el tiempo de espera especificado.

Unknown types

Muestra el número de paquetes de datos con un tipo de datos desconocido que el dispositivo ha recibido del servidor en el puerto de administración.

Packets dropped

Muestra el número de paquetes de datos que el dispositivo ha recibido del servidor en el puerto de administración y, a continuación, ha descartado.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## 4.5 DoS

[ Network Security > DoS ]

La Denegación de servicio (DoS) es un ataque cibernético cuyo objetivo es inhabilitar servicios o dispositivos específicos. En este cuadro de diálogo podrá configurar varios filtros para ayudar a proteger el propio dispositivo y otros dispositivos de la red de un ataque DoS.

El menú contiene los siguientes cuadros de diálogo:
- DoS Global

## 4.5.1 DoS Global

[ Network Security > DoS > Global ]

En este cuadro de diálogo podrá especificar la configuración DoS para los protocolos TCP/UDP, IP y ICMP.

### TCP/UDP

Un escáner utiliza búsquedas de puertos para preparar la red ante ataques. El escáner utiliza diferentes técnicas para identificar dispositivos en funcionamiento y puertos abiertos. Este cuadro le permite activar filtros para técnicas de escaneado específicas.

El dispositivo es compatible con la detección de los siguientes tipos de escaneado:
- Escaneado Null
- Escaneado Xmas
- Escaneado SYN/FIN
- Ataques TCP Offset
- Ataques TCP SYN
- Ataques L4 Port
- Escaneado Minimal Header

Null Scan filter

Activa/desactiva 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.

Valores posibles:
- `marked`
  El filtro está activo.
- `unmarked` (configuración por defecto)
  El filtro está inactivo.

Xmas filter

Activa/desactiva 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.

Valores posibles:
- `marked`
  El filtro está activo.
- `unmarked` (configuración por defecto)
  El filtro está inactivo.

SYN/FIN filter

Activa/desactiva el filtro SYN/FIN.

El dispositivo detecta paquetes de datos entrantes con las marcas TCP *SYN* y *FIN* establecidas simultáneamente y las descarta.

Valores posibles:

- `marked`
  El filtro está activo.
- `unmarked` (configuración por defecto)
  El filtro está inactivo.

TCP Offset protection

Activa/desactiva la protección TCP Offset

La protección TCP Offset detecta paquetes de datos TCP entrantes cuyo campo Offset de fragmentos en el encabezado IP sea igual a 1 y los descarta.

La protección TCP Offset acepta paquetes UDP y ICMP cuyo campo Offset de fragmentos en el encabezado IP sea igual a 1.

Valores posibles:

- `marked`
  La protección está activa.
- `unmarked` (configuración por defecto)
  La protección está inactiva.

TCP SYN protection

Activa/desactiva la protección TCP SYN.

La protección TCP SYN detecta paquetes de datos entrantes con la marca TCP SYN configurada y un puerto de origen L4 < 1024 y los descarta.

Valores posibles:

- `marked`
  La protección está activa.
- `unmarked` (configuración por defecto)
  La protección está inactiva.

L4 Port protection

Activa/desactiva la protección L4 Port.

La protección L4 Port detecta paquetes de datos TCP y UDP entrantes cuyo número de puerto de origen y número de puerto de destino sean idénticos y los descarta.

Valores posibles:

- `marked`
  La protección está activa.
- `unmarked` (configuración por defecto)
  La protección está inactiva.

### IP

Este cuadro le permite activar o desactivar el filtro Land Attack. Con el método del ataque de tierra, la estación atacante envía paquetes de datos cuyas direcciones de origen y de destino sean idénticas a las del receptor. Cuando activa este filtro, el dispositivo detecta paquetes de datos con direcciones de origen y destino idénticas y descarta estos paquetes de datos.

Land Attack filter

Activa/desactiva el filtro Land Attack.

El filtro Land Attack detecta paquetes de datos de IP entrantes cuyas direcciones IP de origen y de destino sean idénticas y las descarta.

Valores posibles:

- `marked`
  El filtro está activo.
- `unmarked` (configuración por defecto)
  El filtro está inactivo.

### ICMP

El cuadro de diálogo le proporciona opciones de filtro para los siguientes parámetros ICMP:
- Paquetes de datos fragmentados
- Paquetes ICMP a partir de un tamaño específico
- Pings Broadcast

Filter fragmented packets

Activa/desactiva el filtro de paquetes ICMP fragmentados.

El filtro detecta paquetes ICMP fragmentados y los descarta.

Valores posibles:

- `marked`
  El filtro está activo.
- `unmarked` (configuración por defecto)
  El filtro está inactivo.

Filter by packet size

Activa/desactiva el filtro de paquetes ICMP entrantes.

El filtro detecta paquetes ICMP cuyo tamaño de carga útil sobrepase el tamaño especificado en el campo *Allowed payload size [byte]* y los descarta.

Valores posibles:

- `marked`
  El filtro está activo.
- `unmarked` (configuración por defecto)
  El filtro está inactivo.

Allowed payload size [byte]

Especifica el tamaño máximo permitido de carga útil de paquetes ICMP en bytes.

Marque la casilla *Filter by packet size* si desea que el dispositivo descarte paquetes de datos entrantes cuyo tamaño de carga útil sobrepase el tamaño máximo permitido para paquetes ICMP.

Valores posibles:

- `0..1472` (configuración por defecto: `512`)

Drop broadcast ping

Activa/desactiva el filtro de Pings Broadcast. Los Pings Broadcast son indicios conocidos de Ataques Smurf.

Valores posibles:

- `marked`
  El filtro está activo.
  El dispositivo detecta Pings Broadcast y los rechaza.
- `unmarked` (configuración por defecto)
  El filtro está inactivo.

### Information

Packets dropped

Muestra el número de paquetes de datos que el dispositivo ha descartado.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## 4.6 DHCP Snooping

[ Network Security > DHCP Snooping ]

DHCP Snooping es una función que admite la seguridad de red. DHCP Snooping supervisa paquetes DHCP entre el cliente y el servidor DHCP y actúa como un cortafuegos entre los hosts no protegidos y los servidores DHCP protegidos.

En este cuadro de diálogo puede configurar y supervisar las siguientes propiedades del dispositivo:

- Valide paquetes DHCP de fuentes no fiables y filtrar paquetes no válidos.
- Limite el tráfico de datos DHCP de fuente fiables y no fiables.
- Configure y actualice la base de datos de vinculación de DHCP Snooping. Esta base de datos contiene la dirección MAP e IP, la VLAN y el puerto de clientes DHCP en puertos no fiables.
- Valide solicitudes de seguimiento de hosts no fiables basándose en la base de datos de vinculación de DHCP Snooping.

Puede activar la función DHCP Snooping globalmente y para una VLAN específica. Especifique el estado de la seguridad (fiable o no fiable) en puertos individuales. Compruebe que se pueda acceder al servicio DHCP a través de puertos fiables. Para DHCP Snooping normalmente debe configurar los puertos de usuario/cliente como no fiables y los puertos de vínculo superior como fiables.

El menú contiene los siguientes cuadros de diálogo:

- DHCP Snooping Global
- DHCP Snooping Configuration
- DHCP Snooping Statistics
- DHCP Snooping Bindings

# 4.6.1 DHCP Snooping Global

[ Network Security > DHCP Snooping > Global ]

Este cuadro de diálogo le permite configurar los parámetros globales de DHCP Snooping de su dispositivo:

- Activar/desactivar *DHCP Snooping* globalmente.
- Activar/desactivar *Auto-Disable* globalmente.
- Activar/desactivar la comprobación de la dirección MAC de origen.
- Configure el nombre, la ubicación de almacenamiento y el intervalo de almacenamiento de la base de datos de vinculación.

### Operation

Operation

Activa/desactiva la función DHCP Snooping globalmente.

Valores posibles:

- `On`
- `Off` (configuración por defecto)

### Configuration

Verify MAC

Activa/desactiva la verificación de la dirección MAC de origen en el paquete de Ethernet.

Valores posibles:

- `marked`
  La verificación de la dirección MAC de origen está activa.
  El dispositivo compara la dirección MAC de origen con la dirección MAC del cliente en el paquete DHCP recibido.
- `unmarked` (configuración por defecto)
  La verificación de la dirección MAC de origen está inactiva.

Auto-disable

Activa/desactiva la función *Auto-Disable* para la *DHCP Snooping*.

Valores posibles:

- `marked`
  La función *Auto-Disable* de *DHCP Snooping* está activa.
  Marque también la casilla de verificación en la columna *Auto-disable* de la pestaña *Port* en el cuadro de diálogo *Network Security > DHCP Snooping > Configuration* para los puertos correspondientes.
- `unmarked` (configuración por defecto)
  La función *Auto-Disable* de *DHCP Snooping* está inactiva.

### Binding database

Remote file name

Especifica el nombre del archivo en el que el dispositivo guarda la base de datos de vinculación de DHCP Snooping.

**Nota:**

El dispositivo guarda solo vinculaciones dinámicas en la base de datos de vinculación persistente. El dispositivo guarda vinculaciones estáticas en el perfil de configuración.

Remote IP address

Especifica la dirección IP remota en la que el dispositivo guarda la base de datos de vinculación de DHCP Snooping persistente. Con el valor `0.0.0.0` el dispositivo guarda la base de datos de vinculación localmente.

Valores posibles:

- Dirección IPv4 válida
- `0.0.0.0` (configuración por defecto)
  El dispositivo guarda la base de datos de vinculación de DHCP Snooping localmente.

Store interval [s]

Especifica el período de tiempo en segundos tras el cual el dispositivo guarda la base de datos de vinculación de DHCP Snooping cuando el dispositivo identifica un cambio en la base de datos.

Valores posibles:

- `15..86400` (configuración por defecto: `300`)

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## 4.6.2 DHCP Snooping Configuration

[ Network Security > DHCP Snooping > Configuration ]

Este cuadro de diálogo le permite configurar DHCP Snooping para puertos y VLAN individuales.

El cuadro de diálogo contiene las siguientes pestañas:
- [Port]
- [VLAN ID]

### [Port]

En esta pestaña, configure la función *DHCP Snooping* para puertos individuales.
- Configure un puerto como fiable/no fiable.
- Active/desactive el registro de paquetes no válidos para puertos individuales.
- Limite el número de paquetes DHCP.
- Desactive un puerto automáticamente si el tráfico de datos DHCP supera el límite especificado.

#### Tabla

Port

Muestra el número de puerto.

Trust

Activa/desactiva el estado de la seguridad (fiable o no fiable) del puerto.

Si la función está activa, el puerto se configurará como fiable. Normalmente, tiene conectado el puerto de confianza a un servidor DHCP.

Cuando esta función está inactiva, el puerto se configura como no fiable.

Valores posibles:
- `marked`
  El puerto está especificado como fiable. DHCP Snooping desvía paquetes de cliente permitidos a través de puertos fiables.
- `unmarked` (configuración por defecto)
  El puerto está configurado como no fiable. En puertos no fiables, el dispositivo compara el puerto receptor con el puerto cliente en la base de datos de vinculación.

Log

Activa/desactiva el registro de paquetes no válidos que el dispositivo determina en este puerto.

Valores posibles:
- `marked`
  El registro de paquetes no válidos está activo.
- `unmarked` (configuración por defecto)
  El registro de paquetes no válidos está inactivo.

Rate limit

Especifica el número máximo de paquetes DHCP por intervalo de ráfaga para este puerto. Si el número de paquetes DHCP entrantes está superando actualmente el límite especificado en un intervalo de ráfaga, el dispositivo descartará los paquetes DHCP entrantes adicionales.

Valores posibles:

- `-1` (configuración por defecto)
  Desactiva la limitación del número de paquetes DHCP por intervalo de ráfaga en este puerto.
- `0..150`paquetes por intervalo
  Limita el número máximo de paquetes DHCP por intervalo de ráfaga en este puerto.

Especifique el intervalo de ráfaga en la columna *Burst interval*.

Si activa la función de desactivación automática, el dispositivo desactivará también el puerto. La función de desactivación automática se encuentra en la columna *Auto-disable*.

Burst interval

Especifica la duración del intervalo de ráfaga en segundos en este puerto. El intervalo de ráfaga es relevante para la función de limitación de velocidad.

Especifique el número máximo de paquetes DHCP por intervalo de ráfaga en la columna *Rate limit*.

Valores posibles:

- `1..15` (configuración por defecto: `1`)

Auto-disable

Activa/desactiva la función *Auto-Disable* para los parámetros que la función *DHCP Snooping* está supervisando en el puerto.

Valores posibles:

- `marked` (configuración por defecto)
  La función *Auto-Disable* está activa en el puerto.
  Como requisito previo, en el cuadro de diálogo *Network Security > DHCP Snooping > Global* debe estar marcada la casilla de verificación *Auto-disable* del cuadro *Configuration*.
  - Si el puerto recibe más paquetes DHCP que los especificados en el campo *Rate limit* en el tiempo especificado en la columna *Burst interval*, el dispositivo desactiva el puerto. El LED de "Estado de enlace" del puerto parpadea 3 veces por período.
  - El cuadro de diálogo *Diagnostics > Ports > Auto-Disable* muestra qué puertos están desactivados actualmente debido a que se han superado los parámetros.
  - La función *Auto-Disable* reactiva el puerto automáticamente. Para esto, vaya al cuadro de diálogo *Diagnostics > Ports > Auto-Disable* y especifique un período de espera para el puerto correspondiente en la columna *Reset timer [s]*.
- `unmarked`
  La función *Auto-Disable* en el puerto está inactiva.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## [VLAN ID]

En esta pestaña, configure la función *DHCP Snooping* para VLAN individuales.

### Tabla

VLAN ID

Muestra el ID de la VLAN al que hace referencia la entrada de la tabla.

Active

Activa/desactiva la función *DHCP Snooping* en esta VLAN.

La función *DHCP Snooping* reenvía mensajes de cliente DHCP válidos a los puertos de confianza de VLAN sin la función *Routing*.

Valores posibles:

- `marked`
  La función *DHCP Snooping* debe estar activa en esta VLAN.
- `unmarked` (configuración por defecto)
  La función *DHCP Snooping* está inactiva en esta VLAN.
  El dispositivos reenvía paquetes DHCP de acuerdo con los ajustes de conmutación sin supervisar los paquetes. La base de datos de vinculación no sufre modificaciones.

**Nota:** Para activar DHCP Snooping para un puerto, active la función *DHCP Snooping* globalmente en el cuadro de diálogo *Network Security > DHCP Snooping > Global*. Compruebe que ha asignado el puerto a una VLAN que tenga DHCP Snooping activado.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

# 4.6.3 DHCP Snooping Statistics

[ Network Security > DHCP Snooping > Statistics ]

Con DHCP Snooping, el dispositivo registra los errores detectados y genera estadísticas. En este cuadro de diálogo podrá supervisar las estadísticas de DHCP Snooping de cada puerto.

El dispositivo registra lo siguiente:
- Errores detectados durante la validación de la dirección MAC del cliente DHCP
- Mensajes de cliente DHCP con un puerto incorrecto detectado
- Mensajes de servidor DHCP a puertos no fiables

### Tabla

Port

Muestra el número de puerto.

MAC verify failures

Muestra el número de discrepancias existentes entre la dirección MAC del cliente DHCP en el campo "chaddr" del paquete de datos de DHCP y la dirección de origen en el paquete de Ethernet.

Invalid client messages

Muestra el número de mensajes de cliente DHCP entrantes recibidos en el puerto para el que el dispositivo espera al cliente de otro puerto de acuerdo con la base de datos de vinculación de DHCP Snooping.

Invalid server messages

Muestra el número de mensajes del servidor DHCP recibidos por el dispositivo en el puerto no fiable.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

Reset

Restablece toda la tabla.

# 4.6.4 DHCP Snooping Bindings

[Network Security > DHCP Snooping > Bindings]

DHCP Snooping utiliza mensajes DHCP para configurar y actualizar la base de datos de vinculación.

- Vinculaciones estáticas
  El dispositivo le permite especificar hasta 256 vinculaciones de DHCP Snooping estáticas en la base de datos.
- Vinculaciones dinámicas
  La base de datos de vinculaciones dinámicas contiene datos para clientes solamente en los puertos no fiables.

Este menú le permite especificar la configuración de las vinculaciones estáticas y dinámicas.

- Configure nuevas vinculaciones estáticas y establézcalas como activas/inactivas.
- Muestre, active/desactive o elimine vinculaciones estáticas que se hayan configurado.

### Tabla

MAC address

Especifica la dirección MAC en la entrada de tabla que vincula a una *IP address* y un *VLAN ID*.

Valores posibles:

- Dirección MAC Unicast válida
  Especifique el valor separándolo con dos puntos, por ejemplo `00:11:22:33:44:55`.

IP address

Especifica la dirección IP para la asignación de DHCP Snooping estática.

Valores posibles:

- Dirección Unicast IPv4 válida inferior a `224.x.x.x` y situada fuera del intervalo `127.0.0.0/8` (configuración por defecto: `0.0.0.0`)

VLAN ID

Especifica el ID de la VLAN a la que se aplica la entrada de la tabla.

Valores posibles:

- `<ID of the VLANs that are set up>`

Port

Especifica el puerto para la vinculación de DHCP Snooping estática.

Valores posibles:

- Puertos disponibles

Remaining binding time

Muestra el tiempo restante para la vinculación de DHCP Snooping dinámica.

Active

Activa/desactiva la vinculación de DHCP Snooping estática.

Valores posibles:

- `marked`
  La vinculación de DHCP Snooping estática está activa.
- `unmarked` (configuración por defecto)
  La vinculación de DHCP Snooping estática está inactiva.

**Botones**

Encontrará la descripción de los botones estándar en la sección "Botones" en página 17.

Abre la ventana *Create* para añadir una entrada nueva a la tabla.

En el campo *MAC address*, especifique la dirección MAC que vincula a una dirección IP y un ID de VLAN.

Elimina la entrada de la tabla seleccionada.

Como requisito previo, la casilla de la columna *Active* debe estar sin marcar.

Asimismo, el dispositivo elimina las vinculaciones dinámicas de este puerto creadas mediante la función *IP Source Guard*.

## 4.7 IP Source Guard

[Network Security > IP Source Guard]

*IP Source Guard* (IPSG) es una función que admite la seguridad de red. La función filtra paquetes de datos de IP basados en el ID de origen (dirección IP de origen o dirección MAC de origen) del suscriptor. IPSG le ayuda a proteger la red frente a ataques de tipo suplantación de identidad de direcciones IP/MAC.

**IPSG y DHCP Snooping**
La protección de fuente IP actúa en combinación con la función *DHCP Snooping* del puerto.

*DHCP Snooping* descarta los paquetes de datos IP en puertos no fiables, excepto los mensajes DHCP. Cuando el dispositivo recibe respuestas de DHCP y la base de datos de vinculación de DHCP Snooping está configurada, el dispositivo crea una lista de control de acceso de VLAN (VACL) para cada puerto que contiene los ID de origen de los suscriptores.

Configure los parámetros de la función *DHCP Snooping* para puertos y VLAN individuales en el cuadro de diálogo *Network Security > DHCP Snooping > Configuration*.

**La protección de fuente IPSG**
*IP Source Guard* actúa en combinación con la función *Port Security*. Consulte el cuadro de diálogo *Network Security > Port Security*. Previa solicitud, IPSG informa a la función *Port Security* si una dirección MAC pertenece a una vinculación válida.

- Si ha desactivado IPSG en el puerto de entrada, IPSG identifica el paquete de datos como válido.
- Si ha activado IPSG en el puerto de entrada, IPSG comprueba la dirección MAC mediante la base de datos de vinculaciones. Si se introduce la dirección MAC en la base de datos de vinculaciones, IPSG identifica el paquete de datos como válido o, de lo contrario, como no válido.

La función *Port Security* asume el procesamiento posterior de paquetes de datos no válidos. Especifique los ajustes de la función *Port Security* en el cuadro de diálogo *Network Security > Port Security*.

**Nota:** Para que el dispositivo pueda comprobar la dirección IP y MAC de los paquetes de datos recibidos en el puerto, active la función *Verify MAC*.

Para que el dispositivo compruebe el ID de VLAN y la dirección MAC del origen antes de reenviar el paquete de datos, active además la función *Port Security*. Consulte el cuadro de diálogo *Network Security > Port Security*.

El menú contiene los siguientes cuadros de diálogo:

- IP Source Guard Port
- IP Source Guard Bindings

## 4.7.1 IP Source Guard Port

[ Network Security > IP Source Guard > Port ]

Este cuadro de diálogo le permite mostrar y configurar las siguientes propiedades del dispositivo para cada puerto:

- Incluya/excluya direcciones MAC para la filtración.
- Active/desactive la función *IP Source Guard*.

### Tabla

Port

Muestra el número de puerto.

Verify MAC

Activa/desactiva la filtración basándose en la dirección MAC de origen si la función *IP Source Guard* está activa. El dispositivo ejecuta esta filtración además de la basada en la dirección IP de origen.

Valores posibles:

- `marked`
  La filtración basada en la dirección MAC de origen está activa.
  Para activar la función, marque la casilla de verificación *Active*.
- `unmarked` (configuración por defecto)
  La filtración basada en la dirección MAC de origen está inactiva.
  Para desactivar la función, desmarque también la casilla de verificación *Active*.

Active

Activa/desactiva la función *IP Source Guard* en el puerto.

Valores posibles:

- `marked`
  La función *IP Source Guard* está activa.
  Active también la función *DHCP Snooping* en el cuadro de diálogo *Network Security > DHCP Snooping > Global*.
- `unmarked` (configuración por defecto)
  La función *IP Source Guard* está inactiva.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## 4.7.2 IP Source Guard Bindings

[Network Security > IP Source Guard > Bindings]

Este cuadro de diálogo muestra vinculaciones de protección de origen IP estáticas y dinámicas.
- El dispositivo aprende vinculaciones dinámicas a través de DHCP Snooping. Consulte el cuadro de diálogo *Network Security > DHCP Snooping > Configuration*.
- Las vinculaciones estáticas son vinculaciones de protección de origen IP configuradas manualmente por el usuario. El cuadro de diálogo le permite editar vinculaciones estáticas.

### Tabla

MAC address

Muestra la dirección MAC de la vinculación.

IP address

Muestra la dirección IP de la vinculación.

VLAN ID

Muestra el ID de la VLAN de la vinculación.

Port

Muestra el número del puerto de la vinculación.

Hardware status

Muestra el estado del hardware de la vinculación.

El dispositivo aplica la vinculación al hardware solamente si la configuración es correcta. Antes de que el dispositivo aplique la vinculación IPSG estática al hardware, comprueba los siguientes requisitos previos:
- La casilla *Active* está marcada.
- La función *IP Source Guard* del puerto está activa y, en el cuadro de diálogo *Network Security > IP Source Guard > Port*, la casilla de verificación *Active* está marcada.

Valores posibles:
- `marked`
  La vinculación está activa y el dispositivo aplica esta al hardware.
- `unmarked`
  La vinculación está inactiva.

Active

Activa/desactiva la vinculación IPSG estática especificada entre la dirección MAC e IP especificada para la VLAN especificada en el puerto especificado.

Valores posibles:

- `marked`
  La vinculación IPSG estática está activa.
- `unmarked` (configuración por defecto)
  La vinculación IPSG estática está inactiva.

**Nota:** Para que la vinculación estática sea efectiva, active la función *IP Source Guard* en el puerto correspondiente. En el cuadro de diálogo *Network Security > IP Source Guard > Port*, marque la casilla de verificación *Active*.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

Abre la ventana *Create* para añadir una entrada nueva a la tabla.

- En el campo *MAC address*, especifique la dirección MAC de la vinculación estática.
- En el campo *IP address*, especifique la dirección IP de la vinculación estática.
- En el campo *VLAN ID*, especifique el ID de la VLAN.
- En el campo *Port*, especifique el ID de la VLAN.

Elimina la entrada de la tabla seleccionada.

Como requisito previo, la casilla de la columna *Active* debe estar sin marcar.

## 4.8 Dynamic ARP Inspection

[ Network Security > Dynamic ARP Inspection ]

*Dynamic ARP Inspection* es una función que admite la seguridad de red. Esta función analiza paquetes ARP, los registra y descarta paquetes ARP no válidos y hostiles.

La función *Dynamic ARP Inspection* ayuda a evitar un rango de ataques de intermediarios. Con este tipo de ataque, una estación hostil escucha el tráfico de datos de otros suscriptores invadiendo la caché ARP de sus incautos vecinos. La estación hostil envía solicitudes y respuestas ARP e introduce la dirección IP de otro suscriptor para su propia dirección MAC en la relación de dirección IP a MAC (vinculación).

Mediante las siguientes mediciones, la función *Dynamic ARP Inspection* ayuda a garantizar que el dispositivo solamente reenvíe solicitudes y respuestas ARP válidas.

- Escuchando solicitudes y respuestas ARP en puertos no fiables.
- Verificando que los paquetes determinados tengan una relación de dirección IP a MAC válida (vinculación) antes de que el dispositivo actualice la caché ARP local y antes de que reenvíe los paquetes a la dirección de destino relacionada.
- Descartando paquetes ARP no válidos.

El dispositivo le permite especificar hasta 100 ACL ARP activos (listas de acceso). Puede activar hasta 20 reglas para cada ACL ARP.

El menú contiene los siguientes cuadros de diálogo:

- Dynamic ARP Inspection Global
- Dynamic ARP Inspection Configuration
- Dynamic ARP Inspection ARP Rules
- Dynamic ARP Inspection Statistics

# 4.8.1 Dynamic ARP Inspection Global

[Network Security > Dynamic ARP Inspection > Global]

### Configuration

Verify source MAC

Activa/desactiva la verificación de la dirección MAC de origen. El dispositivo ejecuta la comprobación en solicitudes y respuestas ARP.

Valores posibles:

- `marked`
  La verificación de la dirección MAC de origen está activa.
  El dispositivo comprueba la dirección MAC de origen de los paquetes ARP recibidos.
  - El dispositivo transmite paquetes ARP con una dirección MAC de origen válida a la dirección de destino relacionada y actualiza la caché ARP local.
  - El dispositivo descarta paquetes ARP con una dirección MAC de origen no válida.
- `unmarked` (configuración por defecto)
  La verificación de la dirección MAC de origen está inactiva.

Verify destination MAC

Activa/desactiva la verificación de la dirección MAC de destino. El dispositivo ejecuta la comprobación en respuestas ARP.

Valores posibles:

- `marked`
  La verificación de la dirección MAC de destino está activa.
  El dispositivo comprueba la dirección MAC de destino de los paquetes ARP entrantes.
  - El dispositivo transmite paquetes ARP con una dirección MAC de destino válida a la dirección de destino relacionada y actualiza la caché ARP local.
  - El dispositivo descarta paquetes ARP con una dirección MAC de destino no válida.
- `unmarked` (configuración por defecto)
  La comprobación de la dirección MAC de destino de los paquetes ARP entrantes está inactiva.

Verify IP address

Activa/desactiva la verificación de la dirección IP.

En solicitudes ARP, el dispositivo comprueba la dirección IP de origen. En respuestas ARP, el dispositivo comprueba la dirección IP de origen y de destino.

El dispositivo designa las siguientes direcciones IP como no válidas:

- `0.0.0.0`
- Direcciones Broadcast `255.255.255.255`
- Direcciones Multicast `224.0.0.0/4` (clase D)
- Direcciones de clase E `240.0.0.0/4` (reservado para fines posteriores)
- Direcciones Loopback en el rango `127.0.0.0/8`.

Valores posibles:

- `marked`
  La verificación de la dirección IP está activa.
  El dispositivo comprueba la dirección IP de los paquetes ARP entrantes. El dispositivo transmite paquetes ARP con una dirección IP válida a la dirección de destino relacionada y actualiza la caché ARP local. El dispositivo descarta paquetes ARP con una dirección IP no válida.
- `unmarked` (configuración por defecto)
  La verificación de la dirección IP está inactiva.

Auto-disable

Activa/desactiva la función *Auto-Disable* para la *Dynamic ARP Inspection*.

Valores posibles:

- `marked`
  La función *Auto-Disable* de *Dynamic ARP Inspection* está activa.
  Marque también la casilla de verificación en la columna *Port* de la pestaña *Auto-disable* en el cuadro de diálogo *Network Security > Dynamic ARP Inspection > Configuration* para los puertos correspondientes.
- `unmarked` (configuración por defecto)
  La función *Auto-Disable* de *Dynamic ARP Inspection* está inactiva.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

# 4.8.2 Dynamic ARP Inspection Configuration

[Network Security > Dynamic ARP Inspection > Configuration]

El cuadro de diálogo contiene las siguientes pestañas:
- [Port]
- [VLAN ID]

## [Port]

### Tabla

Port

Muestra el número de puerto.

Trust

Activa/desactiva la supervisión de paquetes ARP en puertos no fiables.

Valores posibles:

- `marked`
  La supervisión está activa.
  El dispositivo supervisa los paquetes ARP en puertos no fiables.
  El dispositivo envía inmediatamente paquetes ARP a través de puertos fiables.
- `unmarked` (configuración por defecto)
  La supervisión está inactiva.

Rate limit

Especifica el número máximo de paquetes ARP por intervalo en este puerto. Si la velocidad de los paquetes ARP entrantes está superando actualmente el límite especificado en un intervalo de ráfaga, el dispositivo descartará los paquetes ARP entrantes adicionales. Especifique el intervalo de ráfaga en la columna *Burst interval*.

El dispositivo puede también desactivar el puerto si activa la función de desactivación automática. Active/desactive la función *Auto-Disable* en la columna *Auto-disable*.

Valores posibles:

- `-1` (configuración por defecto)
  Desactiva la limitación del número de paquetes ARP por intervalo de ráfaga en este puerto.
- `0..300`paquetes por intervalo
  Limita el número máximo de paquetes ARP por intervalo de ráfaga en este puerto.

Burst interval

Especifica la duración del intervalo de ráfaga en segundos en este puerto. El intervalo de ráfaga es relevante para la función de limitación de velocidad.

Especifique el número máximo de paquetes ARP por intervalo de ráfaga en la columna *Rate limit*.

Valores posibles:

- `1..15` (configuración por defecto: `1`)

Auto-disable

Activa/desactiva la función *Auto-Disable* para los parámetros que la función *Dynamic ARP Inspection* está supervisando en el puerto.

Valores posibles:

- `marked` (configuración por defecto)
  La función *Auto-Disable* está activa en el puerto.
  Como requisito previo, en el cuadro de diálogo *Network Security > Dynamic ARP Inspection > Global* debe estar marcada la casilla de verificación *Auto-disable* del cuadro *Configuration*.
  - Si el puerto recibe más paquetes ARP que los especificados en el campo *Rate limit* en el tiempo especificado en la columna *Burst interval*, el dispositivo desactiva el puerto. El LED de "Estado de enlace" del puerto parpadea 3 veces por período.
  - El cuadro de diálogo *Diagnostics > Ports > Auto-Disable* muestra qué puertos están desactivados actualmente debido a que se han superado los parámetros.
  - La función *Auto-Disable* reactiva el puerto automáticamente. Para esto, vaya al cuadro de diálogo *Diagnostics > Ports > Auto-Disable* y especifique un período de espera para el puerto correspondiente en la columna *Reset timer [s]*.
- `unmarked`
  La función *Auto-Disable* en el puerto está inactiva.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## [VLAN ID]

### Tabla

VLAN ID

Muestra el ID de la VLAN al que hace referencia la entrada de la tabla.

Log

Activa/desactiva el registro de paquetes ARP no válidos que el dispositivo determina en esta VLAN. Si el dispositivo detecta un error a la hora de comprobar la IP, la dirección MAC de origen o de destino o la relación de dirección IP a MAC (vinculación), el dispositivo identifica un paquete ARP como no válido.

Valores posibles:

- `marked`
  El registro de paquetes no válidos está activo.
  El dispositivo registra paquetes ARP no válidos.
- `unmarked` (configuración por defecto)
  El registro de paquetes no válidos está inactivo.

Binding check

Activa/desactiva la comprobación de paquetes ARP entrantes que el dispositivo recibe en puertos no fiables y en VLAN para las que la función *Dynamic ARP Inspection* se encuentra activa. Para estos paquetes ARP, el dispositivo comprueba el ACL ARP y la relación DHCP Snooping (vinculaciones).

Valores posibles:

- `marked` (configuración por defecto)
  La comprobación de la vinculación de paquetes ARP está activa.
- `unmarked`
  La comprobación de la vinculación de paquetes ARP está inactiva.

ACL strict

Activa/desactiva la comprobación estricta de paquetes ARP entrantes basada en las reglas ACL ARP especificadas.

Valores posibles:

- `marked`
  La comprobación estricta está activa.
  El dispositivo comprueba los paquetes ARP entrantes basados en la regla ACL ARP especificada en la columna *ARP ACL*.
- `unmarked` (configuración por defecto)
  La comprobación estricta está inactiva.
  El dispositivo comprueba los paquetes ARP entrantes basándose en la regla ACL ARP especificada en la columna *ARP ACL* y posteriormente en las entradas de la base de datos de DHCP Snooping.

ARP ACL

Especifica el ACL ARP que utiliza el dispositivo.

Valores posibles:

- `<rule mane>`
  Cree y Edite las reglas en el cuadro de diálogo *Network Security > Dynamic ARP Inspection > ARP Rules*.

Active

Activa/desactiva la función *Dynamic ARP Inspection* en esta VLAN.

Valores posibles:

- `marked`
  La función *Dynamic ARP Inspection* debe estar activa en esta VLAN.
- `unmarked` (configuración por defecto)
  La función *Dynamic ARP Inspection* está inactiva en esta VLAN.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

# 4.8.3 Dynamic ARP Inspection ARP Rules

[Network Security > Dynamic ARP Inspection > ARP Rules]

Este cuadro de diálogo le permite especificar reglas para comprobar y filtrar paquetes ARP.

### Tabla

Name

Muestra el nombre de la regla ARP.

Source IP address

Especifica la dirección de origen de los paquetes de datos de IP a los que el dispositivo aplica la regla.

Valores posibles:

- Dirección IPv4 válida
  El dispositivo aplica la regla a paquetes de datos de IP con la dirección de origen especificada.

Source MAC address

Especifica la dirección de origen de los paquetes de datos de MAC a los que el dispositivo aplica la regla.

Valores posibles:

- Dirección MAC válida
  El dispositivo aplica la regla a paquetes de datos de MAC con la dirección de origen especificada.

Active

Activa/desactiva la regla *ARP*.

Valores posibles:

- `marked` (configuración por defecto)
  La regla está activa.
- `unmarked`
  La regla está inactiva.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

Abre la ventana *Create* para añadir una entrada nueva a la tabla.

- En el campo *Name*, especifique el nombre de la regla ARP.
- En el campo *Source IP address*, especifique la dirección IP de origen de la regla ARP.
- En el campo *Source MAC address*, especifique la dirección MAC de origen de la regla ARP.

## 4.8.4 Dynamic ARP Inspection Statistics

[Network Security > Dynamic ARP Inspection > Statistics]

Esta ventana muestra el número de paquetes ARP descargados y reenviados en una descripción general.

### Tabla

VLAN ID

Muestra el ID de la VLAN al que hace referencia la entrada de la tabla.

Packets forwarded

Muestra el número de paquetes ARP que el dispositivo reenvía tras comprobarlos mediante la función *Dynamic ARP Inspection*.

Packets dropped

Muestra el número de paquetes ARP que el dispositivo descarta tras comprobarlos mediante la función *Dynamic ARP Inspection*.

DHCP drops

Muestra el número de paquetes ARP que el dispositivo descarta tras comprobar la relación de DHCP Snooping (vinculación).

DHCP permits

Muestra el número de paquetes ARP que el dispositivo reenvía tras comprobar la relación DHCP Snooping (vinculación).

ACL drops

Muestra el número de paquetes ARP que el dispositivo descarta tras comprobarlos mediante las reglas ACL ARP.

ACL permits

Muestra el número de paquetes ARP que el dispositivo reenvía tras comprobarlos mediante las reglas ACL ARP.

Bad source MAC

Muestra el número de paquetes ARP que el dispositivo descarta después de que la función *Dynamic ARP Inspection* haya detectado un error en la dirección MAC de origen.

Bad destination MAC

Muestra el número de paquetes ARP que el dispositivo descarta una vez que la función *Dynamic ARP Inspection* ha detectado un error en la dirección MAC de destino.

Invalid IP address

Muestra el número de paquetes ARP que el dispositivo descarta una vez que la función *Dynamic ARP Inspection* detecta un error en la dirección IP.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

Reset

Restablece toda la tabla.

## 4.9 ACL

[ Network Security > ACL ]

En este menú, puede especificar la configuración de las Listas de control de acceso (ACL). Las listas de control de acceso contienen reglas que el dispositivo aplica sucesivamente al flujo de datos en sus puertos o VLAN.

Si un paquete de datos cumple con los criterios de una o más reglas, el dispositivo aplicará la acción especificada en la primera regla que sea relevante para el flujo de datos. El dispositivo ignora las reglas siguientes. Las acciones posibles incluyen:
- *permit*: El dispositivo transmite el paquete de datos a un puerto o a una VLAN.
- *deny*: El dispositivo anula el paquete de datos.

En la configuración por defecto, el dispositivo reenvía todos los paquetes de datos. Una vez asigne una Lista de control de acceso a una interfaz o a una VLAN, este comportamiento cambiará. El dispositivo introduce una regla Deny-All implícita al final de una Lista de control de acceso. Como consecuencia, el dispositivo descarta paquetes de datos que no cumplan con ninguna de estas reglas. Si desea un comportamiento diferente, añada una regla de "permiso" al final de sus Listas de control de acceso.

Proceda de la siguiente manera para configurar Listas de control de acceso y reglas:
- ☐ Cree una regla y especifique su configuración. Consulte el cuadro de diálogo *Network Security > ACL > IPv4 Rule*, o el cuadro de diálogo *Network Security > ACL > MAC Rule*.
- ☐ Asigne la Lista de control de acceso a los puertos y VLAN del dispositivo. Consulte el cuadro de diálogo *Network Security > ACL > Assignment*.

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

# 4.9.1 ACL IPv4 Rule

[ Network Security > ACL > IPv4 Rule ]

En este cuadro de diálogo, especifique las reglas que el dispositivo aplicará a los paquetes de datos de IP.

Una Lista de control de acceso (grupo) contiene una o más reglas. El dispositivo aplica las reglas de una Lista de control de acceso de manera consecutiva, empezando con la regla con el valor más bajo en la columna *Index*.

El dispositivo le permite filtrar según los siguientes criterios:
- Dirección IP de origen o destino de un paquete de datos
- Tipo de protocolo de transmisión
- Puerto de origen o destino de un paquete de datos

### Tabla

Group name

Muestra el nombre de la Lista de control de acceso. La Lista de control de acceso contiene las reglas.

Index

Muestra el número de la regla en Lista de control de acceso.

Si la Lista de control de acceso contiene varias reglas, el dispositivo procesará primero la regla con el valor más bajo.

Match every packet

Especifica a qué paquetes de datos de IP el dispositivo aplicará la regla.

Valores posibles:

- `marked` (configuración por defecto)
  El dispositivo aplica la regla a todos los paquetes de datos de IP.
- `unmarked`
  El dispositivo aplica la regla a paquetes de datos de IP en función del valor en los campos *Source IP address*, *Destination IP address* y *Protocol*.

Source IP address

Especifica la dirección de origen de los paquetes de datos de IP a los que el dispositivo aplica la regla.

Valores posibles:

- `?.?.?.?` (configuración por defecto)
  El dispositivo aplica la regla a paquetes de datos de IP con cualquier dirección de origen.

- Dirección IPv4 válida
  El dispositivo aplica la regla a paquetes de datos de IP con la dirección de origen especificada. Utilice el carácter `?` como comodín.
  Por ejemplo `192.?.?.32`: el dispositivo aplica la regla a paquetes de datos de IP cuya dirección de origen empiece con `192.` y termine con `.32`.
- Dirección IPv4/máscara de bits válida
  El dispositivo aplica la regla a paquetes de datos de IP con la dirección de origen especificada. La máscara de bits inversa le permite especificar el rango de direcciones con precisión a nivel de bit.
  Por ejemplo `192.168.1.0/0.0.0.127`: el dispositivo aplica la regla a paquetes de datos de IP con una dirección de origen dentro del rango de `192.168.1.0` a `….127`.

Destination IP address

Especifica la dirección de destino de los paquetes de datos de IP a los que el dispositivo aplica la regla.

Valores posibles:

- `?.?.?.?` (configuración por defecto)
  El dispositivo aplica la regla a paquetes de datos con cualquier dirección de destino.
- Dirección IPv4 válida
  El dispositivo aplica la regla a paquetes de datos con la dirección de destino especificada. Utilice el carácter `?` como comodín.
  Por ejemplo `192.?.?.32`: el dispositivo aplica la regla a paquetes de datos de IP cuya dirección de origen empiece con `192.` y termine con `.32`.
- Dirección IPv4/máscara de bits válida
  El dispositivo aplica la regla a paquetes de datos con la dirección de destino especificada. La máscara de bits inversa le permite especificar el rango de direcciones con precisión a nivel de bit.
  Por ejemplo `192.168.1.0/0.0.0.127`: el dispositivo aplica la regla a paquetes de datos de IP con una dirección de destino dentro del rango de `192.168.1.0` a `….127`.

Protocol

Especifica el tipo de protocolo de los paquetes de datos de IP a los que el dispositivo aplica la regla.

Valores posibles:

- `any` (configuración por defecto)
  El dispositivo aplica la regla a todos los paquetes de datos de IP sin tener en cuenta el tipo de protocolo.
- `icmp`
- `igmp`
- `ip-in-ip`
- `tcp`
- `udp`
- `ip`

Source TCP/UDP port

Especifica el puerto de origen de los paquetes de datos de IP a los que el dispositivo aplica la regla. Como requisito previo, debe especificar el valor `TCP` o `UDP` en la columna *Protocol*.

Valores posibles:

- `any` (configuración por defecto)
  El dispositivo aplica la regla a todos los paquetes de datos de IP sin tener en cuenta el puerto de origen.
- `1..65535`
  El dispositivo aplica la regla únicamente a paquetes de datos de IP que contengan el puerto de origen especificado.

Destination TCP/UDP port

Especifica el puerto de destino de los paquetes de datos de IP a los que el dispositivo aplica la regla. Como requisito previo, debe especificar el valor `TCP` o `UDP` en la columna *Protocol*.

Valores posibles:

- `any` (configuración por defecto)
  El dispositivo aplica la regla a todos los paquetes de datos de IP sin tener en cuenta el puerto de destino.
- `1..65535`
  El dispositivo aplica la regla únicamente a paquetes de datos de IP que contengan el puerto de destino especificado.

Action

Especifica cómo procesará el dispositivo los paquetes de datos de IP recibidos cuando el dispositivo aplique la regla.

Valores posibles:

- *permit* (configuración por defecto)
  El dispositivo transmite los paquetes de datos de IP.
- *deny*
  El dispositivo anula los paquetes de datos de IP.

Log

Activa/desactiva el registro en el archivo de registro. Consulte el cuadro de diálogo *Diagnostics* > Report > *System Log*.

Valores posibles:

- `marked`
  El registro está activado.
  Como requisito previo, debe asignar la Lista de control de acceso en el cuadro de diálogo *Network Security > ACL > Assignment* a una VLAN o un puerto.
  El dispositivo registra en el archivo de registro, con un intervalo de 30 s, cuántas veces ha aplicado la regla de denegación a los paquetes de datos de IP.
- `unmarked` (configuración por defecto)
  El registro está desactivado.

El dispositivo le permite activar esta función para hasta 128 reglas de denegación.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

Abre la ventana *Create* para añadir una entrada nueva a la tabla.

- En el campo *Group name*, especifique el nombre de la Lista de control de acceso a la que pertenece esta regla.
- En el campo *Index*, especifique el número de la regla en Lista de control de acceso. Si la Lista de control de acceso contiene varias reglas, el dispositivo procesará primero la regla con el valor más bajo.

## 4.9.2 ACL MAC Rule

[ Network Security > ACL > MAC Rule ]

En este cuadro de diálogo, especifique las reglas que el dispositivo aplicará a los paquetes de datos de MAC.

Una Lista de control de acceso (grupo) contiene una o más reglas. El dispositivo aplica las reglas de una Lista de control de acceso de manera consecutiva, empezando con la regla con el valor más bajo en la columna *Index*.

El dispositivo le permite filtrar según la dirección MAC de origen o destino de un paquete de datos.

### Tabla

Group name

Muestra el nombre de la Lista de control de acceso. La Lista de control de acceso contiene las reglas.

Index

Muestra el número de la regla en Lista de control de acceso.

Si la Lista de control de acceso contiene varias reglas, el dispositivo procesará primero la regla con el valor más bajo.

Match every packet

Especifica a qué paquetes de datos de MAC el dispositivo aplicará la regla.

Valores posibles:

- `marked` (configuración por defecto)
  El dispositivo aplica la regla a todos los paquetes de datos de MAC.
- `unmarked`
  El dispositivo aplica la regla a paquetes de datos de MAC en función del valor en los campos *Source MAC address* y *Destination MAC address*.

Source MAC address

Especifica la dirección de origen de los paquetes de datos de MAC a los que el dispositivo aplica la regla.

Valores posibles:

- `??:??:??:??:??:??` (configuración por defecto)
  El dispositivo aplica la regla a paquetes de datos de MAC con cualquier dirección de origen.

- Dirección MAC válida
  El dispositivo aplica la regla a paquetes de datos de MAC con la dirección de origen especificada.
  Utilice el carácter `?` como comodín.
  Por ejemplo `00:11:??:??:??:??`: el dispositivo aplica la regla a paquetes de datos de MAC cuya dirección de origen empiece con `00:11`.
- Dirección MAC/máscara de bits válida
  El dispositivo aplica la regla a paquetes de datos de MAC con la dirección de origen especificada. La máscara de bits le permite especificar el rango de direcciones con precisión a nivel de bit.
  Por ejemplo `00:11:22:33:44:54/FF:FF:FF:FF:FF:FC`: el dispositivo aplica la regla a paquetes de datos de MAC con una dirección de origen dentro del rango de `00:11:22:33:44:54` a `…:57`.

Destination MAC address

Especifica la dirección de destino de los paquetes de datos de MAC a los que el dispositivo aplica la regla.

Valores posibles:

- `??:??:??:??:??:??` (configuración por defecto)
  El dispositivo aplica la regla a paquetes de datos de MAC con cualquier dirección de destino.
- Dirección MAC válida
  El dispositivo aplica la regla a paquetes de datos de MAC con la dirección de destino especificada.
  Utilice el carácter `?` como comodín.
  Por ejemplo `00:11:??:??:??:??`: el dispositivo aplica la regla a paquetes de datos de MAC cuya dirección de destino empiece con `00:11`.
- Dirección MAC/máscara de bits válida
  El dispositivo aplica la regla a paquetes de datos de MAC con la dirección de origen especificada. La máscara de bits le permite especificar el rango de direcciones con precisión a nivel de bit.
  Por ejemplo `00:11:22:33:44:54/FF:FF:FF:FF:FF:FC`: El dispositivo aplica la regla a paquetes de datos de MAC con una dirección de destino dentro del rango de `00:11:22:33:44:54` a `…:57`.

Action

Especifica cómo procesará el dispositivo los paquetes de datos de MAC recibidos cuando el dispositivo aplique la regla.

Valores posibles:

- *`permit`* (configuración por defecto)
  El dispositivo transmite los paquetes de datos de MAC.
- *`deny`*
  El dispositivo descarta los paquetes de datos de MAC.

Log

Activa/desactiva el registro en el archivo de registro. Consulte el cuadro de diálogo *Diagnostics* > Report > *System Log*.

Valores posibles:

- `marked`
  El registro está activado.
  Como requisito previo, debe asignar la Lista de control de acceso en el cuadro de diálogo *Network Security > ACL > Assignment* a una VLAN o un puerto.
  El dispositivo registra en el archivo de registro, con un intervalo de 30 s, cuántas veces ha aplicado la regla de denegación a los paquetes de datos de MAC.
- `unmarked` (configuración por defecto)
  El registro está desactivado.

El dispositivo le permite activar esta función para hasta 128 reglas de denegación.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

Abre la ventana *Create* para añadir una entrada nueva a la tabla.

- En el campo *Group name*, especifique el nombre de la Lista de control de acceso a la que pertenece esta regla.
- En el campo *Index*, especifique el número de la regla en Lista de control de acceso. Si la Lista de control de acceso contiene varias reglas, el dispositivo procesará primero la regla con el valor más bajo.

## 4.9.3 ACL Assignment

[Network Security > ACL > Assignment]

Este diálogo le permite asignar una o más Listas de control de acceso a los puertos y VLAN del dispositivo. Al asignar una prioridad estará especificando la secuencia de procesamiento, a condición de que haya asignado una o más Listas de control de acceso a un puerto o VLAN.

El dispositivo aplica las reglas de manera consecutiva, es decir, en la secuencia especificada en el índice de reglas. Especifique la prioridad de un grupo en la columna *Priority*. Cuanto menor sea el número, mayor será la prioridad. En este proceso, el dispositivo aplica las reglas con alta prioridad antes que las reglas con baja prioridad.

La asignación de Listas de control de acceso a puertos y VLAN produce los siguientes tipos de ACL:
- ACL de IPv4 basada en puerto
- ACL de MAC basada en puerto
- ACL de IPv4 basada en VLAN
- ACL de MAC basada en VLAN

El dispositivo le permite aplicar las listas de control de acceso a paquetes de datos recibidos (`inbound`).

**Nota:** Antes de activar la función, compruebe que al menos una entrada activa de la tabla le permite el acceso. De lo contrario, la conexión con el dispositivo finalizará si cambia la configuración. 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.

### Tabla

Group name

Muestra el nombre de la Lista de control de acceso. La Lista de control de acceso contiene las reglas.

Type

Muestra si la Lista de control de acceso contiene reglas MAC o reglas IPv4.

Valores posibles:

- *mac*
  La Lista de control de acceso contiene reglas MAC.
- *ip*
  La Lista de control de acceso contiene reglas IPv4.

Puede editar las Listas de control de acceso con reglas IPv4 en el cuadro de diálogo *Network Security > ACL > IPv4 Rule*. Puede editar las Listas de control de acceso con reglas MAC en el cuadro de diálogo *Network Security > ACL > MAC Rule*.

Port

Muestra el puerto al que se ha asignado la Lista de control de acceso. Este campo queda vacío si se ha asignado la Lista de control de acceso a una VLAN.

VLAN ID

Muestra la VLAN al que se ha asignado la Lista de control de acceso. Este campo queda vacío si se ha asignado la Lista de control de acceso a un puerto.

Direction

Muestra que el dispositivo aplica las Listas de control de acceso a los paquetes de datos recibidos.

Priority

Muestra la prioridad de la Lista de control de acceso.

Utilizando la prioridad, especifique la secuencia en la que el dispositivo aplica las Listas de control de acceso al flujo de datos. El dispositivo aplica las reglas en orden ascendente empezando por la prioridad `1`.

Valores posibles:

- `1..4294967295`

Si se ha asignado una Lista de control de acceso a un puerto y a una VLAN con la misma prioridad, el dispositivo aplicará primero las reglas al puerto.

Active

Muestra si la Lista de control de acceso en el puerto o en la VLAN está activa.

Valores posibles:

- `marked` (configuración por defecto)
  La Lista de control de acceso está activa.
- `unmarked`
  La Lista de control de acceso está inactiva.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

Abre el cuadro de diálogo *Create* para asignar una regla a un puerto o a una VLAN.

- En el campo *Port/VLAN*, especifique el puerto o el ID de VLAN.
- En el campo *Priority*, especifique la dirección MAC de origen de la regla ARP.
- En el campo *Direction*, especifique los paquetes de datos a los que el dispositivo aplica la regla.
- En el campo *Group name*, especifique qué regla el dispositivo asignará al puerto o a la VLAN.

# 5 Switching

El menú contiene los siguientes cuadros de diálogo:
- Switching Global
- Rate Limiter
- Filter for MAC Addresses
- IGMP Snooping
- Time-Sensitive Networking
- MRP-IEEE
- GARP
- QoS/Priority
- VLAN
- L2-Redundancy

## 5.1 Switching Global

[ Switching > Global ]

Este cuadro de diálogo le permite especificar los siguientes ajustes:
- Cambiar el Tiempo de caducidad de la tabla de direcciones
- Activar el control de flujo en el dispositivo

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.

A continuación, los dispositivos conectados no envían más paquetes de datos mientras dura la señalización. En puertos Uplink, esto puede provocar la aparición de pausas no deseadas durante el envío en el segmento de red de nivel superior ("contrapresión de ralentización").

### Configuration

MAC address

Muestra la dirección MAC del dispositivo.

Aging time [s]

Especifica el tiempo de caducidad en segundos.

Valores posibles:

- `10..500000` (configuración por defecto: `30`)

El dispositivo controla la antigüedad de las direcciones MAC Unicast aprendidas. El dispositivo elimina las entradas de direcciones que superen una antigüedad en particular (tiempo de caducidad) de su tabla de direcciones.

Puede encontrar la tabla de direcciones en el cuadro de diálogo *Switching > Filter for MAC Addresses*.

Flow control

Activa/desactiva el control de flujo en el dispositivo.

Valores posibles:

- `marked`
  El control de flujo está activo en el dispositivo.
  Active también el control de flujo en los puertos necesarios. Consulte el cuadro de diálogo *Basic Settings > Port*, pestaña *Configuration*, casilla en la columna *Flow control*.
- `unmarked` (configuración por defecto)
  El control de flujo está inactivo en el dispositivo.

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.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

# 5.2 Rate Limiter

[ Switching > Rate Limiter ]

El dispositivo le permite limitar el tráfico en los puertos para ayudarle a ofrecer un funcionamiento estable incluso con un volumen de tráfico elevado. Si el tráfico de un puerto supera el valor del tráfico introducido, el dispositivo descarta el exceso de tráfico en este puerto.

La función de limitador de carga solo funciona en la Capa 2 y se utiliza para limitar los efectos de las tormentas de paquetes de datos que desbordan el dispositivo (normalmente Broadcast).

La función de limitador de carga ignora la información del protocolo en capas superiores, como IP o TCP.

El cuadro de diálogo contiene las siguientes pestañas:
- [Ingress]
- [Egress]

## [Ingress]

En esta pestaña podrá activar la función *Rate Limiter*. El valor umbral especifica la cantidad máxima de tráfico que recibe el puerto. Si el tráfico de este puerto supera el valor límite, el dispositivo descarta el exceso de tráfico en este puerto.

### Tabla

Port

Muestra el número de puerto.

Threshold unit

Especifica la unidad del valor límite:

Valores posibles:
- *percent* (configuración por defecto)
  Especifica el valor límite como un porcentaje de la velocidad de transferencia del puerto.
- *pps*
  Especifica el valor límite en paquetes de datos por segundo.

Broadcast mode

Activa/desactiva la función de limitador de carga para los paquetes de datos Broadcast recibidos.

Valores posibles:
- marked
- unmarked (configuración por defecto)

Si se supera el valor límite, el dispositivo descarta los paquetes de datos Broadcast sobrantes en este puerto.

Broadcast threshold

Especifica el valor límite de los mensajes Broadcast en este puerto.

Valores posibles:

- `0..14880000` (configuración por defecto: `0`)
  El valor `0` desactiva la función del limitador de carga en este puerto.
  - Si selecciona el valor *`percent`* en la columna *Threshold unit*, introduzca un valor de porcentaje comprendido entre `1` y `100`.
  - Si selecciona el valor *`pps`* en la columna *Threshold unit*, introduzca un valor absoluto para la velocidad de transferencia.

Known multicast mode

Activa/desactiva la función de limitador de carga para los paquetes de datos Multicast conocidos recibidos.

Valores posibles:

- `marked`
- `unmarked` (configuración por defecto)

Si se supera el valor límite, el dispositivo descarta los paquetes de datos Multicast sobrantes en este puerto.

Known multicast threshold

Especifica el valor límite de los paquetes Multicast en este puerto.

Valores posibles:

- `0..14880000` (configuración por defecto: `0`)
  El valor `0` desactiva la función del limitador de carga en este puerto.
  - Si selecciona el valor *`percent`* en la columna *Threshold unit*, introduzca un valor de porcentaje comprendido entre `0` y `100`.
  - Si selecciona el valor *`pps`* en la columna *Threshold unit*, introduzca un valor absoluto para la velocidad de transferencia.

Unknown frame mode

Activa/desactiva la función de limitador de carga para los paquetes de datos Unicast y Multicast recibidos con una dirección de destino desconocida.

Valores posibles:

- `marked`
- `unmarked` (configuración por defecto)

Si se supera el valor límite, el dispositivo descarta los paquetes de datos Unicast sobrantes en este puerto.

Unknown frame threshold

Especifica el valor límite de los paquetes Unicast recibidos con una dirección de destino desconocida en este puerto.

Valores posibles:

- `0..14880000` (configuración por defecto: `0`)
  El valor `0` desactiva la función del limitador de carga en este puerto.
  - Si selecciona el valor *`percent`* en la *Threshold unit*, introduzca un valor de porcentaje comprendido entre `0` y `100`.
  - Si selecciona el valor *`pps`* en la columna *Threshold unit*, introduzca un valor absoluto para la velocidad de transferencia.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## [Egress]

En esta pestaña, especifique la velocidad de transmisión de salida del puerto.

### Tabla

Port

Muestra el número de puerto.

Bandwidth [%]

Especifica la velocidad de transmisión de salida.

Valores posibles:

- `0` (configuración por defecto)
  La limitación del ancho de banda está desactivada.
- `1..100`
  La limitación del ancho de banda está activada.
  Este valor especifica el porcentaje de la velocidad de enlace general del puerto en incrementos de 1%.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

# 5.3 Filter for MAC Addresses

[ Switching > Filter for MAC Addresses ]

Este cuadro de diálogo le permite visualizar y editar filtros de direcciones para la tabla de direcciones. Los filtros de direcciones especifican el modo en que se reenvían los paquetes de datos en el dispositivo en función de la dirección MAC de destino.

Cada fila de la tabla representa un filtro. El dispositivo configura los filtros automáticamente. El dispositivo le permite configurar filtros adicionales manualmente.

El dispositivo transmite los paquetes de datos del modo siguiente:

- Cuando la tabla contiene una entrada para la dirección de destino de un paquete de datos, el dispositivo transmite el paquete de datos desde el puerto de recepción hasta el puerto especificado en la entrada de la tabla.
- Si no hay ninguna entrada de tabla para la dirección de destino, el dispositivo transmite el paquete de datos desde el puerto de recepción hasta todos los demás puertos.

### Tabla

Para eliminar las direcciones MAC de la tabla de direcciones, haga clic en el botón *Reset MAC address table* del cuadro de diálogo *Basic Settings > Restart*.

Address

Muestra la dirección MAC de destino a la que se aplica la entrada de la tabla.

VLAN ID

Muestra el ID de la VLAN a la que se aplica la entrada de la tabla.

El dispositivo aprende las direcciones MAC de cada VLAN por separado (aprendizaje independiente de la VLAN).

Status

Muestra cómo ha configurado el dispositivo el filtro de direcciones.

Valores posibles:

- *learned*
  Filtro de direcciones configurado automáticamente por el dispositivo basándose en los paquetes de datos recibidos.
- *permanent*
  Filtro de direcciones configurado manualmente. El filtro de direcciones permanece configurado permanentemente.
- *IGMP*
  Filtro de direcciones configurado automáticamente por IGMP Snooping.
- *mgmt*
  Dirección MAC del dispositivo. El filtro de direcciones está protegido frente a cambios.
- *MRP-MMRP*
  Filtro de direcciones Multicast configurado automáticamente por MMRP.
- *GMRP*
  Filtro de direcciones Multicast configurado automáticamente por GMRP.

<Port number>

Muestra cómo transmite el puerto correspondiente paquetes de datos que dirige a la dirección de destino adyacente.

Valores posibles:

- `-`
  El puerto no transmite paquetes de datos a la dirección de destino.
- `learned`
  El puerto transmite paquetes de datos a la dirección de destino. El dispositivo creó el filtro automáticamente basándose en los paquetes de datos recibidos.
- `IGMP learned`
  El puerto transmite paquetes de datos a la dirección de destino. El dispositivo creó el filtro automáticamente basándose en IGMP.
- `unicast static`
  El puerto transmite paquetes de datos a la dirección de destino. Un usuario creó el filtro.
- `multicast static`
  El puerto transmite paquetes de datos a la dirección de destino. Un usuario creó el filtro.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

Abre la ventana *Create* para añadir una entrada nueva a la tabla.

- En el campo *Address*, especifique la dirección MAC de destino.
- En el campo *VLAN ID*, especifique el ID de la VLAN.
- En el campo *Port*, especifique el puerto.
  - Seleccione un puerto si la dirección MAC de destino es una dirección Unicast.
  - Seleccione uno o más puertos si la dirección MAC de destino es una dirección Multicast.
  - No seleccione ningún puerto para crear un filtro de descarte. El dispositivo descarta paquetes de datos con la dirección MAC de destino especificada en la entrada de la tabla.

Reset MAC address table

Elimina las direcciones MAC de la tabla de reenvíos que tienen el valor `learned` en la columna *Status*.

# 5.4 IGMP Snooping

[ Switching > IGMP Snooping ]

El Internet Group Management Protocol (IGMP) es un protocolo para administrar grupos Multicast de manera dinámica. El protocolo describe la distribución de paquetes de datos Multicast entre enrutadores y dispositivos terminales en la Capa 3.

El dispositivo le permite utilizar la función IGMP Snooping para utilizar también los mecanismos IGMP en la Capa 2:
- Sin IGMP Snooping, el dispositivo transmite paquetes de datos Multicast a través de todos los puertos.
- Con la función IGMP Snooping activada, el dispositivo transmite los paquetes de datos Multicast solo a través de puertos a los que están conectados receptores Multicast. Esto reduce la carga de la red. El dispositivo evalúa los paquetes de datos IGMP transmitidos en la Capa 3 y utiliza la información en la Capa 2.

No active la función IGMP Snooping hasta que se cumplan las siguientes condiciones:
- Cuando exista un enrutador Multicast en la red que cree consultas IGMP (consultas periódicas).
- Los dispositivos que participan en IGMP Snooping reenvían las consultas IGMP.

El dispositivo vincula los informes IGMP con las entradas en su tabla de direcciones. Cuando un receptor Multicast se une a un grupo Multicast, el dispositivo crea una entrada de tabla para este puerto en el cuadro de diálogo *Switching > Filter for MAC Addresses*. Cuando el receptor Multicast abandona el grupo Multicast, el dispositivo elimina la entrada de la tabla.

El menú contiene los siguientes cuadros de diálogo:
- IGMP Snooping Global
- IGMP Snooping Configuration
- IGMP Snooping Enhancements
- IGMP Snooping Querier
- IGMP Snooping Multicasts

# 5.4.1 IGMP Snooping Global

[ Switching > IGMP Snooping > Global ]

Este cuadro de diálogo le permite activar el protocolo *IGMP Snooping* en el dispositivo y configurarlo para cada puerto y cada VLAN.

### Operation

Operation

Activa/desactiva la función *IGMP Snooping* en el dispositivo.

Valores posibles:

- *On*
  La función *IGMP Snooping* está activada en el dispositivo conforme al RFC 4541 (consideraciones sobre el Protocolo de gestión de grupos de Internet [IGMP, Internet Group Management Protocol] y los switches Snooping de Descubrimiento de escucha de multidifusión [MLD, Multicast Listener Discovery]).
- *Off* (configuración por defecto)
  La función *IGMP Snooping* está desactivada en el dispositivo.
  El dispositivo transmite la consulta recibida y el informe, y abandona paquetes de datos sin evaluarlos. El dispositivo transmite los paquetes de datos recibidos con una dirección de destino Multicast a cada puerto.

### Information

Multicast control packets processed

Muestra el número de paquetes de datos de control Multicast procesados.

Esta estadística abarca los siguientes tipos de paquetes:

- Informes IGMP
- Consultas IGMP versión V1
- Consultas IGMP versión V2
- Consultas IGMP versión V3
- Consultas IGMP con una versión incorrecta
- Paquetes PIM o DVMRP

El dispositivo utiliza paquetes de datos de control Multicast para crear la tabla de direcciones a fin de transmitir los paquetes de datos Multicast.

Valores posibles:

- $0..2^{31}-1$

Utilice el botón *Reset IGMP snooping data* del cuadro de diálogo *Basic Settings > Restart* o el comando `clear igmp-snooping` con la interfaz de línea de comando para restablecer las entradas de IGMP Snooping, incluido el contador de paquetes de datos de control Multicast procesados.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

Reset IGMP snooping counters

Elimina las entradas de IGMP Snooping y restablece el contador en el cuadro *Information* a `0`.

## 5.4.2 IGMP Snooping Configuration

[ Switching > IGMP Snooping > Configuration ]

Este cuadro de diálogo le permite activar la función *IGMP Snooping* en el dispositivo y configurarlo para cada puerto y cada VLAN.

El cuadro de diálogo contiene las siguientes pestañas:
- [VLAN ID]
- [Port]

### [VLAN ID]

En esta pestaña podrá configurar la función *IGMP Snooping* para cada VLAN.

#### Tabla

VLAN ID

Muestra el ID de la VLAN a la que se aplica la entrada de la tabla.

Active

Activa/desactiva la función *IGMP Snooping* para esta VLAN.

Como requisito previo, la función *IGMP Snooping* debe estar activada a nivel global.

Valores posibles:
- `marked`
  IGMP Snooping está activado para esta VLAN. La VLAN se ha unido al flujo de datos Multicast.
- `unmarked` (configuración por defecto)
  IGMP Snooping está desactivado para esta VLAN. La VLAN ha abandonado el flujo de datos Multicast.

Group membership interval

Especifica en segundos el tiempo durante el cual permanece introducida una VLAN de un grupo Multicast dinámico en la tabla de direcciones cuando el dispositivo no recibe ningún paquete de datos de informe más de la VLAN.

Especifique un valor superior al de la columna *Max. response time*.

Valores posibles:

- `2..3600` (configuración por defecto: `260`)

Max. response time

Especifica en segundos el tiempo que tienen los miembros de un grupo Multicast para responder a un paquete de datos de consulta. Como respuesta, los miembros especifican un tiempo aleatorio dentro del tiempo de respuesta. De este modo, ayuda a evitar que los miembros del grupo Multicast respondan a la consulta al mismo tiempo.

Especifique un valor más pequeño que el de la columna *Group membership interval*.

Valores posibles:

- `1..25` (configuración por defecto: `10`)

Fast leave admin mode

Activa/desactiva la función Fast Leave para esta VLAN.

Valores posibles:

- `marked`
  Cuando la función Fast Leave está activa y el dispositivo recibe un mensaje IGMP Leave de un grupo Multicast, el dispositivo elimina inmediatamente la entrada de su tabla de direcciones.
- `unmarked` (configuración por defecto)
  Cuando la función Fast Leave está inactiva, el dispositivo primero envía consultas basadas en MAC a los miembros del grupo Multicast y elimina una entrada cuando una VLAN no envía ningún mensaje de informe más.

MRP expiration time

Tiempo de caducidad presente del enrutador Multicast. Especifica en segundos el tiempo que espera el dispositivo una consulta en este puerto que pertenece a una VLAN. Si el puerto no recibe un paquete de datos de consulta, el dispositivo elimina el puerto de la lista de puertos con enrutadores Multicast conectados.

Solamente tiene la opción de configurar este parámetro si el puerto pertenece a una VLAN existente.

Valores posibles:

- `0`
  tiempo de espera ilimitado - sin tiempo de caducidad
- `1..3600` (configuración por defecto: `260`)

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## [Port]

En esta pestaña puede configurar la función *IGMP Snooping* para cada puerto.

### Tabla

Port

Muestra el número de puerto.

Active

Activa/desactiva la función *IGMP Snooping* para este puerto.

Como requisito previo, la función *IGMP Snooping* debe estar activada a nivel global.

Valores posibles:

- `marked`
  IGMP Snooping está activo en este puerto. El dispositivo incluye el puerto en el flujo de datos Multicast.
- `unmarked` (configuración por defecto)
  IGMP Snooping está inactivo en este puerto. El puerto ha abandonado el flujo de datos Multicast.

Group membership interval

Especifica en segundos el tiempo durante el cual un puerto de un grupo Multicast dinámico permanece introducido en la tabla de direcciones cuando el dispositivo no recibe ningún paquete de datos de informe más del puerto.

Valores posibles:

- `2..3600` (configuración por defecto: `260`)

Especifique el valor superior al de la columna *Max. response time*.

Max. response time

Especifica en segundos el tiempo que tienen los miembros de un grupo Multicast para responder a un paquete de datos de consulta. Como respuesta, los miembros especifican un tiempo aleatorio dentro del tiempo de respuesta. De este modo, ayuda a evitar que los miembros del grupo Multicast respondan a la consulta al mismo tiempo.

Valores posibles:

- `1..25` (configuración por defecto: `10`)

Especifique un valor inferior al de la columna *Group membership interval*.

MRP expiration time

Especifica el tiempo de caducidad presente del enrutador Multicast. El tiempo de caducidad de MRP es el tiempo en segundos que espera el dispositivo un paquete de consulta en este puerto. Si el puerto no recibe un paquete de datos de consulta, el dispositivo elimina el puerto de la lista de puertos con enrutadores Multicast conectados.

Valores posibles:

- `0`
  tiempo de espera ilimitado - sin tiempo de caducidad
- `1..3600` (configuración por defecto: `260`)

Fast leave admin mode

Activa/desactiva la función Fast Leave para este puerto.

Valores posibles:

- `marked`
  Cuando la función Fast Leave está activa y el dispositivo recibe un mensaje IGMP Leave de un grupo Multicast, el dispositivo elimina inmediatamente la entrada de su tabla de direcciones.
- `unmarked` (configuración por defecto)
  Cuando la función Fast Leave está inactiva, el dispositivo primero envía consultas basadas en MAC a los miembros del grupo Multicast y elimina una entrada cuando un puerto no envía ningún mensaje de informe más.

Static query port

Activa/desactiva el modo *Static query port*.

Valores posibles:

- `marked`
  El modo *Static query port* está activo.
  El puerto es un puerto de consulta estático en las VLAN configuradas.
  Si utiliza la función *Redundant Coupling Protocol* y el dispositivo actúa como esclavo, no active el modo *Static query port* para los puertos de la red/anillo secundario.
- `unmarked` (configuración por defecto)
  El modo *Static query port* está inactivo.
  El puerto no es un puerto de consulta estático. El dispositivo transmite mensajes de informe IGMP al puerto solamente si recibe consultas IGMP.

VLAN IDs

Muestra el ID de las VLAN a las que se aplica la entrada de la tabla.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

# 5.4.3 IGMP Snooping Enhancements

[ Switching > IGMP Snooping > Snooping Enhancements ]

Este cuadro de diálogo le permite seleccionar un puerto para un ID de VLAN y configurar el puerto.

### Tabla

VLAN ID

Muestra el ID de la VLAN a la que se aplica la entrada de la tabla.

<Port number>

Muestra para cada VLAN configurada en el dispositivo si el puerto correspondiente es de consulta. Además, el campo muestra si el dispositivo transmite cada flujo Multicast de la VLAN a través de este puerto.

Valores posibles:

- `-`
  El puerto no es un puerto de consulta en esta VLAN.
- `L`= Learned
  El dispositivo detectó el puerto como un puerto de consulta debido a que recibió consultas IGMP en esta VLAN. El puerto no es un puerto de consulta configurado estáticamente.
- `A`= Automatic
  El dispositivo detectó el puerto como un puerto de consulta. Como requisito previo, debe configurar el puerto como *`Learn by LLDP`*.
- `S`= Static (configuración manual)
  Un usuario especificó el puerto como puerto de consulta estático. El dispositivo transmite informes IGMP solamente a puertos en los que ha recibido consultas IGMP previamente (y a puertos de consulta configurados estáticamente).
  Para asignar este valor, lleve a cabo los siguientes pasos:
  - ☐ Abra la ventana *Wizard*.
  - ☐ En el cuadro de diálogo *Configuration*, marque la casilla de verificación *`Static`*.
- `P`= Learn by LLDP (configuración manual)
  Un usuario especificó el puerto como *`Learn by LLDP`*.
  Con el Link Layer Discovery Protocol (LLDP), el dispositivo detecta los dispositivos Schneider Electric conectados directamente al puerto. El dispositivo señala los puertos de consulta detectados mediante `A`.
  Para asignar este valor, lleve a cabo los siguientes pasos:
  - ☐ Abra la ventana *Wizard*.
  - ☐ En el cuadro de diálogo *Configuration*, marque la casilla de verificación *`Learn by LLDP`*.
- `F`= Forward All (configuración manual)
  Un usuario especificó el puerto para que el dispositivo transmita cada flujo Multicast recibido en la VLAN a través de este puerto. Utilice esta configuración para fines de diagnóstico, por ejemplo.
  Para asignar este valor, lleve a cabo los siguientes pasos:
  - ☐ Abra la ventana *Wizard*.
  - ☐ En el cuadro de diálogo *Configuration*, marque la casilla de verificación *`Forward all`*.

Display categories

Mejora la calidad de la visualización. La tabla resalta las celdas que contienen el valor especificado. Esto ayuda a analizar y ordenar la tabla conforme a sus necesidades.

- *Learned (L)*
  La tabla muestra celdas que contienen el valor `L` y posiblemente valores adicionales. Celdas que contienen otros valores aparte de `L` solamente, la tabla muestra el símbolo "`-`".
- *Static (S)*
  La tabla muestra celdas que contienen el valor `S` y posiblemente valores adicionales. Celdas que contienen otros valores aparte de `S` solamente, la tabla muestra el símbolo "`-`".
- *Automatic (A)*
  La tabla muestra celdas que contienen el valor `A` y posiblemente valores adicionales. Celdas que contienen otros valores aparte de `A` solamente, la tabla muestra el símbolo "`-`".
- *Learned by LLDP (P)*
  La tabla muestra celdas que contienen el valor `P` y posiblemente valores adicionales. Celdas que contienen otros valores aparte de `P` solamente, la tabla muestra el símbolo "`-`".
- *Forward all (F)*
  La tabla muestra celdas que contienen el valor `F` y posiblemente valores adicionales. Celdas que contienen otros valores aparte de `F` solamente, la tabla muestra el símbolo "`-`".

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

Abre la ventana *Wizard* que le ayuda a seleccionar y configurar los puertos.

## [Selection VLAN/Port (Wizard)]

En el cuadro de diálogo *Selection VLAN/Port*, deberá asignar el ID de la VLAN al puerto.

En el cuadro de diálogo *Configuration*, deberá especificar la configuración del puerto.

Tras cerrar la ventana *Wizard*, haga clic en el botón  para guardar su configuración.

## [Selection VLAN/Port (Wizard) – Selection VLAN/Port]

VLAN ID

Seleccione el ID de la VLAN.

Valores posibles:

- `1..4042`

Port

Seleccione el puerto.

Valores posibles:

- `<Port number>`

## [Selection VLAN/Port (Wizard) – Configuration]

VLAN ID

Muestra el ID de la VLAN seleccionada.

Port

Muestra el número del puerto seleccionado.

Static

Especifica el puerto como un puerto de consulta estático en las VLAN configuradas. El dispositivo transmite mensajes de informe IGMP a los puertos en los que se reciben consultas IGMP. Esto le permite transmitir también mensajes de informe IGMP a otros puertos seleccionados (activación) o dispositivos Schneider Electric (`Automatic`).

Learn by LLDP

Especifica el puerto como *`Learn by LLDP`*. Permite que el dispositivo detecte los dispositivos Schneider Electric conectados directamente mediante LLDP y aprender los puertos relacionados como un puerto de consulta.

Forward all

Especifica el puerto como *`Forward all`*. Con la configuración *`Forward all`*, el dispositivo transmite en este puerto todos los paquetes de datos con una dirección Multicast en el campo de dirección de destino.

# 5.4.4 IGMP Snooping Querier

[ Switching > IGMP Snooping > Querier ]

El dispositivo le permite enviar un flujo Multicast solamente a aquellos puertos a los que está conectado un receptor Multicast.

Para determinar a qué puertos están conectados los receptores Multicast, el dispositivo envía paquetes de datos de consulta a los puertos a un intervalo definible. Cuando hay conectado un receptor Multicast, se une al flujo Multicast respondiendo al dispositivo con un paquete de datos de informe.

Este cuadro de diálogo le permite configurar los ajustes de Snooping Querier globalmente y para las VLAN que estén configuradas.

### Operation

Operation

Activa/desactiva la función IGMP Querier globalmente en el dispositivo.

Valores posibles:

- *On*
- *Off* (configuración por defecto)

### Configuration

En este cuadro, se especifican los ajustes de IGMP Snooping para los paquetes de datos de consulta general.

Protocol version

Especifica la versión de IGMP de los paquetes de datos de consulta general.

Valores posibles:

- 1
  IGMP v1
- 2 (configuración por defecto)
  IGMP v2
- 3
  IGMP v3

Query interval [s]

Especifica en segundos el tiempo que debe transcurrir para que el dispositivo genere paquetes de datos de consulta general cuando ha recibido paquetes de datos de consulta del enrutador Multicast.

Valores posibles:

- `1..1800` (configuración por defecto: `60`)

Expiry interval [s]

Especifica en segundos el tiempo que debe transcurrir para que un solicitante activo cambie del estado pasivo al activo si no ha recibido ningún paquete de datos durante más tiempo del aquí especificado.

Valores posibles:

- `60..300` (configuración por defecto: `125`)

### Tabla

En la tabla, especifique la configuración de Snooping Querier para las VLAN que están configuradas.

VLAN ID

Muestra el ID de la VLAN a la que se aplica la entrada de la tabla.

Active

Activa/desactiva la función IGMP Snooping Querier para esta VLAN.

Valores posibles:

- `marked`
  La función IGMP Snooping Querier está activa para esta VLAN.
- `unmarked` (configuración por defecto)
  La función IGMP Snooping Querier está inactiva para esta VLAN.

Current state

Muestra si Snooping Querier está activo para esta VLAN.

Valores posibles:

- `marked`
  El Snooping Querier está activo para esta VLAN.
- `unmarked`
  El Snooping Querier está inactivo para esta VLAN.

Address

Especifica la dirección IP que el dispositivo añade como dirección de origen en los paquetes de datos de consulta general generados. Utilice la dirección del enrutador Multicast.

Valores posibles:

- Dirección IPv4 válida (configuración por defecto: `0.0.0.0`)

Protocol version

Muestra la versión del protocolo IGMP de los paquetes de datos de consulta general.

Valores posibles:

- `1`
  IGMP v1
- `2`
  IGMP v2
- `3`
  IGMP v3

Max. response time

Muestra en segundos el tiempo que tienen los miembros de un grupo Multicast para responder a un paquete de datos de consulta. Como respuesta, los miembros especifican un tiempo aleatorio dentro del tiempo de respuesta. Esto ayuda a evitar que cada grupo Multicast responda a la consulta al mismo tiempo.

Last querier address

Muestra la dirección IP del enrutador Multicast desde la que se envió la última consulta IGMP recibida.

Last querier version

Muestra la versión de IGMP utilizada por el enrutador Multicast al enviar la última consulta IGMP recibida en esta VLAN.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

# 5.4.5 IGMP Snooping Multicasts

[ Switching > IGMP Snooping > Multicasts ]

El dispositivo le permite especificar cómo desea que transmita paquetes de datos con direcciones Multicast desconocidas: el dispositivo descarta estos paquetes de datos, los desborda a cada puerto o los transmite solamente a los puertos que recibieron paquetes de consulta previamente.

El dispositivo también le permite transmitir los paquetes de datos con direcciones Multicast conocidas a los puertos de consulta.

### Configuration

Unknown multicasts

Especifica cómo transmite el dispositivo los paquetes de datos con direcciones Multicast desconocidas.

Valores posibles:

- *discard*
  El dispositivo descarta paquetes de datos con direcciones MAC/IP Multicast desconocidas.
- *flood* (configuración por defecto)
  El dispositivo reenvía paquetes de datos con una dirección Multicast MAC/IP desconocida a cada puerto.

### Tabla

En la tabla, especifique la configuración de las direcciones Multicast conocidas para las VLAN que están configuradas.

VLAN ID

Muestra el ID de la VLAN a la que se aplica la entrada de la tabla.

Known multicasts

Especifica cómo transmite el dispositivo los paquetes de datos con direcciones Multicast conocidas.

Valores posibles:

- *send to query and registered ports*
  El dispositivo reenvía paquetes de datos con direcciones MAC/IP Multicast desconocidas a los puertos de consulta y a los puertos registrados.
- *send to registered ports* (configuración por defecto)
  El dispositivo reenvía paquetes de datos con direcciones MAC/IP Multicast desconocidas a los puertos registrados.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## 5.5 Time-Sensitive Networking

[ Switching > TSN ]

El menú contiene los siguientes cuadros de diálogo:

- TSN Configuration
- TSN Gate Control List

## 5.5.1 TSN Configuration

[ Switching > TSN > Configuration ]

En este cuadro de diálogo podrá activar la función *TSN* y especificar la configuración específica del tiempo.

El dispositivo admite la colocación en cola con reconocimiento de tiempo definida en IEEE 802.1 Qbv. La función *TSN* permite que los puertos compatibles con TSN transmitan paquetes de datos de todas las clases de tráfico programadas relativas a un ciclo definido en la Lista de control de puertas. La etiqueta VLAN de un paquete de Ethernet (o la prioridad del puerto en caso de paquetes sin etiquetas) contiene la prioridad.

La función ayuda a evitar la latencia y la pérdida de congestión de flujos de datos reservados. La sincronización precisa de ciclos y estados de puertas que utilizan IEEE1588 (PTP) permite obtener una comunicación sin congestión y con una latencia reducida. El requisito previo es que cada dispositivo de la red admita IEEE 802.1 Qbv.

**Nota:** En contraste con la interfaz de línea de comandos, confirmará los ajustes inmediatamente si hace clic en el botón ☑.

### Operation

Operation

Activa/desactiva la función *TSN* en el dispositivo.

Valores posibles:

- *On*
  La función *TSN* se activa globalmente.
  El dispositivo procesa cuadros de enlace-local en puertos compatibles con TSN con la prioridad de clase de tráfico 6. Como resultado, los cuadros de enlace-local compiten con otros paquetes de datos con la misma prioridad o una superior a la hora del reenvío. Esto afecta a los siguientes tipos de cuadros:
  - RSTP
  - LLDP
  - IEEE 802.1AS
  - PTP Peer Delay
- *Off* (configuración por defecto)
  La función *TSN* está desactivada globalmente.
  Mientras la función *TSN* esté activa en un puerto, el puerto utilizará las puertas abiertas 0,1,2,3,4,5,6,7. Esta configuración está preestablecida por el fabricante.

### Base time

Date
Time
[ns]

Especifica la hora a la que se inicia el ciclo según el horario UTC.

El dispositivo convierte el valor en una escala de tiempo PTP directamente sin tener en cuenta los segundos de salto.

Valores posibles:

- `MM/DD/AA`
  Mes/Día/Año
  (en función de las preferencias de idioma de su navegador web)
- `hh:mm:ss`
  Hora:Minuto:Segundo
- `0..999999999`
  Especifica la desviación en nanosegundos

**Nota:** Cuando especifique la hora base en el futuro, el ciclo se iniciará con los segundos de antelación especificados en el campo *UTC offset [s]*. Consulte el cuadro de diálogo *Time > PTP > Boundary Clock > Global*.

### Configuration

Cycle time [ns]

Especifica la duración de un ciclo en nanosegundos.

Valores posibles:

- `50000..10000000` (configuración por defecto: `1000000`)
  50 µs .. 10 ms

### Tabla

Port

Muestra el número de puerto.

Active

Activa/desactiva la función *TSN* en el puerto.

Valores posibles:

- `marked`
  La función *TSN* está activa en el puerto.
  Cuando especifique la hora de base en el futuro, el ciclo se iniciará a la hora especificada en el cuadro *Base time*.
  El requisito previo es que la función *PTP* esté activada y el dispositivo sincronizado.
  Mientras la función *TSN* esté activada globalmente, el puerto utilizará el ciclo especificado en el cuadro de diálogo *Switching > TSN > Gate Control List > Configured*.
- `unmarked` (configuración por defecto)
  La función *TSN* está inactiva en el puerto.
  Mientras la función *TSN* esté activada globalmente, el puerto utilizará las puertas abiertas `0,1,2,3,4,5,6,7`.

Port state

Muestra el estado del ciclo en el puerto.

Valores posibles:

- *running*
  El ciclo está ejecutándose.
  El puerto utiliza el ciclo especificado en el cuadro de diálogo *Switching > TSN > Gate Control List > Configured*.
- *waitForTimeSync*
  El ciclo todavía no se ha iniciado.
  El reloj del dispositivo no está sincronizado.
  Compruebe la configuración de *PTP*.
- *pending*
  El ciclo todavía no se ha iniciado.
  La hora base especificada corresponde al futuro.
- *disabled*
  El ciclo no está en ejecución.
  La función *TSN* está inactiva en el puerto.
  - Compruebe la configuración en el cuadro *Operation*.
  - Compruebe la configuración en la columna *Active*.

  El puerto utiliza los estados de puertas especificados en la columna *Default gate states*.
- *error*
  El ciclo no está en ejecución.
  Se ha detectado un error.

Time of last activation

Muestra la fecha y la hora en que se activaron los ajustes de hora por última vez.

Este valor se corresponde con el tiempo PTP.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## 5.5.2 TSN Gate Control List

[ Switching > TSN > Gate Control List ]

El menú contiene los siguientes cuadros de diálogo:

- TSN Configured Gate Control List
- TSN Current Gate Control List

# 5.5.2.1 TSN Configured Gate Control List

[ Switching > TSN > Gate Control List > Configured ]

En este cuadro de diálogo puede especificar las franjas horarias del ciclo para puertos compatibles con TSN. Mediante la adición de una entrada de tabla, podrá especificar las puertas abiertas y la duración de la franja horaria.

**Nota:** En contraste con la interfaz de línea de comandos, confirmará los ajustes inmediatamente si hace clic en el botón ✓.

El cuadro de diálogo contiene las siguientes pestañas:

- Una pestaña para cada puerto compatible con TSN.
  El número de puertos compatibles con TSN depende del dispositivo.

## [<Port number>]

### Configuration

Status

Muestra la plantilla asignada a la Lista de control de puertas.

Valores posibles:

- `-`
  Ninguna plantilla. No se ha asignado ninguna entrada a la Lista de control de puertas.
- *`default 2 time slots`*
  Plantilla con 3 entradas:
  - La primera entrada es de clase de tráfico `7`.
  - La segunda entrada es de clase de tráfico `6` a `0`.
  - La tercera entrada es una banda de protección.
- *`default 3 time slots`*
  Plantilla con 5 entradas:
  - La primera entrada es de clase de tráfico `7`.
  - La segunda entrada es una banda de protección.
  - La tercera entrada es la clase de tráfico `6`.
  - La cuarta entrada es la clase de tráfico `5` a `0`.
  - La quinta entrada es una banda de protección.
- <`any other template name`>
  La plantilla se ha asignado mediante una interfaz de línea de comandos.

Template

Abre la ventana *Template* para asignar una plantilla diferente a la Lista de control de puertas. Cuando seleccione una plantilla diferente y haga clic en el botón *Ok*, el dispositivo sustituirá las entradas de la tabla.

En la lista desplegable, seleccione una de las siguientes plantillas:

- *default 2 time slots*
- *default 3 time slots*

El dispositivo le permite asignar plantillas adicionales mediante la interfaz de línea de comandos.

Delete

Elimina la plantilla asignada a la Lista de control de puertas. Después de eso, no se asigna ninguna entrada más a la Lista de control de puertas.

### Tabla

Index

Muestra el número de índice de la entrada en la Lista de control de puertas, que especifica el orden cronológico de las franjas horarias.

Gate states

Especifica las puertas abiertas en caso de que la función *TSN* del puerto esté activa.

- Los paquetes de datos cuya clase de tráfico esté asignada a una puerta seleccionada se seleccionan para la transmisión: estado de la puerta OPEN.
- Los paquetes de datos cuya clase de tráfico está asignada a una puerta no seleccionada no se seleccionan para la transmisión: estado de la puerta CLOSED.

Valores posibles:

- `-` (configuración por defecto)
  Ninguna puerta seleccionada.
  El dispositivo no abre ninguna puerta del puerto durante el procesamiento de la franja horaria.
  En la lista desplegable, cancele la selección de cada puerta.
- `0..7`
  El dispositivo abre las puertas seleccionadas del puerto durante el procesamiento de la franja horaria. En la lista desplegable, seleccione una o más puertas.
  Asigne las prioridades de VLAN a una clase de tráfico en el cuadro de diálogo *Switching > QoS/Priority > 802.1D/p Mapping*.

Interval [ns]

Especifica la duración de la franja horaria en nanosegundos.

Valores posibles:

▶ `1000..10000000`

Cuando especifique la duración de las franjas horarias, tenga en cuenta las siguientes condiciones:

- Una única franja horaria
  - Confirme que la franja horaria sea al menos lo suficientemente larga para que el puerto transmita el paquete de datos más largo esperado.
  - Confirme que una franja horaria sea igual o inferior a la duración del ciclo.
- La suma de franjas horarias especificadas
  - Es recomendable que la suma de las franjas horarias equivalga a la duración del ciclo.
  - Si la suma supera la duración del ciclo, las franjas horarias superpuestas se descartarán y el ciclo se reiniciará.
  - Si la suma es inferior a la duración del ciclo, el intervalo de la última franja horaria se ampliará para encajarlo en el ciclo.

**Nota:** Las discrepancias existentes entre las franjas horarias especificadas y la duración del ciclo no aparecen resaltadas en el cuadro de diálogo *Switching > TSN > Gate Control List > Current*.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## 5.5.2.2 TSN Current Gate Control List

[ Switching > TSN > Gate Control List > Current ]

En este cuadro de diálogo podrá supervisar la configuración actual del ciclo para los puertos compatibles con TSN. Cada entrada de la tabla representa una franja horaria especificada.

Si la hora de inicio del ciclo (*Base time*) corresponde al futuro, los valores mostrados serán diferentes de los especificados en el cuadro de diálogo *Switching > TSN > Gate Control List > Configured*.

En el cuadro de diálogo *Switching > TSN > Configuration*, la columna *Port state* muestra si el ciclo se está ejecutando en un puerto.

El cuadro de diálogo contiene las siguientes pestañas:
- Una pestaña para cada puerto compatible con TSN.
  El número de puertos compatibles con TSN depende del dispositivo.

### [<Port number>]

#### Tabla

Index

Muestra el número de índice de la entrada en la Lista de control de puertas, que especifica el orden cronológico de las franjas horarias.

Gate states

Muestra las puertas abiertas en caso de que la función *TSN* del puerto esté activa.

Interval [ns]

Muestra la duración de la franja horaria en nanosegundos.

#### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

# 5.6 MRP-IEEE

[ Switching > MRP-IEEE ]

La modificación IEEE 802.1ak al estándar IEEE 802.1Q introdujo el Multiple Registration Protocol (MRP, Multiple Registration Protocol) para sustituir al Generic Attribute Registration Protocol (GARP, Generic Attribute Registration Protocol). El IEEE también modificó y sustituyó las aplicaciones GARP, GARP Multicast Registration Protocol (GMRP) y GARP VLAN Registration Protocol (GVRP). El Multiple MAC Registration Protocol (MMRP, Multiple MAC Registration Protocol) y el Multiple VLAN Registration Protocol (MVRP, Multiple VLAN Registration Protocol) sustituyen a estos protocolos.

MRP-IEEE ayuda a confinar el tráfico a las zonas requeridas de la LAN. Para confinar el tráfico, las aplicaciones MRP-IEEE distribuyen valores de atributos a dispositivos MRP-IEEE participantes en una LAN registrando y cancelando el registro de suscripciones a grupos Multicast e identificadores de VLAN.

El registro de participantes en grupos le permite reservar recursos para tráfico específico que atraviesa una LAN. La definición de requisitos de recursos regula el nivel del tráfico, permite a los dispositivos determinar los recursos necesarios y proporciona el mantenimiento dinámico de los recursos asignados.

El menú contiene los siguientes cuadros de diálogo:

- MRP-IEEE Configuration
- MRP-IEEE Multiple MAC Registration Protocol
- MRP-IEEE Multiple VLAN Registration Protocol

## 5.6.1 MRP-IEEE Configuration

[ Switching > MRP-IEEE > Configuration ]

Este cuadro de diálogo le permite establecer los diferentes temporizadores de MRP. Al mantener una relación entre los diferentes valores del temporizador, el protocolo funciona de manera eficiente y con una menor probabilidad de que se produzcan retiradas innecesarias de atributos y cancelaciones de registros. Los valores predeterminados del temporizador permiten mantener estas relaciones de manera eficaz.

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, especifique el valor de LeaveTime (Hora de abandono) para: `≥ (2x JoinTime) + 60`
- 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).

### Tabla

Port

Muestra el número de puerto.

Join time [1/100s]

Especifica el temporizador de Join (Unión) que controla el intervalo entre oportunidades de transmisión aplicadas a la máquina de estado del aspirante.

Valores posibles:

- `10..100` (configuración por defecto: `20`)

Leave time [1/100s]

Especifica el temporizador de Leave (Abandono) que controla el período que la máquina de estado del registrador debe esperar en estado Leave (LV) (Abandono) antes de pasar al estado Empty (MT) (Vacío).

Valores posibles:

- `20..600` (configuración por defecto: `60`)

Leave all time [1/100s]

Especifica el temporizador LeaveAll (Abandonar todo) que controla la frecuencia con la que la máquina de estado de LeaveAll (Abandonar todo) genera PDU de LeaveAll (Abandonar todo).

Valores posibles:

- `200..6000` (configuración por defecto: `1000`)

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## 5.6.2 MRP-IEEE Multiple MAC Registration Protocol

[ Switching > MRP-IEEE > MMRP ]

El Multiple MAC Registration Protocol (MMRP, Multiple MAC Registration Protocol) permite a los dispositivos terminales y a los switches MAC registrar y cancelar el registro de suscripciones a grupos e información de direcciones MAC individuales con switches situados en la misma LAN. Los switches de la LAN diseminan la información por switches que admiten servicios de filtrado ampliado. Utilizando la información de la dirección MAC, el MMRP le permite confinar el tráfico Multicast a las zonas requeridas de una red de Capa 2.

Para obtener un ejemplo de cómo funciona un MMRP, imagine una cámara de seguridad montada en un mástil con vistas a un edificio. La cámara envía paquetes Multicast a una LAN. Dispone de 2 dispositivos terminales instalados para realizar la vigilancia en ubicaciones separadas. Registre las direcciones MAC de la cámara y los 2 dispositivos terminales en el mismo grupo Multicast. A continuación, especifique la configuración del MMRP en los puertos para enviar los paquetes del grupo Multicast a los 2 dispositivos terminales.

El cuadro de diálogo contiene las siguientes pestañas:
- [Configuration]
- [Service requirement]
- [Statistics]

### [Configuration]

En esta pestaña, seleccione participantes activos en el puerto MMRP y ajuste el dispositivo para transmitir eventos periódicos. El cuadro de diálogo también le permite activar la transmisión de direcciones MAC registradas en VLAN.

Hay una máquina de estado periódico para cada puerto que transmite eventos periódicos regularmente a las máquinas de estado del aspirante asociadas con puertos activos. Los eventos periódicos contienen información que indica el estado de los dispositivos asociados con el puerto activo.

#### Operation

Operation

Activa/desactiva la función *MMRP* global en el dispositivo. El dispositivo participa en los intercambios de mensajes MMRP.

Valores posibles:
- *On*
  El dispositivo es un participante normal en los intercambios de mensajes MMRP.
- *Off* (configuración por defecto)
  El dispositivo ignora mensajes MMRP.

### Configuration

Periodic state machine

Activa/desactiva la máquina de estado periódico global en el dispositivo.

Valores posibles:

- *On*
  Con el MMRP *Operation* activado globalmente, el dispositivo transmite mensajes MMRP en intervalos de un segundo a través de puertos participantes del MMRP.
- *Off* (configuración por defecto)
  Desactiva la máquina de estado periódico en el dispositivo.

### Tabla

Port

Muestra el número de puerto.

Active

Activa/desactiva la participación de MMRP del puerto.

Valores posibles:

- `marked` (configuración por defecto)
  Con el MMRP activado globalmente y en este puerto, el dispositivo envía y recibe mensajes MMRP a través de este puerto.
- `unmarked`
  Desactiva la participación de MMRP del puerto.

Restricted group registration

Activa/desactiva la restricción del registro de direcciones MAC dinámicas mediante el MMRP a través del puerto.

Valores posibles:

- `marked`
  Si está activado y existe una entrada de filtro estático para la dirección MAC en la VLAN correspondiente, el dispositivo registra los atributos de la dirección MAC dinámicamente.
- `unmarked` (configuración por defecto)
  Activa/desactiva la restricción del registro de direcciones MAC dinámicas mediante el MMRP a través del puerto.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## [Service requirement]

Esta pestaña contiene parámetros de reenvío para cada VLAN activa, especificando los puertos en los que se aplica el reenvío Multicast. El dispositivo le permite configurar estáticamente puertos de VLAN como *Forward all* o Forbidden. Puede establecer el requisito del servicio MMRP Forbidden estáticamente solo con la interfaz gráfica de usuario o la interfaz de línea de comando.

El puerto solamente se configura como ForwardAll o Forbidden.

### Tabla

VLAN ID

Indicación de la ID de VLAN.

<Port number>

Especifica el manejo del requisito de servicio del puerto.

Valores posibles:

- FA
  Especifica el ajuste del tráfico ForwardAll en el puerto. El dispositivo reenvía tráfico destinado a direcciones MAC Multicast registradas en MMRP a través de la VLAN. El dispositivo reenvía tráfico a puertos que el MMRP ha configurado dinámicamente o a puertos que el administrador ha configurado estáticamente como puertos ForwardAll.
- F
  Especifica el ajuste del tráfico Forbidden en el puerto. El dispositivo bloquea requisitos del servicio ForwardAll de MMRP dinámico. Con solicitudes ForwardAll bloqueadas en este puerto de esta VLAN, el dispositivo bloquea el tráfico destinado a direcciones MAC Multicast registradas en MMRP a través de este puerto. Además, el dispositivo bloquea solicitudes de servicio de MMRP para cambiar este valor a través de este puerto.
- \- (configuración por defecto)
  Desactiva las funciones de reenvío en este puerto.
- Learned
  Muestra valores configurados por solicitudes de servicio de MMRP.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## [Statistics]

Dispositivos en un intercambio de LAN Multiple MAC Registration Protocol Data Units (MMRPDU) para mantener los estados de los dispositivos en un puerto MMRP activo. Esta pestaña le permite supervisar las estadísticas de tráfico de MMRP de cada puerto.

### Information

Transmitted MMRP PDU

Muestra el número de MMRPDU transmitidos en el dispositivo.

Received MMRP PDU

Muestra el número de MMRPDU recibidos en el dispositivo.

Received bad header PDU

Muestra el número de MMRPDU recibidos con una cabecera incorrecta en el dispositivo.

Received bad format PDU

Muestra el número de MMRPDU con un campo de datos incorrectos que no se transmitieron en el dispositivo.

Transmission failed

Muestra el número de MMRPDU no transmitidos en el dispositivo.

### Tabla

Port

Muestra el número de puerto.

Transmitted MMRP PDU

Muestra el número de MMRPDU transmitidos en el puerto.

Received MMRP PDU

Muestra el número de MMRPDU recibidos en el puerto.

Received bad header PDU

Muestra el número de MMRPDU con una cabecera incorrecta recibidos en el puerto.

Received bad format PDU

Muestra el número de MMRPDU con un campo de datos incorrectos que no se transmitieron en el puerto.

Transmission failed

Muestra el número de MMRPDU no transmitidos en el puerto.

Last received MAC address

Muestra la última dirección MAC desde la que el puerto recibió MMRPPDU.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

Reset

Restablece los contadores de estadísticas de puertos y los valores de la columna *Last received MAC address*.

# 5.6.3 MRP-IEEE Multiple VLAN Registration Protocol

[Switching > MRP-IEEE > MVRP]

El Multiple VLAN Registration Protocol (MVRP, Multiple VLAN Registration Protocol) proporciona un mecanismo que le permite distribuir información de la VLAN y configurar la VLAN dinámicamente. Por ejemplo, cuando configura una VLAN en un puerto MVRP activo, el dispositivo distribuye la información de la VLAN a otros dispositivos compatibles con MVRP. Utilizando la información recibida, un dispositivo compatible con el MVRP crea dinámicamente los troncos de VLAN en otros dispositivos compatibles con MVRP según sea necesario.

El cuadro de diálogo contiene las siguientes pestañas:
- [Configuration]
- [Statistics]

## [Configuration]

En esta pestaña, seleccione participantes activos en el puerto MVRP y ajuste el dispositivo para transmitir eventos periódicos.

Hay una máquina de estado periódico para cada puerto que transmite eventos periódicos regularmente a las máquinas de estado del aspirante asociadas con puertos activos. Los eventos periódicos contienen información que indica el estado de las VLAN asociadas con el puerto activo. Mediante el uso de los eventos periódicos, los switches compatibles con MVRP mantienen dinámicamente las VLAN.

### Operation

Operation

Activa/desactiva el control administrativo de aspirantes global que especifica si la máquina de estado del aspirante participa en intercambios de mensajes MMRP.

Valores posibles:
- *On*
  Participante normal. La máquina de estado del aspirante participa en intercambios de mensajes MMRP.
- *Off* (configuración por defecto)
  No participante. La máquina de estado del aspirante ignora los mensajes MMRP.

### Configuration

Periodic state machine

Activa/desactiva la máquina de estado periódico en el dispositivo.

Valores posibles:

- *On*
  La máquina de estado periódico está activada.
  Con el MVRP *Operation* activado globalmente, el dispositivo transmite eventos periódicos de MVRP a intervalos de 1 segundo a través de puertos participantes en MVRP.
- *Off* (configuración por defecto)
  La máquina de estado periódico está desactivada.
  Desactiva la máquina de estado periódico en el dispositivo.

### Tabla

Port

Muestra el número de puerto.

Active

Activa/desactiva la participación en MVRP del puerto.

Valores posibles:

- marked (configuración por defecto)
  Con el MVRP activado globalmente y en este puerto, el dispositivo distribuye información de suscripción a VLAN a los dispositivos con reconocimiento de MVRP conectados a este puerto.
- unmarked
  Desactiva la participación en MVRP del puerto.

Restricted VLAN registration

Activa/desactiva la función *Restricted VLAN registration* en este puerto.

Valores posibles:

- marked
  Si está activado y existe una entrada de registro de VLAN estática, el dispositivo le permite crear una VLAN dinámica para esta entrada.
- unmarked (configuración por defecto)
  Desactiva la función *Restricted VLAN registration* en este puerto.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## [Statistics]

Dispositivos en un intercambio de LAN Multiple VLAN Registration Protocol Data Units (MVRPDU) para mantener los estados de las VLAN en puertos activos. Esta pestaña le permite supervisar el tráfico de MVRP.

### Information

Transmitted MVRP PDU

Muestra el número de MVRPDU transmitidos en el dispositivo.

Received MVRP PDU

Muestra el número de MVRPDU recibidos en el dispositivo.

Received bad header PDU

Muestra el número de MVRPDU recibidos con una cabecera incorrecta en el dispositivo.

Received bad format PDU

Muestra el número de MVRPDU con un campo de datos incorrecto bloqueado por el dispositivo.

Transmission failed

Muestra el número de errores producidos mientras se añade un mensaje a la cola del MVRP.

Message queue failures

Muestra el número de MVRPDU bloqueados por el dispositivo.

### Tabla

Port

Muestra el número de puerto.

Transmitted MVRP PDU

Muestra el número de MVRPDU transmitidos en el puerto.

Received MVRP PDU

Muestra el número de MVRPDU recibidos en el puerto.

Received bad header PDU

Muestra el número de MVRPDU con una cabecera incorrecta recibidos por el dispositivo en el puerto.

Received bad format PDU

Muestra el número de MVRPDU con un campo de datos incorrecto bloqueado por el dispositivo en el puerto.

Transmission failed

Muestra el número de MVRPDU bloqueados por el dispositivo en el puerto.

Registrations failed

Muestra el número de intentos de registro incorrectos en el puerto.

Last received MAC address

Muestra la última dirección MAC desde la que el puerto recibió MMRPDU.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

Reset

Restablece los contadores de estadísticas de puertos y los valores de la columna *Last received MAC address*.

## 5.7 GARP

[ Switching > GARP ]

El Generic Attribute Registration Protocol (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 el 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.

**Nota:** Antes de activar la función *GMRP*, compruebe que la función *MMRP* esté desactivada.

El menú contiene los siguientes cuadros de diálogo:
- GMRP
- GVRP

# 5.7.1 GMRP

[ Switching > GARP > GMRP ]

El GARP Multicast Registration Protocol (GMRP, GARP Multicast Registration Protocol) es un Generic Attribute Registration Protocol (GARP, Generic Attribute Registration Protocol) 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. El GARP también permite a los dispositivos distribuir la información por los dispositivos de red que admiten servicios de filtrado ampliados.

GMRP y GARP son protocolos estándar del sector definidos por el estándar IEEE 802.1P.

### Operation

Operation

Activa/desactiva la función *GMRP* global en el dispositivo. El dispositivo participa en los intercambios de mensajes GMRP.

Valores posibles:

- *On*
  El GMRP está activado.
- *Off* (configuración por defecto)
  El dispositivo ignora mensajes GMRP.

### Multicasts

Unknown multicasts

Activa/desactiva los datos Multicast desconocidos para desbordarlos o descartarlos.

Valores posibles:

- *discard*
  El dispositivo descarta datos Multicast desconocidos.
- *flood* (configuración por defecto)
  El dispositivo reenvía datos Multicast desconocidos a cada puerto.

### Tabla

Port

Muestra el número de puerto.

GMRP active

Activa/desactiva la participación *GMRP* del puerto.

Como requisito previo, la función *GMRP* debe estar activada a nivel global.

Valores posibles:

- `marked` (configuración por defecto)
  La participación *GMRP* del puerto está activa.
- `unmarked`
  La participación *GMRP* del puerto está inactiva.

Service requirement

Especifica los puertos en los que se aplica el reenvío Multicast.

Valores posibles:

- *`Forward all unregistered groups`* (configuración por defecto)
  El dispositivo reenvía datos destinados a direcciones MAC Multicast registradas en *GMRP* en la VLAN. El dispositivo reenvía datos a los grupos no registrados.
- *`Forward all groups`*
  El dispositivo reenvía datos destinados a cada grupo, registrado o no registrado.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## 5.7.2 GVRP

[ Switching > GARP > GVRP ]

El GARP VLAN Registration Protocol (GVRP, GARP VLAN Registration Protocol) o Generic VLAN Registration Protocol es un protocolo que facilita el control de redes de área local virtuales (VLAN) en una red de mayor tamaño. El GVRP es un protocolo de red de Capa 2 utilizado para configurar dispositivos automáticamente en una red VLAN.

El GVRP es una aplicación GARP que permite eliminar una VLAN compatible con IEEE 802.1Q y crear una VLAN dinámica en los puertos de enlace 802.1Q. Con el GVRP, el dispositivo intercambia información de configuración de la VLAN con otros dispositivos GVRP. De este modo, el dispositivo reduce el tráfico Broadcast innecesario y Unicast desconocido. El intercambio de información de configuración de la VLAN también le permite crear y gestionar de forma dinámica VLAN conectadas a través de puertos de enlace 802.1Q.

### Operation

Operation

Activa/desactiva la función *GVRP* globalmente en el dispositivo. El dispositivo participa en los intercambios de mensajes *GVRP*. Si la función está desactivada, el dispositivo ignora los mensajes *GVRP*.

Valores posibles:

- `On`
  La función *GVRP* está activada.
- `Off` (configuración por defecto)
  La función *GVRP* está desactivada.

### Tabla

Port

Muestra el número de puerto.

GVRP active

Activa/desactiva la participación *GVRP* del puerto.

Como requisito previo, la función *GVRP* debe estar activada a nivel global.

Valores posibles:

- `marked` (configuración por defecto)
  La participación *GVRP* del puerto está activa.
- `unmarked`
  La participación *GVRP* del puerto está inactiva.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## 5.8 QoS/Priority

[ Switching > QoS/Priority ]

Las redes de comunicación transmiten un número de aplicaciones al tiempo que disponen de diferentes requisitos relacionados con la disponibilidad, el ancho de banda y los períodos de latencia.

QoS (Quality of Service, Calidad de servicio) es un procedimiento definido en el estándar IEEE 802.1D. Se utiliza para distribuir recursos en la red. Por lo tanto, tiene la posibilidad de ofrecer un ancho de banda mínimo para las aplicaciones necesarias. Como requisito previo, los dispositivos terminales y los dispositivos de la red admiten la transmisión de datos priorizada. A los paquetes de datos con una elevada prioridad se les otorga preferencia cuando son transmitidos por dispositivos en la red. Transferirá paquetes de datos con una menor prioridad cuando no haya ningún paquete de datos con una prioridad superior para transmitir.

El dispositivo ofrece las siguientes opciones de ajuste:
- Podrá especificar cómo evalúa el dispositivo la información de QoS/priorización para paquetes de datos entrantes.
- Para los paquetes salientes, especifique qué información de QoS/priorización desea que escriba el dispositivo en el paquete de datos (por ejemplo, prioridad para paquetes de administración, prioridad de puertos).

**Nota:** Si utiliza las funciones de este menú, desactive el control de flujo. El control de flujo estará inactivo si, en el cuadro de diálogo *Switching > Global*, cuadro *Configuration*, la casilla *Flow control* está `unmarked`.

El menú contiene los siguientes cuadros de diálogo:
- QoS/Priority Global
- QoS/Priority Port Configuration
- 802.1D/p Mapping
- IP DSCP Mapping
- Queue Management

## 5.8.1 QoS/Priority Global

[ Switching > QoS/Priority > Global ]

El dispositivo le permite conservar el acceso a la gestión del dispositivo, incluso en situaciones de uso intensivo. En este cuadro de diálogo, especifique la configuración de QoS/prioridad.

### Configuration

VLAN priority for management packets

Especifica la prioridad de la VLAN para enviar paquetes de datos de administración. En función de la prioridad de la VLAN, el dispositivo asigna el paquete de datos a una clase de tráfico específica y, a continuación, a una cola de prioridad específica del puerto.

Valores posibles:

- `0..7` (configuración por defecto: `0`)

En el cuadro de diálogo *Switching > QoS/Priority > 802.1D/p Mapping*, asigne una clase de tráfico a cada prioridad de VLAN.

IP DSCP value for management packets

Especifica el valor de IP DSCP para enviar paquetes de datos de administración. En función del valor de IP DSCP, el dispositivo asigna el paquete de datos a una clase de tráfico específica y, a continuación, a una cola de prioridad específica del puerto.

Valores posibles:

- `0 (be/cs0)..63` (configuración por defecto: `0 (be/cs0)`)

Algunos valores de la lista también disponen de una palabra clave DSCP, por ejemplo, `0 (be/cs0)`, `10 (af11)` y `46 (ef)`. Estos valores son compatibles con el modelo de precedencia de IP.

En el cuadro de diálogo *Switching > QoS/Priority > IP DSCP Mapping*, asigne una clase de tráfico a cada valor de IP DSCP.

Queues per port

Muestra el número de colas con prioridad por puerto.

El dispositivo tiene 8 colas con prioridad por puerto. Asigne cada cola con prioridad a una clase de tráfico específica (clase de tráfico conforme al estándar IEEE 802.1D).

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## 5.8.2 QoS/Priority Port Configuration

[ Switching > QoS/Priority > Port Configuration ]

En este cuadro de diálogo, especifique para cada puerto cómo procesa el dispositivo los paquetes de datos recibidos en función de su información de QoS/prioridad.

### Tabla

Port

Muestra el número de puerto.

Port priority

Especifica qué información de prioridad de VLAN debe escribir el dispositivo en un paquete de datos si este no contiene ninguna información de prioridad. Tras esto, el dispositivo transmite el paquete de datos en función del valor especificado en la columna *Trust mode*.

Valores posibles:

- `0..7` (configuración por defecto: `0`)

Trust mode

Especifica cómo maneja el dispositivo un paquete de datos recibido si este contiene información de QoS/prioridad.

Valores posibles:

- *untrusted*
  El dispositivo transmite el paquete de datos conforme a la prioridad especificada en la columna *Port priority*. El dispositivo ignora la información sobre la prioridad contenida en el paquete de datos.
  En el cuadro de diálogo *Switching > QoS/Priority > 802.1D/p Mapping*, asigne una clase de tráfico a cada prioridad de VLAN.
- *trustDot1p* (configuración por defecto)
  El dispositivo transmite el paquete de datos conforme a la información de prioridad en la etiqueta de VLAN.
  En el cuadro de diálogo *Switching > QoS/Priority > 802.1D/p Mapping*, asigne una clase de tráfico a cada prioridad de VLAN.
- *trustIpDscp*
  - Si el paquete de datos es un paquete de IP:
    El dispositivo transmite el paquete de datos conforme al valor de IP DSCP contenido en dicho paquete.
    En el cuadro de diálogo *Switching > QoS/Priority > IP DSCP Mapping*, asigne una clase de tráfico a cada valor de IP DSCP.
  - Si el paquete de datos no es un paquete de IP:
    El dispositivo transmite el paquete de datos conforme a la prioridad especificada en la columna *Port priority*.
    En el cuadro de diálogo *Switching > QoS/Priority > 802.1D/p Mapping*, asigne una clase de tráfico a cada prioridad de VLAN.

Untrusted traffic class

Muestra la clase de tráfico asignada a la información de prioridad de VLAN especificada en la columna *Port priority*. En el cuadro de diálogo *Switching > QoS/Priority > 802.1D/p Mapping*, asigne una clase de tráfico a cada prioridad de VLAN.

Valores posibles:

- `0..7`

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

# 5.8.3 802.1D/p Mapping

[ Switching > QoS/Priority > 802.1D/p Mapping ]

El dispositivo transmite paquetes de datos con una etiqueta VLAN conforme a la información de QoS/prioridad contenida con una prioridad superior o inferior.

En este cuadro de diálogo, asigne una clase de tráfico a cada prioridad de VLAN. Asigne las clases de tráfico a las colas de prioridad de los puertos.

### Tabla

VLAN priority

Muestra la prioridad de la VLAN.

Traffic class

Especifica la clase de tráfico asignada a la prioridad de VLAN.

Valores posibles:

- `0..7`
  `0` asignado a la cola con menor prioridad.
  `7` asignado a la cola con mayor prioridad.

**Nota:** Entre otras cosas, los mecanismos de redundancia utilizan la clase de tráfico más alta. Por ello, seleccione otra clase de tráfico para los datos de aplicaciones.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

### Asignación predeterminada de la prioridad de VLAN a clases de tráfico

| Prioridad de VLAN | Clase de tráfico | Descripción de contenidos conforme al estándar IEEE 802.1D |
|---|---|---|
| `0` | 2 | `Best Effort`<br>Datos normales sin priorización |
| `1` | 0 | `Background`<br>Datos que no dependen del tiempo y servicios en segundo plano |
| `2` | 1 | `Standard`<br>Datos normales |
| `3` | 3 | `Excellent Effort`<br>Datos cruciales |
| `4` | 4 | `Controlled Load`<br>Datos que dependen del tiempo con prioridad alta |

| Prioridad de VLAN | Clase de tráfico | Descripción de contenidos conforme al estándar IEEE 802.1D |
|---|---|---|
| 5 | 5 | Video<br>Transmisión de vídeo con retardos y distorsiones < 100 ms |
| 6 | 6 | Voice<br>Transmisión de voz con retardos y distorsiones < 10 ms |
| 7 | 7 | Network Control<br>Datos de administración de red y mecanismos de redundancia |

# 5.8.4 IP DSCP Mapping

[ Switching > QoS/Priority > IP DSCP Mapping ]

El dispositivo transmite paquetes de datos de IP conforme al valor de DSCP contenido en el paquete de datos con una prioridad superior o inferior.

En este cuadro de diálogo, asigne una clase de tráfico a cada valor de DSCP. Asigne las clases de tráfico a las colas de prioridad de los puertos.

### Tabla

DSCP value

Muestra el valor de DSCP.

Traffic class

Especifica la clase de tráfico asignada al valor de DSCP.

Valores posibles:

- `0..7`
  `0` asignado a la cola con menor prioridad.
  `7` asignado a la cola con mayor prioridad.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

### Asignación predeterminada de los valores DSCP a clases de tráfico

| Valor de DSCP | Nombre de DSCP | Clase de tráfico |
|---|---|---|
| 0 | Best Effort /CS0 | 2 |
| 1-7 | | 2 |
| 8 | CS1 | 0 |
| 9,11,13,15 | | 0 |
| 10,12,14 | AF11,AF12,AF13 | 0 |
| 16 | CS2 | 1 |
| 17,19,21,23 | | 1 |
| 18,20,22 | AF21,AF22,AF23 | 1 |
| 24 | CS3 | 3 |
| 25,27,29,31 | | 3 |
| 26,28,30 | AF31,AF32,AF33 | 3 |
| 32 | CS4 | 4 |
| 33,35,37,39 | | 4 |
| 34,36,38 | AF41,AF42,AF43 | 4 |

| Valor de DSCP | Nombre de DSCP | Clase de tráfico |
|---|---|---|
| 40 | CS5 | 5 |
| 41,42,43,44,45,47 | | 5 |
| 46 | EF | 5 |
| 48 | CS6 | 6 |
| 49-55 | | 6 |
| 56 | CS7 | 7 |
| 57-63 | | 7 |

# 5.8.5 Queue Management

[ Switching > QoS/Priority > Queue Management ]

El cuadro de diálogo le permite activar y desactivar la función *Strict priority* para las clases de tráfico. Cuando desactive la función *Strict priority*, el dispositivo procesará las colas de prioridad de los puertos con la "Espera equitativa ponderada".

También dispone de la opción de asignar un mínimo de ancho de banda a cada clase de tráfico que el dispositivo utiliza para procesar las colas con prioridad con "Espera equitativa ponderada".

### Tabla

Traffic class

Muestra la clase de tráfico.

Strict priority

Activa/desactiva el procesamiento de la cola con prioridad del puerto con *Strict priority* para esta clase de tráfico.

Valores posibles:

- `marked` (configuración por defecto)
  El procesamiento de la cola con prioridad del puerto con *Strict priority* está activo.
  - El puerto solamente reenvía paquetes de datos que están en la cola con mayor prioridad. Cuando esta cola con prioridad está vacía, el puerto reenvía los paquetes de datos que están en la cola con la siguiente prioridad inferior.
  - El puerto reenvía los paquetes de datos con una clase de tráfico inferior cuando se vacían las colas con mayor prioridad. En situaciones desfavorables, el puerto no envía estos paquetes de datos.
  - Cuando seleccione este ajuste para una clase de tráfico, el dispositivo también activará la función para las clases de tráfico con una mayor prioridad.
  - Utilice este ajuste para aplicaciones como VoIP o vídeo que requieran el mínimo retardo posible.
- `unmarked`
  El procesamiento de la cola con prioridad del puerto con *Strict priority* está inactivo. El dispositivo utiliza "Espera equitativa ponderada"/"Round Robin ponderada" (WRR) para procesar la cola con prioridad del puerto.
  - El dispositivo asigna un ancho de banda mínimo a cada clase de tráfico.
  - Incluso con cargas de red elevadas, el puerto transmite paquetes de datos con una clase de tráfico baja.
  - Cuando seleccione este ajuste para una clase de tráfico, el dispositivo también desactivará la función para las clases de tráfico con una menor prioridad.

Min. bandwidth [%]

Especifica el ancho de banda mínimo para esta clase de tráfico cuando el dispositivo está procesando las colas con prioridad de los puertos con "Espera equitativa ponderada".

Valores posibles:

- `0..100` (configuración por defecto: `0` = el dispositivo no reserva ningún ancho de banda para esta clase de tráfico)

El valor especificado en porcentaje hace referencia al ancho de banda disponible en el puerto. Cuando desactive la función *Strict priority* para cada clase de tráfico, dispondrá del ancho de banda máximo del puerto para "Espera equitativa ponderada".

El máximo total de los anchos de banda asignados es del 100%.

Max. bandwidth [%]

Especifica la velocidad de formación a la que una clase de tráfico transmite paquetes (formación de cola).

Valores posibles:

- `0` (configuración por defecto)
  El dispositivo no reserva ningún ancho de banda para esta clase de tráfico.
- `1..100`
  El dispositivo reserva el ancho de banda especificado para esta clase de tráfico. El valor especificado en porcentaje hace referencia al ancho de banda máximo disponible en este puerto.

Por ejemplo, utilizar la formación de cola le permite limitar la velocidad de la cola con prioridad estricta alta. Al limitar una cola con prioridad estricta alta, el dispositivo también puede procesar las colas con prioridad baja. Para utilizar la formación de cola, configure el ancho de banda máximo de una cola en particular.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## 5.9 VLAN

[ Switching > VLAN ]

Con una VLAN (red de área local virtual), puede distribuir el tráfico de datos de la red física a redes secundarias lógicas. Esto le ofrece las siguientes ventajas:

- Flexibilidad elevada
  - Con una VLAN, puede distribuir el tráfico de datos a redes lógicas de la infraestructura existente. Sin una VLAN, sería necesario disponer de dispositivos adicionales y de un cableado complicado.
  - Con una VLAN, puede especificar segmentos de red independientemente de la ubicación de los dispositivos terminales individuales.

- Mejora del rendimiento
  - En las VLAN, los paquetes de datos pueden transferirse en función de la prioridad.
    Si la prioridad es elevada, el dispositivo transfiere los datos de una VLAN en función de su preferencia, por ejemplo, para aplicaciones que dependen del tiempo como las llamadas VoIP.
  - Cuando los paquetes de datos y los mensajes Broadcast se distribuyen en pequeños segmentos de red en lugar de en la red completa, la carga de la red se ve reducida de manera considerable.
- Aumento de la seguridad
  La distribución del tráfico de datos entre redes lógicas individuales hace que el acceso no deseado resulte más difícil y fortalece al sistema frente a ataques, como desbordamiento de direcciones MAC o suplantación de direcciones MAC.

El dispositivo admite VLAN "etiquetadas" basadas en paquetes conforme al estándar IEEE 802.1Q. El etiquetado de VLAN del paquete de datos indica la VLAN a la que pertenece el paquete de datos.

El dispositivo transmite los paquetes de datos etiquetados de una VLAN solamente en puertos asignados a la misma VLAN. Esto reduce la carga de la red.

El dispositivo aprende las direcciones MAC de cada VLAN por separado (aprendizaje independiente de la VLAN).

El dispositivo prioriza el flujo de datos recibido en la siguiente secuencia:
- Voice VLAN
- VLAN basada en puerto

El menú contiene los siguientes cuadros de diálogo:
- VLAN Global
- VLAN Configuration
- VLAN Port
- VLAN Voice

## 5.9.1 VLAN Global

[ Switching > VLAN > Global ]

Este cuadro de diálogo le permite ver parámetros de VLAN generales para el dispositivo.

### Configuration

Max. VLAN ID

ID más alto asignable a una VLAN.

Consulte el cuadro de diálogo *Switching > VLAN > Configuration*.

VLANs (max.)

Muestra el número máximo de VLAN posibles.

Consulte el cuadro de diálogo *Switching > VLAN > Configuration*.

VLANs

Número de VLAN configuradas actualmente en el dispositivo.

Consulte el cuadro de diálogo *Switching > VLAN > Configuration*.

El ID 1 de la VLAN está presente constantemente en el dispositivo.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

Clear...

Restablece la configuración VLAN por defecto del dispositivo.

Tenga en cuenta que perderá su conexión con el dispositivo si ha cambiado el ID de VLAN de la gestión del dispositivo en el cuadro de diálogo *Basic Settings > Network*.

## 5.9.2 VLAN Configuration

[ Switching > VLAN > Configuration ]

En este cuadro de diálogo, administre las VLAN. Para configurar una VLAN, cree una fila adicional en la tabla. En ella podrá especificar para cada puerto si transmite paquetes de datos de la VLAN correspondiente y si los paquetes de datos contienen una etiqueta de VLAN.

Puede distinguirse entre las siguientes VLAN:
- El usuario configura VLAN estáticas.
- El dispositivo configura VLAN dinámicas automáticamente y las elimina si dejan de aplicarse los requisitos previos.
  Para las funciones siguientes, el dispositivo crea VLAN dinámicas:
  - *MRP*: si asigna a los puertos de anillo una VLAN no existente, el dispositivo crea esta VLAN.
  - *MVRP*: el dispositivo crea una VLAN en función de los mensajes de dispositivos próximos.

### Tabla

VLAN ID

ID de la VLAN.

El dispositivo admite hasta 128 VLAN configuradas simultáneamente.

Valores posibles:
- `1..4042`

Status

Muestra cómo se configura la VLAN.

Valores posibles:
- *`other`*
  VLAN `1`
  o bien
  VLAN configurada utilizando la función *802.1X Port Authentication*. Consulte el cuadro de diálogo *Network Security > 802.1X Port Authentication*.
- *`permanent`*
  VLAN configurada por el usuario.
  o bien
  VLAN configurada utilizando la función *MRP*. Consulte el cuadro de diálogo *Switching > L2-Redundancy > MRP*.
  Si guarda los cambios en la memoria no volátil, las VLAN con este ajuste permanecerán configuradas tras el reinicio.
- *`dynamicMvrp`*
  VLAN configurada utilizando la función *MVRP*. Consulte el cuadro de diálogo *Switching > MRP-IEEE > MVRP*.
  Las VLAN con este ajuste están protegidas contra escritura. El dispositivo elimina una VLAN de la tabla en cuanto el puerto abandona la VLAN.

Creation time

Muestra la hora de creación de la VLAN.

El campo muestra la marca de hora del tiempo de funcionamiento (tiempo de actividad del sistema).

Name

Especifica el nombre de la VLAN.

Valores posibles:

- Cadena de caracteres ASCII alfanuméricos con entre 1 y 32 caracteres

<Port number>

Especifica si el puerto correspondiente transmite paquetes de datos de la VLAN y si los paquetes de datos contienen una etiqueta de VLAN.

Valores posibles:

- `-` (configuración por defecto)
  El puerto no es miembro de la VLAN y no transmite paquetes de datos de esta.
- `T` = Tagged
  El puerto es miembro de la VLAN y transmite los paquetes de datos con una etiqueta VLAN. Utilice esta configuración para puertos Uplink, por ejemplo.
- `LT` = Tagged Learned
  El puerto es miembro de la VLAN y transmite los paquetes de datos con una etiqueta VLAN. El dispositivo creó la entrada automáticamente basándose en la función *GVRP* o *MVRP*.
- `F` = Forbidden
  El puerto no es miembro de la VLAN y no transmite paquetes de datos de esta.
  Además, el dispositivo ayuda a evitar que el puerto se convierta en un miembro de una VLAN mediante la función *MVRP*.
- `U` = Untagged (configuración por defecto de la VLAN 1)
  El puerto es miembro de la VLAN y transmite los paquetes de datos sin una etiqueta VLAN. Utilice este ajuste si el dispositivo conectado no evalúa ninguna etiqueta de VLAN, por ejemplo, en puertos finales.
- `LU` = Untagged Learned
  El puerto es miembro de la VLAN y transmite los paquetes de datos sin una etiqueta VLAN. El dispositivo creó la entrada automáticamente basándose en la función *GVRP* o *MVRP*.

**Nota:** Compruebe que el puerto en el que está conectada la estación de administración de red sea miembro de la VLAN en la que el dispositivo transmite los datos de administración. Con la configuración por defecto, el dispositivo transmite los datos de administración de la VLAN 1. De lo contrario, la conexión con el dispositivo se cancela cuando transfiere los cambios al dispositivo. El acceso a la gestión del dispositivo solamente es posible utilizando la interfaz de línea de comando a través de la interfaz serie.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

Abre la ventana *Create* para añadir una entrada nueva a la tabla.

En el campo *VLAN ID*, especifique el ID de la VLAN.

## 5.9.3 VLAN Port

[ Switching > VLAN > Port ]

En este cuadro de diálogo, especifique cómo desea que el dispositivo maneje los paquetes de datos recibidos que no disponen de etiqueta de VLAN o cuya etiqueta de VLAN varíe respecto al ID de VLAN del puerto.

Este cuadro de diálogo le permite asignar una VLAN a los puertos y especificar el ID de VLAN del puerto.

Además, también puede especificar para cada puerto cómo desea que transmita paquetes de datos el dispositivo y se producirá una de las siguientes situaciones:
- El puerto recibirá paquetes de datos sin etiquetado de VLAN.
- El puerto recibirá paquetes de datos con información de prioridad de VLAN (ID de VLAN `0`, con etiqueta de prioridad).
- El etiquetado de VLAN del paquete de datos varía respecto al ID de VLAN del puerto.

### Tabla

Port

Muestra el número de puerto.

Port-VLAN ID

Especifica el ID de la VLAN que los dispositivos asignan a los paquetes de datos sin una etiqueta de VLAN.

Requisitos previos:
- En la columna *Acceptable packet types*, especifique el valor `admitAll`.

Valores posibles:
- ID de una VLAN configurada por usted (configuración por defecto: `1`)

Si utiliza la función *MRP* y no ha asignado una VLAN a los puertos de anillo, especifique el valor `1` aquí para los puertos de anillo. De lo contrario, el dispositivo asignará el valor a los puertos de anillo automáticamente.

Acceptable packet types

Especifica si el puerto transmite o descarta paquetes de datos recibidos sin una etiqueta VLAN.

Valores posibles:
- `admitAll` (configuración por defecto)
  El puerto acepta paquetes de datos con y sin una etiqueta VLAN.
- `admitOnlyVlanTagged`
  El puerto solamente acepta paquetes de datos etiquetados con un ID de VLAN ≥ `1`.

Ingress filtering

Activa/desactiva el filtrado de ingreso.

Valores posibles:

- `marked`
  El filtrado de ingreso está activo.
  El dispositivo compara el ID de VLAN del paquete de datos con las VLAN de las que es miembro el dispositivo. Consulte el cuadro de diálogo *Switching > VLAN > Configuration*. Si el ID de VLAN del paquete de datos coincide con una de estas VLAN, el puerto transmite el paquete de datos. De lo contrario, el dispositivo descarta el paquete de datos.
- `unmarked` (configuración por defecto)
  El filtrado de ingreso está inactivo.
  El dispositivo transmite los paquetes de datos recibidos sin comparar el ID de VLAN. De este modo, el puerto también transmite paquetes de datos con un ID de VLAN del que el puerto no es miembro.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## 5.9.4 VLAN Voice

[ Switching > VLAN > Voice ]

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 Voice VLAN es que protege la calidad del tráfico de voz cuando el tráfico de datos del puerto es elevado.

El dispositivo detecta teléfonos de VoIP utilizando Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED). A continuación, el dispositivo añade el puerto adecuado al conjunto de miembros de la Voice VLAN configurada. El conjunto de miembros está etiquetado o no etiquetado. El etiquetado depende del modo de interfaz de Voice VLAN (VLAN ID, Dot1p, None, Untagged).

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 del dispositivo. Como resultado, el teléfono VoIP envía datos de voz etiquetados como prioritarios o sin etiquetar. Esto depende del modo de interfaz de Voice VLAN configurado. Active la Voice VLAN en el puerto que se está conectando al teléfono VoIP.

### Operation

Operation

Activa/desactiva la función *VLAN Voice* del dispositivo globalmente.

Valores posibles:

- *On*
- *Off* (configuración por defecto)

### Tabla

Port

Muestra el número de puerto.

Voice VLAN mode

Especifica si el puerto transmite o descarta paquetes de datos recibidos sin una etiqueta de Voice VLAN o con información de prioridad de Voice VLAN.

Valores posibles:

- *disabled* (configuración por defecto)
  Desactiva la función *VLAN Voice* para esta entrada de tabla.
- *none*
  Permite al teléfono IP utilizar su propia configuración para enviar tráfico de voz sin etiquetar.
- *vlan/dot1p-priority*
  El puerto filtra paquetes de datos de Voice VLAN utilizando las etiquetas de prioridad vlan y dot1p.
- *untagged*
  El puerto filtra paquetes de datos sin una etiqueta de Voice VLAN.

- *vlan*
  El puerto filtra paquetes de datos de Voice VLAN utilizando la etiqueta vlan.
- *dot1p-priority*
  El puerto filtra paquetes de datos de Voice VLAN utilizando las etiquetas de prioridad dot1p. Si selecciona este valor, especifique también un valor adecuado en la columna *Priority*.

Data priority mode

Especifica el modo de confianza para el tráfico de datos en el puerto en particular.

El dispositivo utiliza este modo para el tráfico de datos en Voice VLAN, cuando detecta un teléfono VoIP y un PC y cuando estos dispositivos utilizan el mismo cable para transmitir y recibir datos.

Valores posibles:

- *trust* (configuración por defecto)
  Si el tráfico de voz está presente en la interfaz, el tráfico de datos utiliza la prioridad normal con este ajuste.
- *untrust*
  Si el tráfico de voz está presente y *Voice VLAN mode* está ajustado en *dot1p-priority*, los datos tendrán la prioridad 0. Si la interfaz solamente transmite datos, los datos tienen la prioridad normal.

Status

Muestra el estado de Voice VLAN en el puerto.

Valores posibles:

- marked
  Voice VLAN está activada.
- unmarked
  Voice VLAN está desactivada.

VLAN ID

Especifica el ID de la VLAN a la que se aplica la entrada de la tabla.

Para reenviar el tráfico a este ID de VLAN mediante este filtro, seleccione el valor *vlan* en la columna *Voice VLAN mode*.

Valores posibles:

- 0..4042

Priority

Especifica la prioridad de Voice VLAN del puerto.

Requisitos previos:

- En la columna *Voice VLAN mode*, especifique el valor *dot1p-priority*.

Valores posibles:

- *0..7*
- *none*
  Desactiva la prioridad de Voice VLAN del puerto.

Bypass authentication

Activa el modo de autenticación de Voice VLAN.

Si desactiva la función y ajusta el valor de la columna *Voice VLAN mode* en `dot1p-priority`, los dispositivos de voz requerirán autenticación.

Valores posibles:

- `marked` (configuración por defecto)
  Si ha activado la función en el cuadro de diálogo *Network Security > 802.1X Port Authentication > Global*, ajuste el parámetro *Port control* para este puerto en el valor `multiClient` antes de activar esta función. Puede encontrar el parámetro *Port control* en el cuadro de diálogo *Network Security* > 802.1X Port Authentication > *Global*.
- `unmarked`

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## 5.10 L2-Redundancy

[ Switching > L2-Redundancy ]

El menú contiene los siguientes cuadros de diálogo:

- MRP
- HIPER Ring
- Spanning Tree
- Link Aggregation
- Link Backup
- FuseNet

# 5.10.1 MRP

[ Switching > L2-Redundancy > MRP ]

**⚠ 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.**

El Media Redundancy Protocol (MRP, Media Redundancy Protocol) es un protocolo que le ayuda a configurar estructuras de red en forma de anillo de alta disponibilidad. Un anillo MRP con dispositivos Schneider Electric está compuesto por hasta 100 dispositivos compatibles con el protocolo MRP conforme al estándar IEC 62439.

Si una sección no está funcionando, la estructura de anillo de un anillo MRP vuelve a cambiar a una estructura lineal. Es posible configurar el tiempo de recuperación máximo.

La función Ring Manager del dispositivo cierra los extremos de un backbone de una estructura lineal para formar un anillo redundante.

**Nota:** *Spanning Tree* y la redundancia de anillo se afectan mutuamente. Desactive el protocolo *Spanning Tree* para los puertos conectados al anillo MRP. Consulte el cuadro de diálogo *Switching* > L2-Redundancy > *Spanning Tree* > *Port*.

Cuando trabaje con paquetes de Ethernet sobredimensionados (el valor de la columna *MTU* para el puerto es > `1518`, consulte el cuadro de diálogo *Basic Settings* > *Port*), el intervalo de conmutación de la reconfiguración del anillo MRP dependerá de los siguientes parámetros:

- Ancho de banda de la línea de anillo
- Tamaño de los paquetes de Ethernet
- Número de dispositivos del anillo

Ajuste el tiempo de recuperación lo bastante como para ayudar a evitar retardos en los paquetes MRP debido a latencias en los dispositivos. Puede encontrar la fórmula para calcular el intervalo de conmutación en la norma IEC 62439-2, sección 9.5.

### Operation

Operation

Activa/desactiva la función *MRP*.

Una vez configurados los parámetros para el anillo MRP, active la función aquí.

Valores posibles:

- *On*
  La función *MRP* está activada.
  Una vez configurados los dispositivos en el anillo MRP, la redundancia estará activa.
- *Off* (configuración por defecto)
  La función *MRP* está desactivada.

### Ring port 1/Ring port 2

Port

Especifica el número del puerto que está operando como puerto de anillo.

Valores posibles:

- <Port number>
  Número del puerto de anillo

Operation

Muestra el estado de funcionamiento del puerto de 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.

Fixed backup

Activa/desactiva la función del puerto de reserva para *Ring port 2*.

**Nota:** La conmutación al puerto principal puede superar el tiempo de recuperación máximo del anillo.

Valores posibles:

- marked
  La función de copia de seguridad *Ring port 2* está activa. Si el anillo está cerrado, Ring Manager regresa al puerto de anillo principal.
- unmarked (configuración por defecto)
  La función de copia de seguridad *Ring port 2* está inactiva. Si el anillo está cerrado, Ring Manager continúa enviando datos en el puerto de anillo secundario.

## Configuration

Ring manager

Activa/desactiva la función *Ring manager*.

Si hay un dispositivo en cada extremo de la línea, active esta función.

Valores posibles:

- *On*
  La función *Ring manager* está activada.
  El dispositivo actúa como Ring Manager.
- *Off* (configuración por defecto)
  La función *Ring manager* está desactivada.
  El dispositivo actúa como Ring Client.

Advanced mode

Activa/desactiva el modo avanzado para conseguir tiempos de recuperación rápidos.

Valores posibles:

- `marked` (configuración por defecto)
  Modo avanzado activo.
  Los dispositivos Schneider Electric compatibles con MRP admiten este modo.
- `unmarked`
  Modo avanzado inactivo.
  Seleccione este ajuste si otro dispositivo del anillo no admite este modo.

Ring recovery

Especifica el tiempo de recuperación máximo en milisegundos para efectuar la reconfiguración del anillo. Este ajuste resulta efectivo si el dispositivo actúa como Ring Manager.

Valores posibles:

- *500ms*
- *200ms* (configuración por defecto)

El establecimiento de intervalos de conmutación más cortos provoca que haya mayores demandas de tiempo de respuesta de cada dispositivo individual del anillo. Utilice valores inferiores a *500ms* si los demás dispositivos del anillo también admiten este tiempo de recuperación inferior.

Cuando esté trabajando con paquetes de Ethernet sobredimensionados, el número de dispositivos del anillo estará limitado. Tenga en cuenta que el tiempo de conmutación depende de varios parámetros. Consulte la descripción anterior.

VLAN ID

Especifica el ID de la VLAN que asigna a los puertos de anillo.

Valores posibles:

- `0` (configuración por defecto)
  Ninguna VLAN asignada.
  En el cuadro de diálogo *Switching > VLAN > Configuration*, asigne el valor `1` a los puertos de anillo de la VLAN `U`.
- `1..4042`
  VLAN asignada.
  Si asigna una VLAN no existente a los puertos de anillo, el dispositivo crea esta VLAN. En el cuadro de diálogo *Switching > VLAN > Configuration*, el dispositivo crea una entrada en la tabla para la VLAN y asigna el valor `T` a los puertos de anillo.

### Information

Information

Muestra mensajes para la configuración de la redundancia y las posibles causas de los errores detectados.

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* únicamente 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.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

Delete ring configuration

Desactiva la función de redundancia y restablece los ajustes por defecto en el cuadro de diálogo.

## 5.10.2 HIPER Ring

[ Switching > L2-Redundancy > HIPER Ring ]

**⚠ 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 construir redes de alta disponibilidad y con forma de anillo. El dispositivo proporciona un cliente de anillo HIPER. Esta función le permite ampliar un anillo HIPER existente o sustituir un dispositivo que ya esté participando como cliente en un anillo HIPER.

Un anillo HIPER contiene un Ring Manager (RM) que controla el anillo. El RM envía paquetes guardián al anillo en los puertos principal y secundario. Cuando el RM recibe los paquetes guardián en ambos puertos, el puerto principal permanece en estado de reenvío y el secundario permanece en estado de descarte.

El dispositivo actúa solamente en modo Ring Client. Esto significa que el dispositivo puede reconocer y reenviar los paquetes guardián de los puertos de anillo y también puede reenviar el cambio en un estado de conexión al RM, por ejemplo, paquetes LinkDown y LinkUp.

El dispositivo solamente admite puertos Fast Ethernet y Gigabit Ethernet como puertos de anillo. Además, el dispositivo solamente admite anillos HIPER en VLAN `1`.

**Nota:** *Spanning Tree* y la redundancia de anillo se afectan mutuamente. Desactive el protocolo *Spanning Tree* para los puertos conectados al anillo HIPER. Consulte el cuadro de diálogo *Switching > L2-Redundancy > Spanning Tree > Port*.

**Nota:** Configure los dispositivos del anillo HIPER individualmente. Antes de conectar el trayecto redundante, complete la configuración de cada dispositivo del anillo HIPER. De esta forma, ayuda a evitar bucles durante la fase de configuración.

### Operation

Operation

Activa/desactiva el cliente *HIPER Ring*.

Valores posibles:

- `On`
  El cliente *HIPER Ring* se activa.
- `Off` (configuración por defecto)
  El cliente *HIPER Ring* se desactiva.

### Ring port 1/Ring port 2

Port

Especifica el número de puerto del puerto de anillo principal/secundario.

Valores posibles:

- `-` (configuración por defecto)
  Ningún puerto de anillo principal/secundario seleccionado.
- `<Port number>`
  Número del puerto de anillo

State

Muestra el estado del puerto de anillo principal/secundario.

Valores posibles:

- *`not-available`*
  El cliente *HIPER Ring* se desactiva.
  o bien
  No hay ningún puerto de anillo principal o secundario seleccionado.
- *`active`*
  El puerto de anillo está activado y activo de manera lógica
- *`inactive`*
  El puerto de anillo está inactivo de manera lógica
  En cuanto la conexión baja por un puerto de anillo, el dispositivo envía un paquete LinkDown al Ring Manager del otro puerto de anillo.

### Information

Mode

Muestra que el dispositivo es capaz de operar en modo Ring Client.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## 5.10.3 Spanning Tree

[ Switching > L2-Redundancy > Spanning Tree ]

**⚠ 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.**

El Protocolo Spanning Tree (STP, Spanning Tree Protocol) es un protocolo que desactiva rutas redundantes de una red para ayudar a evitar bucles. Si un componente de red se vuelve inoperable en la ruta, el dispositivo calcula la nueva topología y reactiva estas rutas.

El Protocolo Rapid Spanning Tree (RSTP, Rapid Spanning Tree Protocol) permite la conmutación rápida a una topología recién calculada sin interrumpir las conexiones existentes. El RSTP alcanza tiempos de reconfiguración medios menores de un segundo. Cuando utiliza el RSTP en un anillo con entre 10 y 20 dispositivos, puede obtener tiempos de reconfiguración en milisegundos.

**Nota:** Si conecta el dispositivo a la red a través de SFP de par trenzado en lugar de a través de puertos de par trenzado normales, la reconfiguración de la red lleva un poco más.

El menú contiene los siguientes cuadros de diálogo:
- Spanning Tree Global
- Spanning Tree Dual RSTP (MCSESM-E)
- Spanning Tree Port

# 5.10.3.1 Spanning Tree Global

[ Switching > L2-Redundancy > Spanning Tree > Global ]

En este cuadro de diálogo podrá activar/desactivar la función *Spanning Tree* y especificar la configuración del puente.

### Operation

Operation

Activa/desactiva la función Spanning Tree en el dispositivo.

Valores posibles:

- *On* (configuración por defecto)
- *Off*
  El dispositivo se comporta de manera transparente. El dispositivo desborda paquetes de datos Spanning Tree recibidos como paquetes de datos Multicast a los puertos.

### Variant

Variant

Muestra el protocolo utilizado para la función *Spanning Tree*.

Valores posibles:

- *rstp*
  El protocolo RSTP está activo.
  Con RSTP (IEEE 802.1Q-2005), la función *Spanning Tree* opera para la capa física subyacente.

### Traps

Send trap

Activa/desactiva el envío de trampas SNMP para los siguientes eventos:

- Otro puente asume el rol de puente raíz.
- La topología cambia. El puerto cambia su *Port state* de *forwarding* a *discarding* o de *discarding* a *forwarding*.

Valores posibles:

- marked
  El envío de trampas SNMP está activo.
- unmarked (configuración por defecto)
  El envío de trampas SNMP está inactivo.

### Bridge configuration

Bridge ID

Muestra el ID del puente del dispositivo.

El dispositivo con el menor valor numérico de ID de puente adoptará el rol de puente raíz en la red.

Valores posibles:

- `<Bridge priority> / <MAC address>`
  Valor del campo *Priority*/dirección MAC del dispositivo

Priority

Especifica la prioridad del puente del dispositivo.

Valores posibles:

- `0..61440` en pasos de 4096 (configuración por defecto: `32768`)

Para convertir este dispositivo en puente raíz, asigne el valor de prioridad numérico mínimo en la red al dispositivo.

Hello time [s]

Especifica en segundos el tiempo que desea que transcurra entre el envío de dos mensajes de configuración (paquetes de datos Hello).

Valores posibles:

- `1..2` (configuración por defecto: `2`)

Si el dispositivo asume el rol de puente raíz, los demás dispositivos de la red utilizarán el valor aquí especificado.

En caso contrario, el dispositivo utiliza el valor especificado por el puente raíz. Consulte el cuadro *Root information*.

Debido a la interacción con el parámetro *Tx holds*, es recomendable no cambiar la configuración por defecto.

Forward delay [s]

Especifica el tiempo que desea que transcurra para el cambio de estado en segundos.

Valores posibles:

- `4..30` (configuración por defecto: `15`)

Si el dispositivo asume el rol de puente raíz, los demás dispositivos de la red utilizarán el valor aquí especificado.

En caso contrario, el dispositivo utiliza el valor especificado por el puente raíz. Consulte el cuadro *Root information*.

En el protocolo RSTP, los puentes negocian un cambio de estado sin que se haya especificado un tiempo de retardo.

El protocolo *Spanning Tree* utiliza el parámetro para retrasar el cambio de estado entre los estados *disabled*, *discarding*, *learning*, *forwarding*.

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.

Max age

Especifica la longitud máxima admisible de una rama, por ejemplo, el número de dispositivos que hay hasta el puente raíz.

Valores posibles:

- `6..40` (configuración por defecto: `20`)

Si el dispositivo asume el rol de puente raíz, los demás dispositivos de la red utilizarán el valor aquí especificado.

En caso contrario, el dispositivo utiliza el valor especificado por el puente raíz. Consulte el cuadro *Root information*.

El protocolo *Spanning Tree* utiliza el parámetro para especificar la validez de los BPDU de STP en segundos.

Tx holds

Limita la velocidad de transmisión máxima de envío de BPDU.

Valores posibles:

- `1..40` (configuración por defecto: `10`)

Cuando el dispositivo envía un BPDU, hace avanzar el contador en este puerto.

Si el contador alcanza el valor aquí especificado, el puerto interrumpe el envío de BPDU. Por un lado, esto reduce la carga generada por RSTP y, por el otro, si el dispositivo no recibe BPDU, es posible que se produzca una interrupción en la comunicación.

El dispositivo va descontando del contador `1` cada segundo. En el segundo siguiente, el dispositivo envía como máximo `1` nuevo BPDU.

BPDU guard

Activa/desactiva la función BPDU Guard en el dispositivo.

Con esta función, el dispositivo ayuda a proteger su red frente a configuraciones incorrectas, ataques con BPDU de STP y cambios de topología no deseados.

Valores posibles:

- `marked`
  *BPDU guard* está activo.
  - El dispositivo aplica la función a puertos periféricos especificados manualmente. Para estos puertos, en la pestaña *CIST* del cuadro de diálogo *Switching > L2-Redundancy > Spanning Tree > Port*, la casilla de la columna *Admin edge port* está marcada.
  - Si un puerto periférico recibe un BPDU de STP, el dispositivo desactiva el puerto. Para este puerto, en la pestaña *Configuration* del cuadro de diálogo *Basic Settings > Port*, la casilla de la columna *Port on* está en posición `unmarked`.
- `unmarked` (configuración por defecto)
  *BPDU guard* está activo.

Para restablecer el estado del puerto al valor `forwarding`, haga lo siguiente:

- ☐ Si el puerto continúa recibiendo BPDU:
  - En el cuadro de diálogo *Switching > L2-Redundancy > Spanning Tree > Port*, pestaña *CIST*, desmarque la casilla de la columna *Admin edge port*.
    o bien
  - En el cuadro de diálogo *Switching > L2-Redundancy > Spanning Tree > Global*, desmarque la casilla *BPDU guard*.
- ☐ Para volver a activar el puerto, utilice la función *Auto-Disable*. También puede hacer lo siguiente:
  - Abra el cuadro de diálogo *Basic Settings > Port*, pestaña *Configuration*.
  - Marque la casilla de la columna *Port on*.

BPDU filter (all admin edge ports)

Activa/desactiva el filtro de BPDU de STP en cada puerto periférico especificado manualmente. Para estos puertos, en la pestaña *CIST* del cuadro de diálogo *Switching > L2-Redundancy > Spanning Tree > Port*, la casilla de la columna *Admin edge port* está marcada.

Valores posibles:

- `marked`
  El filtro de BPDU está activo en cada puerto terminal.
  La función no utiliza estos puertos en operaciones *Spanning Tree*.
  - El dispositivo no envía BPDU de STP en estos puertos.
  - El dispositivo anula los BPDU de STP recibidos en estos puertos.
- `unmarked` (configuración por defecto)
  El filtro de BPDU global está inactivo.
  Tiene la opción de activar explícitamente el filtro de BPDU para puertos individuales. Consulte la columna *Port BPDU filter* del cuadro de diálogo *Switching > L2-Redundancy > Spanning Tree > Port*.

Auto-disable

Activa/desactiva la función *Auto-Disable* para los parámetros que *BPDU guard* está supervisando en el puerto.

Valores posibles:

- `marked`
  La función *Auto-Disable* de *BPDU guard* está activa.
  - Cuando el puerto recibe un BPDU de STP, el dispositivo desactiva un puerto periférico. El LED de "Estado de enlace" del puerto parpadea 3 veces por período.
  - El cuadro de diálogo *Diagnostics > Ports > Auto-Disable* muestra qué puertos están desactivados actualmente debido a que se han superado los parámetros.
  - La función *Auto-Disable* reactiva el puerto automáticamente. Para esto, vaya al cuadro de diálogo *Diagnostics > Ports > Auto-Disable* y especifique un período de espera para el puerto correspondiente en la columna *Reset timer [s]*.
- `unmarked` (configuración por defecto)
  La función *Auto-Disable* de *BPDU guard* está inactiva.

### Root information

Bridge ID

Muestra el ID del puente del puente raíz actual.

Valores posibles:

- `<Bridge priority> / <MAC address>`

Priority

Muestra la prioridad del puente raíz actual.

Valores posibles:

- `0..61440` en pasos de 4096

Hello time [s]

Muestra en segundos el tiempo que el puente raíz especifica entre el envío de dos mensajes de configuración (paquetes de datos Hello).

Valores posibles:

- `1..2`

El dispositivo utiliza este valor especificado. Consulte el cuadro *Bridge configuration*.

Forward delay [s]

Especifica en segundos el tiempo de retardo establecido por el puente raíz para que se produzcan los cambios de estado.

Valores posibles:

- `4..30`

El dispositivo utiliza este valor especificado. Consulte el cuadro *Bridge configuration*.

En el protocolo RSTP, los puentes negocian un cambio de estado sin que se haya especificado un tiempo de retardo.

El protocolo *Spanning Tree* utiliza el parámetro para retrasar el cambio de estado entre los estados `disabled`, `discarding`, `learning`, `forwarding`.

Max age

Especifica la longitud máxima admisible de una rama que el puente raíz configura, por ejemplo, el número de dispositivos que hay hasta el puente raíz.

Valores posibles:

- `6..40` (configuración por defecto: `20`)

El protocolo *Spanning Tree* utiliza el parámetro para especificar la validez de los BPDU de STP en segundos.

### Topology information

Bridge is root

Muestra si el dispositivo tiene actualmente el rol de puente raíz.

Valores posibles:

- `marked`
  Actualmente, el dispositivo tiene el rol de puente raíz.
- `unmarked`
  Actualmente, otro dispositivo tiene el rol de puente raíz.

Root port

Muestra el número del puerto desde el que la ruta actual está unida con el puente raíz.

Si el dispositivo asume el rol de puente raíz, el campo muestra el valor `no Port`.

Root path cost

Especifica el coste de la ruta que comunica entre el puerto raíz del dispositivo y el puente raíz de la red de Capa 2.

Valores posibles:

- `0..200000000`
  Si se especifica el valor `0`, el dispositivo asume el rol de puente raíz.

Topology changes

Muestra el número de veces que el dispositivo ha colocado un puerto en estado `forwarding` utilizando la función *Spanning Tree* desde el inicio de la instancia *Spanning Tree*.

Time since topology change

Muestra el tiempo transcurrido desde el último cambio de topología.

Valores posibles:

- `<days, hours:minutes:seconds>`

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

# 5.10.3.2 Spanning Tree Dual RSTP (MCSESM-E)

[ Switching > L2-Redundancy > Spanning Tree > Dual RSTP ]

**⚠ ADVERTENCIA**

**OPERACIÓN INESPERADA DEL EQUIPO**

Para ayudar a evitar bucles durante la fase de configuración, configure 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.

**El incumplimiento de estas instrucciones puede causar la muerte, heridas graves o daños en el equipo.**

En este diálogo especifica la configuración de puente correspondiente a la segunda instancia *Spanning Tree*.

La función *Dual RSTP* se utiliza con la función *RCP*. Si utiliza la función*RCP* tendrá la opción de acoplar uno o más anillosRSTP a la instancia RSTP en un anillo principal. Al acoplar 2 segmentos *Spanning Tree*, el anillo secundario representa una instancia de RSTP independiente para la que se aplica la configuración de 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*.

Especifique los ajustes de la función *RCP* en el cuadro de diálogo *Switching* > *L2-Redundancy* > FuseNet > *RCP*.

### Operation

Operation

Muestra si la función *Dual RSTP* está activada/desactivada en el dispositivo.

Valores posibles:

- *On*
  La función *Dual RSTP* está activada en el dispositivo.
  El dispositivo activa la función *Dual RSTP* si se cumplen los siguientes requisitos previos:
  - En el cuadro de diálogo *Switching* > *L2-Redundancy* > *FuseNet* > *RCP*, ha especificado los puertos para la configuración *Primary ring/network* y *Secondary ring/network*.
  - En el cuadro de diálogo *Switching* > *L2-Redundancy* > *FuseNet* > *RCP*, cuadro *Operation*, ha activado la función *RCP*.
  - En el cuadro de diálogo *Spanning Tree Global*, cuadro *Operation*, ha activado la función*Spanning Tree*.
  - No hay ningún protocolo de redundancia configurado en el anillo secundario.
- *Off* (configuración por defecto)
  La función *Dual RSTP* está desactivada en el dispositivo.

### Traps

Send trap

Activa/desactiva el envío de trampas SNMP para los siguientes eventos:

- Otro puente asume el rol de puente raíz.
- La topología cambia. El puerto cambia su *Port state* de *forwarding* a *discarding* o de *discarding* a *forwarding*.

Valores posibles:

▶ `marked` (configuración por defecto)
El envío de trampas SNMP está activo.

▶ `unmarked`
El envío de trampas SNMP está inactivo.

### Bridge configuration

Bridge ID

Muestra el ID del puente del dispositivo.

El dispositivo con el menor valor numérico de ID de puente adoptará el rol de puente raíz en la red.

Valores posibles:

▶ `<Bridge priority> / <MAC address>`
Valor del campo *Priority*/dirección MAC del dispositivo

Priority

Especifica la prioridad del puente del dispositivo.

Valores posibles:

▶ `0..61440` en pasos de 4096 (configuración por defecto: `32768`)

Para convertir este dispositivo en puente raíz, asigne el valor de prioridad numérico mínimo en la red al dispositivo.

Hello time [s]

Especifica en segundos el tiempo que desea que transcurra entre el envío de dos mensajes de configuración (paquetes de datos Hello).

Valores posibles:

▶ `1..2` (configuración por defecto: `2`)

Si el dispositivo asume el rol de puente raíz, los demás dispositivos de la red utilizarán el valor aquí especificado.

En caso contrario, el dispositivo utiliza el valor especificado por el puente raíz. Consulte el cuadro *Root information*.

Debido a la interacción con el parámetro *Tx holds*, es recomendable no cambiar la configuración por defecto.

Forward delay [s]

Especifica el tiempo que desea que transcurra para el cambio de estado en segundos.

Valores posibles:

- `4..30` (configuración por defecto: `15`)

Si el dispositivo asume el rol de puente raíz, los demás dispositivos de la red utilizarán el valor aquí especificado. En caso contrario, el dispositivo utiliza el valor especificado por el puente raíz. Consulte el cuadro *Root information*.

En el protocolo RSTP, los puentes negocian un cambio de estado sin que se haya especificado un tiempo de retardo.

El protocolo *Spanning Tree* utiliza el parámetro para retrasar el cambio de estado entre los estados `disabled`, `discarding`, `learning`, `forwarding`.

Los parámetros *Forward delay [s]* y *Max age* tienen la siguiente relación:

*Forward delay [s]* ≥ (*Max age*/2) + 1

Max age

Especifica el número máximo admisible de dispositivos que hay hasta el puente raíz.

Valores posibles:

- `6..40` (configuración por defecto: `20`)

Si el dispositivo asume el rol de puente raíz, los demás dispositivos de la red utilizarán el valor aquí especificado. En caso contrario, el dispositivo utiliza el valor especificado por el puente raíz. Consulte el cuadro *Root information*.

Tx holds

Limita la velocidad de transmisión máxima de envío de BPDU.

Valores posibles:

- `1..40` (configuración por defecto: `10`)

Cuando el dispositivo envía un BPDU, hace avanzar el contador en este puerto.

Si el contador alcanza el valor aquí especificado, el puerto interrumpe el envío de BPDU. Por un lado, esto reduce la carga generada por RSTP y, por el otro, si el dispositivo no recibe BPDU, es posible que se produzca una interrupción en la comunicación.

El dispositivo va descontando del contador `1` cada segundo. En el segundo siguiente, el dispositivo envía como máximo `1` nuevo BPDU.

BPDU guard

Activa/desactiva la función BPDU Guard en el dispositivo.

Con esta función, el dispositivo ayuda a proteger su red frente a configuraciones incorrectas, ataques con BPDU de STP y cambios de topología no deseados.

Valores posibles:

- `marked`
  *BPDU guard* está activo.
  - El dispositivo aplica la función a puertos periféricos especificados manualmente. Para estos puertos, en la pestaña *CIST* del cuadro de diálogo *Switching > L2-Redundancy > Spanning Tree > Port*, la casilla de la columna *Admin edge port* está marcada.
  - Si un puerto periférico recibe un BPDU de STP, el dispositivo desactiva el puerto. Para este puerto, en la pestaña *Configuration* del cuadro de diálogo *Basic Settings > Port*, la casilla de la columna *Port on* está en posición `unmarked`.
- `unmarked` (configuración por defecto)
  *BPDU guard* está activo.

Para restablecer el estado del puerto al valor *forwarding*, haga lo siguiente:

- ☐ Si el puerto continúa recibiendo BPDU:
  - En el cuadro de diálogo *Switching > L2-Redundancy > Spanning Tree > Port*, pestaña *CIST*, desmarque la casilla de la columna *Admin edge port*.
    o bien
  - En el cuadro de diálogo *Switching > L2-Redundancy > Spanning Tree > Dual RSTP*, desmarque la casilla *BPDU guard*.
- ☐ Para volver a activar el puerto, haga lo siguiente:
  - Abra el cuadro de diálogo *Basic Settings > Port*, pestaña *Configuration*.
  - Marque la casilla de la columna *Port on*.

BPDU filter (all admin edge ports)

Activa/desactiva el filtro de BPDU de STP en cada puerto periférico especificado manualmente. Para estos puertos, en la pestaña *CIST* del cuadro de diálogo *Switching > L2-Redundancy > Spanning Tree > Port*, la casilla de la columna *Admin edge port* está marcada.

Valores posibles:

- `marked`
  El filtro de BPDU está activo en cada puerto terminal.
  La función no utiliza estos puertos en operaciones *Spanning Tree*.
  - El dispositivo no envía BPDU de STP en estos puertos.
  - El dispositivo anula los BPDU de STP recibidos en estos puertos.
- `unmarked` (configuración por defecto)
  El filtro de BPDU global está inactivo.
  Tiene la opción de activar explícitamente el filtro de BPDU para puertos individuales. Consulte la columna *Port BPDU filter* del cuadro de diálogo *Switching > L2-Redundancy > Spanning Tree > Port*.

### Root information

Root ID

Muestra el ID del puente del puente raíz actual.

Valores posibles:

- `<Bridge priority> / <MAC address>`

Priority

Muestra la prioridad del puente raíz actual.

Valores posibles:

- `0..61440` en pasos de 4096

Hello time [s]

Muestra en segundos el tiempo que el puente raíz especifica entre el envío de dos mensajes de configuración (paquetes de datos Hello).

Valores posibles:

- `1..2`

El dispositivo utiliza este valor especificado. Consulte el cuadro *Bridge configuration*.

Forward delay [s]

Especifica en segundos el tiempo de retardo establecido por el puente raíz para que se produzcan los cambios de estado.

Valores posibles:

- `4..30`

El dispositivo utiliza este valor especificado. Consulte el cuadro *Bridge configuration*.

En el protocolo RSTP, los puentes negocian un cambio de estado sin que se haya especificado un tiempo de retardo.

El protocolo *Spanning Tree* utiliza el parámetro para retrasar el cambio de estado entre los estados *disabled*, *discarding*, *learning*, *forwarding*.

Max age

Especifica la longitud máxima admisible de una rama que el puente raíz configura, por ejemplo, el número de dispositivos que hay hasta el puente raíz.

Valores posibles:

- `6..40` (configuración por defecto: `20`)

El protocolo *Spanning Tree* utiliza el parámetro para especificar la validez de los BPDU de STP en segundos.

### Topology information

Bridge is root

Muestra si el dispositivo tiene actualmente el rol de puente raíz.

Valores posibles:

- `marked`
  Actualmente, el dispositivo tiene el rol de puente raíz.
- `unmarked`
  Actualmente, otro dispositivo tiene el rol de puente raíz.

Root port

Muestra el número del puerto desde el que la ruta actual está unida con el puente raíz.

Si el dispositivo asume el rol de puente raíz, el campo muestra el valor `no Port`.

Root path cost

Especifica el coste de la ruta que comunica entre el puerto raíz del dispositivo y el puente raíz de la red de Capa 2.

Valores posibles:

- `0..200000000`
  Si se especifica el valor `0`, el dispositivo asume el rol de puente raíz.

Topology changes

Muestra el número de veces que el dispositivo ha colocado un puerto en estado *`forwarding`* utilizando la función *Spanning Tree* desde el inicio de la instancia *Spanning Tree*.

Time since topology change

Muestra el tiempo transcurrido desde el último cambio de topología.

Valores posibles:

- `<days, hours:minutes:seconds>`

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

# 5.10.3.3 Spanning Tree Port

[Switching > L2-Redundancy > Spanning Tree > Port]

En este cuadro de diálogo, active la función Spanning Tree en los puertos, y especifique puertos periféricos y la configuración de varias funciones de protección.

El cuadro de diálogo contiene las siguientes pestañas:
- [CIST]
- [Guards]

## [CIST]

En esta pestaña, tiene la opción de activar la función Spanning Tree en los puertos de manera individual, especificar la configuración de los puertos periféricos y ver los valores actuales. CIST son las siglas de Common and Internal Spanning Tree (Spanning Tree común e interno).

**Nota:** Desactive la función *Spanning Tree* en los puertos que están participando en otros protocolos de redundancia de Capa 2. De lo contrario, es posible que los protocolos de redundancia funcionen de un modo distinto al deseado. Esto puede provocar bucles.

### Tabla

Port

Muestra el número de puerto.

STP active

Activa/desactiva la función Spanning Tree en el puerto.

Valores posibles:
- `marked` (configuración por defecto)
  La función *Spanning Tree* está activa en el puerto.
- `unmarked`
  La función *Spanning Tree* está inactiva en el puerto.
  Si la función *Spanning Tree* está activada en el dispositivo e inactiva en el puerto, el puerto no enviará STP-BPDU y anulará los STP-BPDU recibidos.

Port state

Muestra el estado de la transmisión del puerto.

Valores posibles:
- *discarding*
  El puerto está bloqueado y solamente reenvía BPDU de STP.
- *learning*
  El puerto está bloqueado, pero aprende las direcciones MAC de los paquetes de datos recibidos.
- *forwarding*
  El puerto reenvía los paquetes de datos.

- *disabled*
  El puerto está inactivo. Consulte el cuadro de diálogo *Basic Settings > Port*, pestaña *Configuration*.
- *manualFwd*
  La función *Spanning Tree* está desactivada en el puerto. El puerto reenvía los BPDU de STP.
- *notParticipate*
  El puerto no participa en el STP.

Port role

Muestra el rol actual del puerto en CIST.

Valores posibles:

- *root*
  Puerto con la ruta más económica al puente raíz.
- *alternate*
  Puerto con la ruta alternativa al puente raíz (bloqueada actualmente).
- *designated*
  Puerto para el lateral del árbol desviado desde el puente raíz (bloqueada actualmente).
- *backup*
  El puerto recibe BPDU de STP de su propio dispositivo.
- *disabled*
  El puerto está inactivo. Consulte el cuadro de diálogo *Basic Settings > Port*, pestaña *Configuration*.

Port path cost

Especifica los costes de la ruta del puerto.

Valores posibles:

- `0..200000000` (configuración por defecto: `0`)

Cuando el valor es `0`, el dispositivo calcula automáticamente los costes de la ruta en función de la velocidad de transferencia del puerto.

Port priority

Especifica la prioridad del puerto.

Valores posibles:

- `16..240` en pasos de 16 (configuración por defecto: `128`)

Este valor representa los primeros 4 bits del ID del puerto.

Received bridge ID

Muestra el ID del puente del dispositivo desde el que este puerto recibió por última vez un BPDU de STP.

Valores posibles:

- Para puertos con el rol *designated*, el dispositivo muestra la información del último BPDU de STP recibido por el puerto. Esto ayuda a diagnosticar posibles problemas de STP en la red.
- Para los roles de puerto *alternate*, *backup*, *master* y *root*, en estado fijo (topología estática), esta información es idéntica a la del rol de puerto *designated*.
- Si un puerto no tiene conexión o todavía no ha recibido ningún BDPU de STP, el dispositivo mostrará los valores que el puerto puede enviar con el rol *designated*.

Received port ID

Muestra el ID del puerto del dispositivo desde el que este puerto recibió por última vez un BPDU de STP.

Valores posibles:

- Para puertos con el rol `designated`, el dispositivo muestra la información del último BPDU de STP recibido por el puerto. Esto ayuda a diagnosticar posibles problemas de STP en la red.
- Para los roles de puerto `alternate`, `backup`, `master` y `root`, en estado fijo (topología estática), esta información es idéntica a la del rol de puerto `designated`.
- Si un puerto no tiene conexión o todavía no ha recibido ningún BDPU de STP, el dispositivo mostrará los valores que el puerto puede enviar con el rol `designated`.

Received path cost

Muestra el coste de la ruta que tiene el puente de mayor nivel desde su puerto raíz hasta el puente raíz.

Valores posibles:

- Para puertos con el rol `designated`, el dispositivo muestra la información del último BPDU de STP recibido por el puerto. Esto ayuda a diagnosticar posibles problemas de STP en la red.
- Para los roles de puerto `alternate`, `backup`, `master` y `root`, en estado fijo (topología estática), esta información es idéntica a la del rol de puerto `designated`.
- Si un puerto no tiene conexión o todavía no ha recibido ningún BDPU de STP, el dispositivo mostrará los valores que el puerto puede enviar con el rol `designated`.

Admin edge port

Activa/desactiva el modo *Admin edge port*. Si el puerto está conectado a un dispositivo terminal, utilice el modo *Admin edge port*. Esta configuración permite al puerto periférico cambiar más rápidamente al estado de reenvío tras una conexión, lo cual permite conseguir una accesibilidad más rápida al dispositivo terminal.

Valores posibles:

- `marked`
  El modo *Admin edge port* está activo.
  El puerto está conectado a un dispositivo terminal.
  - Una vez configurada la conexión, el puerto cambia al estado `forwarding` sin cambiar al estado `learning` previamente.
  - Si el puerto recibe un BPDU de STP y la función BPDU Guard está activa, el dispositivo desactivará el puerto. Consulte el cuadro de diálogo *Switching > L2-Redundancy > Spanning Tree > Global*.
- `unmarked` (configuración por defecto)
  El modo *Admin edge port* está inactivo.
  El puerto está conectado a otro puente STP.
  Una vez configurada la conexión, el puerto cambia al estado `learning` antes de cambiar al estado `forwarding` si procede.

Auto edge port

Activa/desactiva la detección automática de si conecta un dispositivo terminal al puerto. Como requisito previo, la casilla de la columna *Admin edge port* debe estar `unmarked`.

Valores posibles:

- `marked` (configuración por defecto)
  La detección automática está activa.
  Tras la instalación de la conexión y tras 1,5 × *Hello time [s]*, el dispositivo ajusta el puerto en estado *`forwarding`* (configuración por defecto de 1,5 × 2 s) si el puerto no ha recibido ningún BPDU de STP durante este período.
- `unmarked`
  La detección automática está inactiva.
  Tras la instalación de la conexión y tras *Max age*, el dispositivo ajusta el puerto al estado *`forwarding`*.
  (configuración por defecto: 20 s)

Oper edge port

Muestra si un dispositivo terminal o un puente STP está conectado al puerto.

Valores posibles:

- `marked`
  Hay un dispositivo terminal conectado al puerto. El puerto no recibo ningún BPDU de STP.
- `unmarked`
  Hay un puente STP conectado al puerto. El puerto recibe BPDU de STP.

Oper PointToPoint

Muestra si el puerto está conectado a un dispositivo STP a través de una conexión Full-Dúplex directa.

Valores posibles:

- `marked`
  El puerto está conectado directamente a un dispositivo STP a través de una conexión Full-Dúplex. La comunicación directa y descentralizada entre 2 puentes permite disponer de tiempos de reconfiguración breves.
- `unmarked`
  El puerto está conectado de otro modo, por ejemplo, a través de una conexión Half-Dúplex o mediante un concentrador.

Port BPDU filter

Activa/desactiva la filtración de BPDU de STP en el puerto de manera explícita.

Como requisito previo, el puerto debe ser un puerto periférico especificado manualmente. Para estos puertos, la casilla de la columna *Admin edge port* está marcada.

Valores posibles:

- `marked`
  El filtro de BPDU está activo en el puerto.
  La función excluye el puerto de las operaciones *Spanning Tree*.
  – El dispositivo no envía BPDU de STP en el puerto.
  – El dispositivo anula los BPDU de STP recibidos en el puerto.
- `unmarked` (configuración por defecto)
  El filtro de BPDU está inactivo en el puerto.
  Tiene la opción de activar globalmente el filtro de BPDU para todos los puertos periféricos. Consulte el cuadro *Bridge configuration* del cuadro de diálogo *Switching > L2-Redundancy > Spanning Tree > Global*.
  Si la casilla *BPDU filter (all admin edge ports)* está marcada, el filtro de BPDU continúa activo en el puerto.

BPDU filter status

Muestra si el filtro de BPDU está activo en el puerto.

Valores posibles:

- `marked`
  El filtro de BPDU está activo en el puerto como resultado de los siguientes ajustes:
  – La casilla de la columna *Port BPDU filter* está marcada.
  y/o
  – La casilla de la columna *BPDU filter (all admin edge ports)* está marcada. Consulte el cuadro *Bridge configuration* del cuadro de diálogo *Switching > L2-Redundancy > Spanning Tree > Global*.
- `unmarked`
  El filtro de BPDU está inactivo en el puerto.

BPDU flood

Activa/desactiva el modo *BPDU flood* en el puerto aunque la función *Spanning Tree* esté inactiva en el puerto. El dispositivo desborda BPDU de STP recibidos en el puerto a los puertos en los que la función *Spanning Tree* está inactiva y el modo *BPDU flood* está activo también.

Valores posibles:

- `marked`
  El modo *BPDU flood* está activo.
- `unmarked` (configuración por defecto)
  El modo *BPDU flood* está inactivo.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## [Guards]

Esta pestaña le permite especificar la configuración de varias funciones de protección en los puertos.

### Tabla

Port

Muestra el número de puerto.

Root guard

Activa/desactiva la supervisión de BPDU de STP en el puerto. Como requisito previo, la función *Loop guard* está inactiva.

Con este ajuste, el dispositivo le ayuda a proteger su red de configuraciones incorrectas o ataques con BPDU de STP que intentan cambiar la topología. Este ajuste solamente es relevante para los puertos con el rol de STP *designated*.

Valores posibles:

- `marked`
  La supervisión de BPDU de STP está activa.
  - Si el puerto 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 del puerto al valor *discarding* en lugar de *root*.
  - Si no recibe paquetes BPDU de STP con información de una ruta mejor al puente raíz, el dispositivo vuelve a establecer el estado del puerto tras 2 × *Hello time [s]*.
- `unmarked` (configuración por defecto)
  La supervisión de BPDU de STP está inactiva.

TCN guard

Activa/desactiva la supervisión de "Notificaciones de cambio de topología" en el puerto. Con este ajuste, el dispositivo le ayuda a proteger su red de ataques con BPDU de STP que intentan cambiar la topología.

Valores posibles:

- `marked`
  La supervisión de "Notificaciones de cambio de topología" está activada.
  - El puerto ignora la marca de Cambio de topología de los BPDU de STP recibidos.
  - Si el BPDU recibido contiene otros datos que pueden generar un cambio de topología, el dispositivo los procesa aunque esté activado TCN Guard.
    Ejemplo: el dispositivo recibe una información de ruta mejor para el puente raíz.
- `unmarked` (configuración por defecto)
  La supervisión de "Notificaciones de cambio de topología" está desactivada.
  Si el dispositivo recibe BPDU de STP con una marca de cambio de topología, el dispositivo elimina la tabla de direcciones del puerto y reenvía las notificaciones de cambio de topología.

Loop guard

Activa/desactiva la supervisión de bucles en el puerto. Como requisito previo, la función *Root guard* está inactiva.

Con este ajuste, el dispositivo ayuda a evitar que se produzcan bucles si el puerto no recibe ningún BPDU de STP. Utilice este ajuste solamente para puertos con el rol de STP *alternate*, *backup* o *root*.

Valores posibles:

- `marked`
  La supervisión de bucles está activa. Esto ayuda a evitar la aparición de bucles, por ejemplo, si desactiva la función Spanning Tree en el dispositivo remoto o si la conexión está interrumpida solamente en la dirección de recepción.
  - Si el puerto no recibe ningún BPDU de STP durante un tiempo, el dispositivo establece el estado del puerto en el valor `discarding` y marca la casilla de verificación de la columna *Loop state*.
  - Si el puerto recibe BPDU de STP de nuevo, el dispositivo establece el estado del puerto en un valor correspondiente a *Port role* y desmarca la casilla de verificación en la columna *Loop state*.
- `unmarked` (configuración por defecto)
  La supervisión de bucles está inactiva.
  Si el puerto no recibe ningún BPDU de STP durante un tiempo, el dispositivo ajusta el estado del puerto al valor `forwarding`.

Loop state

Muestra si el estado del bucle del puerto no es coherente.

Valores posibles:

- `marked`
  El estado del bucle del puerto no es coherente:
  - El puerto no está recibiendo ningún BPDU de STP y la función *Loop guard* está activada.
  - El dispositivo ajusta el estado del puerto al valor `discarding`. De este modo, el dispositivo ayuda a evitar posibles bucles.
- `unmarked`
  El estado del bucle del puerto es coherente. El puerto recibe BPDU de STP.

Trans. into loop

Muestra el número de veces que el estado del bucle del puerto se volvió incoherente (casilla de verificación marcada en la columna *Loop state*).

Trans. out of loop

Muestra el número de veces que el estado del bucle del puerto se volvió coherente (casilla de verificación desmarcada en la columna *Loop state*).

BPDU guard effect

Muestra si el puerto ha recibido un BPDU de STP como puerto periférico.

Requisito previo:

- El puerto debe ser un puerto periférico especificado manualmente. En el cuadro de diálogo *Port*, la casilla de este puerto en la columna *Admin edge port* está en posición `marked`.
- En el cuadro de diálogo *Switching > L2-Redundancy > Spanning Tree > Global*, la función BPDU Guard está activa.

Valores posibles:

- `marked`
  El puerto es un puerto periférico y ha recibido un BPDU de STP.
  El dispositivo desactiva el puerto. Para este puerto, en la pestaña *Configuration* del cuadro de diálogo *Basic Settings > Port*, la casilla de la columna *Port on* está en posición `unmarked`.
- `unmarked`
  El puerto es periférico y no ha recibido ningún BPDU de STP o no es ningún puerto periférico.

Para restablecer el estado del puerto al valor `forwarding`, haga lo siguiente:

- ☐ Si el puerto continúa recibiendo BPDU:
  - En la pestaña *CIST*, desmarque la casilla de la columna *Admin edge port*.
    o bien
  - En el cuadro de diálogo *Switching > L2-Redundancy > Spanning Tree > Global*, desmarque la casilla *BPDU guard*.
- ☐ Para activar el puerto, haga lo siguiente:
  - Abra el cuadro de diálogo *Basic Settings > Port*, pestaña *Configuration*.
  - Marque la casilla de la columna *Port on*.

#### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## 5.10.4 Link Aggregation

[ Switching > L2-Redundancy > Link Aggregation ]

**⚠ 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.**

La función *Link Aggregation* le permite agregar varias conexiones paralelas. Como requisito previo, los enlaces deben tener la misma velocidad y ser Full-Dúplex. Las ventajas en comparación con los enlaces convencionales utilizando una línea única son una mayor disponibilidad y un mayor ancho de banda de transmisión.

El Protocolo de control de agregación de enlaces (LACP, Link Aggregation Control Protocol) permite supervisar el estado de conexión continuo basado en paquetes en los puertos físicos. El LACP también ayuda a garantizar que los socios de enlace cumplan con los requisitos previos de agregación.

Si el extremo remoto no admite el Protocolo de control de agregación de enlaces (LACP, Link Aggregation Control Protocol), entonces puede utilizar la función *Static link aggregation*. En este caso, el dispositivo agrega los enlaces en función del enlace, la velocidad de este y de la configuración dúplex.

### Tabla

Trunk port

Muestra el número de la interfaz LAG.

Name

Especifica el nombre de la interfaz LAG.

Valores posibles:

- Cadena de caracteres ASCII alfanuméricos con entre 1 y 15 caracteres

Link/Status

Muestra el modo de funcionamiento actual de la interfaz LAG y los puertos físicos.

Valores posibles:

- *up* (fila `lag/…`)
  La interfaz LAG está operativa.
  Los requisitos previos son:
  - La función *Static link aggregation* debe estar activa en esta interfaz LAG.
    o bien
  - LACP debe estar activo en los puertos físicos asignados a la interfaz LAG. Consulte la columna *LACP active*.
    y
    La clave especificada para la interfaz LAG de la columna *LACP admin key* debe coincidir con las claves especificadas para los puertos físicos en la columna *LACP port actor admin key*.
    y
    El número de puertos físicos operativos asignados a la interfaz LAG debe ser superior o igual al valor especificado en la columna *Active ports (min.)*.
- *up*
  El puerto está operativo.
- *down* (fila `lag/…`)
  La interfaz LAG no está operativa.
- *down*
  El puerto físico está desactivado.
  o bien
  No hay ningún cable conectado o ninguna conexión activa.

Active

Activa/desactiva la interfaz LAG.

Valores posibles:

- `marked` (configuración por defecto)
  La interfaz LAG está activa.
  Tenga en cuenta que los protocolos siguientes no funcionan correctamente en los puertos físicos cuando activa la interfaz LAG:
  - *PTP*
  - *802.1AS*
- `unmarked`
  La interfaz LAG está inactiva.

STP active

Activa/desactiva el protocolo *Spanning Tree* en esta interfaz LAG. Como requisito previo, debe activar la función *Spanning Tree* a nivel global en el cuadro de diálogo *Switching* > *L2-Redundancy* > Spanning Tree > *Global*.

También puede activar/desactivar el protocolo *Spanning Tree* en las interfaces LAG en el cuadro de diálogo *Switching* > *L2-Redundancy* > *Spanning Tree* > *Port*.

Valores posibles:

- `marked` (configuración por defecto)
  El protocolo *Spanning Tree* está activo en esta interfaz LAG.
- `unmarked`
  El protocolo *Spanning Tree* está inactivo en esta interfaz LAG.

Static link aggregation

Activa/desactiva la función *Static link aggregation* en la interfaz LAG. El dispositivo agrega los puertos físicos asignados a la interfaz LAG, aunque el sitio remoto no sea compatible con el LACP.

Valores posibles:

- `marked`
  La función *Static link aggregation* debe estar activa en esta interfaz LAG. El dispositivo agregará un puerto físico asignado a la interfaz LAG en cuanto el puerto físico obtenga un enlace. El dispositivo no envía LACPDU y descarta LACPDU recibidos.
- `unmarked` (configuración por defecto)
  La función *Static link aggregation* está inactiva en esta interfaz LAG. Si la conexión se ha negociado correctamente mediante el LACP, el dispositivo agregará un puerto físico asignado a la interfaz LAG.

MTU

Especifica el tamaño máximo permitido de paquetes de Ethernet en la interfaz LAG en bytes. Las etiquetas de VLAN presentes no se tendrán en cuenta.

Esta configuración le permite aumentar el tamaño de los paquetes de Ethernet para aplicaciones específicas.

Valores posibles:

- `1518..9720` (configuración por defecto: `1518`)
  Con el valor `1518`, la interfaz LAG transmite paquetes de Ethernet con el tamaño máximo siguiente:
  - 1518 bytes sin etiqueta VLAN
    (1514 bytes + CRC de 4 bytes)
  - 1522 bytes con etiqueta VLAN
    (1518 bytes + CRC de 4 bytes)

Active ports (min.)

Especifica el número mínimo de puertos físicos que deben estar activos para que la interfaz LAG permanezca activa. Si el número de puertos físicos activos es inferior al valor especificado, el dispositivo desactivará la interfaz LAG.

Si una función de redundancia como *Spanning Tree* o *MRP* a través de LAGestá activa en el dispositivo, podrá utilizar esta función para forzar al dispositivo a cambiar automáticamente a la línea redundante.

Valores posibles:

- `1` (configuración por defecto)
- `2`
- En función del hardware:
  `4`
  `8`
  `32`

Type

Muestra si la interfaz LAG está basada en la función *Static link aggregation* o en LACP.

Valores posibles:

- *`static`*
  La interfaz LAG está basada en la función *Static link aggregation*.
- *`dynamic`*
  La interfaz LAG está basada en el LACP.

Send trap (Link up/down)

Activa/desactiva el envío de capturas de SNMP cuando el dispositivo detecta un cambio en el estado de vínculo activo/inactivo para esta interfaz.

Valores posibles:

- `marked` (configuración por defecto)
  El envío de trampas SNMP está activo.
  Si el dispositivo detecta un cambio de estado de enlace activo/inactivo, el dispositivo envía una trampa SNMP.
- `unmarked`
  El envío de trampas SNMP está inactivo.

Como requisito previo para enviar trampas SNMP, debe activar la función en el cuadro de diálogo *Diagnostics > Status Configuration > Alarms (Traps)* y especificar al menos un destino de la trampa.

LACP admin key

Especifica la clave de la interfaz LAG. El dispositivo utiliza esta clave para identificar los puertos que se pueden agregar a la interfaz LAG.

Valores posibles:

- `0..65535`
  Especifique el valor correspondiente para los puertos físicos en la columna *LACP port actor admin key*.

Port

Muestra los puertos físicos asignados a la interfaz LAG.

Aggregation port status

Muestra si la interfaz LAG agrega el puerto físico.

Valores posibles:

- *active*
  La interfaz LAG agrega el puerto físico.
- *inactive*
  La interfaz LAG no agrega el puerto físico.

LACP active

Activa/desactiva el LACP en el puerto físico.

Valores posibles:

- `marked` (configuración por defecto)
  El LACP está activo en el puerto físico.
- `unmarked`
  El LACP está inactivo en el puerto físico.

LACP port actor admin key

Especifica la clave del puerto físico. El dispositivo utiliza esta clave para identificar los puertos que se pueden agregar a la interfaz LAG.

Valores posibles:

- `0`
  El dispositivo ignora la clave en este puerto físico al decidir agregar el puerto a la interfaz LAG.
- `1..65535`
  Si este valor coincide con el de la interfaz LAG especificado en la columna *LACP admin key*, el dispositivo solamente agrega este puerto físico a la interfaz LAG.

LACP actor admin state

Especifica los valores de estado del actor que transmite la interfaz LAG en los LACPDU. Esto le permite controlar los parámetros del LACPDU.

El dispositivo le permite mezclar los valores. En la lista desplegable, seleccione uno o más valores.

Valores posibles:

- *ACT*
  (Estado `LACP_Activity`)
  Cuando se selecciona, el enlace transmite los LACPDU cíclicamente, de lo contrario, cuando se solicita.
- *STO*
  (Estado `LACP_Timeout`)
  Cuando se selecciona, el enlace transmite los LACPDU cíclicamente utilizando el tiempo de espera breve, de lo contrario, usando el tiempo de espera largo.
- *AGG*
  (Estado `Aggregation`)
  Cuando se selecciona, el dispositivo interpreta el enlace como un candidato para la agregación, de lo contrario, como un enlace individual.

Si desea obtener más información sobre los valores, consulte el estándar IEEE 802.1AX-2014.

LACP actor oper state

Muestra los valores del estado del actor que transmite la interfaz LAG en los LACPDU.

Valores posibles:

- *ACT*
  (Estado `LACP_Activity`)
  Cuando está visible, el enlace transmite los LACPDU cíclicamente, de lo contrario, cuando se solicita.
- *STO*
  (Estado `LACP_Timeout`)
  Cuando está visible, el enlace transmite los LACPDU cíclicamente utilizando el tiempo de espera breve, de lo contrario, usando el tiempo de espera largo.
- *AGG*
  (Estado `Aggregation`)
  Cuando está visible, el dispositivo interpreta el enlace como un candidato para la agregación, de lo contrario, como un enlace individual.
- *SYN*
  (Estado `Synchronization`)
  Cuando está visible, el dispositivo interpreta el enlace como `IN_SYNC`, de lo contrario, como `OUT_OF_SYNC`.
- *COL*
  (Estado `Collecting`)
  Cuando está visible, se activa la recopilación de tramas entrantes en este enlace, de lo contrario, se desactiva.
- *DST*
  (Estado `Distributing`)
  Cuando está visible, se activa la distribución de tramas salientes en este enlace, de lo contrario, se desactiva.
- *DFT*
  (Estado `Defaulted`)
  Cuando está visible, el enlace utiliza información operativa con valor predeterminado, especificada administrativamente para el Socio. De lo contrario, el enlace utiliza la información operativa recibida de un LACPDU.
- *EXP*
  (Estado `Expired`)
  Cuando está visible, el receptor del enlace se encuentra en estado `EXPIRED`.

LACP partner oper SysID

Muestra la dirección MAC del dispositivo remoto conectado a este puerto físico.

La interfaz LAG ha recibido esta información en un LACPDU del socio.

LACP partner oper port

Muestra el número de puerto del dispositivo remoto conectado a este puerto físico.

La interfaz LAG ha recibido esta información en un LACPDU del socio.

LACP partner oper port state

Muestra los valores del estado del socio que recibe la interfaz LAG en los LACPDU.

Valores posibles:

- *ACT*
- *STO*
- *AGG*
- *SYN*
- *COL*
- *DST*
- *DFT*
- *EXP*

Si desea obtener más información sobre los valores, consulte la descripción de la columna *LACP actor oper state* y el estándar IEEE 802.1AX-2014.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

Abre la ventana *Create* para añadir una entrada de interfaz LAG nueva a la tabla o para asignar un puerto físico a una interfaz LAG.

- Seleccione el número de interfaz LAG en la lista desplegable *Trunk port*.
- Seleccione el número de un puerto físico al que asignar la interfaz LAG en la lista desplegable *Port*.

Tras crear una interfaz LAG, el dispositivo añade la interfaz LAG a la tabla en la pestaña *Statistics* del cuadro de diálogo *Basic Settings > Port*.

## 5.10.5 Link Backup

[ Switching > L2-Redundancy > Link Backup ]

**⚠ 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.**

Mediante Link Backup, puede configurar pares de enlaces redundantes. Cada par dispone de un puerto principal y uno de reserva. El principal desvía tráfico hasta que el dispositivo detecta un error. Si el dispositivo detecta un error en el puerto principal, la función Link Backup transfiere tráfico al puerto de reserva.

El cuadro de diálogo también le permite configurar una opción de conmutación por recuperación. Si activa la función de conmutación por recuperación y el puerto 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.

### Operation

Operation

Activa/desactiva la función Link Backup globalmente en el dispositivo.

Valores posibles:

- *On*
  Activa la función Link Backup.
- *Off* (configuración por defecto)
  Desactiva la función Link Backup.

### Tabla

Primary port

Muestra el puerto principal del par de interfaz. Si activa la función Link Backup, este puerto será responsable de desviar el tráfico.

Valores posibles:

- Puertos físicos

Backup port

Muestra el puerto de reserva en el que el dispositivo desvía el tráfico si detecta un error en el puerto principal.

Valores posibles:

- Puertos físicos, excepto el puerto configurado como principal.

Description

Especifica el par de la función Link Backup. Introduzca un nombre para identificar el par de la función Backup.

Valores posibles:

- Cadena de caracteres ASCII alfanuméricos con entre 0 y 255 caracteres

Primary port status

Muestra el estado del puerto principal para este par de la función Link Backup.

Valores posibles:

- *forwarding*
  El enlace está activo, no apagado, y desviando tráfico.
- *blocking*
  El enlace está activo, no apagado, y bloqueando tráfico.
- *down*
  El puerto está con el enlace inactivo, el cable desconectado o el software desactivado, apagado.
- *unknown*
  La función Link Backup está desactivada globalmente o el par de puertos está inactivo. Por lo tanto, el dispositivo ignora la configuración del par de puertos.

Backup port status

Muestra el estado del puerto de reserva para este par de la función Link Backup.

Valores posibles:

- *forwarding*
  El enlace está activo, no apagado, y desviando tráfico.
- *blocking*
  El enlace está activo, no apagado, y bloqueando tráfico.

- *down*
  El puerto está con el enlace inactivo, el cable desconectado o el software desactivado, apagado.
- *unknown*
  La función Link Backup está desactivada globalmente o el par de puertos está inactivo. Por lo tanto, el dispositivo ignora la configuración del par de puertos.

Fail back

Activa/desactiva la conmutación por recuperación automática.

Valores posibles:

- `marked` (configuración por defecto)
  La conmutación por recuperación automática está activa.
  Una vez finalizado el temporizador de retardo, el puerto de reserva cambia a *blocking* y el principal, a *forwarding*.
- `unmarked`
  La conmutación por recuperación automática está inactiva.
  El puerto de reserva continuará desviando tráfico incluso después de que el puerto principal restablezca un enlace o de que usted cambie manualmente el estado de administración del puerto principal de `shutdown` a `no shutdown`.

Fail back delay [s]

Especifica en segundos el tiempo que desea que espere el dispositivo una vez que el puerto principal restablezca un enlace. Además, este temporizador también se aplica cuando pasa manualmente el estado de administración del puerto principal de `shutdown` a `no shutdown`. Una vez finalizado el temporizador de retardo, el puerto de reserva cambia a *blocking* y el principal, a *forwarding*.

Valores posibles:

- `0..3600` (configuración por defecto: `30`)
  Si se ajusta a `0`, inmediatamente después de que el puerto principal restablezca un enlace, el puerto de reserva cambiará a *blocking* y el principal, a *forwarding*. Además, inmediatamente después de ajustar el estado de administración manualmente de `shutdown` a `no shutdown`, el puerto de reserva cambiará a *blocking* y el principal, a *forwarding*.

Active

Activa/desactiva la configuración del par de la función Link Backup.

Valores posibles:

- `marked`
  El par de la función Link Backup está activo. El dispositivo detecta el enlace y el estado de la administración y desvía el tráfico conforme a la configuración del par.
- `unmarked` (configuración por defecto)
  El par de la función Link Backup está inactivo. Los puertos desvían el tráfico conforme a la conmutación estándar.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

**Create**

Primary port

Especifica el puerto principal del par de la interfaz de reserva. Durante el funcionamiento normal, este puerto será responsable de desviar el tráfico.

Valores posibles:

- Puertos físicos

Backup port

Permite especificar el puerto de reserva al que desea que el dispositivo transfiera el tráfico si detecta un error en el puerto principal.

Valores posibles:

- Puertos físicos, excepto el puerto configurado como principal.

## 5.10.6 FuseNet

[ Switching > L2-Redundancy > FuseNet ]

Los protocolos *FuseNet* permiten acoplar anillos que están funcionando con uno de los siguientes protocolos de redundancia:

- MRP
- Anillo HIPER
- RSTP

**Nota:** Si utiliza el protocolo *Ring/Network Coupling* para acoplar redes, compruebe que estas solamente contengan dispositivos Schneider Electric.

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*<br>*Ring/Network Coupling* | *Redundant Coupling Protocol*<br>*Ring/Network Coupling* |
| **Anillo HIPER** | *Sub Ring* | *Ring/Network Coupling* | *Redundant Coupling Protocol*<br>*Ring/Network Coupling* |
| **RSTP** | *Redundant Coupling Protocol* | *Redundant Coupling Protocol* | *Dual RSTP* |

– ningún protocolo de acoplamiento adecuado

1) con *MRP* configurado en VLAN diferentes

El menú contiene los siguientes cuadros de diálogo:

- Sub Ring
- Ring/Network Coupling
- Redundant Coupling Protocol (MCSESM-E)

# 5.10.6.1 Sub Ring

[ Switching > L2-Redundancy > FuseNet > Sub Ring ]

**⚠ 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.**

Este cuadro de diálogo le permite configurar el dispositivo como Subring Manager.

La función *Sub Ring* le permite acoplar fácilmente segmentos de red a anillos de redundancia existentes. Subring Manager (SRM) acopla un anillo secundario a uno existente (anillo base).

En el anillo secundario puede utilizar todos los dispositivos que admiten el MRP como participantes en el anillo. Estos dispositivos no requieren una función de Subring Manager.

Durante la configuración de anillos secundarios, no olvide las siguientes normas:
- El dispositivo admite *Link Aggregation* en el anillo secundario
- No debe existir ningún árbol de expansión en los puertos de los anillos secundarios
- Debe existir el mismo *MRP domain* en los dispositivos situados dentro de un anillo secundario
- Debe haber VLAN diferentes para el anillo base y el secundario

Especifique la configuración de la VLAN del modo siguiente:
- VLAN `X` para anillo base
  - en los puertos de anillo de los participantes del anillo base
  - en los puertos de anillo base del Subring Manager
- VLAN `Y` para anillo secundario
  - en los puertos de anillo de los participantes del anillo secundario
  - en los puertos del anillo secundario del Subring Manager

**Nota:** Para ayudar a evitar bucles, cierre solamente la línea redundante cuando se especifique la configuración en cada dispositivo que participe en el anillo.

### Operation

Operation

Activa/desactiva la función *Sub Ring*.

Valores posibles:

- `On`
  La función *Sub Ring* está activada.
- `Off` (configuración por defecto)
  La función *Sub Ring* está desactivada.

### Information

Table entries (max.)

Muestra el número máximo de anillos secundarios compatibles con el dispositivo.

### Tabla

Sub ring ID

Muestra el identificador único de este anillo secundario.

Valores posibles:

- `1..8`

Name

Especifica el nombre óptimo del anillo secundario.

Valores posibles:

- Cadena de caracteres ASCII alfanuméricos con entre 0 y 255 caracteres

Active

Activa/desactiva el anillo secundario.

Active el anillo secundario cuando se haya completado la configuración de cada dispositivo de anillo secundario. Cierre el anillo secundario únicamente tras activar la función *Sub Ring*.

Valores posibles:

- `marked`
  El anillo secundario está activo.
- `unmarked` (configuración por defecto)
  El anillo secundario está inactivo.

Configuration status

Muestra el estado operativo de la configuración del anillo secundario.

Valores posibles:

- *noError*
  El dispositivo detecta una configuración de anillo secundario aceptable.
- *ringPortLinkError*
  - El puerto del anillo no tiene enlaces.
  - Una de las líneas del anillo secundario está conectada a un puerto más del dispositivo. Pero la línea del anillo secundario no está conectada a uno de los puertos de anillo del dispositivo.
- *multipleSRM*
  El Subring Manager recibe paquetes de más de un Subring Manager en el anillo secundario.
- *noPartnerManager*
  El Subring Manager recibe sus propias tramas.
- *concurrentVLAN*
  El protocolo MRP del anillo base utiliza la VLAN del dominio del Subring Manager.

- *concurrentPort*
  Un protocolo de redundancia más utiliza el puerto de anillo del dominio del Subring Manager.
- *concurrentRedundancy*
  El dominio del Subring Manager está inactivo debido a que hay un protocolo de redundancia activo más.
- *trunkMember*
  El puerto de anillo del dominio del Subring Manager es miembro de una conexión de *Link Aggregation*.
- *sharedVLAN*
  El dominio del Subring Manager está inactivo debido a que la VLAN compartida está activa y el anillo principal utiliza también el protocolo MRP.

Redundancy available

Muestra el estado operativo de la redundancia de anillo en el anillo secundario.

Valores posibles:

- *redGuaranteed*
  La reserva de la redundancia está disponible.
- *redNotGuaranteed*
  Pérdida de reserva de la redundancia.

Port

Especifica el puerto que enlaza el dispositivo con el anillo secundario.

Valores posibles:

- <Port number>

SRM mode

Especifica el modo del Subring Manager.

Un anillo secundario dispone de 2 administradores simultáneamente que acoplan el anillo secundario en el anillo base. Mientras que el anillo secundario esté cerrado físicamente, un gestor bloqueará el puerto de su anillo secundario.

Valores posibles:

- *manager* (configuración por defecto)
  El puerto del anillo secundario desvía paquetes de datos.
  Cuando este valor esté configurado en ambos dispositivos que acoplan el anillo secundario en el anillo base, el dispositivo con las funciones de dirección MAC mayores funcionará como *redundantManager*.
- *redundantManager*
  El puerto del anillo secundario estará bloqueado mientras el anillo secundario esté cerrado físicamente. Si se interrumpe el anillo secundario, el puerto de este transmitirá los paquetes de datos.
  Cuando este valor esté configurado en ambos dispositivos que acoplan el anillo secundario en el anillo base, el dispositivo con las funciones de dirección MAC mayores funcionará como *redundantManager*.
- *singleManager*
  Utilice este valor cuando el anillo secundario esté acoplado al anillo base mediante un solo dispositivo. Como requisito previo, deben existir 2 instancias del anillo secundario en la tabla. Asigne este valor a ambas instancias. El puerto del anillo secundario de la instancia con el número de puerto mayor estará bloqueado mientras el anillo secundario esté cerrado físicamente.

SRM status

Muestra el modo actual del Subring Manager.

Valores posibles:

- *manager*
  El puerto del anillo secundario desvía paquetes de datos.
- *redundantManager*
  El puerto del anillo secundario estará bloqueado mientras el anillo secundario esté cerrado físicamente. Si se interrumpe el anillo secundario, el puerto de este transmitirá los paquetes de datos.
- *singleManager*
  El anillo secundario está acoplado al anillo base mediante un solo dispositivo. El puerto del anillo secundario de la instancia con el número de puerto mayor estará bloqueado mientras el anillo secundario esté cerrado físicamente.
- *disabled*
  El anillo secundario está inactivo.

Port status

Muestra el estado de conexión del puerto del anillo secundario.

Valores posibles:

- *forwarding*
  El puerto está pasando tramas conforme al comportamiento de desvío del estándar IEEE 802.1D.
- *disabled*
  El puerto está anulando todas las tramas.
- *blocked*
  El puerto está anulando todas las tramas, excepto en los casos siguientes:
  - El puerto pasa tramas utilizadas por el protocolo de anillo seleccionado especificado para pasar puertos bloqueados.
  - El puerto pasa tramas utilizadas de otros protocolos especificados para pasar puertos bloqueados.
- *not-connected*
  El enlace del puerto está inactivo.

VLAN

Especifica la VLAN a la que está asignada este anillo secundario. Si aún no hay ninguna VLAN con el ID de VLAN indicado, el dispositivo crea una automáticamente.

Valores posibles:

- VLAN configuradas disponibles (configuración por defecto: 0)
  Si no desea usar una VLAN independiente para este anillo secundario, deje la entrada en 0.

Partner MAC

Muestra la dirección MAC del Subring Manager en el otro extremo del anillo secundario.

MRP domain

Especifica el dominio MRP del Subring Manager. Asigne el mismo nombre de dominio de MRP a cada miembro de un anillo secundario. Si solo utiliza dispositivos Schneider Electric, utilice el valor predeterminado para el dominio de MRP; de lo contrario, ajuste este valor si es necesario. Si hay varios anillos secundarios, la función le permite utilizar el mismo nombre de dominio de MRP para los anillos secundarios.

Valores posibles:

- Nombres de dominio de MRP permitidos (configuración por defecto: `255.255.255.255.255.255.255.255.255.255.255.255.255.255.255.255`)

Protocol

Especifica el protocolo.

Valores posibles:

- *`iec-62439-mrp`*

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

# 5.10.6.2 Ring/Network Coupling

[ Switching > L2-Redundancy > FuseNet > 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.

**El incumplimiento de estas instrucciones puede causar la muerte, heridas graves o daños en el equipo.**

Utilice la función *Ring/Network Coupling* para acoplar de manera redundante un anillo HIPER, un anillo MRP o un anillo Fast HIPER existente en otra red u otro anillo. Compruebe que los socios de acoplamiento sean dispositivos Schneider Electric.

**Nota:** Con el acoplamiento de dos switches, compruebe que haya configurado un anillo HIPER, un anillo MRP o un anillo Fast HIPER antes de configurar la función *Ring/Network Coupling*.

En el cuadro de diálogo *Ring/Network Coupling*, puede llevar a cabo las siguientes tareas:
- mostrar una vista previa de los *Ring/Network Coupling* existentes
- configurar un *Ring/Network Coupling*
- crear un *Ring/Network Coupling* nuevo
- eliminar *Ring/Network Coupling*
- activar/desactivar *Ring/Network Coupling*

Cuando esté configurando puertos de acoplamiento, especifique los ajustes siguientes en el cuadro de diálogo *Basic Settings > Port*:

| Tipo de puerto | Velocidad de bits | Port on | Automatic configuration | Manual configuration |
|---|---|---|---|---|
| TX | 100 Mbit/s | `marked` | `unmarked` | *`100 Mbit/s FDX`* |
| TX | 1 Gbit/s | `marked` | `marked` | – |
| Optical | 100 Mbit/s | `marked` | `unmarked` | *`100 Mbit/s FDX`* |
| Optical | 1 Gbit/s | `marked` | `marked` | – |
| Óptico | 2.5 Gbit/s | `marked` | – | *`2.5 Gbit/s FDX`* |

**Nota:** Los modos de funcionamiento del puerto que están realmente disponibles dependen de la configuración del dispositivo.

Si ha configurado redes VLAN, tenga en cuenta la configuración de VLAN del acoplamiento y de los puertos de acoplamiento asociados. En la configuración *Ring/Network Coupling*, seleccione los valores siguientes para el acoplamiento y los puertos de acoplamiento asociados.
- `VLAN ID 1` y *Ingress filtering* están desactivados en la tabla de puertos
- Pertenencia a VLAN `T` en la tabla *VLAN Configuration*

Independientemente de la configuración de la VLAN, el dispositivo envía las tramas de acoplamiento de anillo redundante con `VLAN ID 1` y la prioridad `7`. Compruebe que el dispositivo envía tramas de VLAN 1 etiquetadas en el anillo local y en la red conectada. El etiquetado de las tramas de VLAN mantiene la prioridad de las tramas de acoplamiento de anillo redundante.

La función *Ring/Network Coupling* opera con paquetes de prueba. Los dispositivos envían sus paquetes de prueba con una etiqueta VLAN, incluido el ID `1` de la VLAN y la prioridad máxima de VLAN `7`. Si el puerto de reenvío es miembro en la VLAN `1` y transmite los paquetes de datos sin una etiqueta de VLAN, el dispositivo también envía paquetes de prueba.

### Operation

Operation

Activa/desactiva la función *Ring/Network Coupling*.

Valores posibles:

- *On*
  La función *Ring/Network Coupling* está activada.
- *Off* (configuración por defecto)
  La función *Ring/Network Coupling* está desactivada.

### Mode

Type

Especifica el método utilizado para acoplar las redes entre sí.

Valores posibles:

- *one-switch coupling*
  Le permite especificar la configuración del puerto en los cuadros *Coupling port* y *Partner coupling port*.
- *two-switch coupling, master*
  Le permite especificar la configuración del puerto en el cuadro *Coupling port*.
- *two-switch coupling, slave*
  Le permite especificar la configuración del puerto en el cuadro *Coupling port*.
- *two-switch coupling with control line, master*
  Le permite especificar la configuración del puerto en los cuadros *Coupling port* y *Control port*.
- *two-switch coupling with control line, slave*
  Le permite especificar la configuración del puerto en los cuadros *Coupling port* y *Control port*.

### Coupling port

Port

Especifica el puerto al que desea conectar el enlace redundante.

Valores posibles:

- `-`
  Ningún puerto seleccionado.
- `<Port number>`

Si también ha configurado puertos de anillo, especifique los puertos de acoplamiento y de anillo en puertos diferentes.

Para ayudar a evitar bucles continuos, el dispositivo desactiva el puerto de acoplamiento en los casos siguientes:

- desactivación de la función
- cambio de la configuración mientras las conexiones están funcionando en los puertos

Si el dispositivo ha desactivado el puerto de acoplamiento, la casilla *Port on* estará sin marcar en la pestaña *Configuration* del cuadro de diálogo *Basic Settings > Port*.

State

Muestra el estado del puerto seleccionado.

Valores posibles:

- *`active`*
  El puerto está activo.
- *`standby`*
  El puerto está en modo stand-by.
- *`not-connected`*
  El puerto no está conectado.
- *`not-applicable`*
  El puerto no es compatible con el modo de control configurado.

### Partner coupling port

Port

Especifica el puerto al que conecta el puerto asociado.

Valores posibles:

- `-`
  Ningún puerto seleccionado.
- `<Port number>`

Si también ha configurado puertos de anillo, especifique los puertos de acoplamiento y de anillo en puertos diferentes.

State

Muestra el estado del puerto seleccionado.

Valores posibles:

- *active*
  El puerto está activo.
- *standby*
  El puerto está en modo stand-by.
- *not-connected*
  El puerto no está conectado.
- *not-applicable*
  El puerto no es compatible con el modo de control configurado.

IP address

Muestra la dirección IP del socio cuando los dispositivos están conectados.

Como requisito previo, debe seleccionar un método de acoplamiento de dos switches y activar el socio en la red.

### Control port

Port

Muestra el puerto al que conecta la línea de control.

Valores posibles:

- -
  Ningún puerto seleccionado.
- <Port number>

State

Muestra el estado del puerto seleccionado.

Valores posibles:

- *active*
  El puerto está activo.
- *standby*
  El puerto está en modo stand-by.
- *not-connected*
  El puerto no está conectado.
- *not-applicable*
  El puerto no es compatible con el modo de control configurado.

### Configuration

Redundancy mode

Especifica si el dispositivo responde a un fallo detectado en el anillo remoto o en la red.

Valores posibles:

- *redundant ring/network coupling*
  La línea principal o la redundante está activa. Ambas líneas no están activas simultáneamente. Si el dispositivo detecta que el enlace está inactivo entre los dispositivos de la red conectada, el dispositivo en stand-by mantiene el puerto redundante en modo stand-by.
- *extended redundancy*
  La línea principal y la redundante están activas simultáneamente. Si el dispositivo detecta un problema en la conexión entre los dispositivos de la red conectada, el dispositivo en stand-by desvía los datos del puerto redundante. Con el ajuste puede mantener la continuidad en la red remota.

**Nota:** Durante el intervalo de reconfiguración, es posible que se produzcan duplicaciones en los paquetes. Por esa razón, si su aplicación es capaz de detectar duplicaciones de los paquetes, puede seleccionar esta configuración.

Coupling mode

Especifica el modo de acoplamiento de un tipo específico de red.

Valores posibles:

- *ring coupling*
  El dispositivo acopla anillos de redundancia. El dispositivo le permite acoplar anillos que utilizan los siguientes protocolos de redundancia:
  - Anillo HIPER
  - Anillo Fast HIPER
  - Anillo MRP
- *network coupling*
  El dispositivo acopla segmentos de red. La función le permite acoplar redes en malla y en bus entre sí.

### Information

Redundancy available

Muestra si la redundancia está disponible.

Cuando un componente del anillo está inactivo, la línea redundante asume su función.

Valores posibles:

- *redGuaranteed*
  La redundancia está disponible.
- *redNotGuaranteed*
  La redundancia no está disponible.

Configuration failure

Ha configurado la función de forma incorrecta o no hay conexión al puerto de anillo.

Valores posibles:

- *noError*
- *slaveCouplingLinkError*
  La línea de acoplamiento no está conectada al puerto de acoplamiento del dispositivo secundario. En su lugar, la línea de acoplamiento está conectada a otro puerto del dispositivo secundario.
- *slaveControlLinkError*
  El puerto de control del dispositivo secundario no tiene conexión de datos.
- *masterControlLinkError*
  La línea de control no está conectada al puerto de control del dispositivo principal. En su lugar, la línea de control está conectada a otro puerto del dispositivo principal.
- *twoSlaves*
  La línea de control conecta dos dispositivos secundarios.
- *localPartnerLinkError*
  La línea de acoplamiento asociada no está conectada al puerto de acoplamiento asociado del dispositivo secundario. En su lugar, la línea de acoplamiento asociada está conectada a otro puerto del dispositivo secundario en modo *one-switch coupling*.
- *localInvalidCouplingPort*
  En el modo *one-switch coupling*, la línea de acoplamiento no está conectada en el mismo dispositivo que la línea asociada. En su lugar, la línea de acoplamiento está conectada a otro dispositivo.
- *couplingPortNotAvailable*
  El puerto de acoplamiento no está disponible debido a que el módulo al que hace referencia el puerto no está disponible o el puerto no existe en este módulo.
- *controlPortNotAvailable*
  El puerto de control no está disponible debido a que el módulo al que hace referencia el puerto no está disponible o el puerto no existe en este módulo.
- *partnerPortNotAvailable*
  El puerto de acoplamiento asociado no está disponible debido a que el módulo al que hace referencia el puerto no está disponible o el puerto no existe en este módulo.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

Reset

Desactiva el mecanismo de redundancia y restablece los parámetros por defecto en el cuadro de diálogo.

# 5.10.6.3 Redundant Coupling Protocol (MCSESM-E)



**⚠ 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.**

**⚠ 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.**

Las topologías en anillo ofrecen tiempos de transición breves con un uso mínimo de los recursos. No obstante, acoplar estos anillos de manera redundante en una red de nivel superior resulta un mayor desafío.

Si desea utilizar un protocolo estándar como MRP para la redundancia de anillo y RSTP para acoplar los anillos entre sí, *Redundant Coupling Protocol* ayuda a ofrecerle opciones.

No utilice los siguientes protocolos de redundancia en los puertos del anillo principal *RCP* y secundario *RCP*.

- *Sub Ring*
- *Ring/Network Coupling*

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*. Especifique los ajustes de la función *Dual RSTP* en el cuadro de diálogo *Switching > L2-Redundancy*.

Si configura la función *RCP* en una red y no se completa la configuración, es posible que los dispositivos desconecten temporalmente el anillo secundario y el principal. En tal caso, la gestión del dispositivo de los puentes *RCP* no se puede alcanzar desde el anillo secundario. Durante esta fase de configuración, conecte la estación de administración de red al anillo principal.

### Operation

Operation

Activa/desactiva la función *RCP*.

Valores posibles:

- *On*
  La función *RCP* está activada.
- *Off* (configuración por defecto)
  La función *RCP* está desactivada.

### Primary ring/network / Secondary ring/network

Si el dispositivo actúa como secundario (el valor en el campo *Role* es *slave*), no active el modo *Static query port* para los puertos del anillo/red secundario.

Inner port

Especifica el número del puerto interior en el anillo principal/secundario. El puerto está conectado directamente al puente asociado.

Valores posibles:

- - (configuración por defecto)
  Ningún puerto seleccionado.
- <Port number>

Outer port

Especifica el número del puerto exterior en el anillo principal/secundario.

Valores posibles:

- - (configuración por defecto)
  Ningún puerto seleccionado.
- <Port number>

Primary Ring protocol/Secondary Ring protocol

Muestra el protocolo que está activo en el puerto de acoplamiento redundante en los dispositivos en el anillo principal/secundario.

### Coupler configuration

Role

Especifica el rol del dispositivo local.

Valores posibles:

- `master`
  El dispositivo actúa como maestro.
- `slave`
  El dispositivo actúa como esclavo.
- `single`
  El dispositivo acopla 2 redes RSTP con una instancia *Dual RSTP* mediante un puente.
- `auto` (configuración por defecto)
  El dispositivo selecciona por sí solo su rol como *master* o *slave*.

Current role

Muestra el rol actual del dispositivo local. El valor puede ser diferente del rol configurado:

- Si ha configurado ambos puentes asociados como `auto`, el puente asociado que está acoplando las instancias en ese momento adopta el rol `master`. El otro puente asociado adopta el rol `slave`.
- Si ambos puentes asociados están configurados como `master` o `slave`, el puente asociado con la dirección MAC básica menor adoptará el rol `master`.
  El otro puente asociado adopta el rol `slave`.
- Si el protocolo está iniciado y no se puede encontrar el puente asociado para un puente en el rol configurado `master`, `slave` o `auto`, el puente establece su propio rol en `listening`.
- Si el dispositivo detecta un problema de configuración, por ejemplo, si los puertos de anillo interior están conectados transversalmente, entonces el dispositivo establece su propio rol en `error`.

Timeout [ms]

Especifica en milisegundos el tiempo máximo durante el cual el dispositivo esclavo espera paquetes de prueba del dispositivo principal en los puertos exteriores antes de que el dispositivo secundario asuma el acoplamiento. Esto solo se aplica en el estado en el que ambos puertos internos del dispositivo secundario han perdido la conexión con el dispositivo principal.

Defina un tiempo límite mayor que el tiempo máximo de interrupción del protocolo de redundancia previsto para la instancia más rápida. De otro modo pueden producirse bucles (loops).

Valores posibles:

- `5..60000` (configuración por defecto: `45`)

Partner MAC address

Muestra la dirección MAC básica del dispositivo asociado.

Partner IP address

Muestra la dirección IP del dispositivo asociado.

Coupling state

Muestra el estado de acoplamiento del dispositivo local.

Valores posibles:

- *forwarding*
  El estado de acoplamiento del puerto es de desvío.
- *blocking*
  El estado de acoplamiento del puerto es de bloqueo.

Redundancy state

Muestra si la redundancia está disponible.

En configuraciones de maestro-esclavo, ambos puentes muestran esta información.

Valores posibles:

- *redAvailable*
  La redundancia está disponible.
- *redNotAvailable*
  La redundancia no está disponible.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

# 6 Diagnostics

El menú contiene los siguientes cuadros de diálogo:

- Status Configuration
- System
- Email Notification
- Syslog
- Ports
- Loop Protection
- LLDP
- Report

## 6.1 Status Configuration

[ Diagnostics > Status Configuration ]

El menú contiene los siguientes cuadros de diálogo:

- Device Status
- Security Status
- Signal Contact
- MAC Notification
- Alarms (Traps)

## 6.1.1 Device Status

[Diagnostics > Status Configuration > Device Status]

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 muestra los errores detectados en la pestaña *Status* y en el cuadro de diálogo *Basic Settings > System*, cuadro *Device Status*.

El cuadro de diálogo contiene las siguientes pestañas:
- [Global]
- [Port]
- [Status]

### [Global]

#### Device status

Device status

Muestra el estado actual del dispositivo. El dispositivo determina el estado a partir de los resultados de los parámetros supervisados individuales.

Valores posibles:

- *error*
  El dispositivo muestra este valor para indicar un error detectado en uno de los parámetros supervisados.
- *ok*

### Traps

Send trap

Activa/desactiva el envío de trampas SNMP cuando el dispositivo detecta un cambio en una función supervisada.

Valores posibles:

- `marked` (configuración por defecto)
  El envío de trampas SNMP está activo.
  Si el dispositivo detecta un cambio en las funciones supervisadas, el dispositivo envía una trampa SNMP.
- `unmarked`
  El envío de trampas SNMP está inactivo.

Como requisito previo para enviar trampas SNMP, debe activar la función en el cuadro de diálogo *Diagnostics > Status Configuration > Alarms (Traps)* y especificar al menos un destino de la trampa.

### Tabla

Temperature

Activa/desactiva la supervisión de la temperatura del dispositivo.

Valores posibles:

- `marked` (configuración por defecto)
  La supervisión está activa.
  En caso de que la temperatura sobrepase o no alcance el límite especificado, el valor cambia a `error` en el cuadro *Device status*.
- `unmarked`
  La supervisión está inactiva.

Especifique los límites de temperatura en el cuadro de diálogo *Basic Settings > System*, campos *Upper temp. limit [°C]* y *Lower temp. limit [°C]*.

Ring redundancy

Activa/desactiva la supervisión de la redundancia de anillo.

Valores posibles:

- `marked`
  La supervisión está activa.
  En el cuadro *Device status*, el valor 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.
- `unmarked` (configuración por defecto)
  La supervisión está inactiva.

Connection errors

Activa/desactiva la supervisión del estado del enlace del puerto/interfaz.

Valores posibles:

- `marked`
  La supervisión está activa.
  Si el enlace se interrumpe en un puerto/interfaz supervisado, el valor cambia a `error` en el cuadro *Device status*.
  En la pestaña *Port*, tiene la opción de seleccionar los puertos/interfaces que se supervisarán individualmente.
- `unmarked` (configuración por defecto)
  La supervisión está inactiva.

External memory removal

Activa/desactiva la supervisión de la memoria externa activa.

Valores posibles:

- `marked`
  La supervisión está activa.
  Si extrae la memoria externa activa del dispositivo, el valor cambia a `error` en el cuadro *Device status*.
- `unmarked` (configuración por defecto)
  La supervisión está inactiva.

External memory not in sync

Activa/desactiva la supervisión del perfil de configuración en el dispositivo y en la memoria externa.

Valores posibles:

- `marked`
  La supervisión está activa.
  En el cuadro *Device status*, el valor 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.
- `unmarked` (configuración por defecto)
  La supervisión está inactiva.

Power supply

Activa/desactiva la supervisión de la fuente de alimentación.

Valores posibles:

- `marked` (configuración por defecto)
  La supervisión está activa.
  Si el dispositivo detecta un fallo de alimentación eléctrica, el valor cambia a `error` en el cuadro *Device status*.
- `unmarked`
  La supervisión está inactiva.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## [Port]

### Tabla

Port

Muestra el número de puerto.

Propagate connection error

Activa/desactiva la supervisión del enlace en el puerto/interfaz.

Valores posibles:

- `marked`
  La supervisión está activa.
  Si el enlace interrumpe el puerto/interfaz seleccionado, el valor cambia a `error` en el cuadro *Device status*.
- `unmarked` (configuración por defecto)
  La supervisión está inactiva.

Estos ajustes tendrán efecto cuando marque la casilla *Connection errors* de la pestaña *Global*.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## [Status]

### Tabla

Timestamp

Muestra la fecha y hora del evento en el formato `Month Day, Year hh:mm:ss AM/PM`.

Cause

Muestra el evento que causó la trampa SNMP.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## 6.1.2 Security Status

[ Diagnostics > Status Configuration > Security Status ]

El cuadro de diálogo le ofrece un resumen del estado de los ajustes de seguridad del dispositivo.

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 muestra los errores detectados en la pestaña *Status* y en el cuadro de diálogo *Basic Settings > System*, cuadro *Security status*.

El cuadro de diálogo contiene las siguientes pestañas:
- [Global]
- [Port]
- [Status]

### [Global]

#### Security status

Security status

Muestra el estado actual de los ajustes de seguridad del dispositivo. El dispositivo determina el estado a partir de los resultados de los parámetros supervisados individuales.

Valores posibles:
- *error*
  El dispositivo muestra este valor para indicar un error detectado en uno de los parámetros supervisados.
- *ok*

#### Traps

Send trap

Activa/desactiva el envío de trampas SNMP cuando el dispositivo detecta un cambio en una función supervisada.

Valores posibles:
- marked
  El envío de trampas SNMP está activo.
  Si el dispositivo detecta un cambio en las funciones supervisadas, el dispositivo envía una trampa SNMP.
- unmarked (configuración por defecto)
  El envío de trampas SNMP está inactivo.

Como requisito previo para enviar trampas SNMP, debe activar la función en el cuadro de diálogo *Diagnostics > Status Configuration > Alarms (Traps)* y especificar al menos un destino de la trampa.

### Tabla

Password default settings unchanged

Activa/desactiva la supervisión de la contraseña para las cuentas de usuario `user` y `admin` configuradas localmente.

Valores posibles:

- `marked` (configuración por defecto)
  La supervisión está activa.
  Si la contraseña tiene la configuración por defecto para las cuentas de usuario `user` o `admin`, el valor cambia a *`error`* en el cuadro *Security status*.
- `unmarked`
  La supervisión está inactiva.

Establezca la contraseña en el cuadro de diálogo *Device Security > User Management*.

Min. password length < 8

Activa/desactiva la supervisión de la política *Min. password length*.

Valores posibles:

- `marked` (configuración por defecto)
  La supervisión está activa.
  Si el valor de la política *Min. password length* es menor a `8`, el valor cambia a *`error`* en el cuadro *Security status*.
- `unmarked`
  La supervisión está inactiva.

Especifique la política *Min. password length* en el cuadro de diálogo *Device Security > User Management* en el cuadro *Configuration*.

Password policy settings deactivated

Activa/desactiva la supervisión de los ajustes de políticas para la contraseña.

Valores posibles:

- `marked` (configuración por defecto)
  La supervisión está activa.
  Si el valor de al menos una de las siguientes políticas es menor a `1`, el valor cambia a *`error`* en el cuadro *Security status*.
  - *Upper-case characters (min.)*
  - *Lower-case characters (min.)*
  - *Digits (min.)*
  - *Special characters (min.)*
- `unmarked`
  La supervisión está inactiva.

Especifique los ajustes de política en el cuadro de diálogo *Device Security > User Management* en el cuadro *Password policy*.

User account password policy check deactivated

Activa/desactiva la supervisión de la función *Policy check*.

Valores posibles:

- `marked`
  La supervisión está activa.
  Si la función *Policy check* está inactiva para al menos una cuenta de usuario, en el cuadro *Security status* el valor cambiará a `error`.
- `unmarked` (configuración por defecto)
  La supervisión está inactiva.

Puede activar la función *Policy check* en el cuadro de diálogo *Device Security > User Management*.

Telnet server active

Activa/desactiva la supervisión del servidor Telnet.

Valores posibles:

- `marked` (configuración por defecto)
  La supervisión está activa.
  Si activa el servidor Telnet, el valor cambia a `error` en el cuadro *Security status*.
- `unmarked`
  La supervisión está inactiva.

Active/desactive el servidor Telnet en el cuadro de diálogo *Device Security > Management Access > Server*, pestaña *Telnet*.

HTTP server active

Activa/desactiva la supervisión del servidor HTTP.

Valores posibles:

- `marked` (configuración por defecto)
  La supervisión está activa.
  Si activa el servidor HTTP, el valor cambia a `error` en el cuadro *Security status*.
- `unmarked`
  La supervisión está inactiva.

Active/desactive el servidor HTTP en el cuadro de diálogo *Device Security > Management Access > Server*, pestaña *HTTP*.

SNMP unencrypted

Activa/desactiva la supervisión del servidor SNMP.

Valores posibles:

- `marked` (configuración por defecto)
  La supervisión está activa.
  Si al menos una de las siguientes condiciones se cumple, el valor cambia a `error` en el cuadro *Security status*.
  - 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 la columna *SNMP encryption type*.
- `unmarked`
  La supervisión está inactiva.

Especifique los ajustes para el agente SNMP en el cuadro de diálogo *Device Security > Management Access > Server*, pestaña *SNMP*.

Access to system monitor with serial interface possible

Activa/desactiva la supervisión del sistema.

Con el monitor del sistema activado, tiene la posibilidad de cambiar al monitor del sistema a través de una conexión serie.

Valores posibles:

- `marked`
  La supervisión está activa.
  Si activa la supervisión del sistema, el valor cambia a `error` en el cuadro *Security status*.
- `unmarked` (configuración por defecto)
  La supervisión está inactiva.

Puede activar/desactivar la supervisión del sistema en el cuadro de diálogo *Diagnostics > System > Selftest*.

Saving the configuration profile on the external memory possible

Activa/desactiva la supervisión del perfil de configuración en la memoria externa.

Valores posibles:

- `marked`
  La supervisión está activa.
  Si activa el almacenamiento del perfil de configuración en la memoria externa, el valor cambia a `error` en el cuadro *Security status*.
- `unmarked` (configuración por defecto)
  La supervisión está inactiva.

Active/desactive el almacenamiento del perfil de configuración en la memoria externa en el cuadro de diálogo *Basic Settings > External Memory*.

Link interrupted on enabled device ports

Activa/desactiva la supervisión del enlace en los puertos activos.

Valores posibles:

- `marked`
  La supervisión está activa.
  Si el enlace se interrumpe en un puerto activo, el valor cambia a `error` en el cuadro *Security status*. En la pestaña *Port*, tiene la opción de seleccionar los puertos que se supervisarán individualmente.
- `unmarked` (configuración por defecto)
  La supervisión está inactiva.

Access with Ethernet Switch Configurator possible

Activa/desactiva la supervisión de la función Ethernet Switch Configurator.

Valores posibles:

- `marked` (configuración por defecto)
  La supervisión está activa.
  Si activa la función Ethernet Switch Configurator, el valor cambia a `error` en el cuadro *Security status*.
- `unmarked`
  La supervisión está inactiva.

Activa/desactiva la función Ethernet Switch Configurator en el cuadro de diálogo *Basic Settings* > Network.

Load unencrypted config from external memory

Activa/desactiva la supervisión de la carga de perfiles de configuración sin encriptar desde la memoria externa.

Valores posibles:

- `marked` (configuración por defecto)
  La supervisión está activa.
  Si la configuración permite que el dispositivo cargue un perfil de configuración sin encriptar desde la memoria externa, el valor cambia a `error` en el cuadro *Security status*.
  Si se cumplen los siguientes requisitos, el cuadro *Security status* en el cuadro de diálogo *Basic Settings > System* mostrará una alarma.
  - El perfil de configuración almacenado en la memoria externa no está encriptado.
    y
  - La columna *Config priority* en el cuadro de diálogo *Basic Settings > External Memory* tiene el valor `first`.
- `unmarked`
  La supervisión está inactiva.

IEC61850-MMS active

Activa/desactiva la supervisión de la función *IEC61850-MMS*.

Valores posibles:

- `marked` (configuración por defecto)
  La supervisión está activa.
  Si activa la función *IEC61850-MMS*, el valor cambia a `error` en el cuadro *Security status*.
- `unmarked`
  La supervisión está inactiva.

Activa/desactiva la función *IEC61850-MMS* en el cuadro de diálogo *Industrial Protocols > IEC61850-MMS*, cuadro *Operation*.

Self-signed HTTPS certificate present

Activa/desactiva la supervisión del certificado HTTPS.

Valores posibles:

- `marked` (configuración por defecto)
  La supervisión está activa.
  Si el servidor HTTPS utiliza un certificado digital creado de forma autónoma, el valor cambia a `error` en el cuadro *Security status*.
- `unmarked`
  La supervisión está inactiva.

Modbus TCP active

Activa/desactiva la supervisión de la función *Modbus TCP*.

Valores posibles:

- `marked` (configuración por defecto)
  La supervisión está activa.
  Si activa la función *Modbus TCP*, el valor cambia a `error` en el cuadro *Security status*.
- `unmarked`
  La supervisión está inactiva.

Activa/desactiva la función *Modbus TCP* en el cuadro de diálogo *Advanced > Industrial Protocols >* Modbus TCP, cuadro *Operation*.

EtherNet/IP active

Activa/desactiva la supervisión de la función *EtherNet/IP*.

Valores posibles:

- `marked` (configuración por defecto)
  La supervisión está activa.
  Si activa la función *EtherNet/IP*, el valor cambia a `error` en el cuadro *Security status*.
- `unmarked`
  La supervisión está inactiva.

Activa/desactiva la función *EtherNet/IP* en el cuadro de diálogo *Advanced > Industrial Protocols >* EtherNet/IP, cuadro *Operation*.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## [Port]

### Tabla

Port

Muestra el número de puerto.

Link interrupted on enabled device ports

Activa/desactiva la supervisión del enlace en los puertos activos.

Valores posibles:

- `marked`
  La supervisión está activa.
  Si el puerto está activado (cuadro de diálogo *Basic Settings > Port*, pestaña *Configuration*, la casilla *Port on* aparece como `marcada`) y el enlace se interrumpe en el puerto, el valor cambia a *`error`* en el cuadro *Security status*.
- `unmarked` (configuración por defecto)
  La supervisión está inactiva.

Estos ajustes tendrán efecto cuando marque la casilla *Link interrupted on enabled device ports*, en el cuadro de diálogo *Diagnostics > Status Configuration > Security Status*, pestaña *Global*.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## [Status]

### Tabla

Timestamp

Muestra la fecha y hora del evento en el formato `Month Day, Year hh:mm:ss AM/PM`.

Cause

Muestra el evento que causó la trampa SNMP.

**Botones**

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## 6.1.3 Signal Contact

[ Diagnostics > Status Configuration > Signal Contact ]

El contacto de señalización es un contacto de relé sin potencial. El dispositivo le permite realizar un diagnóstico a distancia. El dispositivo utiliza el contacto de relé para indicar la aparición de eventos abriendo el contacto de relé e interrumpiendo el circuito cerrado.

**Nota:** El dispositivo puede contener varios contactos de señalización. Cada contacto incluye las mismas funciones de supervisión. La existencia de varios contactos le permite agrupar varias funciones, ofreciendo así flexibilidad en la supervisión del sistema.

El menú contiene los siguientes cuadros de diálogo:
- Signal Contact 1 / Signal Contact 2

# 6.1.3.1 Signal Contact 1 / Signal Contact 2

[ Diagnostics > Status Configuration > Signal Contact > Signal Contact 1 ]

En este cuadro de diálogo, puede especificar las condiciones para la activación del contacto de señalización.

El contacto de señalización le ofrece las siguientes opciones:
- El control del funcionamiento correcto del dispositivo.
- La señalización del estado del dispositivo.
- La señalización del estado de seguridad del dispositivo.
- El control de dispositivos externos mediante la configuración manual de los contactos de señalización.

El dispositivo muestra los errores detectados en la pestaña *Status* y en el cuadro de diálogo *Basic Settings > System*, cuadro *Signal contact status*.

El cuadro de diálogo contiene las siguientes pestañas:
- [Global]
- [Port]
- [Status]

## [Global]

### Configuration

Mode

Especifica qué eventos debe indicar el contacto de señalización.

Valores posibles:

- `Manual setting` (configuración por defecto para *Signal Contact 2*, si está presente)
  Utilice esta configuración para abrir o cerrar manualmente el contacto de señalización, por ejemplo, para encender o apagar un dispositivo a distancia. Consulte la lista de opciones *Contact*.
- `Monitoring correct operation` (configuración por defecto)
  Con esta configuración, el contacto de señalización indica el estado de los parámetros especificados en la siguiente tabla.
- `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*. Además, puede leer el estado en el cuadro *Signal contact 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*. Además, puede leer el estado en el cuadro *Signal contact 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*. Además, puede leer el estado en el cuadro *Signal contact status*.

Contact

Conmuta el contacto de señalización manualmente. El requisito previo es seleccionar el elemento `Manual setting` en la lista desplegable *Mode*.

Valores posibles:

- `open`
  El contacto de señalización está abierto.
- `close`
  El contacto de señalización está cerrado.

### Signal contact status

Signal contact status

Muestra el estado actual del contacto de señalización.

Valores posibles:

- `Opened (error)`
  El contacto de señalización está abierto. Se ha interrumpido el circuito.
- `Closed (ok)`
  El contacto de señalización está cerrado. El circuito está cerrado.

### Trap configuration

Send trap

Activa/desactiva el envío de trampas SNMP cuando el dispositivo detecta un cambio en una función supervisada.

Valores posibles:

- `marked`
  El envío de trampas SNMP está activo.
  Si el dispositivo detecta un cambio en las funciones supervisadas, el dispositivo envía una trampa SNMP.
- `unmarked` (configuración por defecto)
  El envío de trampas SNMP está inactivo.

Como requisito previo para enviar trampas SNMP, debe activar la función en el cuadro de diálogo *Diagnostics > Status Configuration > Alarms (Traps)* y especificar al menos un destino de la trampa.

### Monitoring correct operation

Especifique en la tabla los parámetros que el dispositivo supervisará. El dispositivo indica la aparición de un evento abriendo el contacto de señalización.

Connection errors

Activa/desactiva la supervisión del estado del enlace del puerto/interfaz.

Valores posibles:

- `marked`
  La supervisión está activa.
  Si el enlace se interrumpe en un puerto/interfaz supervisado, el contacto de señalización se abre.
  En la pestaña *Port*, tiene la opción de seleccionar los puertos/interfaces que se supervisarán individualmente.
- `unmarked` (configuración por defecto)
  La supervisión está inactiva.

Temperature

Activa/desactiva la supervisión de la temperatura del dispositivo.

Valores posibles:

- `marked` (configuración por defecto)
  La supervisión está activa.
  Si la temperatura excede o no alcanza los valores límite, el contacto de señalización se abre.
- `unmarked`
  La supervisión está inactiva.

Especifique los límites de temperatura en el cuadro de diálogo *Basic Settings > System*, campos *Upper temp. limit [°C]* y *Lower temp. limit [°C]*.

Ring redundancy

Activa/desactiva la supervisión de la redundancia de anillo.

Valores posibles:

- `marked`
  La supervisión está activa.
  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.
- `unmarked` (configuración por defecto)
  La supervisión está inactiva.

External memory removed

Activa/desactiva la supervisión de la memoria externa activa.

Valores posibles:

- `marked`
  La supervisión está activa.
  Si extrae la memoria externa activa del dispositivo, el contacto de señalización se abre.
- `unmarked` (configuración por defecto)
  La supervisión está inactiva.

External memory not in sync with NVM

Activa/desactiva la supervisión del perfil de configuración en el dispositivo y en la memoria externa.

Valores posibles:

- `marked`
  La supervisión está activa.
  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.
- `unmarked` (configuración por defecto)
  La supervisión está inactiva.

Ethernet loops

Activa/desactiva la supervisión de los bucles de Ethernet de capa 2. Especifique la configuración de la función *Loop Protection* en el cuadro de diálogo*Diagnostics > Loop Protection*.

Valores posibles:

- `marked`
  La supervisión está activa.
  Si el dispositivo ha detectado un bucle de Ethernet, el contacto de señalización se abre.
- `unmarked` (configuración por defecto)
  La supervisión está inactiva.

Power supply

Activa/desactiva la supervisión de la fuente de alimentación.

Valores posibles:

- `marked` (configuración por defecto)
  La supervisión está activa.
  Si el dispositivo detecta un fallo de alimentación eléctrica, el contacto de señalización se abre.
- `unmarked`
  La supervisión está inactiva.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## [Port]

### Tabla

Port

Muestra el número de puerto.

Propagate connection error

Activa/desactiva la supervisión del enlace en el puerto/interfaz.

Valores posibles:

- `marked`
  La supervisión está activa.
  Si el enlace se interrumpe en el puerto/interfaz seleccionado, el contacto de señalización se abre.
- `unmarked` (configuración por defecto)
  La supervisión está inactiva.

Estos ajustes tendrán efecto cuando marque la casilla *Connection errors* de la pestaña *Global*.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## [Status]

### Tabla

Timestamp

Muestra la fecha y hora del evento en el formato `Month Day, Year hh:mm:ss AM/PM`.

Cause

Muestra el evento que causó la trampa SNMP.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

# 6.1.4 MAC Notification

[ Diagnostics > Status Configuration > MAC Notification ]

El dispositivo le permite seguir los cambios en la red mediante la dirección MAC de los dispositivos de la red. El dispositivo guarda la combinación de puerto y dirección MAC en su tabla de direcciones MAC. Si el dispositivo aprende/olvida la dirección MAC de un dispositivo conectado/desconectado, el dispositivo envía una trampa SNMP.

Esta función está prevista para puertos a los que se conectarán dispositivos terminales y, por lo tanto, cuya dirección MAC no cambiará a menudo.

### Operation

Operation

Activa/desactiva la función *MAC Notification* en el dispositivo.

Valores posibles:

- `On`
  La función *MAC Notification* está activada.
- `Off` (configuración por defecto)
  La función *MAC Notification* está desactivada.

### Configuration

Interval [s]

Especifica el intervalo de envío en segundos. Si el dispositivo aprende/olvida la dirección MAC de un dispositivo conectado/desconectado, el dispositivo envía una trampa SNMP después de este tiempo.

Valores posibles:

- `0..2147483647` (configuración por defecto: `30`)

Antes de enviar una trampa SNMP, el dispositivo registra hasta 20 direcciones MAC. Si el dispositivo detecta un número alto de cambios, el dispositivo envía una trampa SNMP antes de que el intervalo de envío se cumpla.

### Tabla

Port

Muestra el número de puerto.

Active

Activa/desactiva la función *MAC Notification* en el puerto.

Valores posibles:

- `marked`
  La función *MAC Notification* está activa en el puerto.
  El dispositivo envía una trampa SNMP en caso de que ocurra uno de los siguientes eventos:
  - El dispositivo aprende la dirección MAC de un nuevo dispositivo conectado.
  - El dispositivo olvida la dirección MAC de un dispositivo desconectado.
- `unmarked` (configuración por defecto)
  La función *MAC Notification* está inactiva en el puerto.

Como requisito previo para enviar trampas SNMP, debe activar la función en el cuadro de diálogo *Diagnostics > Status Configuration > Alarms (Traps)* y especificar al menos un destino de la trampa.

Last MAC address

Muestra la dirección MAC del último dispositivo conectado a o desconectado del puerto.

El dispositivo detecta las direcciones MAC de los dispositivos que están conectados de la siguiente manera:

- conectados directamente al puerto
- conectados al puerto mediante otros dispositivos de la red

Last MAC status

Muestra el estado del valor *Last MAC address* en este puerto.

Valores posibles:

- `added`
  El dispositivo ha detectado que se ha conectado otro dispositivo al puerto.
- `removed`
  El dispositivo ha detectado que el dispositivo conectado se ha extraído del puerto.
- `other`
  El dispositivo no ha detectado un estado.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

# 6.1.5 Alarms (Traps)

[ Diagnostics > Status Configuration > Alarms (Traps) ]

El dispositivo le permite enviar una trampa SNMP como reacción ante eventos específicos. En el cuadro de diálogo, especifique los destinos a los que el dispositivo envía las trampas SNMP.

Especifique los eventos ante los cuales el dispositivo activará una trampa SNMP, por ejemplo, en los siguientes cuadros de diálogo:
- en el cuadro de diálogo *Diagnostics > Status Configuration > Device Status*
- en el cuadro de diálogo *Diagnostics > Status Configuration > Security Status*
- en el cuadro de diálogo *Diagnostics > Status Configuration > MAC Notification*

### Operation

Operation

Activa/desactiva el envío de trampas SNMP a los destinos de las trampas.

Valores posibles:
- `On` (configuración por defecto)
  El envío de trampas SNMP está activado.
- `Off`
  El envío de trampas SNMP está desactivado.

### Tabla

Name

Especifica el nombre del destino de la trampa.

Valores posibles:
- Cadena de caracteres ASCII alfanuméricos con entre 1 y 32 caracteres

Address

Especifica la dirección IP y el número de puerto del destino de la trampa.

Valores posibles:
- `<Valid IPv4 address>:<port number>`

Active

Activa/desactiva el envío de trampas SNMP a este destino.

Valores posibles:
- `marked` (configuración por defecto)
  El envío de trampas SNMP a este destino está activo.
- `unmarked`
  El envío de trampas SNMP a este destino está inactivo.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

Abre la ventana *Create* para añadir una entrada nueva a la tabla.

- En el campo *Name*, especifique un nombre para el destino de la trampa.
- En el campo *Address*, especifique la dirección IP y el número de puerto del destino de la trampa. Si elige no introducir un número de puerto, el dispositivo añadirá automáticamente el número de puerto `162`.

# 6.2 System

[Diagnostics > System]

El menú contiene los siguientes cuadros de diálogo:

- System Information
- Hardware State
- IP Address Conflict Detection
- ARP
- Selftest

## 6.2.1 System Information

[ Diagnostics > System > System Information ]

Este cuadro de diálogo muestra el estado de funcionamiento actual de los componentes individuales del dispositivo. Los valores mostrados son una vista instantánea; representan el estado de funcionamiento en el momento en que el cuadro de diálogo se cargó en la página.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

Save system information

Abre la página HTML en una nueva ventana o pestaña del navegador web. Puede guardar la página HTML en su PC con el comando adecuado del navegador web.

## 6.2.2 Hardware State

[ Diagnostics > System > Hardware State ]

Este cuadro de diálogo proporciona información sobre la distribución y el estado de la memoria flash del dispositivo.

### Information

Uptime

Muestra el tiempo de funcionamiento total del dispositivo desde que se entregó.

Valores posibles:

▶ `..d ..h ..m ..s`
Día(s) Hora(s) Minuto(s) Segundo(s)

### Tabla

Flash region

Muestra el nombre de la zona de memoria correspondiente.

Description

Muestra una descripción del uso que hace el dispositivo de esa zona de memoria.

Flash sectors

Muestra cuántos sectores se han asignado a la zona de memoria.

Sector erase operations

Muestra el número de veces que el dispositivo ha sobrescrito los sectores de la zona de memoria.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## 6.2.3 IP Address Conflict Detection

[ Diagnostics > System > IP Address Conflict Detection ]

Mediante la función *IP Address Conflict Detection*, el dispositivo comprueba que su dirección IP es única en la red. Para ello, el dispositivo analiza los paquetes ARP recibidos.

En este cuadro de diálogo, especifique el método con el que el dispositivo detectará conflictos de direcciones, además de la configuración necesaria para ello.

El dispositivo muestra los conflictos de direcciones detectados en la tabla.

Cuando el dispositivo detecta un conflicto de direcciones, el LED de estado del dispositivo parpadea en rojo 4 veces.

### Operation

Operation

Activa/desactiva la función *IP Address Conflict Detection*.

Valores posibles:

- `On` (configuración por defecto)
  La función *IP Address Conflict Detection* está activada.
  El dispositivo comprueba que su dirección IP es única en la red.
- `Off`
  La función *IP Address Conflict Detection* está desactivada.

### Configuration

Detection mode

Especifique el método con el que el dispositivo detectará conflictos de direcciones.

Valores posibles:

- `active and passive` (configuración por defecto)
  El dispositivo utiliza la detección activa y pasiva de conflictos de direcciones.

▶ *active*
Detección activa de conflictos de direcciones. El dispositivo ayuda de manera activa a evitar la comunicación con una dirección IP que ya exista en la red. La detección del conflicto de direcciones comienza en cuanto conecta el dispositivo a la red o cambia sus parámetros IP.
- El dispositivo envía 4 paquetes de datos de sonda ARP en los intervalos especificados en el campo *Detection delay [ms]*. Si el dispositivo recibe una respuesta a estos paquetes de datos, entonces hay un conflicto de direcciones.
- Si el dispositivo no detecta un conflicto de direcciones, envía 2 paquetes de datos ARP gratuitos como anuncio. El dispositivo envía también estos paquetes de datos cuando se desactiva la detección de conflicto de direcciones.
- Si la dirección IP ya existe en la red, el dispositivo vuelve a los parámetros IP utilizados anteriormente (si es posible).
  Si el dispositivo recibe sus parámetros IP de un servidor DHCP, envía un mensaje DHCP-DECLINE de vuelta al servidor DHCP.
- Tras el período especificado en el campo *Release delay [s]*, el dispositivo comprueba si el conflicto de direcciones aún existe. Cuando el dispositivo detecta 10 conflictos de direcciones consecutivos, el dispositivo aumenta el tiempo de espera a 60 s para la siguiente comprobación.
- Cuando el dispositivo resuelve el conflicto de direcciones, la gestión del dispositivo vuelve a la red.

▶ *passive*
Detección pasiva de conflictos de direcciones El dispositivo analiza el tráfico de datos en la red. Si otro dispositivo de la red está utilizando la misma dirección IP, el dispositivo "defiende" en primer lugar su dirección IP. El dispositivo deja de enviar si el otro dispositivo sigue enviando con la misma dirección IP.
- Como "defensa", el dispositivo envía paquetes de datos ARP gratuitos. El dispositivo repite este procedimiento el número de veces especificado en el campo *Address protections*.
- Si otro dispositivo continúa enviando desde la misma dirección IP, el dispositivo comprobará periódicamente si el conflicto de direcciones aún existe tras el período especificado en el campo *Release delay [s]*.
- Cuando el dispositivo resuelve el conflicto de direcciones, la gestión del dispositivo vuelve a la red.

Send periodic ARP probes

Activa/desactiva la detección periódica de conflictos de direcciones.

Valores posibles:

▶ `marked` (configuración por defecto)
La detección periódica de conflictos de direcciones está activa.
- El dispositivo envía periódicamente paquetes de datos de sonda ARP cada 90 a 150 segundos y espera una respuesta durante el tiempo especificado en el campo *Detection delay [ms]*.
- Si el dispositivo detecta un conflicto de direcciones, aplica la función de modo de detección pasiva. Si la función *Send trap* está activa, el dispositivo envía una trampa SNMP.

▶ `unmarked`
La detección periódica de conflictos de direcciones está inactiva.

Detection delay [ms]

Especifica el período en milisegundos durante el cual el dispositivo esperará una respuesta después de enviar un paquete de datos ARP.

Valores posibles:

- `20..500` (configuración por defecto: `200`)

Release delay [s]

Especifica el período en segundos tras el cual el dispositivo comprueba otra vez si el conflicto de direcciones aún existe.

Valores posibles:

- `3..3600` (configuración por defecto: `15`)

Address protections

Especifica cuántas veces el dispositivo enviará paquetes de datos ARP gratuitos en el modo de detección pasiva para "defender" su dirección IP.

Valores posibles:

- `0..100` (configuración por defecto: `3`)

Protection interval [ms]

Especifica el período en milisegundos tras el cual el dispositivo enviará paquetes de datos ARP gratuitos otra vez en el modo de detección pasiva para "defender" su dirección IP.

Valores posibles:

- `20..5000` (configuración por defecto: `200`)

Send trap

Activa/desactiva el envío de trampas SNMP cuando el dispositivo detecta un conflicto de direcciones.

Valores posibles:

- `marked`
  El envío de trampas SNMP está activo.
  Si el dispositivo detecta un conflicto de direcciones, el dispositivo envía una trampa SNMP.
- `unmarked` (configuración por defecto)
  El envío de trampas SNMP está inactivo.

Como requisito previo para enviar trampas SNMP, debe activar la función en el cuadro de diálogo *Diagnostics > Status Configuration > Alarms (Traps)* y especificar al menos un destino de la trampa.

### Information

Conflict detected

Muestra si existe un conflicto de direcciones en este momento.

Valores posibles:

- `marked`
  El dispositivo detecta un conflicto de direcciones.
- `unmarked`
  El dispositivo no detecta un conflicto de direcciones.

### Tabla

Timestamp

Muestra la hora a la que el dispositivo detectó un conflicto de direcciones.

Port

Muestra el número del puerto en el que el dispositivo detectó un conflicto de direcciones.

IP address

Muestra la dirección IP que está causando el conflicto de direcciones.

MAC address

Muestra la dirección MAC del dispositivo en el que existe el conflicto de direcciones.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## 6.2.4 ARP

[ Diagnostics > System > ARP ]

Este cuadro de diálogo muestra las direcciones MAC e IP de los dispositivos vecinos conectados a la administración del dispositivo.

El dispositivo puede mostrar las direcciones IPv4 y IPv6. Para el protocolo IPv6, las direcciones de los dispositivos vecinos se obtienen mediante el Neighbor Discovery Protocol (NDP).

### Tabla

Port

Muestra el número de puerto.

IP address

Muestra la dirección IPv4 o la dirección IPv6 de un dispositivo vecino.

MAC address

Muestra la dirección MAC del dispositivo vecino.

Last updated

Muestra el tiempo en segundos desde que se registró la configuración actual de la entrada en la tabla ARP.

Type

Muestra el tipo de entrada.

Valores posibles:

- `static`
  Entrada estática. Cuando se elimina la tabla ARP, el dispositivo mantiene la entrada estática.
- `dynamic`
  Entrada dinámica. Cuando se supera el *Aging time [s]* y el dispositivo no recibe ningún dato de este dispositivo durante este período, el dispositivo elimina la entrada dinámica.
- `local`
  Dirección IP y MAC de la administración del dispositivo.

Active

Muestra que la tabla ARP contiene la asignación de dirección IP/MAC como entrada activa.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

Reset ARP table

Elimina las direcciones configuradas dinámicamente de la tabla ARP.

## 6.2.5 Selftest

[ Diagnostics > System > Selftest ]

Este cuadro de diálogo le permite hacer lo siguiente:
- Activar/desactivar la prueba de RAM al iniciar el dispositivo.
- Activar/desactivar la opción de iniciar la supervisión del sistema al arrancar el sistema.
- Especificar cómo se comportará el dispositivo en caso de error detectado.

### Configuration

Si el dispositivo no detecta un perfil de configuración legible al reiniciar, los siguientes ajustes bloquearán su acceso al dispositivo de forma permanente.
- La casilla *SysMon1 is available* aparece como `unmarked`.
- La casilla *Load default config on error* aparece como `unmarked`.

Este es el casi si, por ejemplo, la contraseña del perfil de configuración que se está cargando es diferente de la contraseña establecida en el dispositivo. Para desbloquear de nuevo el dispositivo, póngase en contacto con su distribuidor.

RAM test

Activa/desactiva la comprobación de la memoria RAM durante el reinicio.

Valores posibles:
- `marked` (configuración por defecto)
  La comprobación de la memoria RAM está activada. Durante el reinicio, el dispositivo comprueba la memoria RAM.
- `unmarked`
  La comprobación de la memoria RAM está desactivada. Esto acorta el tiempo de inicio del dispositivo.

SysMon1 is available

Activa/desactiva el acceso a la supervisión del sistema durante el reinicio.

Valores posibles:
- `marked` (configuración por defecto)
  El dispositivo le permite abrir la supervisión del sistema durante el reinicio.
- `unmarked`
  El dispositivo arranca sin la opción de abrir la supervisión del sistema.

Entre otras cosas, la supervisión del sistema le permite actualizar el software del dispositivo y eliminar los perfiles de configuración guardados.

Load default config on error

Activa/desactiva la carga de la configuración por defecto si el dispositivo no detecta un perfil de configuración legible al reiniciar.

Valores posibles:

- `marked` (configuración por defecto)
  El dispositivo carga la configuración por defecto.
- `unmarked`
  El dispositivo interrumpe el reinicio y se detiene. El acceso a la gestión del dispositivo solamente es posible utilizando la interfaz de línea de comando a través de la interfaz serie. Para recuperar el acceso al dispositivo a través de la red, abra la supervisión del sistema y reinicie la configuración. Al reiniciar, el dispositivo carga la configuración por defecto.

### Tabla

En esta tabla, puede especificar cómo se comportará el dispositivo en caso de error detectado.

Cause

Causas de error ante las que reacciona el dispositivo.

Valores posibles:

- `task`
  El dispositivo detecta errores en las aplicaciones ejecutadas, por ejemplo, si se cancela una tarea o no está disponible.
- `resource`
  El dispositivo detecta errores en los recursos disponibles, por ejemplo, si queda poca memoria.
- `software`
  El dispositivo detecta errores en el software, por ejemplo, un error en el control de coherencia.
- `hardware`
  El dispositivo detecta errores en el hardware, por ejemplo, en el conjunto de chips.

Action

Especifica cómo se comportará el dispositivo si ocurre un evento adyacente.

Valores posibles:

- `reboot` (configuración por defecto)
  El dispositivo activa un reinicio.
- `logOnly`
  El dispositivo registra el error detectado en el archivo de registro. Consulte el cuadro de diálogo *Diagnostics > Report > System Log*.
- `sendTrap`
  El dispositivo envía una trampa SNMP.
  Como requisito previo para enviar trampas SNMP, debe activar la función en el cuadro de diálogo *Diagnostics > Status Configuration > Alarms (Traps)* y especificar al menos un destino de la trampa.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## 6.3 Email Notification

[ Diagnostics > Email Notification ]

El dispositivo le permite informar a varios destinatarios mediante correo electrónico acerca de los eventos que se han producido.

El dispositivo envía los correos electrónicos inmediatamente o de manera periódica en función de la gravedad del evento. Normalmente se especifican eventos con una gravedad elevada para su envío inmediato.

Puede especificar varios destinatarios a los que el dispositivo envíe los correos electrónicos de manera inmediata o periódica.

El menú contiene los siguientes cuadros de diálogo:
- Email Notification Global
- Email Notification Recipients
- Email Notification Mail Server

# 6.3.1 Email Notification Global

[Diagnostics > Email Notification > Global]

En este diálogo deberá especificar la configuración del remitente. Además, debe especificar para qué nivel de gravedad de eventos desea que envíe el dispositivo los correos electrónicos inmediatamente y para cuáles de manera periódica.

### Operation

Operation

Activa/desactiva el envío de correos electrónicos:

Valores posibles:

- *On*
  El envío de correos electrónicos está activado.
- *Off* (configuración por defecto)
  El envío de correos electrónicos está desactivado.

### Certificate

El dispositivo puede enviar mensajes a un servidor a través de redes no protegidas. Para ayudar a denegar un ataque de "intermediario", solicite que la autoridad de certificación cree un certificado para el servidor. Configure el servidor para utilizar el certificado. Transfiera el certificado al dispositivo.

Si especifica la configuración para los servidores de correo, utilice la dirección IP o el nombre de DNS proporcionado como `Common Name` o `Subject Alternative Name` en el certificado. De lo contrario, la validación de certificado fallará.

URL

Especifica la ruta y el nombre de archivo del certificado.

El dispositivo acepta certificados con las siguientes propiedades:

- Formato X.509
- Extensión de nombre de archivo `.PEM`
- Codificación con Base64, acompañado por
  `-----BEGIN CERTIFICATE-----`
  y
  `-----END CERTIFICATE-----`

Por motivos de seguridad, es recomendable utilizar de manera constante un certificado que esté firmado por una autoridad de certificación.

El dispositivo le ofrece las opciones siguientes para copiar el certificado al dispositivo:

- Importar desde el PC
  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.

- Importar desde un servidor FTP
  Cuando el certificado se encuentre en un servidor FTP, especifique la URL correspondiente al archivo en el formato siguiente:
  `ftp://<usuario>:<contraseña>@<dirección IP>:<puerto>/<ruta>/<nombre archivo>`
- Importar desde un servidor TFTP
  Cuando el certificado se encuentre en un servidor TFTP, especifique la URL correspondiente al archivo en el formato siguiente:
  `tftp://<dirección IP>/<ruta>/<nombre archivo>`
- Importar desde un servidor SCP o SFTP
  Cuando el certificado está en un servidor SCP o SFTP, especifique la URL del archivo en el formato siguiente:
  - `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://<user>:<password>@<IP address>/<path>/<file name>`

Start

Copia el certificado especificado en el campo *URL* del dispositivo.

### Sender

Address

Especifica la dirección de correo electrónico del dispositivo.

El dispositivo envía los correos electrónicos utilizando esta dirección de correo electrónico como remitente.

Valores posibles:

- Cadena de caracteres ASCII alfanuméricos con entre 0 y 255 caracteres

### Notification immediate

Aquí deberá especificar la configuración de los correos electrónicos que el dispositivo envía inmediatamente.

Severity

Especifica la gravedad mínima de los eventos para los que el dispositivo envía inmediatamente un correo electrónico. Si se produce un evento de esta gravedad o de una gravedad más urgente, el dispositivo enviará un correo electrónico a los destinatarios.

Valores posibles:

- *emergency*
- *alert* (configuración por defecto)
- *critical*
- *error*
- *warning*
- *notice*

- *informational*
- *debug*

Subject

Especifica el asunto del correo electrónico.

Valores posibles:
- Cadena de caracteres ASCII alfanuméricos con entre 0 y 255 caracteres

### Notification periodic

Aquí deberá especificar la configuración de los correos electrónicos que el dispositivo envía periódicamente.

Severity

Especifica la gravedad mínima de los eventos para los que el dispositivo envía periódicamente un correo electrónico. Si se produce un evento de esta gravedad o de una gravedad más urgente, el dispositivo registra el evento en el búfer. El dispositivo envía el contenido del búfer periódicamente o cuando este se sobrecarga.

Si se produce un evento de una gravedad menos urgente, el dispositivo no registra el evento en el búfer.

Valores posibles:
- *emergency*
- *alert*
- *critical*
- *error*
- *warning* (configuración por defecto)
- *notice*
- *informational*
- *debug*

Subject

Especifica el asunto del correo electrónico.

Valores posibles:
- Cadena de caracteres ASCII alfanuméricos con entre 0 y 255 caracteres

Sending interval [min]

Especifica el intervalo de envío en minutos.

Si el dispositivo ha registrado al menos un evento, el dispositivo envía un correo electrónico con el archivo de registro una vez transcurrido el plazo de tiempo.

Valores posibles:

- `30..1440` (configuración por defecto: `30`)

Send

Envía un correo electrónico inmediatamente con el contenido del búfer y borra el búfer.

### Information

Sent messages

Muestra cuántas veces ha enviado correctamente el dispositivo un correo electrónico al servidor de correo.

Undeliverable messages

Muestra cuántas veces ha intentado sin éxito el dispositivo enviar un correo electrónico al servidor de correo.

Time of the last messages sent

Muestra la fecha y hora a las que el dispositivo ha enviado por última vez un correo electrónico al servidor de correo.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

Clear email notification statistics

Restablece los contadores en el cuadro *Information* a `0`.

### Significado de los niveles de gravedad de eventos

| 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) |
| `notice` | Importante, estado normal |
| `informational` | Mensaje informal |
| `debug` | Mensaje de depuración |

## 6.3.2 Email Notification Recipients

[ Diagnostics > Email Notification > Recipients ]

En este cuadro de diálogo deberá especificar los destinatarios a los que el dispositivo envía los correos electrónicos. El dispositivo le permite especificar hasta 10 destinatarios.

### Tabla

Index

Muestra el número de índice al que la entrada de la tabla hace referencia.

Notification type

Especifica si el dispositivo envía los correos electrónicos a este destinatario de manera inmediata o periódica.

Valores posibles:

- *immediate*
  El dispositivo envía los correos electrónicos a este destinatario de manera inmediata.
- *periodic*
  El dispositivo envía los correos electrónicos a este destinatario de manera periódica.

Address

Especifica la dirección de correo electrónico del destinatario.

Valores posibles:

- Dirección de correo electrónico válida con hasta 255 caracteres

Active

Activa/desactiva el traslado de la información al destinatario.

Valores posibles:

- `marked` (configuración por defecto)
  El traslado de la información al destinatario está activo.
- `unmarked`
  El traslado de la información al destinatario está inactivo.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## 6.3.3 Email Notification Mail Server

[Diagnostics > Email Notification > Mail Server]

En este cuadro de diálogo deberá especifica la configuración de los servidores de correo. El dispositivo admite conexiones encriptadas y no encriptadas con el servidor de correo.

### Tabla

Index

Muestra el número de índice al que la entrada de la tabla hace referencia.

Description

Especifica el nombre del servidor.

Valores posibles:

- Cadena de caracteres ASCII alfanuméricos con entre 0 y 255 caracteres

IP address

Especifica la dirección IP o el nombre de DNS del servidor.

Valores posibles:

- Dirección IPv4 válida (configuración por defecto: `0.0.0.0`)
- Nombre de DNS en formato `domain.tld` o `host.domain.tld`
  Si especifica un nombre de DNS, active también la función *Client* en el cuadro de diálogo *Advanced > DNS > Client > Global*.
  Si establece conexiones encriptadas mediante el certificado, compruebe que el nombre de DNS coincida con el nombre DNS del servidor mencionado en el certificado.

Destination TCP port

Especifica el puerto TCP del servidor.

Valores posibles:

- `1..65535` (configuración por defecto: `25`)
  Excepción: el puerto `2222` está reservado para funciones internas.

Puertos TCP utilizados con frecuencia:

- SMTP `25`
- Message Submission `587`

Encryption

Especifica el protocolo que encripta la conexión entre el dispositivo y el servidor de correo.

Valores posibles:

- `none` (configuración por defecto)
  El dispositivo establece una conexión no encriptada con el servidor.
- `tlsv1`
  El dispositivo establece una conexión encriptada con el servidor utilizando la extensión startTLS.

User name

Especifica el nombre de usuario de la cuenta que utiliza el dispositivo para autenticarse en el servidor de correo.

Valores posibles:

- Cadena de caracteres ASCII alfanuméricos con entre 0 y 255 caracteres

Password

Especifica la contraseña de la cuenta que utiliza el dispositivo para autenticarse en el servidor de correo.

Valores posibles:

- Cadena de caracteres ASCII alfanuméricos con entre 0 y 255 caracteres

Timeout [s]

Especifica el tiempo en segundos que desea que transcurra para que el dispositivo envíe de nuevo un correo electrónico. El requisito previo es que el dispositivo no haya enviado correctamente el correo electrónico completo debido a un error de conexión.

Valores posibles:

- `1..15` (configuración por defecto: `3`)

Active

Activa/desactiva el uso del servidor de correo.

Valores posibles:

- `marked`
  El servidor de correo está activo.
  El dispositivo envía correos electrónicos a este servidor de correo.
- `unmarked` (configuración por defecto)
  El servidor de correo está inactivo.
  El dispositivo no envía correos electrónicos a este servidor de correo.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

Connection test

Abre el cuadro de diálogo *Connection test* para enviar un correo electrónico de prueba.

Si la configuración del servidor de correo es correcta, los destinatarios seleccionados recibirá un correo electrónico de prueba.

- En el campo *Recipient*, especifica a qué destinatarios desea que envíe el dispositivo el correo electrónico de prueba:
  - *immediate*
    El dispositivo envía el correo electrónico de prueba a los destinatarios a los que el dispositivo envía correos electrónicos inmediatamente.
  - *periodic*
    El dispositivo envía el correo electrónico de prueba a los destinatarios a los que el dispositivo envía correos electrónicos periódicamente.
- En el campo *Message text*, especifique el texto del correo electrónico de prueba.

## 6.4 Syslog

[ Diagnostics > Syslog ]

El dispositivo le permite informar sobre los eventos seleccionados, independientemente de la gravedad del evento, a los diferentes servidores Syslog. En este cuadro de diálogo, podrá especificar los ajustes de esta función y gestionar hasta 8 servidores Syslog.

### Operation

Operation

Activa/desactiva el envío de eventos a los servidores Syslog.

Valores posibles:

- `On`
  El envío de eventos está activado.
  El dispositivo envía los eventos especificados en la tabla a los servidores Syslog especificados.
- `Off` (configuración por defecto)
  El envío de eventos está desactivado.

### Certificate

El dispositivo puede enviar mensajes a un servidor a través de redes no protegidas. Para ayudar a denegar un ataque de "intermediario", solicite que la autoridad de certificación cree un certificado para el servidor. Configure el servidor para utilizar el certificado. Transfiera el certificado al dispositivo.

Si especifica los parámetros en el servidor, compruebe que haya especificado la dirección IP y el nombre de DNS proporcionados en el certificado como `Common Name` o `Subject Alternative Name`. De lo contrario, la validación de certificado fallará.

**Nota:** Para que los cambios tengan efecto tras cargar un certificado nuevo, reinicie la función *Syslog*.

URL

Especifica la ruta y el nombre de archivo del certificado.

El dispositivo acepta certificados con las siguientes propiedades:

- Formato X.509
- Extensión de nombre de archivo `.PEM`
- Codificación con Base64, acompañado por
  `-----BEGIN CERTIFICATE-----`
  y
  `-----END CERTIFICATE-----`

Por motivos de seguridad, es recomendable utilizar de manera constante un certificado que esté firmado por una autoridad de certificación.

El dispositivo le ofrece las opciones siguientes para copiar el certificado al dispositivo:

- Importar desde el PC
  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.
- Importar desde un servidor FTP
  Cuando el certificado se encuentre en un servidor FTP, especifique la URL correspondiente al archivo en el formato siguiente:
  `ftp://<usuario>:<contraseña>@<dirección IP>:<puerto>/<ruta>/<nombre archivo>`
- Importar desde un servidor TFTP
  Cuando el certificado se encuentre en un servidor TFTP, especifique la URL correspondiente al archivo en el formato siguiente:
  `tftp://<dirección IP>/<ruta>/<nombre archivo>`
- Importar desde un servidor SCP o SFTP
  Cuando el certificado está en un servidor SCP o SFTP, especifique la URL del archivo en el formato siguiente:
  - `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://<user>:<password>@<IP address>/<path>/<file name>`

Start

Copia el certificado especificado en el campo *URL* del dispositivo.

### Tabla

Index

Muestra el número de índice al que la entrada de la tabla hace referencia.

Cuando elimine una entrada de la tabla, quedará un hueco en la numeración. Al crear una nueva entrada en la tabla, el dispositivo introduce el primer número que falta.

Valores posibles:

- `1..8`

IP address

Especifica la dirección IP del servidor Syslog.

Valores posibles:

- Dirección IPv4 válida (configuración por defecto: `0.0.0.0`)
- Dirección IPv6 válida
- Nombre de host

Destination UDP port

Especifica el puerto TCP o UDP en el que el servidor Syslog espera las entradas del registro.

Valores posibles:

- `1..65535` (configuración por defecto: `514`)

Transport type

Especifica el tipo de transporte que utiliza el dispositivo para enviar los eventos al servidor Syslog.

Valores posibles:

- `udp` (configuración por defecto)
  El dispositivo envía los eventos a través del puerto UDP especificado en la columna *Destination UDP port*.
- `tls`
  El dispositivo envía los eventos a través de TLS en el puerto TCP especificado en la columna *Destination UDP port*.

Min. severity

Especifica el nivel mínimo de gravedad de los eventos. El dispositivo envía una entrada de registro para los eventos con este nivel y con niveles más urgentes de gravedad al servidor Syslog.

Valores posibles:

- `emergency`
- `alert`
- `critical`
- `error`
- `warning` (configuración por defecto)
- `notice`
- `informational`
- `debug`

Type

Especifica el tipo de entrada de registro que el dispositivo transmitirá.

Valores posibles:

- `systemlog` (configuración por defecto)
- `audittrail`

Active

Activa/desactiva la transmisión de eventos al servidor Syslog:

- `marked`
  El dispositivo envía eventos al servidor Syslog.
- `unmarked` (configuración por defecto)
  La transmisión de eventos al servidor Syslog está desactivada.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

# 6.5 Ports

[ Diagnostics > Ports ]

El menú contiene los siguientes cuadros de diálogo:

- SFP
- TP cable diagnosis
- Port Monitor
- Auto-Disable
- Port Mirroring

## 6.5.1 SFP

[ Diagnostics > Ports > SFP ]

Este cuadro de diálogo le permite ver los transceptores SFP conectados en este momento al dispositivo y sus propiedades.

### Tabla

La tabla muestra valores válidos si el dispositivo está equipado con transceptores SFP.

Port

Muestra el número de puerto.

Module type

Tipo de transceptor SFP, por ejemplo, M-SFP-SX/LC.

Serial number

Muestra el número de serie del transceptor SFP.

Connector type

Muestra el tipo de conector.

Supported

Muestra si el dispositivo es compatible con el transceptor SFP.

Temperature [°C]

La temperatura de funcionamiento del transceptor SFP en grados centígrados.

Tx power [mW]

La potencia de emisión del transceptor SFP en mW.

Rx power [mW]

La potencia de recepción del transceptor SFP en mW.

Tx power [dBm]

La potencia de emisión del transceptor SFP en dBm.

Rx power [dBm]

La potencia de recepción del transceptor SFP en dBm.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

# 6.5.2 TP cable diagnosis

[Diagnostics > Ports > TP cable diagnosis]

Esta función comprueba si el cable conectado a una interfaz tiene un cortocircuito o circuito abierto. La tabla muestra el estado del cable y la longitud estimada. El dispositivo muestra también los pares de cables individuales conectados al puerto. Cuando el dispositivo detecta un cortocircuito o un circuito abierto en el cable, muestra también la distancia estimada del problema.

Para obtener resultados fiables, utilice la función *TP cable diagnosis* para cable de par trenzados con una longitud mínima de 3 metros

**Nota:** Esta prueba interrumpe el tráfico en el puerto.

### Information

Port

Muestra el número de puerto.

Status

Estado del dispositivo de prueba de cable virtual.

Valores posibles:

- *active*
  La prueba del cable está en curso.
  Para iniciar la prueba, haga clic en el botón ☰ y, a continuación, en el elemento *Start cable diagnosis...*. Esta acción abrirá el cuadro de diálogo *Select port*.
- *success*
  El dispositivo mostrará esta entrada después de llevar a cabo una prueba con éxito.
- *failure*
  El dispositivo mostrará esta entrada después de una interrupción de la prueba.
- *uninitialized*
  El dispositivo mostrará esta entrada mientras esté en espera.

### Tabla

Cable pair

Muestra el par de cables al que se refiere esta entrada. El dispositivo utiliza el primer índice PHY compatible para mostrar los valores.

Result

Muestra los resultados de la prueba del cable.

Valores posibles:

- *normal*
  El cable funciona correctamente.

- *open*
  Hay una rotura en el cable que está causando una interrupción.
- *short*
  Los conductores del cable están en contacto y provocan un cortocircuito.
- *unknown*
  El dispositivo muestra este valor para los pares de cables sin probar.

El dispositivo muestra valores diferentes a los esperados en los siguientes casos:

- Si no hay un cable conectado al puerto, el dispositivo muestra el valor *unknown* en lugar de *open*.
- Si el puerto está desactivado, el dispositivo muestra el valor *short*.

Min. length

Muestra la longitud mínima estimada del cable en metros.

Si la longitud del cable es desconocida o si, en el cuadro *Information*, el campo *Status* muestra el valor *active*, *failure* o *uninitialized*, el dispositivo mostrará el valor 0.

Max. length

Muestra la longitud máxima estimada del cable en metros.

Si la longitud del cable es desconocida o si, en el cuadro *Information*, el campo *Status* muestra el valor *active*, *failure* o *uninitialized*, el dispositivo mostrará el valor 0.

Distance [m]

Muestra la distancia estimada en metros desde un extremo del cable al otro extremo, o hasta la interrupción del cable.

Si la longitud del cable es desconocida o si, en el cuadro *Information*, el campo *Status* muestra el valor *active*, *failure* o *uninitialized*, el dispositivo mostrará el valor 0.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

Start cable diagnosis...

Abre el cuadro de diálogo *Select port*.

En la lista desplegable *Port*, seleccione el puerto que se va a probar. Utilice únicamente puertos de cobre.

Para iniciar la prueba del cable en el puerto seleccionado, haga clic en el botón *Ok*.

## 6.5.3 Port Monitor

[Diagnostics > Ports > Port Monitor]

La función *Port Monitor* supervisa la adherencia de los puertos a los parámetros especificados. Si la función *Port Monitor* detecta que se han excedido los parámetros, el dispositivo realizará una acción.

Para aplicar la función *Port Monitor*, lleve a cabo los pasos siguientes:
- Pestaña *Global*
  - ☐ Active la función *Operation* en el cuadro *Port Monitor*.
  - ☐ Active en cada puerto los parámetros que desee que la función *Port Monitor* supervise.
- Pestañas *Link flap*, *CRC/Fragments* y *Overload detection*
  - ☐ Especifique los valores límite para los parámetros de cada puerto.
- Pestaña *Link speed/Duplex mode detection*
  - ☐ Active las combinaciones de velocidad y modo dúplex permitidas para cada puerto.
- Pestaña *Global*
  - ☐ Especifique para cada puerto una acción que el dispositivo llevará a cabo si la función *Port Monitor* detecta que se han excedido los parámetros.
- Pestaña *Auto-disable*
  - ☐ Marque la casilla *Auto-disable* para los parámetros supervisados si ha especificado la acción `auto-disable` al menos una vez.

El cuadro de diálogo contiene las siguientes pestañas:
- [Global]
- [Auto-disable]
- [Link flap]
- [CRC/Fragments]
- [Overload detection]
- [Link speed/Duplex mode detection]

### [Global]

Active en esta pestaña la función *Port Monitor* y especifique los parámetros que la función *Port Monitor* está supervisando. Especifique también la acción que el dispositivo llevará a cabo si la función *Port Monitor* detecta que se han excedido los parámetros.

#### Operation

Operation

Activa/desactiva la función *Port Monitor* globalmente.

Valores posibles:
- `On`
  La función *Port Monitor* está activada.
- `Off` (configuración por defecto)
  La función *Port Monitor* está desactivada.

### Tabla

Port

Muestra el número de puerto.

Link flap on

Activa/desactiva la supervisión de inestabilidades de enlace en el puerto.

Valores posibles:

- `marked`
  La supervisión está activa.
  - La función *Port Monitor* supervisa las inestabilidades de enlace en el puerto.
  - Si el dispositivo detecta demasiados casos de inestabilidad, el dispositivo ejecutará la acción especificada en la columna *Action*.
  - En la pestaña *Link flap*, especifique los parámetros que se supervisarán.
- `unmarked` (configuración por defecto)
  La supervisión está inactiva.

CRC/Fragments on

Activa/desactiva la supervisión de errores de fragmentos/CRC detectados en el puerto.

Valores posibles:

- `marked`
  La supervisión está activa.
  - La función *Port Monitor* supervisa los errores de fragmentos/CRC detectados en el puerto.
  - Si el dispositivo detecta demasiados errores de fragmentos/CRC, el dispositivo ejecutará la acción especificada en la columna *Action*.
  - En la pestaña *CRC/Fragments*, especifique los parámetros que se supervisarán.
- `unmarked` (configuración por defecto)
  La supervisión está inactiva.

Duplex mismatch detection active

Activa/desactiva la supervisión de desajustes del dúplex en el puerto.

Valores posibles:

- `marked`
  La supervisión está activa.
  - La función *Port Monitor* supervisa los desajustes del dúplex en el puerto.
  - Si el dispositivo detecta demasiados desajustes del dúplex, el dispositivo ejecutará la acción especificada en la columna *Action*.
- `unmarked` (configuración por defecto)
  La supervisión está inactiva.

Overload detection on

Activa/desactiva la detección de sobrecarga en el puerto.

Valores posibles:

- `marked`
  La supervisión está activa.
  - La función *Port Monitor* supervisa la carga de datos en el puerto.
  - Si el dispositivo detecta una sobrecarga de datos en el puerto, el dispositivo ejecutará la acción especificada en la columna *Action*.
  - En la pestaña *Overload detection*, especifique los parámetros que se supervisarán.
- `unmarked` (configuración por defecto)
  La supervisión está inactiva.

Link speed/Duplex mode detection on

Activa/desactiva la supervisión de la velocidad de enlace y modo dúplex en el puerto.

Valores posibles:

- `marked`
  La supervisión está activa.
  - La función *Port Monitor* supervisa la velocidad de enlace y modo dúplex en el puerto.
  - Si el dispositivo detecta una combinación no permitida de velocidad de enlace y modo dúplex, el dispositivo ejecutará la acción especificada en la columna *Action*.
  - En la pestaña *Link speed/Duplex mode detection*, especifique los parámetros que se supervisarán.
- `unmarked` (configuración por defecto)
  La supervisión está inactiva.

Active condition

Muestra el parámetro supervisado que ha causado la acción en el puerto.

Valores posibles:

- `-`
  No hay parámetros supervisados.
  El dispositivo no lleva a cabo ninguna acción.
- *`Link flap`*
  Demasiados cambios de enlace durante el período observado.
- *`CRC/Fragments`*
  Demasiados errores de fragmentos/CRC durante el período observado.
- *`Duplex mismatch`*
  Desajuste del dúplex detectado.
- *`Overload detection`*
  Sobrecarga detectada durante el período observado.
- *`Link speed/Duplex mode detection`*
  Combinación inadmisible de velocidad y modo dúplex detectada.

Action

Especifica la acción que el dispositivo llevará a cabo si la función *Port Monitor* detecta que se han excedido los parámetros.

Valores posibles:

- `disable port`
  El dispositivo desactiva el puerto y envía una trampa SNMP.
  El LED de "Estado de enlace" del puerto parpadea 3 veces por período.
  - Para volver a activar el puerto, señale el puerto y haga clic en el botón ☰ y, a continuación, en el elemento *Reset*.
  - Si ya no se están sobrepasando los parámetros, la función *Auto-Disable* vuelve a activar el puerto correspondiente después del período de espera especificado. El requisito previo es que la casilla del parámetro supervisado en la pestaña *Auto-disable* esté marcada.
- `send trap`
  El dispositivo envía una trampa SNMP.
  Como requisito previo para enviar trampas SNMP, debe activar la función en el cuadro de diálogo *Diagnostics > Status Configuration > Alarms (Traps)* y especificar al menos un destino de la trampa.
- `auto-disable` (configuración por defecto)
  El dispositivo desactiva el puerto y envía una trampa SNMP.
  El LED de "Estado de enlace" del puerto parpadea 3 veces por período.
  El requisito previo es que la casilla del parámetro supervisado en la pestaña *Auto-disable* esté marcada.
  - El cuadro de diálogo *Diagnostics > Ports > Auto-Disable* muestra qué puertos están desactivados actualmente debido a que se han superado los parámetros.
  - La función *Auto-Disable* reactiva el puerto automáticamente. Para esto, vaya al cuadro de diálogo *Diagnostics > Ports > Auto-Disable* y especifique un período de espera para el puerto correspondiente en la columna *Reset timer [s]*.

Port status

Muestra el modo de funcionamiento del puerto.

Valores posibles:

- `up`
  El puerto está activado.
- `down`
  El puerto está desactivado.
- `notPresent`
  Puerto físico no disponible.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

Reset

Vuelve a activar el puerto señalado en la tabla y reinicia su contador a `0`. Esto afectará los contadores de los siguientes cuadros de diálogo:

- Cuadro de diálogo *Diagnostics > Ports > Port Monitor*
  - Pestaña *Link flap*
  - Pestaña *CRC/Fragments*
  - Pestaña *Overload detection*
- Cuadro de diálogo *Diagnostics > Ports > Auto-Disable*

## [Auto-disable]

En esta pestaña deberá activar la función *Auto-Disable* para los parámetros supervisados por la función *Port Monitor*.

### Tabla

Reason

Muestra los parámetros supervisados por la función *Port Monitor*.

Marque la casilla adyacente para que la función *Port Monitor* lleve a cabo la acción `auto-disable` si detecta que se han excedido los parámetros supervisados.

Auto-disable

Activa/desactiva la función *Auto-Disable* para los parámetros adyacentes.

Valores posibles:

- `marked`
  La función *Auto-Disable* para los parámetros adyacentes está activa.
  Si se han excedido los parámetros adyacentes y el valor `auto-disable` aparece especificado en la columna *Action*, el dispositivo llevará a cabo la función *Auto-Disable*.
- `unmarked` (configuración por defecto)
  La función *Auto-Disable* para los parámetros adyacentes está inactiva.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

Reset

Vuelve a activar el puerto señalado en la tabla y reinicia su contador a `0`. Esto afectará los contadores de los siguientes cuadros de diálogo:

- Cuadro de diálogo *Diagnostics > Ports > Port Monitor*
  - Pestaña *Link flap*
  - Pestaña *CRC/Fragments*
  - Pestaña *Overload detection*
- Cuadro de diálogo *Diagnostics > Ports > Auto-Disable*

## [Link flap]

En esta pestaña, especifique para cada puerto por separado los siguientes ajustes:

- Número de cambios de enlace.
- El período durante el cual la función *Port Monitor* supervisa un parámetro para detectar discrepancias.

También puede ver la cantidad de cambios de enlace que la función *Port Monitor* ha detectado hasta este momento.

La función *Port Monitor* supervisa los puertos para los que la casilla de la columna *Link flap on* está marcada en la pestaña *Global*.

### Tabla

Port

Muestra el número de puerto.

Sampling interval [s]

Especifica en segundos el período durante el cual la función *Port Monitor* supervisa un parámetro para detectar discrepancias.

Valores posibles:

- `1..180` (configuración por defecto: `10`)

Link flaps

Especifica el número de cambios de enlace.

Si la función *Port Monitor* detecta este número de cambios de enlace en el tiempo supervisado, el dispositivo lleva a cabo la acción especificada.

Valores posibles:

- `1..100` (configuración por defecto: `5`)

Last sampling interval

Muestra el número de errores que el dispositivo ha detectado durante el período que ha transcurrido.

Total

Muestra el número total de errores que el dispositivo ha detectado desde que se activó el puerto.

### Botones

Encontrará la descripción de los botones estándar en la sección "Botones" en página 17.

Reset

Vuelve a activar el puerto señalado en la tabla y reinicia su contador a `0`. Esto afectará los contadores de los siguientes cuadros de diálogo:

- Cuadro de diálogo *Diagnostics > Ports > Port Monitor*
  - Pestaña *Link flap*
  - Pestaña *CRC/Fragments*
  - Pestaña *Overload detection*
- Cuadro de diálogo *Diagnostics > Ports > Auto-Disable*

## [CRC/Fragments]

En esta pestaña, especifique para cada puerto por separado los siguientes ajustes:

- Índice de errores de fragmentos detectados.
- El período durante el cual la función *Port Monitor* supervisa un parámetro para detectar discrepancias.

También puede ver el índice de errores de fragmentos que el dispositivo ha detectado hasta este momento.

La función *Port Monitor* supervisa los puertos para los que la casilla de la columna *CRC/Fragments on* está marcada en la pestaña *Global*.

### Tabla

Port

Muestra el número de puerto.

Sampling interval [s]

Especifica en segundos el período durante el cual la función *Port Monitor* supervisa un parámetro para detectar discrepancias.

Valores posibles:

- `5..180` (configuración por defecto: `10`)

CRC/Fragments count [ppm]

Especifica el índice de errores de fragmentos (en partes por millón).

Si la función *Port Monitor* detecta este índice de errores de fragmentos en el tiempo supervisado, el dispositivo lleva a cabo la acción especificada.

Valores posibles:

- `1..1000000` (configuración por defecto: `1000`)

Last active interval [ppm]

Muestra el índice de errores de fragmentos que el dispositivo ha detectado durante el período que ha transcurrido.

Total [ppm]

Muestra el índice de errores de fragmentos que el dispositivo ha detectado desde que se activó el puerto.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

Reset

Vuelve a activar el puerto señalado en la tabla y reinicia su contador a `0`. Esto afectará los contadores de los siguientes cuadros de diálogo:

- Cuadro de diálogo *Diagnostics > Ports > Port Monitor*
  - Pestaña *Link flap*
  - Pestaña *CRC/Fragments*
  - Pestaña *Overload detection*
- Cuadro de diálogo *Diagnostics > Ports > Auto-Disable*

## [Overload detection]

En esta pestaña, especifique para cada puerto por separado los siguientes ajustes:

- Los valores límite de carga.
- El período durante el cual la función *Port Monitor* supervisa un parámetro para detectar discrepancias.

También puede ver el número de paquetes de datos que el dispositivo ha detectado hasta este momento.

La función *Port Monitor* supervisa los puertos para los que la casilla de la columna *Overload detection on* está marcada en la pestaña *Global*.

La función *Port Monitor* no supervisa ningún puerto que sea miembro de un grupo de agregación de enlaces.

### Tabla

Port

Muestra el número de puerto.

Traffic type

Especifica el tipo de paquetes de datos que el dispositivo tiene en cuenta al supervisar la carga en el puerto.

Valores posibles:

- `all`
  La función *Port Monitor* supervisa paquetes Broadcast, Multicast y Unicast.
- `bc` (configuración por defecto)
  La función *Port Monitor* solo supervisa paquetes Broadcast.
- `bc-mc`
  La función *Port Monitor* solo supervisa paquetes Broadcast y Multicast.

Threshold type

Especifica la unidad de la velocidad de transferencia:

Valores posibles:

- `pps` (configuración por defecto)
  paquetes por segundo
- `kbps`
  kbit por segundo
  Como requisito previo, el valor de la columna *Traffic type* = `all`.

Lower threshold

Especifica el límite inferior de la velocidad de transferencia.

La función *Auto-Disable* volverá a activar el puerto solo si la carga en el puerto es menor que el valor especificado aquí.

Valores posibles:

- `0..10000000` (configuración por defecto: `0`)

Upper threshold

Especifica el límite superior de la velocidad de transferencia.

Si la función *Port Monitor* detecta esta carga en el período supervisado, el dispositivo lleva a cabo la acción especificada.

Valores posibles:

- `0..10000000` (configuración por defecto: `0`)

Interval [s]

Especifica en segundos el período en el que la función *Port Monitor* observa un parámetro para detectar que se ha sobrepasado.

Valores posibles:

- `1..20` (configuración por defecto: `1`)

Packets

Muestra el número de paquetes Broadcast, Multicast y Unicast que el dispositivo ha detectado durante el período que ha transcurrido.

Broadcast packets

Muestra el número de paquetes Broadcast que el dispositivo ha detectado durante el período que ha transcurrido.

Multicast packets

Muestra el número de paquetes Multicast que el dispositivo ha detectado durante el período que ha transcurrido.

Kbit/s

Muestra la velocidad de transferencia en Kbits por segundo que el dispositivo ha detectado durante el período que ha transcurrido.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

Reset

Vuelve a activar el puerto señalado en la tabla y reinicia su contador a `0`. Esto afectará los contadores de los siguientes cuadros de diálogo:

- Cuadro de diálogo *Diagnostics > Ports > Port Monitor*
  - Pestaña *Link flap*
  - Pestaña *CRC/Fragments*
  - Pestaña *Overload detection*
- Cuadro de diálogo *Diagnostics > Ports > Auto-Disable*

## [Link speed/Duplex mode detection]

En esta pestaña, active las combinaciones de velocidad y modo dúplex permitidas para cada puerto.

La función *Port Monitor* supervisa los puertos para los que la casilla de la columna *Link speed/Duplex mode detection on* está marcada en la pestaña *Global*.

La función *Port Monitor* solo supervisa los puertos físicos activados.

### Tabla

Port

Muestra el número de puerto.

10 Mbit/s HDX

Activa/desactiva la supervisión del puerto para aceptar una combinación de Half-Dúplex y una velocidad de transferencia de 10 Mbits/s en el puerto.

Valores posibles:

- `marked`
  La supervisión del puerto tiene en cuenta la combinación de velocidad y dúplex.
- `unmarked`
  Si la supervisión del puerto detecta una combinación de velocidad y dúplex en el puerto, el dispositivo ejecutará la acción especificada en la pestaña *Global*.

10 Mbit/s FDX

Activa/desactiva la supervisión del puerto para aceptar una combinación de Full-Dúplex y una velocidad de transferencia de 10 Mbits/s en el puerto.

Valores posibles:

- `marked`
  La supervisión del puerto tiene en cuenta la combinación de velocidad y dúplex.
- `unmarked`
  Si la supervisión del puerto detecta una combinación de velocidad y dúplex en el puerto, el dispositivo ejecutará la acción especificada en la pestaña *Global*.

100 Mbit/s HDX

Activa/desactiva la supervisión del puerto para aceptar una combinación de Half-Dúplex y una velocidad de transferencia de 100 Mbits/s en el puerto.

Valores posibles:

- `marked`
  La supervisión del puerto tiene en cuenta la combinación de velocidad y dúplex.
- `unmarked`
  Si la supervisión del puerto detecta una combinación de velocidad y dúplex en el puerto, el dispositivo ejecutará la acción especificada en la pestaña *Global*.

100 Mbit/s FDX

Activa/desactiva la supervisión del puerto para aceptar una combinación de Full-Dúplex y una velocidad de transferencia de 100 Mbits/s en el puerto.

Valores posibles:

- `marked`
  La supervisión del puerto tiene en cuenta la combinación de velocidad y dúplex.
- `unmarked`
  Si la supervisión del puerto detecta una combinación de velocidad y dúplex en el puerto, el dispositivo ejecutará la acción especificada en la pestaña *Global*.

1,000 Mbit/s FDX

Activa/desactiva la supervisión del puerto para aceptar una combinación de Full-Dúplex y una velocidad de transferencia de 1 Gbits/s en el puerto.

Valores posibles:

- `marked`
  La supervisión del puerto tiene en cuenta la combinación de velocidad y dúplex.
- `unmarked`
  Si la supervisión del puerto detecta una combinación de velocidad y dúplex en el puerto, el dispositivo ejecutará la acción especificada en la pestaña *Global*.

2.5 Gbit/s FDX

Activa/desactiva el supervisor del puerto para aceptar una combinación de velocidad de datos dúplex completo y de 2,5 Gbit/s en el puerto.

Valores posibles:

- `marked`
  La supervisión del puerto tiene en cuenta la combinación de velocidad y dúplex.
- `unmarked`
  Si la supervisión del puerto detecta una combinación de velocidad y dúplex en el puerto, el dispositivo ejecutará la acción especificada en la pestaña *Global*.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

Reset

Vuelve a activar el puerto señalado en la tabla y reinicia su contador a `0`. Esto afectará los contadores de los siguientes cuadros de diálogo:

- Cuadro de diálogo *Diagnostics > Ports > Port Monitor*
  - Pestaña *Link flap*
  - Pestaña *CRC/Fragments*
  - Pestaña *Overload detection*
- Cuadro de diálogo *Diagnostics > Ports > Auto-Disable*

## 6.5.4 Auto-Disable

[Diagnostics > Ports > Auto-Disable]

La función *Auto-Disable* le permite desactivar los puertos supervisados automáticamente y volver a activarlos cuando desee.

Por ejemplo, la función *Port Monitor* y las funciones seleccionadas en el menú *Network Security* utilizan la función *Auto-Disable* para desactivar puertos si se exceden los parámetros supervisados.

Si ya no se están sobrepasando los parámetros, la función *Auto-Disable* vuelve a activar el puerto correspondiente después del período de espera especificado.

El cuadro de diálogo contiene las siguientes pestañas:
- [Port]
- [Status]

### [Port]

Esta pestaña muestra qué puertos están desactivados actualmente debido a que se han superado los parámetros. Si ya no se están sobrepasando los parámetros y ha especificado un período de espera en la columna *Reset timer [s]*, la función *Auto-Disable* vuelve a activar automáticamente el puerto correspondiente.

#### Tabla

Port

Muestra el número de puerto.

Reset timer [s]

Especifica el tiempo de espera en segundos después del cual la función *Auto-Disable* vuelve a activar el puerto.

Valores posibles:
- `0` (configuración por defecto)
  El temporizador está inactivo. El puerto permanece desactivado.
- `30..4294967295`
  Si ya no se están sobrepasando los parámetros, la función *Auto-Disable* vuelve a activar el puerto después del período de espera especificado aquí.

Error time

Muestra cuándo desactivó el dispositivo el puerto debido a que se excedieron los parámetros.

Remaining time [s]

Muestra el tiempo restante en segundos hasta que la función *Auto-Disable* vuelva a activar el puerto.

Component

Muestra el componente de software en el dispositivo que desactivó el puerto.

Valores posibles:

- `PORT_MON`
  *Port Monitor*
  Consulte el cuadro de diálogo *Diagnostics > Ports > Port Monitor*.
- `PORT_ML`
  *Port Security*
  Consulte el cuadro de diálogo *Network Security > Port Security*.
- `DHCP_SNP`
  *DHCP Snooping*
  Consulte el cuadro de diálogo *Network Security > DHCP Snooping*.
- `DOT1S`
  *BPDU guard*
  Consulte el cuadro de diálogo *Switching > L2-Redundancy > Spanning Tree > Global*.
- `DAI`
  *Dynamic ARP Inspection*
  Consulte el cuadro de diálogo *Network Security > Dynamic ARP Inspection*.

Reason

Muestra el parámetro supervisado que ha causado la desactivación del puerto.

Valores posibles:

- `none`
  No hay parámetros supervisados.
  El puerto está activado.
- `link-flap`
  Demasiados cambios de enlace. Consulte el cuadro de diálogo *Diagnostics > Ports > Port Monitor*, pestaña *Link flap*.
- `crc-error`
  Se han detectado demasiados errores de fragmentos/CRC. Consulte el cuadro de diálogo *Diagnostics > Ports > Port Monitor*, pestaña *CRC/Fragments*.
- `duplex-mismatch`
  Desajuste del dúplex detectado. Consulte el cuadro de diálogo *Diagnostics > Ports > Port Monitor*, pestaña *Global*.
- `dhcp-snooping`
  Demasiados paquetes DHCP de fuentes que no son de confianza. Consulte el cuadro de diálogo *Network Security > DHCP Snooping > Configuration*, pestaña *Port*.
- `arp-rate`
  Demasiados paquetes ARP de fuentes que no son de confianza. Consulte el cuadro de diálogo *Network Security > Dynamic ARP Inspection > Configuration*, pestaña *Port*.
- `bpdu-rate`
  BPDU de STP recibidos. Consulte el cuadro de diálogo *Switching > L2-Redundancy > Spanning Tree > Global*.
- `mac-based-port-security`
  Demasiados paquetes de datos de emisores no deseados. Consulte el cuadro de diálogo *Network Security > Port Security*.
- `overload-detection`
  Sobrecarga. Consulte el cuadro de diálogo *Diagnostics > Ports > Port Monitor*, pestaña *Overload detection*.

- `speed-duplex`
  Combinación inadmisible de velocidad y modo dúplex detectada. Consulte el cuadro de diálogo *Diagnostics > Ports > Port Monitor*, pestaña *Link speed/Duplex mode detection*.
- `Loop protection`
  Se ha detectado un bucle de red de capa 2 en el puerto. Consulte el cuadro de diálogo *Diagnostics > Loop Protection*, columna *Loop detected*.

Active

Muestra si el puerto está desactivado actualmente debido a que se han superado los parámetros.

Valores posibles:

- `marked`
  El puerto está desactivado en este momento.
- `unmarked`
  El puerto está activado.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## [Status]

Esta pestaña muestra los parámetros supervisados para los que la función *Auto-Disable* está activada.

### Tabla

Reason

Muestra los parámetros que el dispositivo supervisará.

Marque la casilla adyacente para que la función *Auto-Disable* desactive y, si corresponde, vuelva a activar el puerto si se han excedido los parámetros supervisados.

Category

Muestra a qué función pertenece el parámetro adyacente.

Valores posibles:

- `port-monitor`
  El parámetro pertenece a las funciones del menú *Diagnostics > Port > Port Monitor*.
- `network-security`
  El parámetro pertenece a las funciones del menú *Network Security*.
- `l2-redundancy`
  El parámetro pertenece a las funciones del menú *Switching > L2-Redundancy*.

Auto-disable

Muestra si la función *Auto-Disable* está activada/desactivada para el parámetro adyacente.

Valores posibles:

- `marked`
  La función *Auto-Disable* para los parámetros adyacentes está activa.
  La función *Auto-Disable* desactiva y, si corresponde, vuelve a activar el puerto correspondiente si se exceden los parámetros supervisados.
- `unmarked` (configuración por defecto)
  La función *Auto-Disable* para los parámetros adyacentes está inactiva.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

Reset

Vuelve a activar el puerto señalado en la tabla y reinicia su contador a `0`. Esto afectará los contadores de los siguientes cuadros de diálogo:

- Cuadro de diálogo *Diagnostics > Ports > Port Monitor*
  - Pestaña *Link flap*
  - Pestaña *CRC/Fragments*
  - Pestaña *Overload detection*
- Cuadro de diálogo *Diagnostics > Ports > Auto-Disable*

# 6.5.5 Port Mirroring

[ Diagnostics > Ports > Port Mirroring ]

La función *Port Mirroring* le permite copiar los paquetes de datos recibidos y enviados desde puertos seleccionados a un puerto de destino. Puede ver y procesar el flujo de datos utilizando un analizador o una sonda RMON, conectado a un puerto de destino. Los paquetes de datos permanecen sin modificar en el puerto de origen.

**Nota:** Para activar el acceso a la gestión del dispositivo a través del puerto de destino, marque la casilla *Allow management* en el cuadro *Destination port* antes de activar la función *Port Mirroring*.

### Operation

Operation

Activa/desactiva la función *Port Mirroring*.

Valores posibles:

- *On*
  La función *Port Mirroring* está activada.
  El dispositivo copia los paquetes de datos desde los puertos de origen seleccionados hasta el puerto de destino.
- *Off* (configuración por defecto)
  La función *Port Mirroring* está desactivada.

### Destination port

Primary port

Especifica el puerto de destino.

Los puertos adecuados son los puertos que no se utilizan para los siguientes propósitos:

- Puerto de origen
- Protocolos de redundancia L2

Valores posibles:

- `no Port` (configuración por defecto)
  Ningún puerto de destino seleccionado.
- `<Port number>`
  Número del puerto de destino. El dispositivo copia los paquetes de datos desde los puertos de origen hasta este puerto.

En el puerto de destino, el dispositivo solo añade una etiqueta VLAN a los paquetes de datos que el puerto de origen transmite. El puerto de destino transmite los paquetes de datos sin modificar que el puerto de origen recibe.

**Nota:** El puerto de destino necesita ancho de banda suficiente para absorber el flujo de datos. Si el flujo de datos copiado excede el ancho de banda del puerto de destino, el dispositivo descarta los paquetes de datos sobrantes en el puerto de destino.

Secondary port

Especifica un segundo puerto de destino. El requisito previo es que debe haber especificado un puerto principal.

Valores posibles:

- `no Port` (configuración por defecto)
  Ningún puerto de destino seleccionado.
- `<Port number>`
  Número del puerto de destino. El dispositivo copia los paquetes de datos desde los puertos de origen hasta este puerto.

Allow management

Activa/desactiva el acceso a la gestión del dispositivo mediante el puerto de destino.

Valores posibles:

- `marked`
  El acceso a la gestión del dispositivo mediante el puerto de destino está activo.
  El dispositivo permite a los usuarios tener acceso a la gestión del dispositivo a través del puerto de destino sin interrumpir la sesión *Port Mirroring* activa.
  - 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. El requisito previo para el acceso a la gestión del dispositivo mediante el puerto de destino es que el puerto de destino no sea miembro de la VLAN de administración del dispositivo.
- `unmarked` (configuración por defecto)
  El acceso a la gestión del dispositivo mediante el puerto de destino está inactivo.
  El dispositivo prohíbe el acceso a la gestión del dispositivo a través del puerto de destino.

## Tabla

Source port

Especifica el número de puerto.

Valores posibles:

- `<Port number>`

Enabled

Activa/desactiva la copia de paquetes de datos desde este puerto de origen hasta el puerto de destino.

Valores posibles:

- `marked`
  La copia de paquetes de datos está activa.
  El puerto está especificado como puerto de origen.

- `unmarked` (configuración por defecto)
  La copia de paquetes de datos está inactiva.
- (Pantalla sombreada)
  No es posible copiar los paquetes de datos para este puerto.
  Causas posibles:
  - El puerto ya está especificado como puerto de destino.
  - El puerto es un puerto lógico, no un puerto físico.

**Nota:** El dispositivo le permite activar todos los puertos físicos como puerto de origen, excepto para el puerto de destino.

Type

Especifica qué paquetes de datos copia el dispositivo al puerto de destino.

En el puerto de destino, el dispositivo solo añade una etiqueta VLAN a los paquetes de datos que el puerto de origen transmite. El puerto de destino transmite los paquetes de datos sin modificar que el puerto de origen recibe.

Valores posibles:

- `none` (configuración por defecto)
  Ningún paquete de datos.
- `tx`
  Paquetes de datos que el puerto de origen transmite.
- `rx`
  Paquetes de datos que el puerto de origen recibe.
- `txrx`
  Paquetes de datos que el puerto de origen transmite y recibe.

**Nota:** Con el ajuste `txrx`, el dispositivo copia paquetes de datos transmitidos y recibidos. Los puertos de destino necesitan al menos el ancho de banda correspondiente a la suma del canal de envío y recepción de los puertos de origen. Por ejemplo, para puertos similares, el puerto de destino está al 100 % de capacidad cuando el canal de envío y recepción de un puerto de origen están al 50 % de capacidad respectivamente.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

Reset config

Restablece los ajustes en el cuadro de diálogo a la configuración por defecto y transfiere los cambios a la memoria volátil del dispositivo (*RAM*).

# 6.6 LLDP

[ Diagnostics > LLDP ]

El dispositivo le permite recoger información sobre los dispositivos vecinos. Para ello, el dispositivo utiliza el Link Layer Discovery Protocol (LLDP). Con esta información, una estación de administración de red puede representar la estructura de su red.

Este menú le permite configurar la detección de la topología y mostrar la información recibida en forma de tabla.

El menú contiene los siguientes cuadros de diálogo:

- LLDP Configuration
- LLDP Topology Discovery

# 6.6.1 LLDP Configuration

[Diagnostics > LLDP > Configuration]

Este cuadro de diálogo le permite configurar la detección de la topología para todos los puertos.

### Operation

Operation

Activa/desactiva la función *LLDP*.

Valores posibles:

- `On` (configuración por defecto)
  La función *LLDP* está activada.
  La detección de la topología mediante LLDP está activa en el dispositivo.
- `Off`
  La función *LLDP* está desactivada.

### Configuration

Transmit interval [s]

Especifica en segundos el intervalo con el que el dispositivo transmite paquetes de datos LLDP.

Valores posibles:

- `5..32768` (configuración por defecto: `30`)

Transmit interval multiplier

Especifica el factor para determinar el valor de período de vida de los paquetes de datos LLDP.

Valores posibles:

- `2..10` (configuración por defecto: `4`)

El valor de período de vida codificado en la cabecera LLDP es el resultado de multiplicar este valor por el valor en el campo *Transmit interval [s]*.

Reinit delay [s]

Especifica en segundos el tiempo de retardo para la reinicialización del puerto.

Valores posibles:

- `1..10` (configuración por defecto: `2`)

Si se ha especificado el valor `Off` en la columna *Operation*, el dispositivo intentará reinicializar el puerto después de que haya transcurrido el tiempo especificado aquí.

Transmit delay [s]

Especifica en segundos el tiempo de retardo para la transmisión de los paquetes de datos LLDP después de que haya cambios en la configuración del dispositivo.

Valores posibles:

- `1..8192` (configuración por defecto: `2`)

El valor recomendado se encuentra entre un mínimo de `1` y un máximo de un cuarto del valor del campo *Transmit interval [s]*.

Notification interval [s]

Especifica el intervalo en segundos para la transmisión de notificaciones LLDP.

Valores posibles:

- `5..3600` (configuración por defecto: `5`)

Después de transmitir una trampa de notificación, el dispositivo espera al menos durante el tiempo especificado aquí antes de transmitir la siguiente trampa de notificación.

### Tabla

Port

Muestra el número de puerto.

Operation

Especifica si el puerto transmite y recibe paquetes de datos LLDP.

Valores posibles:

- *`transmit`*
  El puerto transmite paquetes de datos LLDP pero no guarda información sobre los dispositivos vecinos.
- *`receive`*
  El puerto recibe paquetes de datos LLDP pero no transmite información a los dispositivos vecinos.
- *`receive and transmit`* (configuración por defecto)
  El puerto transmite paquetes de datos LLDP y guarda información sobre los dispositivos vecinos.
- *`disabled`*
  El puerto no transmite paquetes de datos LLDP y no guarda información sobre los dispositivos vecinos.

Notification

Activa/desactiva las notificaciones LLDP en el puerto.

Valores posibles:

- `marked`
  Las notificaciones LLDP están activas en el puerto.
- `unmarked` (configuración por defecto)
  Las notificaciones LLDP no están activas en el puerto.

Transmit port description

Activa/desactiva la transmisión de un TLV (Tipo Longitud Valor) con la descripción del puerto.

Valores posibles:

- `marked` (configuración por defecto)
  La transmisión del TLV está activa.
  El dispositivo transmite el TLV con la descripción del puerto.
- `unmarked`
  La transmisión del TLV no está activa.
  El dispositivo no transmite el TLV con la descripción del puerto.

Transmit system name

Activa/desactiva la transmisión de un TLV (Tipo Longitud Valor) con el nombre del dispositivo.

Valores posibles:

- `marked` (configuración por defecto)
  La transmisión del TLV está activa.
  El dispositivo transmite el TLV con el nombre del dispositivo.
- `unmarked`
  La transmisión del TLV no está activa.
  El dispositivo no transmite el TLV con el nombre del dispositivo.

Transmit system description

Activa/desactiva la transmisión del TLV (Tipo Longitud Valor) con la descripción del sistema.

Valores posibles:

- `marked` (configuración por defecto)
  La transmisión del TLV está activa.
  El dispositivo transmite el TLV con la descripción del sistema.
- `unmarked`
  La transmisión del TLV no está activa.
  El dispositivo no transmite el TLV con la descripción del sistema.

Transmit system capabilities

Activa/desactiva la transmisión del TLV (Tipo Longitud Valor) con las capacidades del sistema.

Valores posibles:

- `marked` (configuración por defecto)
  La transmisión del TLV está activa.
  El dispositivo transmite el TLV con las capacidades del sistema.
- `unmarked`
  La transmisión del TLV no está activa.
  El dispositivo no transmite el TLV con las capacidades del sistema.

Neighbors (max.)

Limita la cantidad de dispositivos vecinos que se registrarán para este puerto.

Valores posibles:

- `1..50` (configuración por defecto: `10`)

FDB mode

Especifica qué función utiliza el dispositivo para registrar los dispositivos vecinos en este puerto.

Valores posibles:

- `lldpOnly`
  El dispositivo solo utiliza paquetes de datos LLDP para registrar los dispositivos vecinos en este puerto.
- `macOnly`
  El dispositivo utiliza direcciones MAC aprendidas para registrar los dispositivos vecinos en este puerto. El dispositivo solo utiliza la dirección MAC si no hay otra entrada en la tabla de direcciones (FDB, base de datos de reenvíos) para este puerto.
- `both`
  El dispositivo utiliza paquetes de datos LLDP y direcciones MAC aprendidas para registrar los dispositivos vecinos en este puerto.
- `autoDetect` (configuración por defecto)
  Si el dispositivo recibe paquetes de datos LLDP en este puerto, el dispositivo funcionará igual que si tuviera la configuración `lldpOnly`. En caso contrario, el dispositivo funcionará igual que si tuviera la configuración `macOnly`.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## 6.6.2 LLDP Topology Discovery

[Diagnostics > LLDP > Topology Discovery]

Los dispositivos en redes envían notificaciones en forma de paquetes, también conocidos como "LLDPDU" (unidades de datos LLDP). Los datos que se envían y reciben mediante LLDPDU son útiles por múltiples razones. De este modo, el dispositivo detecta qué dispositivos de la red son vecinos y mediante qué puertos están conectados.

El cuadro de diálogo le permite mostrar la red y detectar los dispositivos conectados junto con sus características específicas.

El cuadro de diálogo contiene las siguientes pestañas:
- [LLDP]
- [LLDP-MED]

### [LLDP]

La pestaña muestra la información LLDP recogida para los dispositivos vecinos. Con esta información, una estación de administración de red puede representar la estructura de su red.

Si en un puerto hay conectados dispositivos con la función de detección de topología deshabilitada, estos no aparecen en la tabla de topología.

Cuando solo dispositivos sin la detección de topología activa están conectados a un puerto, la tabla contiene una línea para que el puerto represente todos los dispositivos. La línea contiene el número de dispositivos conectados.

La tabla de direcciones de la base de datos de reenvíos (FDB) contiene las direcciones MAC de los dispositivos que la tabla de topología mantiene ocultos para que sea más sencilla de comprender.

Cuando utilice un puerto para conectar varios dispositivos, por ejemplo, mediante un concentrador, la tabla contiene una línea por cada dispositivo conectado.

#### Tabla

Port

Muestra el número de puerto.

Neighbor identifier

Muestra el ID del chasis del dispositivo vecino. Puede ser la dirección MAC básica del dispositivo vecino, por ejemplo.

FDB

Muestra si el dispositivo conectado tiene la compatibilidad LLDP activa.

Valores posibles:

- `marked`
  El dispositivo conectado no tiene la compatibilidad LLDP activa.
  El dispositivo utiliza información de su tabla de direcciones (FDB, Forwarding Database)
- `unmarked` (configuración por defecto)
  El dispositivo conectado tiene la compatibilidad LLDP activa.

Neighbor IP address

Muestra la dirección IP con la que es posible el acceso a la gestión del dispositivo vecino.

Neighbor port description

Muestra una descripción para el puerto del dispositivo vecino.

Neighbor system name

Muestra el nombre del dispositivo vecino.

Neighbor system description

Muestra una descripción del dispositivo vecino.

Port ID

Muestra el ID del puerto a través del cual el dispositivo vecino está conectado al dispositivo.

Autonegotiation supported

Muestra si el puerto del dispositivo vecino es compatible con la configuración automática.

Autonegotiation

Muestra si la configuración automática está activada en el puerto del dispositivo vecino.

PoE supported

Muestra si el puerto del dispositivo vecino es compatible con Power over Ethernet (PoE).

PoE enabled

Muestra si Power over Ethernet (PoE) está activado en el puerto del dispositivo vecino.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## [LLDP-MED]

LLDP para dispositivos de punto final multimedia (LLDP-MED) es una extensión de LLDP que funciona entre dispositivos de punto final y dispositivos de red. Proporciona específicamente soporte para las aplicaciones VoIP. En este papel de apoyo, proporciona un conjunto adicional de mensajes de advertencia comunes, Tipo Longitud Valor (TLV). El dispositivo utiliza los TLV para funciones de detección, como la política de red, Power over Ethernet, la administración de inventario y la información de ubicación.

### Tabla

Port

Muestra el número de puerto.

Device class

Muestra el la clase del dispositivo conectado de manera remota.

- Un valor de `notDefined` indica que el dispositivo tiene capacidades no cubiertas por ninguna de las clases *LLDP-MED*.
- Un valor de `endpointClass1..3` indica que el dispositivo tiene capacidades de "clase de punto final 1 a 3".
- Un valor de `networkConnectivity` indica que el dispositivo tiene capacidades de dispositivo de conectividad de red.

VLAN ID

Muestra la extensión del Identificador VLAN para el sistema remoto conectado a este puerto, tal y como se define en la norma IEEE 802.3.

- El dispositivo utiliza un valor de `1` a `4042` para especificar un ID de VLAN del puerto válido.
- El dispositivo muestra el valor `0` para paquetes con etiqueta de prioridad. Esto significa que solo la prioridad 802.1D es relevante y el dispositivo utilizará el ID de VLAN por defecto en el puerto de acceso.

Priority

Muestra el valor de la prioridad 802.1D, asociado con el sistema remoto conectado al puerto.

DSCP

Muestra el valor de Punto de código de servicios diferenciados (DSCP), asociado con el sistema remoto conectado al puerto.

Unknown bit status

Muestra el estado de bit desconocido del tráfico entrante.

- Un valor de `true` indica que no se conoce la política de red para el tipo de aplicación especificado en ese momento. En este caso, el ID de VLAN ignora la prioridad de Capa 2 y el valor del campo *DSCP*.
- Un valor de `false` indica que hay una política de red especificada.

Tagged bit status

Muestra el estado de bit etiquetado.

- Un valor de `true` indica que la aplicación utiliza una VLAN etiquetada.
- Un valor de `false` indica que el dispositivo utiliza el funcionamiento de VLAN sin etiquetar para este tipo de aplicación específico. En este caso, el dispositivo ignora el ID de VLAN y la prioridad de Capa 2. Sin embargo, el valor de DSCP es relevante.

Hardware revision

Muestra la cadena de revisión de hardware específico del proveedor, tal y como indica el punto final remoto.

Firmware revision

Muestra la cadena de revisión de firmware específico del proveedor, tal y como indica el punto final remoto.

Software revision

Muestra la cadena de revisión de software específico del proveedor, tal y como indica el punto final remoto.

Serial number

Muestra el número de serie específico del proveedor, tal y como indica el punto final remoto.

Manufacturer name

Muestra el nombre del fabricante específico del proveedor, tal y como indica el punto final remoto.

Model name

Muestra el nombre del modelo específico del proveedor, tal y como indica el punto final remoto.

Asset ID

Muestra el identificador de seguimiento de archivos específico del proveedor, tal y como indica el punto final remoto.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

# 6.7 Loop Protection

[ Diagnostics > Loop Protection ]

La función *Loop Protection* 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 a una configuración incorrecta 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.

En topologías de red redundantes, normalmente hay activos varios protocolos de redundancia. Normalmente se debe desactivar la función *Spanning Tree* en los puertos implicados en otros protocolos de redundancia. Los protocolos de redundancia ya ayudan a evitar bucles.

### Operation

Operation

Activa/desactiva la función *Loop Protection*.

Valores posibles:

▶ `On`
La función *Loop Protection* está activada.
– En puertos activos y pasivos, el dispositivo evalúa paquetes de *detección de bucles* recibidos.
En puertos activos, el dispositivo envía paquetes de *detección de bucles* a intervalos regulares tal y como se especifica en el campo *Transmit interval*.
El requisito previo es que la función *Loop Protection* esté activa en el puerto.
– El dispositivo permite supervisar bucles de Ethernet con el contacto de la señal. Consulte el cuadro de diálogo *Diagnostics > Status Configuration > Signal Contact > Signal Contact 1*, casilla de verificación del parámetro *Ethernet loops*.

▶ `Off` (configuración por defecto)
La función *Loop Protection* está desactivada.
El dispositivo no envía paquetes de *detección de bucles* ni evalúa paquetes de *detección de bucles* recibidos.

### Global

Transmit interval

Especifica el intervalo en segundos en el que el dispositivo envía paquetes de *detección de bucles* si la función *Loop Protection* está activa en el puerto.

Valores posibles:

- `1..10`

Receive threshold

Especifica el valor de umbral correspondiente al número de paquetes de *detección de bucles* recibidos en una fila. Si el número alcanza o supera este umbral, el dispositivo llevará a cabo la acción especificada en la columna *Action*.

Valores posibles:

- `1..50`

### Configuration

Auto-disable

Activa/desactiva la función *Auto-Disable* para la *Loop Protection*.

Valores posibles:

- `marked`
  La función *Auto-Disable* de *Loop Protection* está activa.
  El requisito previo para la desactivación del puerto es que la acción *auto-disable* o *all* se haya especificado en la columna *Action*.
  El dispositivo le permite especificar el período de espera en segundos que desea que transcurra después de que la función *Auto-Disable* active el puerto de nuevo. Para ello, en el cuadro de diálogo *Diagnostics > Ports > Auto-Disable*, especifique el período de espera en la columna *Reset timer [s]*.
- `unmarked` (configuración por defecto)
  La función *Auto-Disable* de *Loop Protection* está inactiva.

### Tabla

Port

Muestra el número de puerto.

Active

Activa/desactiva la función *Loop Protection* en el puerto.

Valores posibles:

- `marked`
  La función *Loop Protection* está activa en el puerto.
  Active la función únicamente en puertos que no formen parte de una ruta de red redundante. Esto ayuda a evitar un apagado accidental de rutas de red redundantes.
  Si el dispositivo recibe un paquete de *detección de bucles* en este puerto, enviado desde otro puerto del mismo dispositivo, el dispositivo realizará la acción especificada en la columna *Action*.
- `unmarked` (configuración por defecto)
  La función *Loop Protection* está inactiva en el puerto. El puerto no envía paquetes de *detección de bucles* ni evalúa paquetes de *detección de bucles* recibidos.

Mode

Especifica el comportamiento de la función *Loop Protection* en el puerto.

Valores posibles:

- *active*
  El dispositivo envía paquetes de *detección de bucles* y evalúa paquetes de *detección de bucles* recibidos.
- *passive*
  El dispositivo evalúa paquetes de *detección de bucles* recibidos.

Action

Especifica la acción que el dispositivo lleva a cabo cuando detecta un bucle de red de capa 2 en este puerto.

Valores posibles:

- *trap*
  El dispositivo envía una trampa.
- *auto-disable*
  El dispositivo desactiva el puerto mediante la función *Auto-Disable*.
  El requisito previo para la desactivación del puerto es que la casilla de verificación *Auto-disable* del cuadro *Configuration* esté marcada.
- *all*
  El dispositivo envía una trampa. A continuación, el dispositivo desactiva el puerto utilizando la función *Auto-Disable*.
  El requisito previo para la desactivación del puerto es que la casilla de verificación *Auto-disable* del cuadro *Configuration* esté marcada.

VLAN ID

Especifica la VLAN en la que el dispositivo envía los paquetes de *detección de bucles*.

Valores posibles:

- `0` (configuración por defecto)
  El dispositivo envía los paquetes de *detección de bucles* sin una etiqueta VLAN.
- `1..4042`
  El dispositivo envía los paquetes de *detección de bucles* en la VLAN especificada. El requisito previo consiste en que la VLAN ya esté configurada y que el puerto sea miembro de la VLAN. Consulte el cuadro de diálogo *Switching > VLAN > Port*.

Loop detected

Muestra si el dispositivo ha detectado un bucle de red de capa 2 en el puerto.

Valores posibles:

- *yes*
  El dispositivo ha detectado un bucle de red de capa 2 en el puerto.
  Una vez finalizado el bucle y activado el puerto de nuevo, el dispositivo restablecerá el valor a *no*.
- *no*
  El dispositivo no ha detectado un bucle de red de capa 2 en el puerto.

Loop count

Muestra el número de bucles que ha detectado el dispositivo en el puerto desde el último restablecimiento de las estadísticas del puerto o desde el último reinicio del dispositivo.

Last loop time

Muestra el momento en el que el dispositivo detectó el último bucle en el puerto.

El requisito previo de la evaluación correcta del valor es que sincronice la hora del sistema del dispositivo con la hora de referencia adecuada. Consulte el cuadro de diálogo *Time > Basic Settings*.

Sent frames

Muestra el número de paquetes de *detección de bucles* enviados en el puerto desde el último restablecimiento de las estadísticas del puerto o desde el último reinicio del dispositivo.

Received frames

Muestra el número de paquetes de *detección de bucles* enviados y recibidos en el puerto desde el último restablecimiento de las estadísticas del puerto o desde el último reinicio del dispositivo.

Discarded frames

Muestra el número de paquetes de *detección de bucles* descartados en el puerto.

Ejemplos de motivos para el descarte de paquetes:

- El dispositivo detecta paquetes con un formato incorrecto.
- El dispositivo detecta paquetes con marcas de tiempo caducadas (paquetes recibidos más de 5 segundos después de su envío).

- El dispositivo ha recibido un paquete de datos con una información de VLAN inesperada.
- El dispositivo detecta paquetes recibidos en un puerto desactivado.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

Clear port statistics

Restablece los valores de las siguientes columnas:

- *Loop count*
- *Sent frames*
- *Received frames*

# 6.8 Report

[ Diagnostics > Report ]

El menú contiene los siguientes cuadros de diálogo:

- Report Global
- Persistent Logging
- System Log
- Audit Trail

# 6.8.1 Report Global

[Diagnostics > Report > Global]

El dispositivo le permite registrar eventos específicos utilizando las siguientes salidas:
- en la consola
- en uno o más de los servidores Syslog
- en una conexión con la interfaz de línea de comando configurada mediante el uso de SSH
- en una conexión a la interfaz de línea de comando configurada mediante el uso de Telnet

En este cuadro de diálogo, especifique la configuración necesaria. Al asignar la gravedad, especificará qué eventos registrará el dispositivo.

El cuadro de diálogo le permite guardar un archivo ZIP con información del sistema en su PC.

### Console logging

Operation

Activa/desactiva la función *Console logging*.

Valores posibles:
- *On*
  La función *Console logging* está activada.
  El dispositivo registra los eventos en la consola.
- *Off* (configuración por defecto)
  La función *Console logging* está desactivada.

Severity

Especifica el nivel mínimo de gravedad de los eventos. El dispositivo registra los eventos con este nivel y con niveles más urgentes de gravedad.

El dispositivo envía los mensajes en la interfaz serie.

Valores posibles:
- `emergency`
- `alert`
- `critical`
- `error`
- `warning` (configuración por defecto)
- `notice`
- `informational`
- `debug`

### Buffered logging

El dispositivo almacena en búfer los eventos registrados en 2 áreas de almacenamiento individuales para mantener las entradas de registro de eventos urgentes.

Este cuadro de diálogo le permite especificar la gravedad mínima de los eventos que el dispositivo debe registrar en el área de almacenamiento en búfer con una prioridad más alta.

Severity

Especifica el nivel mínimo de gravedad de los eventos. El dispositivo registra en el búfer entradas de registro para los eventos con este nivel y con niveles más urgentes de gravedad en el área de almacenamiento con una prioridad más alta.

Valores posibles:

- `emergency`
- `alert`
- `critical`
- `error`
- `warning` (configuración por defecto)
- `notice`
- `informational`
- `debug`

### SNMP logging

Cuando activa el registro de peticiones SNMP, el dispositivo envía estas como eventos con la gravedad preconfigurada `notice` a la lista de servidores Syslog. La gravedad mínima preconfigurada para una entrada del servidor SYSLOG es `critical`.

Hay varias posibilidades de cambiar la configuración por defecto para enviar solicitudes de SNMP a un servidor Syslog. Seleccione aquella que sea más adecuada a sus necesidades.

- ☐ Establezca la gravedad con la cual desea que el dispositivo cree solicitudes SNMP como eventos en `warning` o `error`. Cambie la gravedad mínima para una entrada de Syslog para uno o más servidores Syslog del mismo valor.
  También tiene la opción de crear una entrada de servidor Syslog separada para ello.
- ☐ Establezca solamente la gravedad para solicitudes SNMP en `critical` o un valor superior. El dispositivo enviará entonces peticiones SNMP como eventos con la gravedad `critical` o superior a los servidores Syslog.
- ☐ Establezca solo la gravedad mínima de una o más entradas de servidor Syslog en `notice` o un valor inferior. Entonces será posible que el dispositivo envíe muchos eventos a los servidores Syslog.

Log SNMP get request

Activa/desactiva el inicio de sesión de SNMP Get requests.

Valores posibles:

- *On*
  El inicio de sesión está activado.
  El dispositivo registra SNMP Get requests como eventos en el Syslog.
  Seleccione la gravedad para este evento en la lista desplegable *Severity get request*.
- *Off* (configuración por defecto)
  El inicio de sesión está desactivado.

Log SNMP set request

Activa/desactiva el inicio de sesión de SNMP Set requests.

Valores posibles:

- *On*
  El inicio de sesión está activado.
  El dispositivo registra SNMP Set requests como eventos en el Syslog.
  Seleccione la gravedad para este evento en la lista desplegable *Severity set request*.
- *Off* (configuración por defecto)
  El inicio de sesión está desactivado.

Severity get request

Especifica la gravedad del evento que el dispositivo debe registrar para SNMP Get requests.

Valores posibles:

- emergency
- alert
- critical
- error
- warning
- notice (configuración por defecto)
- informational
- debug

Severity set request

Especifica la gravedad del evento que el dispositivo debe registrar para SNMP Set requests.

Valores posibles:

- emergency
- alert
- critical
- error
- warning
- notice (configuración por defecto)
- informational
- debug

### CLI logging

Operation

Activa/desactiva la función *CLI logging*.

Valores posibles:

- `On`
  La función *CLI logging* está activada.
  El dispositivo registra todos los comandos recibidos mediante la interfaz de línea de comando.
- `Off` (configuración por defecto)
  La función *CLI logging* está desactivada.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

Download support information

Genera un archivo ZIP que el navegador web le permitirá descargar desde el dispositivo.

El archivo ZIP contiene información del sistema sobre el dispositivo. Encontrará una explicación de los archivos contenidos en el archivo ZIP en la siguiente sección.

### Información de ayuda: archivos contenidos en el archivo ZIP

| Nombre de archivo | Formato | Observaciones |
|---|---|---|
| `audittrail.html` | HTML | Contiene el registro en orden cronológico de los eventos del sistema y los cambios de usuario guardados en el Audit Trail. |
| `defaultconfig.xml` | XML | Contiene el perfil de configuración con la configuración por defecto. |
| `script` | TEXT | Contiene la salida del comando `show running-config script`. |
| `runningconfig.xml` | XML | Contiene el perfil de configuración con la configuración de funcionamiento actual. |
| `supportinfo.html` | TEXT | Contiene información de servicio interna del dispositivo. |
| `systeminfo.html` | HTML | Contiene información sobre la configuración actual y los parámetros de funcionamiento. |
| `systemlog.html` | HTML | Contiene los eventos registrados en el archivo de registro. Consulte el cuadro de diálogo *Diagnostics > Report > System Log*. |

### Significado de los niveles de gravedad de eventos

| Gravedad | Significado |
|---|---|
| `emergency` | El dispositivo no está listo para funcionar |
| `alert` | Se requiere la intervención inmediata del usuario |
| `critical` | Estado crítico |

| Gravedad | Significado |
|---|---|
| `error` | Estado de error |
| `warning` | Warning (advertencia) |
| `notice` | Importante, estado normal |
| `informational` | Mensaje informal |
| `debug` | Mensaje de depuración |

## 6.8.2 Persistent Logging

[ Diagnostics > Report > Persistent Logging ]

El dispositivo le permite guardar entradas de registro de forma permanente en un archivo en la memoria externa. Por lo tanto, tendrá acceso a las entradas de registro incluso después de reiniciar el dispositivo.

En este cuadro de diálogo, puede limitar el tamaño del archivo de registro y especificar la gravedad mínima para los eventos a guardar. Cuando el archivo de registro alcanza el tamaño especificado, el dispositivo almacena este archivo y guarda las siguientes entradas de registro en un nuevo archivo.

El dispositivo muestra en la tabla los archivos de registro almacenados en la memoria externa. En cuanto se alcanza el número máximo de archivos especificados, el dispositivo elimina el archivo más antiguo y proporciona un nuevo nombre al resto de archivos. Esto ayuda a asegurar que haya espacio de almacenamiento suficiente en la memoria externa.

**Nota:** Compruebe que haya una memoria externa conectada. Para comprobar si hay una memoria externa conectada, consulte la columna *Status* del cuadro de diálogo *Basic Settings > External Memory*. Recomendamos que supervise la conexión de la memoria externa mediante la función *Device Status*; consulte el parámetro *External memory removal* en el cuadro de diálogo *Diagnostics* > Status Configuration > *Device Status*.

### Operation

Operation

Activa/desactiva la función *Persistent Logging*.

Active está función únicamente si la memoria externa está disponible en el dispositivo.

Valores posibles:

- *On* (configuración por defecto)
  La función *Persistent Logging* está activada.
  El dispositivo guarda las entradas de registro en un archivo en la memoria externa.
- *Off*
  La función *Persistent Logging* está desactivada.

### Configuration

Max. file size [kbyte]

Especifica el tamaño máximo de los archivos de registro en KBytes. Cuando el archivo de registro alcanza el tamaño especificado, el dispositivo almacena este archivo y guarda las siguientes entradas de registro en un nuevo archivo.

Valores posibles:

- `0..4096` (configuración por defecto: `1024`)

El valor `0` desactiva el almacenamiento de entradas de registro en el archivo de registro.

Files (max.)

Especifica el número de archivos de registro que el dispositivo mantiene en la memoria externa.

En cuanto se alcanza el número máximo de archivos especificados, el dispositivo elimina el archivo más antiguo y proporciona un nuevo nombre al resto de archivos.

Valores posibles:

- `0..25` (configuración por defecto: `4`)

El valor `0` desactiva el almacenamiento de entradas de registro en el archivo de registro.

Severity

Especifica el nivel mínimo de gravedad de los eventos. El dispositivo guarda la entrada de registro para los eventos con este nivel y con niveles más urgentes de gravedad en el archivo de registro de la memoria externa.

Valores posibles:

- `emergency`
- `alert`
- `critical`
- `error`
- `warning` (configuración por defecto)
- `notice`
- `informational`
- `debug`

Log file target

Especifica el dispositivo de memoria externa para el registro.

Valores posibles:

- `usb`
  Memoria USB externa (EAM)

### Tabla

Index

Muestra el número de índice al que la entrada de la tabla hace referencia.

Valores posibles:

- `1..25`

El dispositivo asigna este número automáticamente.

File name

Muestra el nombre de archivo del archivo de registro en la memoria externa.

Valores posibles:

- `messages`
- `messages.X`

File size [byte]

Muestra el tamaño del archivo de registro en la memoria externa en bytes.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

Delete persistent log file

Elimina los archivos de registro de la memoria externa.

## 6.8.3 System Log

[ Diagnostics > Report > System Log ]

El dispositivo registra los eventos internos del dispositivo en un archivo de registro (System Log).

Este cuadro de diálogo muestra el archivo de registro (System Log). El cuadro de diálogo le permite guardar un archivo de registro en formato HTML en su PC.

Para buscar términos de búsqueda en el archivo de registro, utilice la función de búsqueda de su navegador web.

El archivo de registro se mantiene hasta que se reinicie el dispositivo. Después del reinicio, el dispositivo vuelve a crear el archivo.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

Save log file

Abre la página HTML en una nueva ventana o pestaña del navegador web. Puede guardar la página HTML en su PC con el comando adecuado del navegador web.

Delete log file

Elimina los eventos registrados del archivo de registro.

## 6.8.4 Audit Trail

[ Diagnostics > Report > Audit Trail ]

Este cuadro de diálogo muestra el archivo de registro (Audit Trail). El cuadro de diálogo le permite guardar un archivo de registro como un archivo HTML en su PC.

Para buscar términos de búsqueda en el archivo de registro, utilice la función de búsqueda de su navegador web.

El dispositivo registra eventos del sistema y acciones de escritura por parte del usuario en el dispositivo. Esto le permitirá hacer un seguimiento de QUIÉN ha cambiado el QUÉ en el dispositivo y CUÁNDO. El requisito previo es que su cuenta de usuario tenga asignado el rol de usuario `auditor` o `administrator`.

El dispositivo registra las siguientes acciones del usuario, entre otras:
- Un usuario que inicia sesión mediante la interfaz de línea de comando (local o de manera remota)
- Un usuario que cierra sesión manualmente
- Cierre de sesión automático de un usuario en la interfaz de línea de comando después de un período de inactividad especificado
- Reinicio del dispositivo
- Bloqueo de una cuenta de usuario debido a demasiados intentos fallidos de iniciar sesión.
- Bloqueo del acceso a la gestión del dispositivo debido a intentos fallidos de iniciar sesión
- Comandos ejecutados en la interfaz de línea de comando, además de los comandos `show`
- Cambios en las variables de configuración
- Cambios en la hora del sistema
- Operaciones de transferencia de archivos, incluyendo actualizaciones de firmware
- Cambios de configuración mediante Ethernet Switch Configurator
- Actualizaciones de firmware y configuración automática del dispositivo mediante la memoria externa
- Apertura y cierre de SNMP a través de un túnel HTTPS

El dispositivo no registra contraseñas. Las entradas registradas están protegidas contra escritura y permanecen guardadas en el dispositivo después de un reinicio.

Durante el reinicio, es posible acceder a la supervisión del sistema con la configuración por defecto del dispositivo. Si un atacante consigue acceso físico al dispositivo, podrá reiniciar la configuración del dispositivo a sus valores de fábrica con la supervisión del sistema. Después de esto, se podrá acceder al dispositivo y al archivo de registro usando una contraseña estándar.

**⚠ ADVERTENCIA**

**OPERACIÓN INESPERADA DEL EQUIPO**

Tome las medidas adecuadas para restringir el acceso físico al dispositivo. Si no, desactive el acceso a la supervisión del sistema. Consulte el cuadro de diálogo *Diagnostics > System > Selftest*, casilla *SysMon1 is available*.

**El incumplimiento de estas instrucciones puede causar la muerte, heridas graves o daños en el equipo.**

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

Save audit trail file

Abre la página HTML en una nueva ventana o pestaña del navegador web. Puede guardar la página HTML en su PC con el comando adecuado del navegador web.

# 7 Advanced

El menú contiene los siguientes cuadros de diálogo:
- DHCP L2 Relay
- DHCP Server
- DNS
- Industrial Protocols
- Digital IO Module
- Command Line Interface

## 7.1 DHCP L2 Relay

[Advanced > DHCP L2 Relay]

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 L2 para añadir la información del cliente DHCP. Los *agentes de retransmisión* L3 y los servidores DHCP necesitan la información del cliente DHCP para asignar una dirección IP y una configuración a los clientes.

Cuando está activa, la retransmisión añade la información de *Option 82* configurada en este cuadro de diálogo a los paquetes antes de retransmitir las solicitudes DHCP de los clientes al servidor. Los campos *Option 82* proporcionan información única sobre el cliente y la retransmisión. Este identificador único está formado por un *ID de circuito* para el cliente y un *ID remoto* para la retransmisión.

Además de los campos de tipo, longitud y Multicast, el *ID de circuito* incluye el ID de la VLAN, el número de unidad, el número de ranura y el número de puerto del cliente conectado.

El *ID remoto* consta de un campo de tipo y longitud, y de una dirección MAC, una dirección IP, un identificador de cliente o una descripción del dispositivo definido por el usuario. El identificador de cliente es el nombre del sistema definido por el usuario para el dispositivo.

Para el protocolo DHCPv6, el dispositivo 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:

- Mensajes *Relay-Forward*
  El *agente de retransmisión* reenvía mensajes *Relay-Forward* que contienen información única sobre el cliente. Entre la información del cliente se incluye la dirección de mismo nivel, es decir, la dirección local del vínculo IPv6 del cliente y la información del *ID de interfaz*. La información del *ID de interfaz*, también denominada *Option 18*, proporciona información que identifica la interfaz por la que se ha enviado la solicitud del cliente.
- Mensajes *Relay-Reply*
  El servidor DHCPv6 envía mensajes *Relay-Reply*. El *agente de retransmisión* valida los mensajes para incluir la información del mensaje *Relay-Forward* inicial. Si la información es válida, el *agente de retransmisión* reenvía el paquete al cliente.

El menú contiene los siguientes cuadros de diálogo:

- DHCP L2 Relay Configuration
- DHCP L2 Relay Statistics

# 7.1.1 DHCP L2 Relay Configuration

[ Advanced > DHCP L2 Relay > Configuration ]

Este cuadro de diálogo le permite activar la función de retransmisión en una interfaz y VLAN. Cuando activa esta función en un puerto, el dispositivo retransmite la información *Option 82* o descarga la información en puertos que no son de confianza. Además, el dispositivo le permite especificar el identificador remoto.

La información *Option 82* es específica de la función de retransmisión DHCPv4 L2. Para la función de retransmisión DHCPv6 L2, la información *Option 18* se utiliza en el intercambio de paquetes entre el cliente y el servidor DHCPv6. El dispositivo descarta paquetes DHCPv6 recibidos en puertos que no contienen la información *Option 18*.

El cuadro de diálogo contiene las siguientes pestañas:
- [Interface]
- [VLAN ID]

### Operation

Operation

Activa/desactiva la función de retransmisión DHCP L2 del dispositivo a nivel global.

Con esta función activada, es posible utilizar al mismo tiempo las funciones de retransmisión DHCPv4 L2 y DHCPv6 L2 en el dispositivo.

Valores posibles:
- `On`
  Activa la función *DHCP L2 Relay* en el dispositivo.
- `Off` (configuración por defecto)
  Desactiva la función *DHCP L2 Relay* en el dispositivo.

## [Interface]

### Tabla

Port

Muestra el número de puerto.

Active

Activa/desactiva la función *DHCP L2 Relay* en el puerto.

Como requisito previo, la función debe estar activa a nivel global.

Valores posibles:

- `marked`
  La función *DHCP L2 Relay* está activa.
- `unmarked` (configuración por defecto)
  La función *DHCP L2 Relay* está inactiva.

Trusted port

Activa/desactiva el modo de *DHCP L2 Relay* seguro para el puerto correspondiente.

Valores posibles:

- `marked`
  El dispositivo acepta paquetes DHCPv4 con información *Option 82*.
  El dispositivo acepta paquetes DHCPv6 con información *Option 18*.
- `unmarked` (configuración por defecto)
  El dispositivo descarta paquetes DHCPv4 recibidos en puertos no seguros que contienen la información *Option 82*.
  El dispositivo descarta paquetes DHCPv6 recibidos en puertos que no contienen la información *Option 18*.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## [VLAN ID]

### Tabla

VLAN ID

VLAN a la que se refiere la entrada de la tabla.

Active

Activa/desactiva la función *DHCP L2 Relay* en la VLAN.

Como requisito previo, la función debe estar activa a nivel global.

Valores posibles:

- `marked`
  La función *DHCP L2 Relay* está activa.
- `unmarked` (configuración por defecto)
  La función *DHCP L2 Relay* está inactiva.

Circuit ID

Activa o desactiva la incorporación del *ID de circuito* a la información *Option 82*.

Valores posibles:

- `marked` (configuración por defecto)
  Permite el envío conjunto del *ID de circuito* y el *ID remoto*.
- `unmarked`
  El dispositivo solo envía el *ID remoto*.

Remote ID type

Especifica los componentes del *ID remoto* para esta VLAN.

Valores posibles:

- `ip`
  Especifica la dirección IP del dispositivo como *ID remoto*.
- `mac` (configuración por defecto)
  Especifica la dirección MAC del dispositivo como *ID remoto*.
- `client-id`
  Especifica el nombre del sistema del dispositivo como *ID remoto*.
- `other`
  Al utilizar este valor, introduzca la información definida por el usuario en la columna *Remote ID*.

Remote ID

Muestra el *ID remoto* de la VLAN.

Al especificar el valor `other` en la columna *Remote ID type*, especifique el identificador.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## 7.1.2 DHCP L2 Relay Statistics

[ Advanced > DHCP L2 Relay > Statistics ]

El dispositivo controla el tráfico en los puertos y muestra los resultados en forma de tabla.

Esta tabla está dividida en varias categorías para ayudarle a analizar el tráfico.

Las opciones de retransmisión DHCPv6 no se muestran en la tabla de estadísticas.

### Tabla

Port

Muestra el número de puerto.

Untrusted server messages with Option 82

Muestra el número de mensajes recibidos del servidor DHCP con la información *Option 82* en la interfaz que no es de confianza.

Untrusted client messages with Option 82

Muestra el número de mensajes recibidos del cliente DHCP con la información *Option 82* en la interfaz que no es de confianza.

Trusted server messages without Option 82

Muestra el número de mensajes recibidos del servidor DHCP sin la información *Option 82* en la interfaz de confianza.

Trusted client messages without Option 82

Muestra el número de mensajes recibidos del cliente DHCP sin la información *Option 82* en la interfaz de confianza..

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

Reset

Restablece toda la tabla.

# 7.2 DHCP Server

[Advanced > DHCP Server]

Con el servidor DHCP, puede gestionar una base de datos de direcciones IP disponibles e información de configuración. Cuando el dispositivo recibe una petición de un cliente, el servidor DHCP valida la red del cliente DHCP y, a continuación, cede una dirección IP. Al activarse, el servidos DHCP también asigna la información de configuración adecuada para ese cliente. La información de configuración especifica, por ejemplo, qué dirección IP, qué servidor DNS y qué ruta por defecto utiliza un cliente.

El servidor DHCP asigna una dirección IP a un cliente durante un período de tiempo definido por el usuario. El cliente DHCP es responsable de renovar la dirección IP antes de que ese período expire. Si el cliente DHCP no puede renovar la dirección, la dirección vuelve al grupo para volver a ser asignada.

El menú contiene los siguientes cuadros de diálogo:

- DHCP Server Global
- DHCP Server Pool
- DHCP Server Lease Table

## 7.2.1 DHCP Server Global

[ Advanced > DHCP Server > Global ]

Active la función globalmente o por puerto según sus necesidades.

### Operation

Operation

Activa/desactiva la función del servidor DHCP del dispositivo globalmente.

Valores posibles:

- `On`
- `Off` (configuración por defecto)

### Configuration

IP Probe

Activa/desactiva la búsqueda de direcciones IP únicas. Antes de asignar una dirección IP, el servidor utiliza una petición *ICMP Echo* para comprobar si esta dirección IP ya está en uso en la red.

Valores posibles:

- `marked` (configuración por defecto)
  La función *IP Probe* está activa.
- `unmarked`
  La función *IP Probe* está inactiva.

### Tabla

Port

Muestra el número de puerto.

DHCP server active

Activa/desactiva la función del servidor DHCP en este puerto.

Como requisito previo, la función debe estar activa a nivel global.

Valores posibles:

- `marked` (configuración por defecto)
  La función del servidor DHCP está activa.
- `unmarked`
  La función del servidor DHCP está inactiva.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## 7.2.2 DHCP Server Pool

[ Advanced > DHCP Server > Pool ]

Asigne una dirección IP a un dispositivo terminal o switch conectado a un puerto o incluido en una VLAN.

El servidor DHCP proporciona grupos de direcciones IP, o "Pools", desde los que asigna direcciones IP a los clientes. Un Pool consta de una lista de entradas. Defina una entrada como estática para una dirección IP determinada, o como dinámica para un rango de direcciones IP. El dispositivo alberga hasta un máximo de 128 Pools. El conjunto de Pools alberga un máximo de 1000 entradas.

Con la asignación estática, el servidor DHCP asigna una 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. Utilizará esta dirección IP en todos los puertos o en un puerto específico del dispositivo. Para utilizar la asignación estática, introduzca una dirección IP para la asignación en el campo *IP address* y deje la columna *Last IP address* vacía. Introduzca un identificador de hardware con el que el servidor DHCP pueda identificar claramente al cliente. Este identificador puede ser una dirección MAC, un ID de cliente, un ID remoto o un ID de circuito. Si un cliente pone el dispositivo en contacto con un identificador de hardware conocido, el servidor DHCP le asigna una dirección IP estática.

Con la asignación dinámica, si un cliente DHCP envía una señal a un puerto, el servidor DHCP asigna a este una dirección IP disponible de un Pool para este puerto. Para la asignación dinámica, cree un Pool para todos los puertos asignando un rango de direcciones IP. Especifique la primera y la última dirección IP del rango de direcciones IP. Deje los campos *MAC address*, *Client ID*, *Remote ID* y *Circuit ID* vacíos. Puede crear múltiples entradas de Pool. Esto le permitirá crear un rango de direcciones IP que contenga huecos.

Este cuadro de diálogo muestra la información necesaria para la asignación de una dirección IP para un puerto o una VLAN. Utilice el botón  para añadir una entrada. El dispositivo añade una entrada con permisos de lectura y escritura.

### Tabla

Index

Muestra el número de índice al que la entrada de la tabla hace referencia.

Active

Activa/desactiva la función del servidor DHCP en este puerto.

Valores posibles:

- `marked`
  La función del servidor DHCP está activa.
- `unmarked` (configuración por defecto)
  La función del servidor DHCP está inactiva.

IP address

Especifica la dirección IP para la asignación de dirección IP estática. Al usar la asignación de dirección IP dinámica, este valor especifica el inicio del rango de direcciones IP.

Valores posibles:

- Dirección IPv4 válida

Last IP address

Al usar la asignación de dirección IP dinámica, este valor especifica el fin del rango de direcciones IP.

Valores posibles:

- Dirección IPv4 válida

Port

Muestra el número de puerto.

VLAN ID

Muestra la VLAN a la que la entrada de la tabla hace referencia.

Un valor de `1` se corresponde con la VLAN de administración del dispositivo por defecto.

Valores posibles:

- `1..4042`

MAC address

Especifica la dirección MAC del dispositivo que está utilizando la dirección IP.

Valores posibles:

- Dirección MAC Unicast válida
  Especifique el valor separándolo con dos puntos, por ejemplo `00:11:22:33:44:55`.
- `-`
  Para la asignación de la dirección IP, el servidor ignora esta variable.

DHCP relay

Especifica la dirección IP de la retransmisión DHCP mediante la cual los clientes transmiten sus peticiones al servidor DHCP. Si el servidor DHCP recibe la petición del cliente a través de otra retransmisión DHCP, este ignora la petición.

Valores posibles:

- Dirección IPv4 válida
  Dirección IP de la retransmisión DHCP.
- `-`
  No existe una retransmisión DHCP entre el cliente y el servidor DHCP.

Client ID

Especifica la identificación del dispositivo del cliente que está utilizando la dirección IP.

Valores posibles:

- 1 a 80 bytes (formato `XX XX .. XX`)
- `-`
  Para la asignación de la dirección IP, el servidor ignora esta variable.

Remote ID

Especifica la identificación del dispositivo remoto que está utilizando la dirección IP.

Valores posibles:

- 1 a 80 bytes (formato `XX XX .. XX`)
- `-`
  Para la asignación de la dirección IP, el servidor ignora esta variable.

Circuit ID

Especifica el ID de circuito del dispositivo que está utilizando la dirección IP.

Valores posibles:

- 1 a 80 bytes (formato `XX XX .. XX`)
- `-`
  Para la asignación de la dirección IP, el servidor ignora esta variable.

Schneider Electric device

Activa/desactiva mensajes Multicast Schneider Electric.

Si el dispositivo de este rango de direcciones IP solo sirve a dispositivos Schneider Electric, active esta función.

Valores posibles:

- `marked`
  En este rango de direcciones IP, el dispositivo solo sirve a dispositivos Schneider Electric. Mensajes Multicast Schneider Electric activados.
- `unmarked` (configuración por defecto)
  En este rango de direcciones IP, el dispositivo sirve a dispositivos de diferentes fabricantes. Mensajes Multicast Schneider Electric desactivados.

Configuration URL

Especifica el protocolo a usar, así como el nombre y la ruta del archivo de configuración.

Valores posibles:

- Cadena de caracteres ASCII alfanuméricos con entre 0 y 70 caracteres
  Por ejemplo: `tftp://192.9.200.1/cfg/config.xml`

Si deja este campo vacío, el dispositivo deja este campo de opción vacío en el mensaje DHCP.

Lease time [s]

Especifica el tiempo de concesión en segundos.

Valores posibles:

- `60..220752000` (configuración por defecto: `86400`)
- `4294967295`
  Utilice este valor para asignaciones de tiempo ilimitado y para asignaciones mediante BOOTP.

Default gateway

Especifica la dirección IP de la puerta de enlace por defecto.

Un valor de `0.0.0.0` desactiva el anexo del campo de opción en el mensaje DHCP.

Valores posibles:

- Dirección IPv4 válida

Netmask

Especifica la máscara de la red a la que pertenece el cliente.

Un valor de `0.0.0.0` desactiva el anexo del campo de opción en el mensaje DHCP.

Valores posibles:

- Máscara de red IPv4 válida

WINS server

Especifica la dirección IP del Windows Internet Name Server que convierte los nombres NetBIOS.

Un valor de `0.0.0.0` desactiva el anexo del campo de opción en el mensaje DHCP.

Valores posibles:

- Dirección IPv4 válida

DNS server

Especifica la dirección IP del servidor DNS.

Un valor de `0.0.0.0` desactiva el anexo del campo de opción en el mensaje DHCP.

Valores posibles:

- Dirección IPv4 válida

Hostname

Especifica el nombre de host.

Si deja este campo vacío, el dispositivo deja este campo de opción vacío en el mensaje DHCP.

Valores posibles:

- Cadena de caracteres ASCII alfanuméricos con entre 0 y 64 caracteres

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## 7.2.3 DHCP Server Lease Table

[Advanced > DHCP Server > Lease Table]

Este cuadro de diálogo muestra el estado de la concesión de dirección IP en función del puerto.

### Tabla

Port

Muestra el número de puerto que está utilizando la dirección actualmente.

IP address

Muestra la dirección IP concedida a la que la entrada hace referencia.

Status

Muestra la fase de concesión.

Según la norma técnica para operaciones de DHCP, hay 4 fases para conceder una dirección IP: detección, oferta, solicitud y confirmación.

Valores posibles:

- `bootp`
  Un cliente DHCP está intentando detectar un servidor DHCP para asignar una dirección IP.
- `offering`
  El servidor DHCP está verificando que la dirección IP sea adecuada para el cliente.
- `requesting`
  El cliente DHCP está adquiriendo la dirección IP ofrecida.
- `bound`
  El servidor DHCP está concediendo la dirección IP a un cliente.
- `renewing`
  El cliente DHCP está solicitando una extensión de la concesión.
- `rebinding`
  El servidor DHCP está asignando la dirección IP al cliente tras una renovación correcta.
- `declined`
  El servidor DHCP ha denegado la petición de la dirección IP.
- `released`
  La dirección IP está disponible para otros clientes.

Remaining lifetime

Muestra el tiempo restante de la dirección IP concedida.

Leased MAC address

Muestra la dirección MAC del dispositivo que está utilizando la dirección IP.

Gateway

Muestra la dirección IP de la puerta de enlace del dispositivo que está utilizando la dirección IP.

Client ID

Muestra el identificador del cliente del dispositivo que está utilizando la dirección IP.

Remote ID

Muestra el identificador remoto del dispositivo que está utilizando la dirección IP.

Circuit ID

Muestra el ID de circuito del dispositivo que está utilizando la dirección IP.

**Botones**

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

## 7.3 DNS

[ Advanced > DNS ]

El menú contiene los siguientes cuadros de diálogo:
- DNS Client

### 7.3.1 DNS Client

[ Advanced > DNS > Client ]

El DNS (Sistema de nombres de dominio) es un servicio de la red que traduce los nombres de host a direcciones IP. Esta resolución de nombres le permite contactar con otros dispositivos a través de sus nombres de host en lugar de sus direcciones IP.

La función *Client* permite al dispositivo enviar solicitudes para resolver nombres de host en direcciones IP a un servidor DNS.

El menú contiene los siguientes cuadros de diálogo:
- DNS Client Global
- DNS Client Current
- DNS Client Static
- DNS Client Static Hosts

# 7.3.1.1 DNS Client Global

[ Advanced > DNS > Client > Global ]

En este cuadro de diálogo, se activa la función *Client* y la función *Cache*.

### Operation

Operation

Activa/desactiva la función *Client*.

Valores posibles:

- *On*
  La función *Client* está activada.
  El dispositivo envía solicitudes para resolver los nombres de host en direcciones IP a un servidor DNS.
- *Off* (configuración por defecto)
  La función *Client* está desactivada.

### Cache

Cache

Activa/desactiva la función *Cache*.

Valores posibles:

- *On* (configuración por defecto)
  La función *Cache* está activada.
  El dispositivo guarda temporalmente hasta 128 respuestas de servidor DNS (nombre de host y dirección IP correspondiente) en la caché. Cuando la caché contiene una entrada coincidente, el nombre del host de una solicitud nueva del dispositivo se resuelve automáticamente. Esto hace que no resulte necesario enviar una consulta nueva al servidor DNS.
- *Off*
  La función *Cache* está desactivada.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

Flush cache

Elimina todas las entradas de la caché de DNS.

## 7.3.1.2 DNS Client Current

[ Advanced > DNS > Client > Current ]

Este cuadro de diálogo muestra a qué servidores DNS envía el dispositivo solicitudes para resolver nombres de host en direcciones IP.

### Tabla

Index

Muestra el número secuencial del servidor DNS.

Address

Muestra la dirección IP del servidor DNS. El dispositivo envía solicitudes para resolver nombres de host en direcciones IP a un servidor DNS con esta dirección IP.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

# 7.3.1.3 DNS Client Static

[Advanced > DNS > Client > Static]

En este cuadro de diálogo puede especificar los servidores DNS a los que el dispositivo reenvía solicitudes para resolver nombres de host en direcciones IP.

El dispositivo le permite especificar hasta 4 direcciones IP o transferir las direcciones IP desde un servidor DHCP.

## Configuration

Configuration source

Especifica el origen desde el que el dispositivo obtiene la dirección IP de los servidores DNS a los que el dispositivo dirige solicitudes.

Valores posibles:

- `user`
  El dispositivo utiliza las direcciones IP especificadas en la tabla.
- `mgmt-dhcp` (configuración por defecto)
  El dispositivo utiliza las direcciones IP que el servidor DHCP entrega al dispositivo.

Domain name

Especifica el nombre de dominio de acuerdo con RFC 1034 que el dispositivo añade a los nombres de host sin un sufijo de dominio.

Valores posibles:

- Cadena de caracteres ASCII alfanuméricos con entre 0 y 255 caracteres

Request timeout [s]

Especifica el intervalo de tiempo en segundos para enviar de nuevo una solicitud al servidor.

Valores posibles:

- `0`
  Desactiva la función. El dispositivo no envía de nuevo una solicitud al servidor.
- `1..3600` (configuración por defecto: `3`)

Request retransmits

Especifica el número de veces que el dispositivo retransmite una solicitud.

El requisito previo es que, en el campo *Request timeout [s]*, especifique un valor >`0`.

Valores posibles:

- `0..100` (configuración por defecto: `2`)

### Tabla

Index

Muestra el número secuencial del servidor DNS.

El dispositivo le permite especificar hasta 4 servidores DNS.

Address

Especifica la dirección IP del servidor DNS.

Valores posibles:

- Dirección IPv4 válida (configuración por defecto: `0.0.0.0`)
- Dirección IPv6 válida

Active

Activa/desactiva la entrada de la tabla.

El dispositivo envía solicitudes al servidor DNS configurado en la primera entrada activa de la tabla. Si el dispositivo no recibe una respuesta de este servidor, envía solicitudes al servidor DNS configurado en la siguiente entrada activa de la tabla.

Valores posibles:

- `marked`
  El cliente DNS envía solicitudes a este servidor DNS.
  Requisitos previos:
  - ☐ Active la función de cliente DNS en el cuadro de diálogo *Advanced > DNS > Global*.
  - ☐ Seleccione en el cuadro *Configuration*, lista desplegable *Configuration source*, el valor `user`.
- `unmarked` (configuración por defecto)
  El dispositivo no envía solicitudes a este servidor DNS.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

# 7.3.1.4 DNS Client Static Hosts

[Advanced > DNS > Client > Static Hosts]

Este cuadro de diálogo le permite especificar hasta 64 nombres de host, cada uno vinculado a una dirección IP. Tras recibir una solicitud para resolver los nombres de host en direcciones IP, el dispositivo busca una entrada correspondiente en esta tabla. Si el dispositivo no encuentra una entrada correspondiente, reenvía la solicitud.

### Tabla

Index

Muestra el número de índice al que la entrada de la tabla hace referencia.

Valores posibles:

- `1..64`

Name

Especifica el nombre de host.

Valores posibles:

- Cadena de caracteres ASCII alfanuméricos con entre 0 y 255 caracteres

IP address

Especifica la dirección IP bajo la cual se puede acceder al host.

Valores posibles:

- Dirección IPv4 válida

Active

Activa/desactiva la entrada de la tabla.

Valores posibles:

- `marked`
  El dispositivo resuelve una solicitud para el nombre de host de esta entrada.
- `unmarked`
  Tras recibir una solicitud para este nombre de host, el dispositivo envía una solicitud a uno de los servidores de nombres configurados para su resolución.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

# 7.4 Industrial Protocols

[Advanced > Industrial Protocols]

El menú contiene los siguientes cuadros de diálogo:

- IEC61850-MMS
- Modbus TCP
- EtherNet/IP

# 7.4.1 IEC61850-MMS



IEC 61850-MMS es un protocolo de comunicación industrial estandarizado de la International Electrotechnical Commission (IEC). Por ejemplo, el equipo de conmutación automática utiliza este protocolo cuando se comunica con el equipo de la estación de alimentación.

El protocolo orientado a paquetes define un lenguaje de comunicación uniforme basado en el protocolo de transporte, TCP/IP. Este protocolo utiliza la Especificación de mensajes de fabricación (MMS, Manufacturing Messaging Specification) para la comunicación con el servidor del cliente. El protocolo incluye funciones de SCADA, el dispositivo electrónico inteligente (IED, Intelligent Electronic Device) y los sistemas de control de red.

**Nota:** 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.

Active el acceso de escritura únicamente si ha tomado medidas adicionales (por ejemplo, un cortafuegos, VPN, etc.) para reducir posibles accesos no autorizados.

Este cuadro de diálogo le permite especificar los siguientes ajustes del servidor MMS:
- Activa/desactiva el servidor MMS.
- Activa/desactiva el acceso de escritura al servidor MMS.
- El puerto TCP del servidor MMS.
- El número máximo de sesiones de servidor MMS.

### Operation

Operation

Activa/desactiva el servidor *IEC61850-MMS*.

Valores posibles:

- *On*
  El servidor *IEC61850-MMS* está activado.
- *Off* (configuración por defecto)
  El servidor *IEC61850-MMS* está desactivado.
  Las MIB IEC61850 permanecen accesibles.

### Configuration

Write access

Activa/desactiva el acceso de escritura al servidor MMS.

Valores posibles:

- `marked`
  El acceso de escritura al servidor MMS está activado. Esta configuración le permite cambiar los ajustes del dispositivo mediante el protocolo IEC 61850/MMS.
- `unmarked` (configuración por defecto)
  El acceso de escritura al servidor MMS está desactivado. El servidor MMS es accesible solo en modo lectura.

Technical key

Especifica el nombre IED.

El nombre IED puede elegirse independientemente del nombre del sistema.

Valores posibles:

- Cadena de caracteres ASCII alfanuméricos con entre 0 y 32 caracteres
  Solo se permiten los siguientes caracteres:
  - _
  - `0..9`
  - `a..z`
  - `A..Z` (configuración por defecto: `KEY`)

Para que el servidor MMS utilice el nombre IED, haga clic en el botón ✓ y reinicie el servidor MMS. La conexión con los clientes conectados se interrumpirá.

TCP port

Especifica el puerto TCP para el acceso al servidor MMS.

Valores posibles:

- `1..65535` (configuración por defecto: `102`)
  Excepción: el puerto `2222` está reservado para funciones internas.

**Nota:** El servidor se reinicia automáticamente cuando cambia de puerto. En el proceso, el dispositivo cierra las conexiones abiertas en el servidor.

Sessions (max.)

Especifica el número máximo de conexiones del servidor MMS.

Valores posibles:

- `1..15` (configuración por defecto: `5`)

### Information

Status

Muestra el estado del servidor *IEC61850-MMS* actual.

Valores posibles:

- *unavailable*
- *starting*
- *running*
- *stopping*
- *halted*
- *error*

Active sessions

Muestra el número de conexiones activas del servidor MMS.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

Download ICD file

Copia el archivo ICD en su PC.

# 7.4.2 Modbus TCP

[ Advanced > Industrial Protocols > Modbus TCP ]

*Modbus TCP* es un protocolo utilizado para la integración del sistema de Supervisión, Control y Adquisición de Datos (SCADA). *Modbus TCP* es un protocolo independiente, no influenciado por el proveedor, que se emplea para supervisar y controlar los equipos de automatización industrial, como los controladores lógicos programables (PLC), los sensores y los medidores.

Este cuadro de diálogo le permite especificar los parámetros del protocolo. Para supervisar y controlar los parámetros del dispositivo, necesita un software de Interfaz hombre-máquina (HMI) y la tabla de mapeo de la memoria. Consulte las tablas del manual de usuario de "Configuración" para los objetos admitidos y el mapeo de la memoria.

El cuadro de diálogo le permite habilitar la función, activar el acceso de escritura y controlar el puerto TCP que consulta la Interfaz hombre-máquina (HMI) para obtener datos. También puede especificar el número de sesiones permitidas para que se abran al mismo tiempo.

**Nota:** Si se activa el acceso de escritura *Modbus TCP*, puede surgir una situación de riesgo de seguridad inevitable, ya que el protocolo no autentica el acceso del usuario.

Para ayudar a minimizar los riesgos de seguridad inevitables, especifique el rango de direcciones IP ubicado en el cuadro de diálogo *Device Security > Management Access*. Introduzca solo las direcciones IP asignadas a sus dispositivos antes de activar la función. Además, la configuración por defecto para activar la función de supervisión en el cuadro de diálogo *Diagnostics > Status Configuration > Security Status*, pestaña *Global*, está activa.

### Operation

Operation

Activa/desactiva el servidor *Modbus TCP* en el dispositivo.

Valores posibles:

- *On*
  El servidor *Modbus TCP* está activado.
- *Off* (configuración por defecto)
  El servidor *Modbus TCP* está desactivado.

### Configuration

Write access

Activa/desactiva el acceso de escritura a los parámetros *Modbus TCP*.

**Nota:** Si se activa el acceso de escritura *Modbus TCP*, puede surgir una situación de riesgo de seguridad inevitable, ya que el protocolo no autentica el acceso del usuario.

Valores posibles:

- `marked` (configuración por defecto)
  El acceso de lectura/escritura del servidor *Modbus TCP* está activo. Esto le permite cambiar la configuración del dispositivo mediante el protocolo *Modbus TCP*.
- `unmarked`
  El acceso de solo lectura del servidor *Modbus TCP* está activo.

TCP port

Especifica el número de puerto TCP que el servidor *Modbus TCP* utiliza para la comunicación.

Valores posibles:

- `<TCP Port number>` (configuración por defecto: `502`)
  No se permite especificar `0`.

Sessions (max.)

Especifica el número máximo de sesiones concurrentes que mantiene el servidor *Modbus TCP*.

Valores posibles:

- `1..5` (configuración por defecto: `5`)

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

# 7.4.3 EtherNet/IP

[ Advanced > Industrial Protocols > EtherNet/IP ]

Este cuadro de diálogo le permite especificar los ajustes de *EtherNet/IP*. Tiene las siguientes opciones:

- Activar/desactivar la función *EtherNet/IP* en el dispositivo.
- Especificar una VLAN que reenvíe los paquetes *EtherNet/IP* exclusivamente.
- Activar/desactivar la capacidad de lectura/escritura del protocolo *EtherNet/IP*.
- Descargar el archivo de la hoja de datos electrónica (EDS) del dispositivo.

## Operation

Operation

Activa/desactiva la función *EtherNet/IP* en el dispositivo.

Valores posibles:

- `On`
  La función *EtherNet/IP* está activada.
- `Off` (configuración por defecto)
  La función *EtherNet/IP* está desactivada.

## VLAN Configuration

Ventajas de configurar una VLAN:

- Reducción del desborde de paquetes *EtherNet/IP*. El dispositivo desvía los paquetes *EtherNet/IP* de la VLAN que asigne.
- Seguridad y privacidad mejoradas de la red.

VLAN ID

Especifica una VLAN en la que el dispositivo desvía los paquetes *EtherNet/IP*.

Valores posibles:

- `mgmt` (configuración por defecto)
  El dispositivo desvía los paquetes *EtherNet/IP* de la VLAN en la cual se puede acceder a la gestión del dispositivo a través la red. Especifique esta VLAN en el cuadro de diálogo *Basic Settings > Network > Global*, cuadro *Management interface*, campo *VLAN ID*.
- `1..4042`
  En la lista desplegable, seleccione un elemento. El dispositivo desvía los paquetes *EtherNet/IP* de esta VLAN.
  Requisitos previos:
  - La VLAN ya está configurada en el dispositivo.
    Consulte el cuadro de diálogo *Switching > VLAN > Configuration*.
  - El puerto a través del cual el dispositivo desvía los paquetes *EtherNet/IP* es miembro de la VLAN asignada y transmite los paquetes de datos con una etiqueta VLAN.
    Consulte el cuadro de diálogo *Switching > VLAN > Configuration*.
  - La función *IP Access Restriction* está activada.
    Consulte el cuadro de diálogo *Device Security > Management Access > IP Access Restriction*.

### Configuration

Write access

Activa/desactiva la capacidad de lectura/escritura del protocolo *EtherNet/IP*.

Valores posibles:

- `marked`
  El protocolo *EtherNet/IP* acepta las solicitudes set/get.
- `unmarked` (configuración por defecto)
  El protocolo *EtherNet/IP* solo acepta solicitudes get.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

Download EDS file

Copia la siguiente información como archivo zip en su ordenador:

- Hoja de datos electrónica (EDS) con información relacionada con el dispositivo
- El icono del dispositivo

# 7.5 Digital IO Module

[Advanced > Digital IO Module]

Las entradas digitales le permiten capturar y reenviar señales de sensores digitales. Las salidas digitales le permiten aplicar la señal, retransmitida desde las entradas, a los actuadores. La tensión de salida de 24 VCC le permite operar actuadores como las luces indicadoras.

El dispositivo transmite señales del sensor a través de la red para activar los actuadores adecuados. El módulo captura señales mediante las conexiones de entrada y las envía a las salidas. Basándose en la localización de los actuadores, el dispositivo envía las señales a las salidas situadas en el mismo módulo, en un módulo diferente dentro del mismo dispositivo o en otro dispositivo.

Cuando el dispositivo asigna los puertos de entrada digital a los puertos de salida digital, hay una relación 1:N. El dispositivo refleja el flujo de datos de un puerto de entrada digital en una cantidad indeterminada de puertos de salida digital.

Cuando el dispositivo asigna los puertos de salida digital a los puertos de salida entrada, hay una relación 1:1. Un puerto de salida digital refleja el flujo de datos en un puerto de entrada digital.

El cuadro de diálogo contiene las siguientes pestañas:
- [IO input]

## [IO input]

Esta pestaña le permite:
- activar/desactivar las solicitudes de entradas digitales globalmente
- configurar el intervalo en el que el dispositivo solicita los valores de las entradas digitales
- activar/desactivar el registro de un evento
- activar/desactivar el envío de trampas SNMP

### Operation

Operation

Activa/desactiva las solicitudes cíclicas desde entradas digitales (entrada IO)

Valores posibles:
- *On*
  Le permite solicitar los valores de entrada.
- *Off* (configuración por defecto)

### Configuration

Refresh interval [ms]

Especifica el intervalo de tiempo en milisegundos durante el cual el dispositivo solicita los valores de las entradas digitales.

Valores posibles:

- `1000..10000` (configuración por defecto: `1000`)

### Tabla

Input ID

Muestra el número de ranura del módulo (x) y el número de entrada digital (i) válidos para esta entrada.

Notación: `x.i`

Valores posibles:

- x =`0..7`
  El valor `0` se corresponde con la unidad principal (MU).
- i =`1..4`

Value

Especifica el nivel de entrada digital.

Valores posibles:

- `low`
  La tensión de entrada en la entrada digital es de 0 V.
- `high`
  La tensión de entrada en la entrada digital es de +24 VCC.
- `not-available`
  La tensión de entrada en la entrada digital tiene un valor diferente a 0 V o +24 VCC. Verifique que el módulo se encuentra presente e instalado correctamente.

Log event

Activa/desactiva el registro en el archivo de registro. Consulte el cuadro de diálogo *Diagnostics* > Report > *System Log*.

Valores posibles:

- `marked`
  El registro está activado.
  El dispositivo comprueba el estado de las entradas digitales de acuerdo con el intervalo de tiempo especificado en el cuadro *Configuration*, campo *Refresh interval [ms]*.
  Si se producen cambios en las entradas digitales, el dispositivo registra una entrada en el archivo de registro System Log.
- `unmarked` (configuración por defecto)
  El registro está desactivado.

Send trap

Activa/desactiva el envío de trampas SNMP cuando el dispositivo detecta un cambio en las entradas digitales.

El dispositivo comprueba el estado de las entradas digitales de acuerdo con el intervalo de tiempo especificado en el cuadro *Configuration*, campo *Refresh interval [ms]*.

Valores posibles:

- `marked`
  El envío de trampas SNMP está activo.
  Cuando el dispositivo detecta cambios en las entradas digitales, envía una trampa SNMP.
- `unmarked` (configuración por defecto)
  El envío de trampas SNMP está inactivo.

Como requisito previo para enviar trampas SNMP, debe activar la función en el cuadro de diálogo *Diagnostics > Status Configuration > Alarms (Traps)* y especificar al menos un destino de la trampa.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

# 7.6 Command Line Interface

[ Advanced > CLI ]

El cuadro de diálogo le permite acceder al dispositivo mediante la interfaz de línea de comando.

Los requisitos previos son:
- ☐ En el dispositivo, active el servidor SSH en el cuadro de diálogo *Device Security > Management Access > Server*, pestaña *SSH*.
- ☐ En su estación de trabajo, instale una aplicación cliente compatible con SSH, la cual registrará un operador para URL que empiece por `ssh://` en su sistema operativo.

### Botones

Encontrará la descripción de los botones estándar en la sección “Botones” en página 17.

Open SSH connection

Abre la aplicación cliente compatible son SSH.

Al hacer clic en el botón, la aplicación web pasa la URL del dispositivo que empieza por `ssh://` y el nombre de usuario del usuario actualmente conectado.

Si el navegador web encuentra una aplicación cliente compatible con SSH, el cliente compatible con SSH establece una conexión con el dispositivo mediante el protocolo SSH.

# A Índice