GigaX Series

Switch Administrado de Nivel 2

Manual del Usuario

S2664/ Agosto 2006

Información de Copyright

S2664
Primera Edición
Agosto 2006

La garantía del producto o servicio no será extendida si: (1) el producto es reparado, modificado o alterado, a menos que la reparación, modificación o alteración sea autorizada por escrito por ASUS; o (2) el número de serie del producto no pueda leerse claramente o no esté presente.

ASUS proporciona este manual “tal como se presenta” sin garantías de ningún tipo, ya sean explícitas o implícitas, incluyendo pero no limitándose a las garantías implícitas, condiciones de mercado o ajustes a cualquier propósito. En ningún evento ASUS, sus directores, oficiales, empleados o agentes serán responsables por cualquier daño, ya sea indirecto, especial, incidental, o consecuencial (incluyendo daños por pérdida de beneficios, negocios, pérdidas de uso o datos, interrupción de negocio o similares), incluso si ASUS ha sido advertido de que la posibilidad de estos daños puede surgir por cualquier defecto o error en su manuales o productos.

Las especificaciones e información contenida en este manual está orientada a propósitos informativos y está sujeta a cambios en cualquier momento sin previo aviso, por lo que no puede ser utilizada como compromiso por parte de ASUS. ASUS no asume ninguna responsabilidad por errores o inexactitudes que pudieran aparecer en este manual, incluyendo los productos y/o el software descrito en el.

Los productos y nombres corporativos que aparecen en éste manual podrían (o no) ser marcas registradas o copyright de sus respectivas compañías, y son utilizadas aquí solo por motivos de identificación o explicativos y en beneficio del dueño, sin intención de infringir dichas normas.

SEDE CENTRAL

ASUSTeK COMPUTER INC. (Taiwan)

Tel General:	0800-093-456 (Llamada gratuita desde Taiwan)
Fax General:	+886-2-2895-9254
Formulario de e-mail:	http://vip.ASUS.com/eservice/techserv.aspx
Sitio Web:	http://tw.ASUS.com

ASUSTeK COMPUTER INC. (Asia Pacífico)

Tel General:	+886-2-2894-3447
Fax General:	+886-2-2894-7798
Formulario de e-mail:	http://vip.ASUS.com/eservice/techserv.aspx
Sitio Web:	http://www.ASUS.com

SEDE CENTRAL EUROPEA

ASUS COMPUTER GmbH (Alemania/Austria)

Tel General (Alemania):	+49-(0)2102/9599-10
Tel General (Austria):	0820/240513
Fax General:	+1-502-933-8713
Formulario de e-mail:	http://vip.ASUS.de/support/support.htm
Sitio Web:	http://www.ASUS.de

OFICINAS ESPAÑOLAS

ASUS IBÉRICA S.L. (España)

Soporte técnico:	+34 934 929 806
	902 889 688 (llamadas locales desde España)
Fax de soporte:	+34 934 929 801
Sitio web:	http://es.ASUS.com
Dirección:	Plomo, 5-7 4ª Planta. CP 08038. Barcelona, ESPAÑA
E-mail de soporte:	tsd_acib@ASUS.com

Noticias

Declaración de la Comisión federal de comunicaciones

Este dispositivo cumple con el Apartado 15 de la normativa FCC. Su funcionamiento está sujeto a las siguientes dos condiciones:

- Este dispositivo no debe causar interferencias perjudiciales, y
- Este dispositivo debe aceptar cualquier interferencia recibida, incluyendo interferencias que podrían provocar un funcionamiento no deseado.

Este equipo se ha probado y se ha encontrado que cumple con los límites de un dispositivo digital de Clase B, de acuerdo con el Apartado 15 de la normativa FCC. Estos límites están diseñados para proporcionar una protección razonable contra interferencias perjudiciales en una instalación residencial. Este equipo genera, utiliza y puede radiar energía de frecuencia de radio y, si no se instala y utiliza siguiendo las instrucciones del fabricante, podría provocar interferencias en las comunicaciones de radio. Sin embargo, no se garantiza que no ocurrirá ninguna interferencia en una instalación en particular. Si este equipo provoca interferencias perjudiciales a la recepción de radio o televisión, lo que puede determinarse encendiendo o apagando el equipo, se anima al usuario a intentar corregir las interferencias mediante una o varias de las siguientes medidas:

- Vuelva a orientar o ubicar la antena receptora.
- Aumente la separación entre el equipo y el receptor.
- Conecte el equipo a una toma de corriente de un circuito distinto al utilizado para conectar el receptor.
- Consulte con su proveedor o con un técnico experto de radio y televisión para obtener ayuda.

Declaración del Departamento Canadiense de Comunicaciones

Este aparato digital no excede los límites de Clase B para emisiones de ruido de radio desde un aparato digital como se establece en la normativa sobre interferencias de radio del Departamento de comunicaciones canadiense.

Este aparato digital clase B cumple con la regulación ICES-003 de Canadá.

Tabla de Contenidos

Lista de Figuras

Lista de Tablas

1 Introducción

Enhorabuena por la adquisición de este switch administrado de nivel 2 ASUS GigaX.

Este manual del usuario explica como configurar y personalizar el switch para obtener el máximo rendimiento de este producto.

1.1 Convenciones usadas en este manual

1.1.1 Notaciones

- Los acrónimos son definidos la primera vez que aparecen en el texto y en el glosario.
- Por motivos de brevedad, el switch administrado de nivel 2 ASUS GigaX también es referido como "**el Switch**".
- Los términos **LAN** y **red** son utilizados indistintamente para referirse a un grupo de PCs conectados a un mismo sitio de red.

1.1.2 Tipografía

El texto escrito en **Negrita** se utiliza para elementos seleccionados en menús normales y menús desplegables, o cadenas de caracteres o texto que es escrito en alguna parte del programa. Estos elementos pueden venir entre los símbolos < > o " ". El texto en **Negrita** también se utiliza para dar énfasis.

1.1.3 Símbolos

Este documento utiliza los siguientes iconos para llamar su atención a instrucciones o explicaciones específicas.

Proporciona información aclaratoria o adicional relacionada con el tema que se esté tratando.

Explica términos o acrónimos que podrían no ser familiares para la mayoría de los lectores. Estos términos también estarán incluidos en el glosario.

Proporciona mensajes de alta importancia, incluyendo los relacionados con la seguridad personal o la integridad del sistema.

1.2 Contenidos del embalaje

Compruebe que los siguientes elementos se encuentran presentes en el embalaje de su switch ASUS GigaX Series. Contacte con su punto de venta si alguno de estos elementos está dañado o no se encuentra presente.

- ☑ Switch administrado de nivel 2 GigaX 2024X (26 puertos) o GigaX 2016X (18 puertos)
- ☑ Cable de alimentación AC
- ☑ CD-ROM de soporte
- ☑ Cable Null Modem para la interfaz de consola (DB9)
- ☑ Kit de instalación en rack (dos soportes con seis tornillos #6-32)
- ☑ Cable USB para interfaz de consola
- ☑ CD-ROM de instalación
- ☑ Manual del Usuario

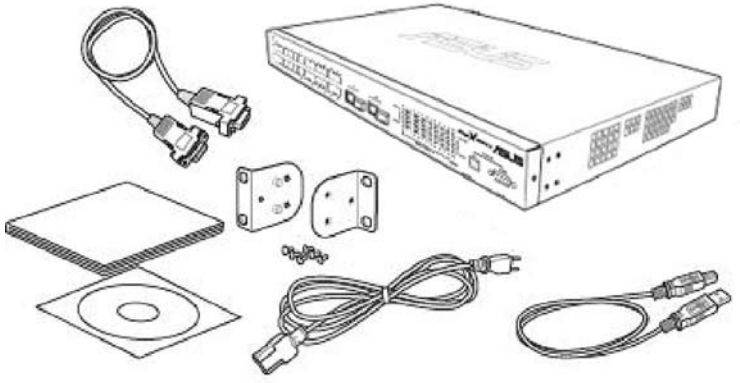


Figura 1. Componentes del Switch Administrado de nivel 2

1.3 Funciones

El Switch ASUS GigaX Series proporciona las siguientes funciones:

- 24 puertos Fast Ethernet 10/100BASE-TX con auto-sensing (GX2024X)
- 16 puertos Fast Ethernet 10/100BASE-TX con auto-sensing (GX2016X)
- 2 puertos de intercambio Gigabit Ethernet 10/100/1000BASE-T con auto-sensing

- Dos zócalos “Small Form Factor” (SFP) para Gigabit Interface Converter (GBIC)
- Protocolo 802.1D/802.1w con bridge/protocolo spanning tree/rapid spanning tree transparente
- Caché con 8K de direcciones MAC y envejecimiento asistido por Hardware
- Control de flujo 802.3x
- VLAN con etiquetas basado en 802.1Q, con hasta 229 VLANs (GX2024X)
- VLAN con etiquetas basado en 802.1Q, con hasta 237 VLANs (GX2016X)
- Red VLAN privada de hasta 4 VLANs
- VLAN basada en puertos de hasta 26 grupos (GX2024X)
- VLAN basada en puertos de hasta 18 grupos (GX2016X)
- Clase de servicio 802.1p, con 4 colas por puerto
- Soporte para Multidifusión Estática . Hasta 127 grupos
- Soporte para monitorización IGMP (v1/v2/v3)
- Agregación de enlaces 802.3ad (manual y LACP), hasta 15 grupos de enlace entre centros de conmutación (Trunks)
- Duplicación de puertos
- Control de ancho de banda
- Cliente DHCP
- Control de acceso a red basado en puertos/MAC 802.1X
- Servicio de autentificación de usuarios telefónica a través de servidor RADIUS
- Autentificación remota TACACS+
- Seguridad en puertos
- Clasificación de calidad de servicio: Prioridad DA/SA MAC, prioridad VLAN, IPv4 ToS/DiffServ, Clase de tráfico IPv6
- Diagnóstico de cable Ethernet
- RMON: Soporte para 4 grupos (1, 2, 3, 9)
- SNMP v1, v2, v3
- MIB-II
- Enterprise MIB para la fuente de alimentación, ventilador, temperatura del sistema, y voltaje
- Inicio de sesión remoto a través de Telnet o SSH
- FTP para actualizaciones del Firmware y copias de seguridad de la configuración
- Syslog
- Intérprete de comandos a través de consola, Telnet y SSH
- Interfaz gráfico Web
- LEDs para informar del estado de los enlaces en puerto
- LEDs de sistema, fuente de alimentación redundante (RPS), y estado del ventilador

1.4 Funciones del panel frontal

El panel frontal incluye indicadores LED que muestran los estados del sistema, fuente de alimentación redundante (RPS), ventilador y puertos.

Figura 2. Panel frontal GigaX 2024X

Figura 3. Panel frontal GigaX 2016X

Tabla 1: Etiquetas y LEDs del panel frontal

Etiqueta	Color	Estado	Descripción
SYSTEM Sistema	Verde	Encendido	Unidad encendida
		Intermitente	
	Ámbar	Encendido	Temperatura o voltaje anormal
	Apagado		Sin alimentación
RPS	Verde	Encendido	La unidad de suministro de energía (Power Supply Unit - PSU) del Switch funciona correctamente y éste tiene un buen suministro de energía redundante
	Ámbar	Encendido	PSU anormal con Switch recibiendo energía a través de RPS
	Apagado		Sin energía (LED SYSTEM también apagado); RPS no funciona apropiadamente o no está instalado (LED SYSTEM encendido)
FAN (ventilador)	Verde	Encendido	Ambos ventiladores funcionando correctamente
	Ámbar	Encendido	Ambos o uno de los ventiladores detenido
Estado en puertos 10/100/1000	Verde	Encendido	Enlace (RJ-45 o SFP) presente; puerto activado
		Intermitente	Transmitiendo o recibiendo datos
	Apagado		No hay enlace Ethernet
Velocidad en puertos 10/100/1000	Verde	Encendido	1000Mbps en puertos Giga port, o 100Mbps en puertos 10/100
	Ámbar	Encendido	100Mbps en puertos Giga
	Apagado		10Mbps o enlace no presente

1.5 Panel Trasero

El panel trasero del Switch contiene los conectores de alimentación y ventiladores.

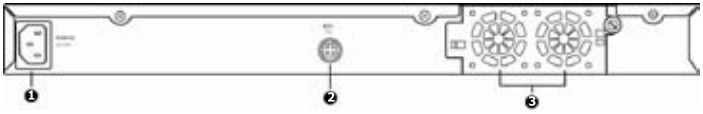


Figura 4. Panel trasero

Tabla 2: Elementos del panel trasero

No	Etiqueta	Descripción
1	POWER	Conecta el cable de alimentación suministrado
2	RPS	Conector para el Módulo de Alimentación Redundante
3	FAN1 - FAN2	Ventiladores del sistema reemplazables

1.6 Especificaciones técnicas

Tabla 3: Especificaciones técnicas

Dimensiones físicas	43.5mm(Alto) X 444 mm(Ancho) X 265mm(Profundidad)		
Alimentación	Entrada: 100-240V AC/2.5A 50-60Hz		
	Consumo: <90 watts		
Sistema de alimentación redundante (RPS)	Entrada: 100-240V AC/1.8A 50-60Hz		
	Salida: 12V DC/12.5A		
Rangos ambientales		Operación	Almacenamiento
	Temperatura	-10 a 50°C (14 a 122°C)	-40 a 70°C (-40 a 158°C)
	Humedad	15 to 90%	0 to 95%
	Altitud	Máximo 10,000 pies (3,000m)	40,000 pies (12,000m)
Ventiladores reemplazables	Dimensiones: 40 x 40 x 20 mm		
	Voltaje y amperaje: 12VDC, 0.13A		
	Velocidad: 8200RPM		

2 Guía de instalación rápida

Esta sección proporciona instrucciones básicas para organizar el entorno operativo del Switch. También puede referirse a la guía de instalación del Switch GigaX.

- La parte 1 explica el proceso de instalación del Switch GigaX en una superficie plana o en un rack.
- La parte 2 proporciona instrucciones para configurar el Hardware.
- La parte 3 describe como configurar los ajustes básicos en el Switch GigaX.

Antes de empezar, obtenga la siguiente información de su administrador de red:

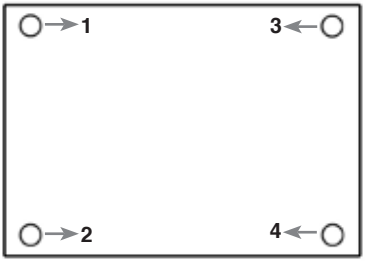
- Dirección IP para el Switch
- Puerta de Enlace por defecto
- Máscara de red para esta red

2.1 Parte 1 — Instalación del Switch

El Switch puede ser instalado en una superficie plana o en un rack.

2.1.1 Instalación del Switch en una superficie plana

El Switch debe ser instalado en una superficie plana que pueda soportar el peso del Switch (o Switches) y sus accesorios. Inserte cuatro soportes de caucho en la parte inferior del Switch.



Inserte los cuatro soportes de caucho en las zonas 1, 2, 3, y 4.

2.1.2 Montaje del Switch en un Rack

1. Con el panel frontal hacia afuera, inserte el Switch entre los postes del rack y alinee los cuatro agujeros de montaje con los del rack.
2. Ajuste el Switch en el rack con dos tornillos en cada cara.

2.2 Parte 2 — Conexión del Hardware

El Switch debe ser conectado a una fuente de alimentación, a un PC y a la red. Refiérase a la figura 5 para una introducción a las conexiones del Hardware.

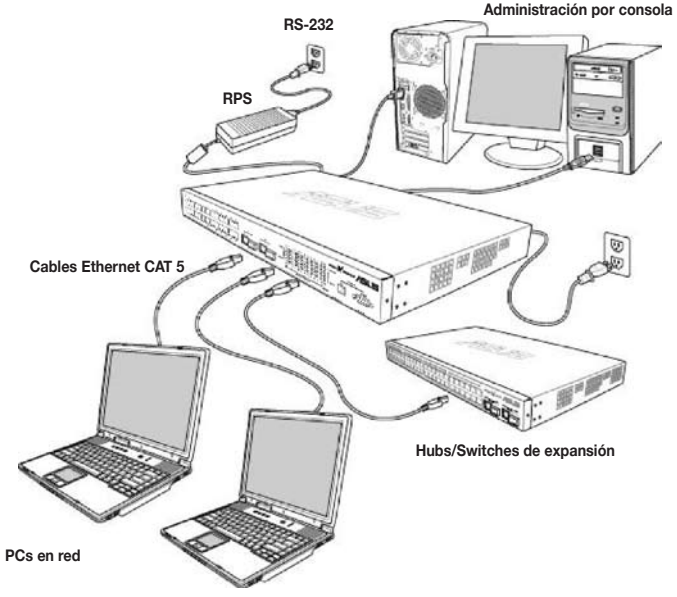


Figura 5. Introducción a las conexiones del Hardware

2.2.1 Conexión del puerto de consola

Para administración a través de consola, utilice un conector RS232 (DB9). Si desea utilizar una Administrador de Configuración, conecte un PC al Switch utilizando un cable Ethernet.

2.2.2 Conexión a PCs o redes

Puede utilizar cables Ethernet para conectar PCs directamente a los puertos del Switch. También puede conectar hubs/Switches a los puertos Ethernet del Switch. Puede utilizar cables Ethernet cruzados o directos. Puede conectar PCs, hubs, o Switches.

Utilice un cable par cruzado Ethernet de categoría 5 para conectar al puerto 1000BASE-T. De otro modo la velocidad del enlace no podrá alcanzar 1Gbps.

2.2.3 Conexión de un módulo RPS

Conecte el modulo de alimentación redundante (RPS) opcional al conector RPS en la parte trasera del Switch, asegurándose de que el otro extremo del RPS está conectado a un cable.

2.2.4 Conexión de una fuente de alimentación

1. Conecte un extremo del cable de alimentación AC al conector para el cable de alimentación (POWER) en la parte trasera del Switch. Conecte el otro extremo del cable a un enchufe o fuente de alimentación.
2. Compruebe que los indicadores LED del panel se ajustan a las descripciones de la tabla 4. Si los LEDs se iluminan como esta descrito, el Hardware del Switch funciona apropiadamente.

Tabla 4: Indicadores LED

No	LED	Descripción
1	SYSTEM	Verde fijo indica que el dispositivo está encendido. Si esta luz esta apagada, asegúrese de que el cable de alimentación esta conectado al switch y conectado a una fuente de alimentación
2	Puertos del Switch [1] a [26] (GX2024X) [1] a [18] (GX2016X)	Verde fijo indica que hay un enlace presente en el puerto; intermitente indica que el dispositivo conectado está enviando o recibiendo datos desde los PCs en red.
3	RPS	Verde fijo indica que un módulo RPS ha sido instalado con éxito.
4	FAN	Verde fijo indica que todos los ventiladores funcionan correctamente

2.2 Parte 3 — Ajustes básicos del Switch

Una vez que las conexiones del hardware hayan sido completadas podrá configurar los ajustes básicos del Switch. Puede administrar el Switch a través de cualquiera de los siguientes métodos:

- **Administrador de Configuración:** El Switch dispone de un grupo de páginas que permiten su fácil administración a través de IE5.0 o superior con Java®. Para más información, refiérase a los capítulos 3 y 4.
- **Interfaz de comandos (CLI):** Utilice el puerto de consola para administrar el Switch.

2.3.1 Administración a través del puerto consola

1. Utilice el cable cruzado RS-232 suministrado para conectar el puerto de consola al panel frontal del Switch. Este puerto es un conector macho DB-9, implementado como conector para equipos terminales de datos (DTE). Ajuste los tornillos del cable para asegurarlo al conector. Conecte el otro extremo del terminal a un PC que utilice un Software de emulación de terminal (p.e. Hyper Terminal).
2. Utilice el cable USB incluido para conectar al PC. Deberá instalar el controlador para USB desde el CD-ROM del Switch antes de realizar la conexión. El controlador USB simula un puerto COM adicional en Sistemas Operativos Windows Me/2K/XP.
3. Asegúrese de que los ajustes del emulador de terminal se ajustan a las siguientes especificaciones:
   a) Seleccione el puerto serie apropiado.
   b) Ajuste la tasa de baudios de datos a 9600.
   c) Ajuste el formato de datos a “no paridad”, “8 bits de datos” y “1 bit de stop”.
   d) Desactive el control de flujo.
4. Tras configurar el terminal, podrá ver el mensaje “(ASUS)%” en la pantalla del terminal.
5. Introduzca “login” para acceder al interfaz de comandos. El nombre de usuario por defecto es “admin”. No escriba la contraseña presionando la tecla **<Entrar>**.

Puede cambiar la contraseña en cualquier momento a través de (consulte sección 5.2: Inicio y finalización de sesión). Para proteger su Switch contra accesos no autorizados, cambie la contraseña por defecto tan pronto como le sea posible.

6. Siga estos pasos para asignar una dirección IP al switch:

a) Escriba “net interface ip sw0 <su dirección IP> <su máscara de red>”. Por ejemplo, si la dirección IP de su Switch es 192.168.10.1 y su máscara de red es 255.255.255.0, deberá escribir “net interface ip sw0 192.168.10.1 255.255.255.0”.

b) Si el switch tiene que ser administrado a través de diferentes redes, será requerido que escriba la puerta de enlace o ruta estática por defecto. Escriba “net route static add 0.0.0.0 <dirección IP de su puerta de enlace> 0.0.0.0 1” como su ruta de entrada por defecto, como se muestra en la figura 6.

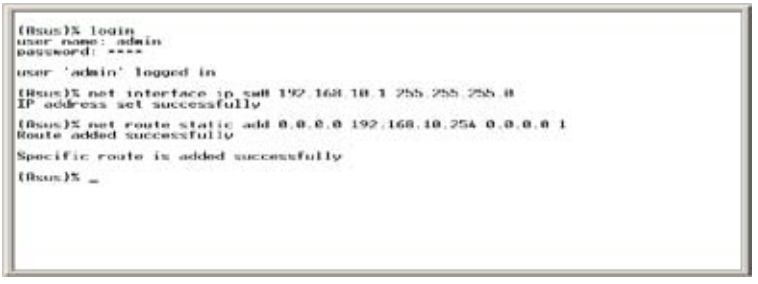


Figura 6. Pantalla de inicio de sesión y configuración IP

2.3.2 Configuración a través de “Configuration Manager”

Puede administrar el Switch a través de la aplicación Web preinstalada **"Configuration Manager"**.

Puede acceder a Configuration Manager a través de cualquier navegador Web (Microsoft Internet Explorer® 5.0 o versiones posteriores. No soporta Netscape) desde cualquier PC conectado al Switch a través de los puertos LAN.

1. Por defecto, la autentificación a través de Web esta desactivada. Deberá activarla para asegurar la configuración del sistema. Para ello, acceda a **System --> Administration**.
2. En el navegador Web (IE 5.0 o versiones posteriores), introduzca la siguiente dirección IP: http://192.168.1.1 (dirección IP por defecto del Switch) y pulse <**Entrar**>.

   Una ventana de inicio de sesión aparecerá como se muestra en la figura 7.

Figura 7. Ventana de inicio de sesión en Configuration Manager

3. Introduzca su nombre de usuario y contraseña, y haga clic en <**Aceptar**>. La primera vez que inicie la sesión, utilice la siguiente configuración:

Username (nombre de usuario): admin

Password (contraseña): (sin contraseña)

Para proteger su Switch contra accesos no autorizados, ´cambie la contraseña por defecto. Consulte el Capítulo 5.2: Inicio y fin de sesión.

3 Usando el Administrador de Configuración

El Switch proporciona una aplicación Web preinstalada llamada **Configuration Manager**. Con ella es posible configurar los ajustes del dispositivo para ajustarse a las necesidades de su red. Podrá acceder a esta aplicación a través de su navegador Web desde cualquier PC conectado al Switch a través de los puertos LAN.

3.1 Inicio de sesión en "Configuration Manager"

La aplicación "Configuration Manager" está preinstalada en el Switch. Para acceder a ella, necesitará lo siguiente:

- Un PC conectado en un puerto LAN del Switch, tal y como se describe en el capítulo de guía rápida.
- Un navegador Web instalado en su PC. Esta aplicación está especialmente diseñada para Microsoft Internet Explorer® 5.0 o superior. Netscape no es soportado por esta aplicación.

También puede acceder al programa desde cualquier PC conectado al Switch a través de los puertos LAN.

3.1.1 Configuración de "Configuration Manager"

1. Por defecto, el sistema de autentificación Web del Switch está desactivado. Para asegurar la configuración Web del sistema deberá activarlo. Para ello, acceda a la página **System --> Administration**.
2. En el navegador Web, introduzca la dirección IP: **http://192.168.1.1** y pulse <**Entrar**>. Esta es la dirección IP por defecto del Switch. Una pantalla de inicio de sesión aparecerá.
3. Introduzca su nombre de usuario y contraseña, y haga clic en <**Aceptar**> para acceder a la aplicación Configuration Manager. La primera vez que inicie su sesión, utilice los siguientes valores por defecto:

   Nombre de usuario por defecto: admin

   Contraseña por defecto: (sin contraseña)

3.1.2 Configuración de una nueva dirección IP

1. Para configurar una nueva dirección IP, acceda a **System --> IP Setup**. Rellene los campos para la dirección IP, máscara de red y puerta de enlace por defecto y haga clic en <**OK**>**.**
2. Si la dirección IP nueva es distinta de la dirección por defecto, el navegador no podrá actualizar la ventana de estado del Swtich o mostrar páginas. Esta situación es normal, ya que es necesario modificar la dirección IP del Switch en la casilla de dirección del navegador para volver a acceder a esta aplicación. Tras hacer ésto, pulse <**Entrar**> para refrescar la información en la página Web.
3. Para activar autentificación en accesos Web haga clic en el elemento **Administration** en la lista, y seleccione **Enabled** para iniciar la protección por contraseña.

La pantalla de configuración IP aparecerá tras hacer clic en <**OK**>. Para más información consulte las figuras 8 y 9.

Figura 8. Configuración IP GX2024X

Figura 9. Configuración IP GX2016X

Las unidades GigaX 2024X y 2016X usan la misma interfaz Web, exceptuando la imagen del panel frontal en la parte superior de la pantalla.

En las figuras que acompañan a este manual, si los contenidos de la pantalla en ambos modelos es el mismo, solo las imágenes del modelo GigaX 2024X serán mostradas. En caso contrario las imágenes de ambos modelos GigaX 2024X y 2016X serán mostradas.

3.2 Disposición funcional

Una página típica de configuración está formada por tres marcos separados. (superior, medio e inferior).

El marco superior (o bandera) muestra el logo del switch y su panel frontal. Este marco actualiza y muestra sus LEDs de manera periódica. Consulte las siguientes tablas para más información sobre los LEDs.

• Tabla 4 para las definiciones de los LED (página 8).

• Tabla 5 para la descripción de los colores según el estado.

Haciendo clic en el icono del puerto mostrará su configuración en el marco inferior derecho.

Tabla 5: Descripción de colores en puertos

Color en puerto	Descripción
Verde	Enlace Ethernet establecido
Negro	No hay enlace Ethernet
Ámbar	Enlace presente pero puerto desactivado manualmente o a través de "spanning tree"

El marco izquierdo contiene la barra de menús incluyendo todas las funciones disponibles para la configuración del Switch. Estas funciones están agrupadas en categorías, tales como System, Bridge, etc. Puede hacer clic en cualquiera de éstas para mostrar una página de configuración específica.

El marco derecho muestras las páginas de configuración o gráficas de estadísticas. Consulte el capítulo 4.7 para más información.

Figura 10. Lista de menús expandida.

3.2.1 Trucos para la navegación en menús

• Para expandir un grupo de menús relacionado, haga doble clic en el icono:

• Para contraer un grupo de menús relacionados, haga doble clic en el icono:

3.2.2 Botones e iconos utilizados comúnmente

La siguiente tabla describe la función de cada botón e icono usado en la aplicación.

Tabla 5: Botones e iconos utilizados comúnmente

Botón / Icono	Función
	Almacena cualquier cambio hecho en la página actual.
	Añade una nueva entrada, p.e. Una regla MAC estática o una regla de Firewall ACL.
	Modifica una entrada existente
	Borra una entrada seleccionada, p.e. Una ruta estática o una regla de filtro ACL.
	Refresca la página actual con estadísticas y configuraciones actualizadas.

Consulte los siguientes capítulos para obtener información sobre los pasos a seguir para configurar el Switch a través del programa Configuration Manager o el intérprete de comandos (CLI).

4 Configuration Manager

Este capítulo describe las funciones que pueden ser usadas en la aplicación Configuration Manager. Estas funciones son:

- System (Sistema)
- Physical Interface (Interfaz física)
- Bridge (Puente)
- SNMP
- Security (Seguridad)
- Cable Diagnosis (Diagnóstico del cable)
- Statistical Chart (Gráfico de estadísticas)
- Save Configuration (Guardar configuración)

Para almacenar cambios o nuevos ajustes hechos en cualquiera de las funciones o configuración del Switch deberá acceder a la página "Save Configuration" y hacer clic en <Save>.

4.1 System (Sistema)

Esta sección describe las tareas que puede realizar relacionadas con el sistema:

- Configurar el nombre del sistema, contacto, localización y otra información relacionada;
- Asignar direcciones IP;
- Activar / Desactivar autentificación Web;
- Reiniciar el sistema; y
- Actualizar el Firmware.

4.1.1 Management (Administración)

La página de administración (**Management**) contiene la siguiente información:

Figura 11. Management

• **Model Name**: El nombre del producto.

• **MAC Address**: Dirección MAC del Switch.

• **System Name**: Nombre para identificar el sistema (editable).

• **System Contact**: Contacto del sistema (editable).

• **System Location**: Localización del sistema (editable).

El caracter "/" no esta permitido al escribir información en los campos editables.

Para almacenar los cambios realizados haga clic en <**OK**>. Utilice <**Reload**> para refrescar los ajustes.

4.1.2 IP Setup (Configuración IP)

El Switch soporta asignaciones IP estáticas y dinámicas. Una IP dinámica es obtenida desde el servidor DHCP dentro de la misma red virtual (VLAN). La página de configuración IP contiene los siguiente parámetros editables:

Figura 12. IP Setup

• **VLAN ID (Identificador de red virtual)**: Identificador de VLAN para el interfaz de administración del sistema. Es necesario estar en la misma VLAN para usos administrativos.

• **DHCP Client (Cliente DHCP)**: Activa DHCP para obtener direcciones IP dinámicas, o desactivar DHCP para especificar direcciones IP estáticas. El servidor DHCP deberán estar en la misma VLAN.

• **IP Address**: Asigna una dirección IP estática para la interfaz de administración del Switch.

• **Network Mask (Máscara de red)**

• **Default Gateway (Puerta de enlace por defecto)**

Para almacenar los cambios realizados haga clic en <**OK**>. Utilice <**Reload**> para refrescar los ajustes.

4.1.3 Administration (administración)

La página **Administration** permite activar / desactivar autentificación para usuarios Web, u agregar/ modificar/eliminar usuarios en la base de datos. Podrá definir hasta 8 usuarios. La configuración por defecto para la interfaz Web no requiere ninguna autentificación.

Figura 13. Administration

- **Password Protection is**: Activa (Enable) o desactiva (Disable) la autentificación Web.
- **User Name**: Nuevo nombre de usuario.
- **Password**: Contraseña para el nuevo usuario.
- **Confirm Password**: Introduzca la contraseña de nuevo.

Para almacenar los cambios realizados haga clic en <**OK**>. Utilice <**Reload**> para refrescar los ajustes. Tras activar la protección por contraseña, deberá iniciar la sesión de nuevo inmediatamente.

4.1.4 Reboot (Reinicio del sistema)

Un reinicio del sistema detendrá todo el tráfico en red y terminará la conexión a Internet.

Para reiniciar el sistema:

1. Haga clic en **System --> Reboot**. La página de reinicio aparecerá.
2. Haga clic en <**Reboot**>.

4.1.5 Firmware Upgrade (Actualización de Firmware)

ASUS podría proporcionar actualizaciones del Firmware. Todo el software esta contenido en un archivo llamado "archivo imagen". La aplicación Configuration Manager proporciona una forma fácil de cargar el nuevo archivo imagen del Firmware. Para ello, haga lo siguiente:

Figura 14. Firmware Upgrade

1. Haga clic en **System --> Firmware Upgrade** para acceder a la página de Firmware. Esta página contiene la siguiente información:

   • **Hardware Version**: Número de revisión del Hardware.

   • **Boot ROM Version**: Versión del código de inicio (Boot Code).

   • **Firmware Version**: Muestra la versión del Firmware actualmente en uso. Este número será actualizado tras actualizar el Firmware.

2. En el cuadro **Firmware or Auto-config file**, introduzca la ruta y nombre del archivo de imagen del Firmware. También puede hacer clic en <**Browse**> para buscar el archivo imagen del Firmware en su PC.

3. Haga clic en <**Upload**> para actualizar el Firmware. El sistema se reiniciará tras completar esta operación.

Si el reinicio automático no se realiza, consulte la sección "4.1.4: Reboot (Reinicio del sistema)" para realizar una reinicio de sistema manual.

El nombre de archivo del archivo de autoconfiguración debe ser llamado "config.bat", y la primera línea de éste archivo debe ser "#autoconfig".

4.1.6 Configuration Backup (Copias de seguridad de la configuración)

Esta página contiene las funciones de copia de seguridad y restauración del sistema.

Figura 15. Configuration Backup

Para hacer una copia de seguridad del sistema

Haga clic en <**Backup**> para guardar el archivo de configuración del sistema (config.bac).

Para restaurar el archivo de configuración

Podrá acceder a la localización del archivo del sistema en el cuadro "**Restore configuration file**" directamente, o bien haciendo clic en <**Browse**> para seleccionar el nombre del archivo de configuración en la ventana que aparecerá. Haga clic en <**Restore**> para restaurar el archivo de configuración.

4.2 Physical Interface (Interfaz física)

La interfaz física muestra el estado de los puertos Ethernet en tiempo real.

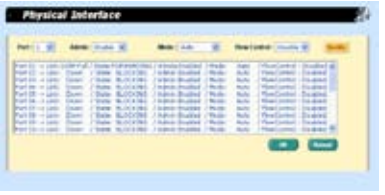


Figura 16. Interfaz física

Puede configurar los siguientes campos en cada puerto:

- **Port (Puerto):** Puerto a configurar
- **Admin (Administración):** Activa (enable) o desactiva (disable) este puerto
- **Mode (Modo):** selecciona la velocidad y modo dúplex
- **Flow Control (Control de Flujo):** Activa (enable) o desactiva (disable) el mecanismo de control de flujo 802.3x
- **Ventana de estado de los puertos**: Muestra la siguiente información en cada puerto:

Link Status	Velocidad y modo duplex de un enlace existente, de lo contrario el enlace está desactivado
State	Estado STP
Admin	Puerto activado (enabled) o desactivado (disabled)
Mode	Velocidad de enlace y modo dúplex configurado por el usuario
Flow Control	Mecanismo de control 802.3x activado (enable) o desactivado (disable)

Para modificar esta página, seleccione el número de puerto correspondiente y haga clic en <**Modify**>. El campo modificado será actualizado en la ventana de estado. Sin embargo, la modificación no tendrá efecto hasta que ejecute **Save Configuration** (para más información consulte el capítulo 4.9: Save Configuration (Guardar configuración)).

4.3 Bridge (Puente)

La página de puentes de grupo contiene la mayoría de la configuración de nivel 2, como por ejemplo la agregación de enlaces o STP.

Figura 17. Spanning Tree

4.3.1 Spanning Tree (arbol de cobertura)

La página de configuración para el protocolo del árbol de cobertura (Spanning Tree Protocol - STP) puede desactivar y activar esta función en tiempo real. Esta página esta formada por tres partes:

a) Información raíz;

b) Configuración STP; y

c) Configuración de puertos.

Información raíz

La primera parte muestra la información raíz, con la configuración STP raíz del Switch.

Configuración STP

La segunda parte es la configuración STP. Las siguientes opciones están disponibles:

• **Disable/STP Enable/RSTP Enabled**: Activa/desactiva STP/RSTP. Al activar STP/RSTP, éste usará los siguientes ajustes si el Switch es un Switch raíz.

• **Hello Time**: Intervalo entre BPDUs (BPDUs son unidades de datos en protocolos de puente).

• **Max Age**: Tiempo máximo para recibir la información del protocolo antes de ser descartado.

• **Forward Delay**: Tiempo de retraso en el envio de BPDUs. Este valor será usado por todos los puentes de la red.

• **Bridge Priority**: La prioridad de cada Switch en la red.

Configuración de puertos

La tercera parte es la configuración de puertos. Esta compuesta por una ventana que muestra la configuración actual de cada puerto. Haga clic en <**Modify**> para cambiar la configuración de STP/RSTP. Los siguientes campos estarán disponibles:

• **Port (Puerto)**: Seleccione el correspondiente puerto a configurar.

• **Priority (Prioridad)**: Prioridad en cada puerto del Switch, en valores numéricos. Un valor numérico bajo indica una prioridad alta. El puerto con una prioridad inferior será bloqueado por el STP si se detecta un bucle en la red. El rango de valores válidos es de 0 a 240.

• **Path Cost (Coste de ruta)**: El rango de valores válido es de 1 a 200000000

o Auto. El coste de ruta configurado por el usuario será mostrado en AdminCost, y el coste de ruta de operación será mostrado en OperCost. Un coste mayor suele ser bloqueado por el STP si se detecta un bucle de red.

• **Edge Port (Puerto terminal)**: Por defecto, todos los puertos están configurados como terminales. Los puertos terminales se convierten en puertos STP cuando un BPDU es recibido. Un puerto terminal necesita de un tiempo muy corto para estar en estado de reenvío.

• **Point to Point (Punto a punto): Auto/Yes/No (Auto/Si/No)**: Un enlace full dúplex es considerado como enlace Punto a Punto. En caso contrario, es un enlace compartido. Un enlace Punto a Punto podría tener un tiempo de convergencia menor. Auto es recomendado en la mayoría de los casos.

Haga clic en <**OK**> para almacenar los cambios realizados. Utilice <**Reload**> para refrescar la información mostrada.

4.3.2 Link Aggregation (Agregación de enlaces)

Esta página configura el grupo de agregación de enlaces (port trunking). El Switch puede disponer de hasta 15 grupos de agregación de enlaces. Los parámetros de configuración son los siguientes:

Figura 18. Agregación de enlaces en GX2024X

Figura 19. Agregación de enlaces en GX2016X

• **Show Trunk (Mostrar Trunk)**: Seleccione **Add a new Trunk (Agregar un nuevo Trunk)** para crear un nuevo grupo. O seleccione un grupo existente para mostrar los siguientes campos e iconos de puertos.

• **Name**: El nombre del grupo.

• **Trunk ID**: Un número para identificar al grupo Trunk junto al nombre del grupo.

• **LACP**: Activa (Enable)/Desactiva (Disable) LCAP en el Trunk seleccionado. El modo LACP esta fijado como Activo.

• **Remove Trunk**: Borrar el Trunk seleccionado.

• **Iconos de puertos**: Estos iconos estan listados de la misma forma que aparecen en el panel frontal. haga clic en el icono para seleccionar los miembros de su grupo. El puerto puede ser borrado de un grupo haciendo de nuevo clic en el puerto seleccionado.

Haga clic en <**OK**> para enviar la configuración al Switch a través del

Todos los puertos del grupo de agregación de enlaces DEBEN operar en modo full-duplex a la misma velocidad.

Todos los puertos del grupo de agregación de enlaces DEBEN estar configurados en modo de auto-negociación o modo full duplex. Esta configuración hará posible en enlace full duplex. Si configura los puertos en modo full duplex forzado, el compañero de enlace DEBERÁ estar configurado de la misma manera. De lo contrario el enlace de agregación podría operar de forma anormal.

Todos los puertos del grupo de agregación de enlaces DEBEN tener la misma configuración VLAN.

Todos los puertos del grupo de agregación de enlaces son tratados como un solo enlace lógico. Esto quiere decir que un cambio de atributos realizado en uno de los miembros será reflejado en el resto. Por ejemplo, si un grupo Trunk está formado por los puertos 1 y 2, y la configuración VLAN del puerto 1 se modifica, también lo hará la del puerto 2.

servidor HTTP. Haga clic en <**Reload**> para refrescar la pantalla. Para almacenar la nueva configuración de forma permanente, vaya a la página **Save Configuration** y haga clic en <**Save**>.

Para asegurarse de que el enlace esta físicamente activo, deberá comprobar la velocidad del enlace y el modo dúplex en tiempo real. Vaya a **Physical Interface** y seleccione el modo de enlace de los puertos del Trunk en la ventana de estado en tiempo real (Runtime Status). Si todos los miembros del Trunk estan en la misma velocidad y modo full duplex, entonces el grupo Trunk ha sido configurado con éxito. Si alguno de los miembros no esta en la misma velocidad o modo duplex, entonces el Trunk no ha sido configurado correctamente. Compruebe el enlace compañero y haga las modificaciones oportunas para que todos los miembros del mismo grupo Trunk estén en la misma velocidad y modo duplex.

4.3.3 Mirroring (Puertos Espejo)

El **Mirroring**, junto a un analizador del tráfico en red, le ayudará a controlar el tráfico en red. También podrá controlar los paquetes entrantes y salientes de puertos seleccionados.

• **Mirror Mode (Modo de espejo)**: Activa (Enable) o desactiva (Disable) la función de espejo en el grupo seleccionado.

• **Monitor Port (Puerto espejo)**: Recibe las copias de todo el tráfico a los puertos espejo seleccionados.

El puerto monitor no puede pertenecer a ningún grupo de agregación de enlaces, y no opera como un puerto normal del Switch. Éste no intercambia paquetes ni aprende direcciones. Sólo soporta 8 puertos espejo de salida, y los paquetes de estos puertos irán sin etiquetas.

Figura 20. Página de puertos espejo en GX2024X

Figura 21. Página de puertos espejo en GX2016X

Haga clic en <**OK**> para enviar los cambios al Switch a través del servidor HTTP. Haga clic en <**Reload**> para refrescar la página.

4.3.4 Static Multicast (Multidifusión estática)

Esta página permite agregar direcciones de multidifusión a la tabla de multidifusión. Este Switch puede mantener hasta 127 entradas. Todos los puertos del grupo reenviarán los paquetes de multidifusión especificados a otros puertos en el grupo.

Figura 22. Multidifusión estática en GX2024X

• **Show Group (Mostrar grupo)**: Seleccione **Add a new Group** para introducir una nueva entrada, o seleccione una dirección de grupo existente para mostrar ésta.

• **MAC Address (Dirección MAC)**: Selecciona la dirección de multidifusión

• **VLAN**: Selecciona el grupo VLAN

Figura 23. Multidifusión estática en GX2016X

Haga clic en <**OK**> para almacenar los cambios realizados. Utilice <**Reload**> para refrescar la información mostrada.

4.3.5 IGMP Snooping (Monitorización IGMP)

Figura 24. Monitorización IGMP

La función de monitorización IGMP puede ser activada o desactivada. Esto ayuda a reducir el tráfico en multidifusiones en red. Cuando esta función está activada, el Switch toma los paquetes IGMP y coloca el nuevo grupo en la tabla de multidifusión. Sin embargo, si las entradas estáticas ocupan totalmente los 256 espacios, el sistema de monitorización IGMP no funcionará correctamente. El Switch sólo permite 256 grupos de grupos de multidifusión de nivel 2.

4.3.6 Bandwidth Control (Control de ancho de banda)

El control de ancho de banda controla los límites de la tasa de transmisión de los Frames seleccionados. El Switch soporta esta función en cada puerto configurando los siguientes elementos:

Figura 25. Control de ancho de banda

Ingress bandwidth control (Control de ancho de banda en paquetes entrantes)

- **Port (Puerto)**: Selecciona el puerto a configurar.
- **Control**: Activa (Enable) o Desactiva (Disable) el control de ancho de banda en paquetes entrantes.
- **Mode (Modo)**:
  - **Bcast**: Limita los paquetes de difusión (broadcast).
  - **Bcast, Mcast**: Limita los paquetes de difusión y multidifusión (multicast).
  - **Bcast, Mcast, Dlf**: Limita los paquetes de difusión, multidifusión y unidifusión (unicast) en caso que haya fallos de comprobación de las direcciones de destino en paquetes.
  - **All**: Limita todo tipo de paquetes.
- **Limit Rate (tasa límite)**: El rango que limita el número de paquetes máximo del tipo seleccionado. Por ejemplo, si activa difusión/ multidifusión, la cantidad de tráfico de cada tipo no podrá exceder el valor límite. El rango de valores válido es de entre 70 a 250000(Kbps).

Egress bandwidth control (Control de ancho de banda en paquetes salientes)

- **Port (Puerto)**: Selecciona el puerto a configurar.
- **Control**: Activa(Enable)/Desactiva(Disable) en control de ancho de banda.
- **Limit Rate (tasa límite)**: Tasa máxima de transmisión de paquetes salientes. El rango de valores válido es de entre 70 a 250000(Kbps).

Haga clic en <**OK**> para enviar los cambios al Switch a través del servidor HTTP. Haga clic en <**Reload**> para refrescar la página. Para almacenar la configuración de forma permanente, vaya a la página **Save Configuration** y haga clic en <**Save**>.

4.3.7 Dynamic addresses (Direcciones dinámicas)

Figura 26. Direcciones dinámicas

La dirección dinámica será la dirección MAC especificada en la búsqueda, y envejecerá en la tabla si ésta no es aprendida de nuevo tras un periodo de tiempo. Es posible ajustar el tiempo de envejecimiento en segundos introduciendo un número válido entre 15 y 3825. Haga clic en <**OK**> para almacenar los cambios realizados. Para almacenar la configuración de forma permanente, vaya a la página **Save Configuration** y haga clic en <**Save**>.

Puede acceder a las direcciones MAC haciendo clic en el puerto, VLAN ID, y/o dirección MAC, y haga clic en <**Query**>. La ventana de direcciones mostrará el resultado de su consulta.

4.3.8 Static addresses (Direcciones estáticas)

Direcciones MAC agregadas de esta manera no envejecerán y permanecerán en la tabla de direcciones hasta que las elimine de la lista de direcciones.

La página **Static Addresses** incluye los siguientes parámetros:

- **MAC Address (Dirección MAC)**: Introduzca la dirección MAC
- **VLAN ID**: Introduzca el identificador de VLAN al cual la dirección MAC pertenece
- **Port Selection (Selección de puertos)**: Seleccione el puerto al cual la dirección MAC pertenece
- **Discard on (Descartar)**: Puede filtrar paquetes cuando la dirección MAC aparezca en los paquetes como dirección de destino.

Para crear una nueva dirección MAC estática

Haga clic en <**Add**>. La nueva entrada será mostrada en la ventana de direcciones. Un máximo de 15 entradas serán mostradas en la primera ventana de direcciones, y las otras entradas serán mostradas en las siguientes páginas. Haga clic en los enlaces **First (Primero)**, **Previous (Anterior)**, **Next (Siguiente)**, y **Last (Última)** para navegar a través de la lista de entradas.

Para modificar una dirección MAC

Seleccione la dirección MAC que desee modificar y haga clic en <**Modify**>.

Para borrar una dirección MAC

Seleccione la dirección MAC que desee eliminar y haga clic en <**Remove**>.

Para mostrar una dirección MAC

Seleccione la dirección MAC e identificador de VLAN, y haga clic en <**Query**>. Su solicitud será mostrada en la ventana de direcciones .

Haga clic en <**OK**> para almacenar los cambios realizados. Utilice <**Reload**> para refrescar la información mostrada. Para almacenar la configuración de forma permanente, vaya a la página **Save Configuration** y haga clic en <**Save**>.

4.3.9 VLAN (Red Virtual)

4.3.9.1 VLAN Mode (Modo VLAN)

Hay dos modos VLAN en su Switch: (1) VLAN basada en puertos y, (2) VLAN con etiqueta 802.1Q. El Switch soporta esta función por puertos con la posibilidad de configurar los siguientes campos:

a) **Port (Puerto)**: Seleccione el puerto a configurar.

b) **VLAN Mode (Modo VLAN)**

- **VLAN con etiqueta 802.1Q**: La decisión de reenvío sigue VLAN con etiqueta 802.1Q.
- **VLAN basada en puertos**: Si la VLAN está en modo basada en puertos: 1) Cuando el puerto recibe un paquete etiquetado, la decisión de reenvío sigue la norma de VLAN 802.1Q con etiquetas Tagged VLAN; y 2) Cuando recibe un paquete sin etiqueta, la decisión de reenvío sigue la VLAN basada en puertos.

Restricciones

- Si un puerto está en modo VLAN basada en puertos, no podrá ser un puerto promiscuo, y no podrá ejecutar 802.1x y IGMP snooping.
- Miembros de un Trunk deberán estar en el mismo modo VLAN.

Haga clic en <**OK**> para enviar los cambios al Switch a través del servidor HTTP. Haga clic en <**Reload**> para refrescar la página. Para almacenar la configuración de forma permanente, vaya a la página **Save Configuration** y haga clic en <**Save**>.

4.3.9.2 Tagged VLAN (VLAN con etiquetas)

Puede configurar hasta 229 (GX2024X) o 237 (GX2016X) grupos VLAN y mostrar éstos en esta página. El Switch crea una VLAN por defecto (VLAN1), para evitar que no sea posible la conexión la primera vez que se usa. Puede borrar cualquier VLAN existente excepto la VLAN1.

Figura 27. VLAN con etiquetas en GX2024X

Para que el puerto sea asignado como puerto marcado o sin marcar puede activar el botón correspondiente del puerto. El panel de selección dispone de tres tipos de botones:

- **Tipo "U":** Puerto sin marcar que borrará las etiquetas VLAN desde los paquetes transmitidos.
- **Tipo "T":** Todos los paquetes transmitidos desde este puerto serán marcados.

Figura 28. VLAN con etiquetas en GX2016X

- **Tipo "Vacío":** Éste puerto no será miembro del grupo VLAN.

Los otros campos configurables son los siguientes:

- **Show VLAN (Mostrar VLAN)**: Seleccione una VLAN existente para mostrar o seleccionar ésta.
- **Add a new VLAN (Agregar una nueva VLAN)**: Crea un nuevo grupo VLAN.
- **Name (Nombre)**: Nombre de la VLAN.
- **VLAN ID (Identificador VLAN)**: Este campo es requerido al crear una nueva VLAN.

- **Remove VLAN (Borrar VLAN)**: Borrar una VLAN existente. Este campo no aparece en la página de creación de VLANs.
- **Private VLAN (VLAN Privada)**: Convierte la VLAN en privada (PVLAN). Una PVLAN proporciona seguridad con la simplicidad de una configuración VLAN. El administrador/a del sistema puede reducir el consumo de recursos VLAN y IP proporcionando la misma seguridad a su red. VLAN 1 no puede ser usada como PVLAN. El número total de PVLANs es cuatro. Un puerto imagen monitor no puede ser un miembro PVLAN. La multidifusión estática no puede ser aplicada a VLANs privadas. Hay dos tipos de puertos en una PVLAN: 1) Puerto promiscuo y 2) Puerto aislado.

a) **Promiscuous Port (Puerto promiscuo)**: Una PVLAN debe y sólo puede tener un puerto promiscuo. Éste comunica con todas las interfaces en la PVLAN. Algunas restricciones de los puertos promiscuos son:

- Un puerto promiscuo no puede estar sin etiqueta.
- Un puerto promiscuo no puede ser un puerto Trunk.
- Un puerto promiscuo no puede estar en modo VLAN basado en puertos.

b) **Isolated Port (Puerto aislado)**: Es el puerto no promiscuo en una PVLAN. Tiene una completa separación de nivel 2 con los otros puertos de la misma PVLAN, pero no del puerto promiscuo. Las PVLANs bloquean el tráfico en puertos aislados, enviando ésta sólo a puertos promiscuos. Algunas restricciones de los puertos aislados son:

- Un puerto aislado sólo puede procesar paquetes sin etiquetas. Paquetes con etiquetas serán descartados por éste puerto.
- Un puerto aislado sólo puede pertenecer a una VLAN, y esta será una VLAN privada.
- Un puerto aislado no puede ejecutar monitorizaciones IGMP.

- **Priority Override (Anulación de prioridades)**: Cuando seleccione la casilla "Priority override", esta opción solo será aplicada a los miembros de esta VLAN. Cuando esto ocurre, el campo de prioridad de todos los paquetes con dicho identificador de VLAN (VLAN ID) serán reescritos con una prioridad superior. Esta prioridad será superior a la definida por defecto en el puerto, y a la prioridad IP.

- **Priority (Prioridad)**: El valor de prioridad se utiliza para modificar la prioridad de cualquier Frame asociado con el ID de esta VLAN, siempre que la casilla "Priority override" sea seleccionada.

Si desea que la decisión de reenvío de los miembros de la VLAN siga las reglas de VLAN con etiquetas 802.1Q, deberá ir a la página **VLAN Mode** y seleccionar "**802.1Q Tagged VLAN**" como el modo VLAN de estos puertos miembros.

Haga clic en <**OK**> para enviar los cambios al Switch a través del servidor HTTP. Haga clic en <**Reload**> para refrescar la página. Para almacenar la configuración de forma permanente, vaya a la página **Save Configuration** y haga clic en <**Save**>.

4.3.9.3 Port-Based VLAN (VLAN basada en puertos)

VLAN basada en puertos es una VLAN donde la decisión de reenvío de paquetes se basa en la dirección MAC de destino y su puerto asociado. Es la más simple y común forma de VLAN. En una VLAN basada en puertos, el administrador/a de sistema asigna los puertos del Switch a un grupo VLAN específico. Puede configurar hasta 26 (GX2024X) o 18 (GX2016X) grupos VLAN basados en puertos y mostrar los grupos VLAN en esta página.

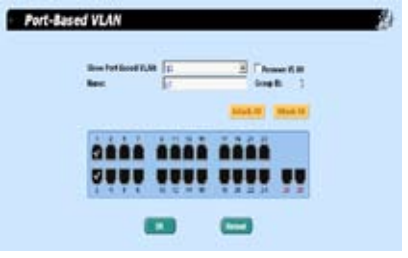


Figura 29: VLAN basada en puertos en GX2024X

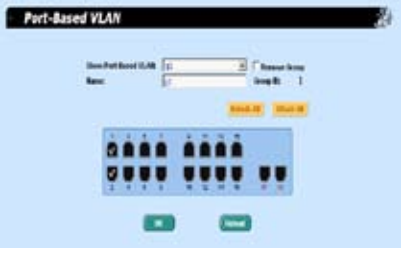


Figura 30: VLAN basada en puertos en GX2016X

• **Show Port-Based VLAN (Mostrar VLAN basada en puertos)**: Seleccione **Add a new VLAN** para crear un nuevo grupo, o seleccione un grupo existente para mostrar los siguientes campos e iconos de puertos:

• **Name (Nombre)**: El nombre del grupo.

• **Group ID (Identificador de grupo)**: Este campo será requerido para introducir un identificador de grupo al crear una nueva VLAN basada en puertos. El rango válido de identificadores de grupo es de entre 1 y 26 (GX2024X) o entre 1 y 18(GX2016X).

• **Remove Group (Eliminar grupo)**: Elimina una VLAN basada en grupos existentes. Este campo no aparece en la página de creación de VLANs.

Si desea que el grupo VLAN basado en puertos creado sea efectivo, deberá ir a la página **VLAN Mode** y seleccionar **Port-Based VLAN** como el modo VLAN de los puertos miembros.

Haga clic en <**OK**> para enviar los cambios al Switch a través del servidor HTTP. Haga clic en <**Reload**> para refrescar la página. Para almacenar la configuración de forma permanente, vaya a la página **Save Configuration** y haga clic en <**Save**>.

4.3.9.4 Puerto por defecto en VLAN y CoS

Esta página incluye algunos de los elementos relacionados con las etiquetas de VLANs en cada puerto.

• **Port (Puerto)**: Seleccione el puerto a configurar

• **PVID**: VLAN ID basada en puerto. Cada paquete sin etiqueta recibido en este puerto será etiquetado con este identificador de grupo de dicha VLAN.

• **CoS value (Valor en Clase de Servicio)**: Cada paquete sin etiqueta recibido en este puerto será asignado a esta CoS en la VLAN etiquetada.

Haga clic en <**Modify**> para cambiar los contenidos de la ventana de la lista de puertos. Haga clic en <**OK**> para enviar los cambios al Switch a través del servidor HTTP. Haga clic en <**Reload**> para refrescar la página. Para almacenar la configuración de forma permanente, vaya a la página **Save Configuration** y haga clic en <**Save**>.

4.4 SNMP

Simple Network Management Protocol (SNMP) se utiliza para administrar la red. Puede usar la página de configuración de SNMP para activar o desactivar el soporte SNMP.

Para proporcionar una administración y control de acceso más seguros, SNMPv3 es soportado. SNMP dispone de los siguientes parámetros de configuración:

4.4.1 Community table (Tabla de comunidad)

Puede escribir diferentes nombres de comunidades y especificar si la comunidad tiene el privilegio para hacer ajustes (acceso de escritura) marcando el cuadro. Haga clic en <**OK**> para almacenar la configuración o <**Reload**> para refrescar la página.

Figura 31. Tabla de comunidad

4.4.2 Host Tabla (Tabla Host)

Esta página enlaza la dirección IP del Host al nombre de comunidad introducido en la página de tabla de comunidades. Escriba una dirección IP y seleccione el nombre de comunidad desde el menú desplegable. Haga clic en <**OK**> para almacenar la configuración o <**Reload**> para refrescar la página.

Figura 32. Tabla Host

4.4.3 Trap Setting (Configuración de trampas)

Definiendo trampas en direcciones IP de destino y nombres de comunidades, puede activar la función de trampa SNMP para enviar paquetes trampa en diferentes versiones (v1 o v2c). Haga clic en <**OK**> para almacenar la configuración o <**Reload**> para refrescar la página.

Figura 33. Configuración de trampas

4.4.4 VACM Group (Grupo VACM)

VACM (View-based Access Control Model) Group se utiliza para configurar la información del grupo SNMPV3 VACM.

Figura 34. Grupo VACM

La página del grupo VACM dispone de los siguientes parámetros de configuración:

• **Group Name (Nombre del grupo)**: Nombre del grupo de seguridad.

• **Read View Name (Nombre de Vista de Lectura)**: Nombre de vista de lectura al cual este grupo pertenece. Los mensajes SNMP relacionados son Get (Recoger), GetNext (Recoger el siguiente) y GetBulk (recoger un grupo).

• **Write View Name (Nombre de Vista de Escritura)**: Nombre de vista de escritura al cual este grupo pertenece. El mensaje SNMP relacionado es Set.

• **Notify View Name (Nombre de Vista de Notificación)**: Nombre de vista de notificación al cual este grupo pertenece. Los mensajes SNMP relacionados son Trap (Trampa) y Report (Informe).

• **Security Model (Modelo de seguridad)**: Modelo de seguridad al cual este grupo pertenece. Todos son apropiados para v1,v2 y v3. USM esta relacionado con SNMPv3.

• **Security level (Nivel de seguridad)**: Nivel de seguridad. Puede seleccionar NoAuth (no autentificar), AuthNopriv (autentificar no privados) y AuthPriv (autentificar privados).

Haga clic en <**Add**> para crear un nuevo grupo VACM. Para borrar un grupo VACM existente, seleccione el grupo y haga clic en <**Remove**>. Para actualizar una entrada existente, seleccione el grupo y haga clic en <**Modify**>. Haga clic en <**OK**> para almacenar la configuración o <**Reload**> para refrescar la página. Para almacenar la configuración de forma permanente, vaya a la página **Save Configuration** y haga clic en <**Save**>.

4.4.5 VACM View (Vista VACM)

Vista VACM (View-based Access Control Model) es usada para ver la información del grupo SNMPV3 VACM.

Figura 35. Vista VACM

La página de vista VACM dispone de los siguientes parámetros de configuración:

• **View Name (nombre de vista):** Nombre del grupo de seguridad.

• **View Type (tipo de vista):** Introduzca el tipo de vista al cual la vista pertenece, "Included" (incluido) o "Excluded" (excluido), cuando la vista del subtree coincida con el Oid en el mensaje SNMPv3.

• **View Subtree (subárbol de vistas):** Introduzca el subárbol de vista al cual la vista pertenece. El subárbol es el Identificador de Objeto (OID) que coincide con el OID en el mensaje SNMPv3. La equivalencia es correcta cuando el subárbol es más corto que el OID en el mensaje SNMPv3.

• **View Mask (Máscara de vista)**: Introduzca la nueva máscara de vista al cual la vista pertenece. Cada bit en la máscara representa un dígito entre los puntos del subárbol de vistas de la parte izquierda. El bit '0' significa 'nada'.

Haga clic en <**Add**> para crear una nueva vista VACM. Para borrar un grupo VACM existente, seleccione el grupo y haga clic en <**Remove**>. Para actualizar una entrada existente, seleccione el grupo y haga clic en <**Modify**>. Haga clic en <**OK**> para almacenar la configuración o <**Reload**> para refrescar la página. Para almacenar la configuración de forma permanente, vaya a la página **Save Configuration** y haga clic en <**Save**>.

4.4.6 USM User (Usuario USM)

El **usuario USM (User-based Security Model)** se usa para configurar la información del usuario SNMPV3 USM.

La página "USM User" dispone de los siguientes parámetros:

Figura 36. Usuario USM

• **Engine Id (Identificador de motor)**: Introduzca el identificador de motor que coincida con el identificador en el administrador (Manager).

• **Name (nombre)**: Introduzca el nombre combinado con el identificador de motor que debería coincidir con el nombre e identificador de motor del Administrador (Manager).

• **Auth Protocol (Protocolo de autentificación):** Protocolo de autentificación al cual el usuario SNMP y el grupo de seguridad pertenecen. Puede seleccionar NoAuth ,MD5, o SHA1. Si selecciona NoAuth, no necesitará introducir ninguna contraseña.

• **Auth Password (Contraseña de autentificación):** Contraseña utilizada por el protocolo de autentificación. La contraseña deberá contener al menos 8 caracteres o dígitos.

• **Priv Protocol (Protocolo de privacidad):** Protocolo de privacidad al cual el usuario SNMP y el grupo de seguridad pertenecen. Puede seleccionar NoPriv o DES. Si selecciona NoPriv, no necesitará introducir ninguna contraseña.

• **Priv Password (Protocolo de privacidad):** Contraseña utilizada por el protocolo de privacidad. La contraseña deberá contener al menos 8 caracteres o dígitos.

Haga clic en <**Add**> para crear un nuevo usuario USM. Para borrar un usuario USM existente, selecciónelo y haga clic en <**Remove**>. Para actualizar una entrada existente, seleccione el grupo y haga clic en <**Modify**>. Haga clic en <**OK**> para almacenar la configuración o <**Reload**> para refrescar la página. Para almacenar la configuración de forma permanente, vaya a la página **Save Configuration** y haga clic en <**Save**>.

4.5 Security (Seguridad)

El switch utiliza la función de seguridad soportada por los puertos basados en 802.1x. Solamente Hosts autorizados tendrán permiso para acceder al puerto del switch. El tráfico será bloqueado si viene de un Host no autentificado. La autentificación puede ser proporcionada a través de un servidor RADIUS o una base de datos local en el switch.

El switch también soporta asignación dinámica VLAN a través del proceso de autentificación 802.1x. La información VLAN para los usuarios/puertos deberá ser configurada apropiadamente en el servidor de autentificación antes de activar esta función.

4.5.1 Port access control (Control de acceso a puertos)

Port access control se utiliza para configurar varios parámetros 802.1x. 802.1x utiliza un servidor RADIUS/ TACACS+ o en una base de datos local para autentificar usuarios de puertos.

Figura 37. Control de Acceso a Puertos

El control de acceso a puerto dispone de dos tipos de ajuste: Ajustes de Bridge (Global) y ajustes de puerto.

Bridge settings (Ajustes de Bridge)

La página de ajustes de Bridge (Global) dispone de los siguientes parámetros de configuración:

• **Reauthentication (Reautentificación):** Si está activado, el switch intentará autentificar al usuario del puerto de nuevo cuando el tiempo de reautentificación se haya agotado.

• **ReAuthentication Time (Tiempo de reautentificación):** Si activa "Reauthentication", este campo indicará el periodo de tiempo que el switch utilizará para enviar una petición de reautentificación al usuario del puerto.

• **Authentication Method (Método de autentificación)**: Puede usar RADIUS o una base de datos local para autentificar el usuario del puerto.

• **Quiet Period (Periodo de Espera):** Si la autentificación fallara, el switch esperará este periodo de tiempo antes de enviar otra petición al usuario del puerto.

• **Retransmission Time (Tiempo de transmisión):** Si el usuario del puerto falla al responder a la petición de autentificación desde el switch, éste esperará este periodo de tiempo antes de enviar otra petición de autentificación al usuario del puerto.

• **Max Reauthentication Attempts (Número máximo de intentos de reautentificación):** Cada fallo del usuario del puerto al responder a la petición de autentificación del switch será contada.

Port settings (Ajustes de Puerto)

La página de configuración de puertos dispone de los siguientes parámetros:

• **Port (Puerto)**: Especifica el puerto a configurar.

• **AuthMode (Modo de autentificación)**: Si selecciona **Port_based**, sólo necesitará que un único Host sea autentificado por un servidor RADIUS remoto, servidor remoto TACACS+, o una base de datos local. 'Port_based' soporta Multi-host y GuestVID. Si selecciona **MAC_based**, cada Host deberá ser autentificado antes de acceder a la red. 'MAC_based' no soporta ni Multi-host ni GuestVID. El sistema soporta hasta 256 Hosts que podrán ser autentificados por "MAC_based". Si selecciona "MAC_based", se recomienda activar "Reauthentication" en "bridge settings".

• **AuthCtrl (Control de autentificación)**: Si selecciona **Force_authorized**, el puerto seleccionado será forzado a ser autorizado. En este caso, el tráfico proveniente de todos los Hosts podrá pasar. De lo contrario, si selecciona **Force_unauthorized**, el puerto seleccionado será bloqueado, y ningún tráfico podrá pasar. Si selecciona "Auto", el comportamiento del puerto seleccionado será controlado por el protocolo 802.1x.

• **Multi-host**: Si activa esta opción, todos los Hosts conectados al puerto seleccionado podrán usar el puerto si AL MENOS UNO de ellos pasa el proceso de autentificación. Si desactiva esta opción, SÓLO UNO de los Hosts entre todos los que pasen el proceso de autentificación podrá usar el puerto. Multi-host será desactivado si selecciona **MAC_based** en **Auth Mode**.

• **GuestVID**: Una VLAN para usuarios invitados permite a éstos que sin clientes 802.1x tengan un acceso limitado a la red.

Haga clic en <**OK**> para almacenar la configuración o <**Reload**> para refrescar la página. Para almacenar la configuración de forma permanente, vaya a la página **Save Configuration** y haga clic en <**Save**>.

4.5.2 Port Access Control Status (Estado de Control de Acceso a Puertos)

La página **Port Access Control Status** dispone de dos partes: Información de control de acceso 802.1x para todos los puertos, e inicialización de puertos.

Figura 38. Estado de Control de Acceso a Puertos

802.1x access control information (Información de control de acceso 802.1x)

Esta parte incluye la siguiente información:

• **Port**: Número de puerto.

• **AuthMode**: Muestra el modo de autentificación de un puerto (port_based o MAC_based).

• **AuthCtrl**: Muestra el control de autentificación de un puerto (Force_authorized, Force_unauthorized o Auto).

• **Status**: Muestra el resultado de autentificar un puerto (o MAC suplicante) y pueden ser autorizado (authorized), o desautorizado (unauthorized).

• **VID**: Muestra el identificador VLAN de un puerto.

• **MAC**: Muestra el estado del MAC suplicante como autorizado (authorized) o desautorizado (unauthorized).

Port Initialize (Inicialización de puerto)

Esta parte incluye las siguientes funciones:

• **Port**: Número de puerto que será forzado para ejecutar la inicialización. Una vez seleccionado haga clic en <**OK**> para guardar los ajustes. La función de inicialización puede ser utilizada para descubrir nuevos Hosts conectados a este puerto a través de un Hub, y requerir que nuevos Hosts sean autentificados.

Haga clic en <**Reload**> para refrescar los estados.

4.5.3 Dial-In User (Usuario remoto)

Dial-in User se usa para definir usuarios en la base de datos local del Switch. Esta función dispone de los siguientes parámetros de configuración:

Figura 39. Usuario remoto

- **User Name**: Nombre de usuario.
- **Password**: Contraseña para el usuario.
- **Confirm Password**: Confirme la contraseña introducida en el campo anterior.
- **Dynamic VLAN (VLAN dinámica):** Especifica el identificador para VLAN asignada a los clientes autentificados con 802.1x.

Haga clic en <**Add**> para crear un nuevo usuario. Haga clic en <**Modify**> para confirmar modificaciones. Haga clic en <**OK**> para almacenar la configuración o <**Reload**> para refrescar la página.

4.5.4 RADIUS

Para utilizar un servidor RADIUS externo, necesitará configurar los siguientes parámetros:

Figura 40. RADIUS

- **Authentication Server IP (Servidor IP para autentificación):** Dirección IP del servidor RADIUS.
- **Authentication Server Port (Puerto para autentificación):** Número de puerto que el servidor RADIUS escuchará.
- **Authentication Server Key (Contraseña del servidor para autentificación):** La contraseña utilizada para comunicaciones entre el switch GigaX y el servidor RADIUS.
- **Confirm Authentication Key(Confirmación de contraseña para autentificación):** Escriba de nuevo la contraseña del campo anterior.

Haga clic en <**OK**> para almacenar la configuración o <**Reload**> para refrescar la página.

La VLAN de un servidor RADIUS conectado al Switch debe ser la misma que la VLAN del interfaz de administración del sistema.

4.5.5 TACACS+

Para usar un servidor externo TACACS+ necesitará configurar los siguientes parámetros:

Figura 41. TACACS+

• **Authentication Server IP**: Dirección IP del servidor TACACS+.

• **Authentication Server Port**: Número de puerto al cual TACACS+ va a escuchar.

• **Authentication Server Key**: Clave a usar en comunicaciones entre el Switch y el servidor TACACS+.

• **Confirm Authentication Key**: Repita la clave escrita en el cuadro anterior.

Haga clic en <**OK**> para enviar la configuración al Switch a través del servidor HTTP. Haga clic en <**Reload**> para reflescar la pantalla. Para almacenar la nueva configuración de forma permanente, vaya a la página **Save Configuration** y haga clic en <**Save**>.

La VLAN de un servidor TACACS+ conectado al Switch debe ser la misma que la VLAN del interfaz de administración del sistema.

4.5.6 Port Security (Seguridad en puertos)

La página de seguridad en puertos incluye configuración, estado, y función de direcciones MAC seguras.

4.5.6.1 Port configuration (Configuración de puertos)

Esta página permite la configuración de varios parámetros de seguridad en puertos. El número total de direcciones MAC seguras en el Switch es 1024. Los siguientes campos pueden ser configurados:

Figura 42. Configuración de puertos

• **Port**: Seleccione el puerto a configurar.

• **Admin**: Activa (Enable) o desactiva (Disable) la función de seguridad en puertos.

• **Violation Mode**: Define el modo de violación. Esta acción será ejecutada cuando ocurra una violación de la seguridad. Una violación de la seguridad ocurre en las siguientes situaciones:

1) El número máximo de direcciones MAC seguras ha sido agregado a la tabla de direcciones, y una estación cuya dirección MAC no está en la tabla intenta acceder al interfaz.

2) Una dirección aprendida o configurada en una interfaz de seguridad es vista en otra interfaz segura en la misma VLAN. Puede configurar la interfaz en cualquiera de los siguientes tres modos de violación:

a) **Protect**: Es este modo, no será notificado si ocurre una violación en la seguridad.

b) **Restrict**: Es este modo, si ocurre una violación en la seguridad será notificado. Una trampa SNMP será enviada, un mensaje syslog será almacenado, y el contador de violaciones será incrementado.

c) **Shutdown**: Es este modo, una violación de la seguridad en puertos causará que la interfaz entre en estado de bloqueo de forma inmediata. Una trampa SNMP será enviada, un mensaje syslog será almacenado, y el contador de violaciones será incrementado.

• **Max MAC Addresses**: Define los números máximos de direcciones MAC seguras. El rango de valores es de 1 a 132. La suma de este valor en todos los puertos debe ser menor o igual al número máximo de direcciones MAC permitidas en el Switch.

• **Aging Time**: Define el tiempo de envejecimiento. Este valor es de 0 a 1440 (minutos). El mecanismo de envejecimiento sólo es efectivo para direcciones MAC seguras dinámicas. Si el tiempo es 0, el mecanismo de envejecimiento será desactivado en este puerto.

• **Aging Type**: Define el tipo de envejecimiento para determinar la acción una vez que el tiempo de envejecimiento se haya cumplido. Defina el tipo de envejecimiento para determinar la acción cuando las direcciones seguras MAC dinámicas hayan envejecido. Cada puerto soporta dos tipos de envejecimiento:

a) **Absolute**: Las direcciones seguras en el puerto serán borradas tras el periodo de envejecimiento especificado.

b) **Inactivity**: Las direcciones seguras en el puerto serán borradas solo si no hay tráfico de datos desde las direcciones seguras MAC de origen para el periodo de tiempo especificado.

Seleccione el número de puerto correspondiente y configúrelo, haciendo clic en <**Modify**> cuando haya terminado. Haga clic en <**OK**> para almacenar la configuración o <**Reload**> para refrescar la página. Para almacenar la configuración de forma permanente, vaya a la página **Save Configuration** y haga clic en <**Save**>.

4.5.6.2 Port Status (Estado del puerto)

Esta página muestra información de seguridad en todos los puertos. La información de seguridad que aparecerá es la siguiente:

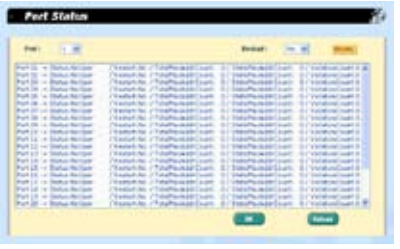


Figura 43. Estado del puerto

• **Port**: Número del puerto.

• **Status (Estado)**:

a) **NoOper**: Indica que la seguridad en el puerto seleccionado ha sido desactivada.

b) **SecureUp**: Indica que la seguridad en el puerto seleccionado está operativo.

c) **SecureDown:** Indica que la seguridad en puerto no está operativa. Esto ocurre cuando la seguridad en puerto esta configurada pero no pudo ser activada debido a ciertos motivos como por ejemplo un conflicto con otras funciones.

d) **Restrict:** Indica que ha ocurrido una violación en puerto cuando el modo de violación es 'restrict'.

e) **Shutdown:** Indica que el puerto ha sido apagado debido a una violación en la seguridad del puerto cuando el modo de violación es 'shutdown'.

• **Restart**: Si el puerto será reiniciado en estado apagado (Yes - Si) / No)).

• **TotalMacAddrCount**: Número total de direcciones MAC (estáticas y dinámicas) seguras actuales.

• **StaticMacAddrCount**: Número total de direcciones MAC estáticas seguras actuales.

• **ViolationCount**: Número total de violaciones en seguridad.

El estado de seguridad en el puerto será '**SecureDown**' (seguridad detenida) cuando se dén una de las siguientes situaciones:

- El enlace del puerto está desactivado.
- El puerto Bridge administrativo está desactivado.

- El puerto es un puerto Trunk.
- El puerto es un puerto monitor en puertos espejo.
- El puerto está ejecutando 802.1x y en modo de Host simple.

Si el estado del puerto es '**Shutdown**', puede seleccionar el número de puerto correspondiente y reiniciar a '**Yes**'. Haga clic en <**Modify**>. El campo modificado será actualizado en la ventana de visualización. Haga clic en <**OK**> para almacenar la configuración o <**Reload**> para refrescar la página. Para almacenar la configuración de forma permanente, vaya a la página **Save Configuration** y haga clic en <**Save**>.

4.5.6.3 Secure MAC address (Direcciones MAC seguras)

Puede agregar direcciones MAC en la tabla de direcciones MAC seguras en un puerto. Las direcciones MAC agregadas de esta forma no envejecerán en esta tabla. Estas direcciones se llaman "Direcciones MAC seguras".

Figura 44. Direcciones MAC seguras

• **MAC Address (Dirección MAC)**: Introduzca la dirección MAC.

• **Port Selection (Selección de puerto)**: Seleccione el puerto al cual la dirección MAC pertenece.

Haga clic en <**Add**> una vez que haya creado una nueva dirección MAC estática. La nueva entrada será mostrada en la ventana de direcciones.

Puede seleccionar un puerto de la selección, y hacer clic en <**Query**>. Podrá ver el total de direcciones MAC seguras actuales del puerto mostradas en la ventana de direcciones.

Puede borrar una dirección existente seleccionando ésta desde la lista y haciendo clic en <**Remove**>. Mantenga pulsada la tecla **mayúsculas** para seleccionar varias entradas.

Haga clic en <**Add**> o <**Remove**> para que la configuración tenga efecto inmediato. Para guardar la dirección MAC segura de forma permanente, vaya a la página **Save Configuration**, y haga clic en <**Save**>.

4.6 QoS (Calidad de servicio)

La página QoS incluye estado de fiabilidad mapeado, anulación de prioridad, y función CoS.

4.6.1 Trust State (Estado de fiabilidad)

La política de bloqueo de paquetes entrantes tiene el trabajo de determinar la prioridad de cada Frame en el controlador de colas. El Switch soporta esta función en cada puerto a través de los siguientes campos:

Figura 45. Estado de fiabilidad

• **Port**: Seleccione el puerto a configurar.

• **Trust State**: DSCP o CoS.

a) **Trust CoS**: Utiliza etiquetas IEEE. Utilice el campo Clase de Tráfico IEEE 802.1p para prioridad de datos si el Frame esta etiquetado como IEEE 802.3ac. De lo contrario, utilice la prioridad de datos por defecto del puerto.

b) **Trust DSCP**: Utilizado para prioridad IP. Utilice campos IPv4 TOS y/o Diffserv si el Frame es IPv4, y utilice campos IPv6 Traffic Class si el Frame es IPv6. De lo contrario, utilice la prioridad de datos por defecto del puerto. En Trust DSCP, la configuración es la misma de la de las páginas **Mapping** y **CoS**.

Haga clic en <**OK**> para enviar la configuración al Switch a través del servidor HTTP. Haga clic en <**Reload**> para reflescar la pantalla. Para almacenar la nueva configuración de forma permanente, vaya a la página **Save Configuration** y haga clic en <**Save**>.

4.6.2 Mapping (Mapeado)

Esta página se utiliza para mapear el valor DSCP (Differentiated Services Code Point) a prioridad CoS (Classification of Service). El rango de valores DSCP válido es de 0 a 63. Para IPv6, 4 multiplicado por el valor DSCP es el valor de case de tráfico (Traffic Class). Por ejemplo, un valor DSCP 4 quiere decir un valor 16 de clase de tráfico IPv6. El Switch soporta ésto ajustando la configuración de los siguientes campos:

Figura 46. Mapping

• **DSCP**: Seleccione el valor DSCP.

• **CoS**: Seleccione la prioridad CoS.

Haga clic en <**OK**> para enviar la configuración al Switch a través del servidor HTTP. Haga clic en <**Reload**> para reflescar la pantalla. Para almacenar la nueva configuración de forma permanente, vaya a la página **Save Configuration** y haga clic en <**Save**>.

4.6.3 Priority Override (Anulación de prioridad)

La página **Priority Override** permite activar o desactivar la anulación de prioridad MAC de QoS basada origen o en destino.

Figura 47. Anulación de prioridad

Si activa la anulación de prioridad MAC basada en origen, ésta puede ocurrir en todos los puertos. Una anulación de prioridad MAC en origen ocurre cuando la dirección de origen de un paquete resulta en una entrada donde la dirección origen ya ha sido agregada a la lista de direcciones MAC estáticas y asignada una prioridad. Cuando esto ocurre, el valor de la prioridad asignado a la tabla ARL estática se una para anular la prioridad del paquete determinada anteriormente. La anulación de prioridad MAC en origen tiene una prioridad superior que la prioridad por defecto en puerto, prioridad IP, y anulación de prioridad VLAN.

Si activa la anulación de prioridad MAC basada en destino, ésta puede ocurrir en todos los puertos. Una anulación de prioridad MAC en destino ocurre cuando la dirección de destino de un paquete resulta en una entrada donde la dirección origen ya ha sido agregada a la lista de direcciones MAC estáticas y asignada una prioridad. Cuando esto ocurre, el valor de la prioridad asignado a la tabla ARL estática se una para anular la prioridad del paquete determinada anteriormente. La anulación de prioridad MAC en destino tiene una prioridad superior que la prioridad por defecto en puerto, prioridad IP, anulación de prioridad VLAN, y anulación de prioridad MAC en origen.

Si desea crear una entrada estática MAC combinada con prioridad CoS, vaya a la página **Static Addresses (Direcciones estáticas)**.

Haga clic en <**OK**> para enviar la configuración al Switch a través del servidor HTTP. Haga clic en <**Reload**> para reflescar la pantalla. Para almacenar la nueva configuración de forma permanente, vaya a la página **Save Configuration** y haga clic en <**Save**>.

4.6.4 CoS

El Switch soporta cuatro colas de salida para cada puerto. Cada valor CoS puede ser mapeado en una de estas cuatro colas. La cola 4 tiene la prioridad

más alta a la hora de transmitir los paquetes. Puede especificar los tipos de programación de la siguiente forma:

Figura 48. CoS

• **Strict priority scheduling (Programación de prioridad estricta)**: Los paquetes en la cola de baja prioridad no serán transmitidos hasta que las colas de alta prioridad estén vacías.

• **Weighted round-robin (WRR) scheduling (Programación a través de peso en forma circular)**: La programación WRR previene que las colas de baja prioridad sean completamente ignoradas en periodos de alta prioridad de tráfico. La programación WRR transmite algunos paquetes de cada cola en turnos. El número de paquetes enviados corresponden a la importancia relativa de la cola. Por ejemplo, si una cola tiene un peso de 2 y otra tiene un peso de 4, dos paquetes enviados desde la primera cola por cada cuatro paquetes que sean enviados desde la segunda. Usando esta programación, las colas de baja prioridad tendrán la oportunidad de enviar paquetes aunque las colas de alta prioridad no estén vacías. En este Switch, el peso de la cola 1 es 1, el peso de la cola 2 es 2, el peso de la cola 3 es 4, el peso de la cola 4 es 8.

Haga clic en <**OK**> para enviar la configuración al Switch a través del servidor HTTP. Haga clic en <**Reload**> para reflescar la pantalla. Para almacenar la nueva configuración de forma permanente, vaya a la página **Save Configuration** y haga clic en <**Save**>.

4.7 Cable Diagnosis (Diagnóstico de cableado)

La función principal de **Cable Diagnosis** es la de detectar fallos en cableado (abierto o cortocircuito) e informar haciendo una estimación de la localización del error. Los diagnósticos de cableado también pueden detectar tipo PHY (10M, 100M o 1000M) y estimaciones sobre la longitud de un cable normal. La estimación de longitud de cable solo es soportada en modo de velocidad Giga.

Figura 49. Diagnostico de cableado

Simplemente seleccione un número de puerto y haga clic en <**Go**>. Los resultados del test de dicho puerto aparecerán.

Al activar el diagnóstico de cableado en un puerto, las conexiones de éste serán desconectadas durante el proceso de diagnóstico.

4.8 Statistics Chart (Gráficas de estadísticas)

La página de gráfico de estadísticas proporciona una muestra del tráfico de red en diferentes gráficas. Puede especificar un periodo de tiempo de refresco de éstas. Puede visualizar la cantidad de tráfico en diferentes gráficas. En ellas se muestran la mayoría de contadores MIB-II.

Haga clic en <**Auto Refresh**> o <**Refresh Rate**> para definir el periodo de recolección de nuevos datos del switch. Puede diferenciar las estadísticas o puertos seleccionando **Color**. Finalmente, haga clic en <**Draw**> para permitir al navegador dibujar la gráfica. Cada nuevo dibujo reiniciará la visualización de las estadísticas.

4.8.1 Traffic comparison (Comparaciones del tráfico)

Esta página muestra una estadística de todos los puertos. Especifique el elemento de estadística a mostrar y haga clic en <**Draw**>. La pantalla mostrará los datos actualizados, refrescando la gráfica de forma periódica.

Figura 50. Comparación de tráfico en GX2024X

Figura 51. Comparación de tráfico en GX2016X

4.8.2 Error Group (Grupo de errores)

Seleccione el **puerto (Port)** y **color** de muestra, y haga clic en <**Draw**>. la ventana de estadísticas muestra una cuenta de errores para el puerto específico. Los datos son actualizados periódicamente.

Figura 52. Grupo de errores

4.8.3 Historical Status (Gráfico de históricos)

Esta gráfica muestra información en diferentes puertos y sus estadísticas. Esta gráfica muestra un histórico de la información estadística.

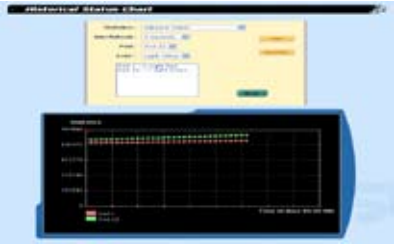


Figura 53. Gráfico de Históricos

4.9 Save Configuration (Guardar configuración)

Haga clic en <**Save**> para almacenar la configuración. Para restaurar los valores predeterminados de fábrica, haga clic en <**Restore**>. Al seleccionar esta última opción perderá cualquier cambio en su configuración original.

Figura 54. Guardar configuración

5 Interfaz de Comandos (CLI)

Este capítulo describe como utilizar la Interfaz de la consola **(Command Line Interface)** para configurar el switch. El switch proporciona conectores RS232 y USB para conectar con su PC. Utilice un emulador de terminal, como por ejemplo HyperTerminal, y un intérprete de comandos para configurar el switch. Deberá configurar el emulador de terminal de la siguiente manera: a) Tasa de baudios = 9600; b) 8 bits datos; c) sin paridad; d) 1 bit de stop; y e) sin control de flujo.

Una vez en modo CLI (modo interprete de comandos), escriba "?" para mostrar todos los comandos disponibles. Esto es muy útil si no está familiarizado con los comandos CLI. El modo CLI se desconecta automaticamente si permanece sin uso durante 10 minutos. Si esto ocurriera deberá iniciar la sesión de nuevo.

Todos los comandos CLI distinguen mayúsculas y minúsculas. Para facilitar su uso, puede entrar en una categoría de comandos escribiendo éste, haciendo de dicha categoría su categoría de trabajo. Por ejemplo, al entrar en la categoría de sistema ("sys") ya no necesitará introducir esta palabra antes de cada subcomando del sistema. La línea de comandos será "(nombre del sistema) sys%" cuando su categoría de trabajo sea "sys".

5.1 Power On Self Test (Auto comprobación durante el encendido)

POST se ejecuta durante el inicio del sistema. Este sistema comprueba la memoria del sistema, LEDs y chips de Hardware en el switch. También muestra información del sistema como resultado de la comprobación del sistema y su inicialización. Puede ignorar la información hasta la línea "(ASUS) %" (consulte la figura 55).

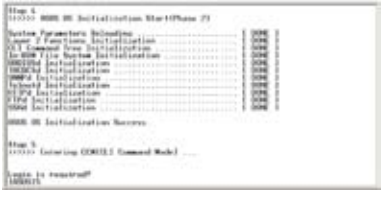


Figura 55. Interfaz CLI

5.1.1 Boot ROM Command Mode (Modo de comandos de inicio en ROM)

Durante el proceso POST, puede entrar en modo "**Boot ROM Command**" presionando la tecla <**Entrar**>.

La figura 56 muestra imágenes duales en el Switch. Un Firmware está en el zócalo 1 y el otro en el zócalo 2.

Figura 56. Modo de comandos de inicio en ROM

Escriba "?" para mostrar mensajes de ayuda disponibles en cualquier comando.

A pesar de que los comandos son útiles en ciertas situaciones, RECOMENDAMOS que no los utilice a menos que conozca bien el uso del comando.

5.1.2 Comandos de inicio en ROM

Escriba "**?**" en el modo de inicio (boot) para mostrar la lista de comandos.

Tabla 7: Comandos de inicio ROM

Comando	Parámetros	Uso	Notas
a	Ninguno	Muestra la dirección MAC	
b	1, 2, a	Soporte para imagen dual. Puede seleccionar el Firmware a ejecutar indicando el identificador de zócalo, o usar "a" para el modo automático. El modo automático ejecutará el Firmware más actualizado. Esta es la configuración por defecto.	Si una actualización de Firmware falla, podrá usar este comando para reiniciar el Switch usando el Firmware anterior. Tras actualizar el Firmware con éxito cambie al modo automático.
c	Dirección IP y máscara / Ninguno	Configura / muestra la dirección IP del cliente TFTP	
g	Ninguno	Carga y ejecuta el Firmware	
h	Ninguno	Muestra ayuda online	
p	Ninguno	Muestra la configuración actual	
r	Ninguno	Reinicia el sistema	
s	Dirección IP y máscara / Ninguno	Configura / muestra la dirección IP del cliente TFTP	
t	Ninguno	Cambia al modo seguro	Cuando el archivo de configuración esta dañado u olvidó la contraseña, utilice el modo seguro para entrar en el modo CLI. El archivo de configuración se perderá en este modo. Necesitará restaurar su configuración, o reconfigurar el sistema.
u	Nombre de archivo	Carga el módulo de inicio / Firmware a través de la red usando el protocolo TFTP	
v	Ninguno	Muestra la versión de inicio en ROM	
w	Ninguno	Cambia a reinicio con clave de administrador	

5.2 Inicio y fin de sesión

La primera vez que inicie la sesión, puede introducir "**admin**" como nombre de usuario sin necesidad de contraseña. Por razones de seguridad se recomienda cambiar de nombre de usuario y contraseña tras iniciar la sesión. Si olvida el nombre de usuario o contraseña, necesitará contactar con el equipo de soporte ASUS o restaurar la cuenta de usuario por defecto en el modo de comandos de inicio en ROM. Si selecciona esta última opción, perderá toda la configuración del sistema, necesitando configurar el Switch de nuevo.

Para salir con seguridad del modo CLI escriba "**logout**".

5.3 Comandos CLI

Este switch proporciona comandos CLI para todas las funciones de administración. Todos los comandos están listados por categorías en el interfaz Web de administración. De esta manera, puede seguir las instrucciones y configurar el switch correctamente de una forma tan fácil como usando el interfaz Web. El comando **"Save"** es utilizado para guardar la configuración en la memoria flash. Algunos comandos CLI sólo serán efectivos tras ejecutar el comando **"save"**.

NOTA: - Utilice "?" para obtener una lista de todos los comandos disponibles y ayuda
- Utilice "/" para regresar al directorio raíz.
- Utilice ".." para subir un directorio.
- Escriba el nombre del comando para obtener ayuda sobre éste.

5.3.1 Comandos del sistema

[Nombre del Sistema]

Muestra el nombre del switch. Este es un objeto RFC-1213 MIB definido en el grupo de Sistema, y proporciona información sobre el nodo administrado.

Comando CLI: sys info name <nombre>

Figura 57. Comandos SYS

Escribiendo un nombre en el campo "nombre", el nombre del sistema del switch cambiará al nuevo nombre escrito.

[Contacto del Sistema]

Muestra información detallada de contacto sobre este switch. Este es un objeto RFC-1213 MIB definido en el grupo de Sistema, y proporciona información sobre el nodo administrado.

Comando CLI: sys info contact <nombre>

Escribiendo un nombre en el campo "nombre", la información de contacto del switch cambiará al nuevo nombre escrito.

[Localización del Sistema]

Muestra la localización física del switch. Este es un objeto RFC-1213 MIB definido en el grupo de Sistema, y proporciona información sobre el nodo administrado.

Comando CLI : sys info location <localización>

Escriba una nueva localización en este campo para cambiar su descripción.

[Identificador VLAN]

Muestra el identificador de la VLAN en el switch. Es necesario estar en la misma VLAN para realizar tareas de administración de ésta.

Comando CLI: net interface vlan sw0 <identificador VLAN>

[Cliente DHCP]

Activa (enable) DHCP para obtener una dirección IP dinámica, o desactiva (disable) DHCP para especificar una dirección IP estática. Si activa DHCP, puede renovar (renew) o liberar (release) la dirección IP del Switch, usando el comando **show** para mostrar la dirección IP dinámica.

Comando CLI: net interface dhcp sw0 *<enable/ disable/ renew/ release/ show>*

[Dirección IP]

Muestra la dirección IP estática del switch. Esta dirección IP es usada por aplicaciones tales como servidores http, servidores SNMP, servidores ftp, servidores de telnet y servidores SSH en el switch utilizan esta dirección IP.

Comando CLI: net interface ip sw0 < dirección IP> <máscara de red>

[Máscara de Red]

Muestra la máscara de subred del switch.

Comando CLI: net interface ip sw0 < dirección IP> <máscara de red>

[Puerta de Enlace por Defecto]

Muestra la dirección IP de la puerta de enlace por defecto. Este campo no es necesario si la red del switch contiene uno o más enrutadores.

Comando CLI: net route static add <subred/IP de destino> <puerta de enlace> <máscara de red> <métrica>

[Contraseña de Protección] [Activar/Desactivar]

Cuando la protección por contraseña es activada, la interfaz Web requerirá nombre de usuario y contraseña de autentificación al acceder al switch a través del navegador Web.

Comando CLI: sys web set <enable/disable>

[Nombre de usuario] [Contraseña] [Confirmar Contraseña]

El nombre de usuario por defecto es "admin". Por defecto, no necesita contraseña. Puede definir una contraseña configurando los siguientes campos.

Comando CLI: sys users modify <user name, 'admin' por defecto>

user name (nombre previo de usuario, 'admin' por defecto): <nuevo nombre de usuario>

password (contraseña previa,): <nueva contraseña>

[Reinicio]

Es posible reiniciar el switch a través del comando de reinicio.

Comando CLI: sys reboot

[Cargar]

No hay comando CLI para esta función. Consulte los comandos de inicio en ROM para esta función.**[Copia de seguridad del archivo de configuración]**

Realiza una copia de seguridad del archivo de configuración del sistema. Consulte el capítulo 7.4.7 Copia de seguridad de la configuración del sistema a través de la consola.

Comando CLI: sys files config backup

[Restauración del archivo de configuración]

Restaura el archivo de configuración del sistema. Consulte el capítulo 7.4.7 Copia de seguridad de la configuración del sistema a través de la consola.

Comando CLI: sys files config restore

5.3.2 Comandos de la Interfaz física

[Admin] [Activar/Desactivar]

Muestra el estado de administración del puerto y permite a usuarios activar o desactivar el puerto.

Comando CLI: l2 port admin <número de puerto> <enable/disable>

[Modo] [Auto/10M-Half/10M-Full/100M-Half/100M-Full/1G-Full]

Muestra la velocidad y el modo duplex actual en el puerto. La velocidad y modo duplex puede ser detectada automáticamente cuando auto-negociación esté activada en el puerto.

Comando CLI: l2 port autoneg <número de puerto> <enable/disable>

Comando CLI: l2 port speed <número de puerto> <10/100/1000>

Comando CLI: l2 port duplex <número de puerto> <full/half>

[Control de Flujo] [Activar/Desactivar]

Muestra el control de flujo IEEE802.3x en un puerto. Tenga en cuenta que el control de flujo puede operar solamente en modo full duplex.

Comando CLI: l2 port flow <número de puerto> <enable/disable>

[Recargar]

Restaura la configuración de puerto previa desde el archivo de configuración.

Comando CLI: l2 port retrieve

5.3.3 Comandos de Puente (Bridge)

[Arbol de cobertura] [*STP Activado/ RSTP Activado/ Desactivado*]

Permite especificar si el Switch participa en un protocolo de árbol de cobertura (Spanning Tree Protocol - STP/ RSTP).

Comando CLI: l2 stp start <*stp / rstp*>

Comando CLI: l2 stp *stop*

[Hello Time] Mensaje de saludo
[Forward Delay] Retraso en reenvío
[Max Age] Máximo tiempo de envejecimiento
[Bridge Priority] Prioridad en el Puente

Muestra la configuración de los parámetros STP/RSTP en el Puente.

Comando CLI: l2 stp bridge set

Hello Time (1..10 segundos): [*Tiempo de saludo anterior*] <*Tiempo de saludo nuevo*>

Max Age (6..40 segundos): [Tiempo máximo de envejecimiento anterior] <Tiempo máximo de envejecimiento anterior>

F**orward Delay (4..30 segundos)**: [Retraso en reenvío anterior] <Retraso en reenvío nuevo>

Bridge Priority (0.. 61440): [Prioridad en Puente anterior] <Prioridad en Puente nueva>

[Priority] Prioridad
[Path Cost] Coste de ruta
[Edge Port] Puerto terminal
[Point-to-point] Punto a punto

Muestra la configuración de los éstos parámetros de puerto STP/RSTP en el Puente.

Comando CLI: l2 stp port set

Port Settings (1,2,3,4-26/* para todos los puertos): <Lista de puertos>

Port <número de puerto> Priority (0..240): [Prioridad anterior en puerto] <Nueva prioridad en puerto>

Port <número de puerto> Path Cost (1..200000000): [Coste de ruta anterior] <Nuevo coste de ruta>

Port <número de puerto> EdgePort (yes/no): [Puerto terminal anterior] <Nuevo puerto terminal>

Port <número de puerto> Point-to-Point (yes/no/auto): [Puerto punto-a-punto anterior] <Nuevo puerto punto-a-punto>

[Recargar]

Restaura los ajustes previos desde un archivo de configuración.

Comando CLI: l2 stp retrieve

Comando CLI: l2 stp bridge retrieve

Comando CLI: l2 stp port retrieve

[Mostrar Trunk]

Muestra la configuración de un grupo Trunk específico. Es posible crear un nuevo grupo Trunk seleccionando un identificador de Trunk único, un nombre descriptivo, modo LACP (activado - enabled - o desactivado - disable), y los puertos miembro del grupo Trunk.

Comando CLI: l2 trunk show *<identificador de Trunk>*

[Crear Trunk]

Crea un nuevo grupo Trunk insertando un identificador, nombre, modo LACP y número de puertos.

Comando CLI: l2 trunk create <identificador> <nombre> <lacp (enable/ disable)> <lista de puertos>

[Agregar/Borrar Trunk]

Los miembros de un grupo Trunk existente pueden ser agregados o borrados.

Comando CLI: l2 trunk add <identificador> <lista de puertos>

Comando CLI: l2 trunk remove <identificador> <lista de puertos>

[Acción LACP]

Puede activar (enable) o desactivar (disable) LACP en un grupo Trunk específico.

Comando CLI: l2 trunk lacp action *<Identificador de Trunk> <enable/ disable>*

[Prioridad en sistema LACP]

Puede asignar la prioridad del sistema para la ejecución de LACP.

Comando CLI: l2 trunk lacp syspri *<prioridad (1-65535)>*

[Prioridad en puerto LACP]

Puede asignar la prioridad en puertos para la ejecución de LACP.

Comando CLI: l2 port lacppri *<prioridad>* <lista de puertos / *Use * para todos los puertos*>

[Recargar]

Restaura una configuración de Trunk previamente almacenada en un archivo.

Comando CLI: l2 trunk retrieve

[Modo Espejo] [Activado/Desactivado] [Puerto Espejo] [*Número de Puerto*]

Muestra la configuración del modo espejo del Switch.

Comando CLI: l2 mirror create <Número de puerto espejo> <*enable/disable*>

Comando CLI: l2 mirror ingress <lista de puertos de entrada>

Comando CLI: l2 mirror egress <*lista de puertos de salida*>

Comando CLI: l2 mirror remove <*ingress/egress*> <*lista de puertos*>

[Recargar]

Restaura los ajustes previos desde un archivo de configuración.

Comando CLI: l2 mirror retrieve

[Mostrar Grupo de Multidifusión]

Muestra los grupos que están presentes en la tabla de multidifusión.

Comando CLI: l2 mcast show

[Definir Grupo de Multidifusión]

Permite la agregación o modificación de un grupo de multidifusión estático especificando la dirección MAC, ID de VLAN, puertos miembro de la VLAN, y puertos miembro sin etiquetas. Tenga en cuenta que la combinación de dirección MAC e identificador VLAN forman una única entrada en la tabla del grupo de multidifusión.

Comando CLI: l2 mcast set

mac address [formato: xx:xx:xx:xx:xx:xx]: <Dirección MAC de multidifusión>

vlan id [1 por defecto]: <*Identificador de VLAN*>

port list [formato: 1 2 3 4 - 26/* para todos los puertos]: <*lista de puertos*> (*GX2024X*)

port list [formato: 1 2 3 4 - 18/* para todos los puertos]: <*lista de puertos*> (*GX2016X*)

[Borrar Grupo de Multidifusión]

Permite el borrado de una entrada del grupo de multidifusión estática de su tabla a través de la dirección MAC y su identificador VLAN.

Comando CLI: l2 mcast delete

mac address [formato: *xx:xx:xx:xx:xx:xx*]: <Dirección MAC de multidifusión>

vlan id: <Identificador VLAN>

[Recargar]

Restaura los ajustes previos desde un archivo de configuración.

Comando CLI: l2 mcast retrieve

[IGMP es] [Activar/Desactivar]

La monitorización IGMP de nivel 2 puede ser iniciada (start) o terminada (stop).

Comando CLI: l2 igmp <*start/stop*>

[Recargar]

Restaura los ajustes previos desde un archivo de configuración.

Comando CLI: l2 igmp retrieve

[Control de ancho de banda en entrada] [Activar/Desactivar] [Modo][Difusión] o [Difusión, Multidifusión] o [Difusión, Multidifusión, DLF] o [Todo]

[Tasa Límite]

El rango de límites para el número total de paquetes del tipo seleccionado.

Comando CLI: l2 rate ingress <número de puerto: * para todos los puertos> <enable/disable> [<modo (1:solo difusión, 2: difusión y multidifusión, 3:difusión, multidifusión y unidifusión desconocida, 4: todo)> <rango (70~250000 Kbps)>]

[Control de ancho de banda en salida] [Activar/Desactivar] [Tasa Límite]

Tasa de transmisión máxima en salida.

Comando CLI: l2 rate egress <número de puerto: * para todos los puertos> <enable/disable>[<rango (70~250000 Kbps)>]

[Recargar]

Restaura los ajustes previos desde un archivo de configuración.

Comando CLI: l2 rate retrieve

[Tiempo de envejecimiento]

Es posible configurar el tiempo de envejecimiento en entradas ARL (Lógica de resolución de direcciones - Address Resolution Logic) modificando su valor.

Comando CLI: l2 arl age [tiempo de envejecimiento]

[Consultas por Puerto]

Las entradas ARL existente en la tabla ARL puede ser consultadas a través del número de puerto.

Comando CLI: l2 arl port <*número de p*uerto>

[Consultas por identificador de VLAN]

Las entradas ARL existente en la tabla ARL puede ser consultadas a través del identificador VLAN.

Comando CLI: l2 arl vlan <*identifi*cador VLAN>

[Consultas por dirección MAC]

Las entradas ARL existente en la tabla ARL puede ser consultadas a través de la dirección MAC.

Comando CLI: l2 arl mac <dirección MAC> [*identifi*cador VLAN]

[Dirección MAC]
[identificador VLAN]
[Selección de Puertos]

Puede agregar o modificar una entrada ARL estática especificando su dirección MAC, ID de VLAN, número de puerto, ID del Trunk, una condición de paquete descartado, y una prioridad.

Comando CLI: l2 arl static <dirección MAC> <identificador VLAN> <número de puerto> <ID del Trunk (0: no Trunk)> <descartar (0:Número 1: destinación)> <priordad (‘none’ o 0-7)>

[Borrar]

Entradas ARL estáticas pueden ser borradas indicando la dirección MAC y su identificador VLAN. La combinación de estos dos campos forma una entrada única en la tabla ARL.

Comando CLI: l2 arl delete <*dirección M*AC> <*identifi*cador VLAN>

[Recargar]

Restaura los ajustes previos desde un archivo de configuración.

Comando CLI: l2 arl retrieve

[Modo VLAN] [VLAN 802.1Q con Etiquetas/VLAN basada en puertos]

En modo VLAN 802.1Q con etiquetas, la decisión de reenvío sigue la especificación VLAN 802.1Q con etiquetas, pero en modo VLAN basado en puertos: 1) Cuando el puerto recibe un paquete con etiqueta, la decisión de reenvío sigue la especificación VLAN 802.1Q con etiquetas 2) Cuando el puerto recibe un paquete sin etiqueta, la decisión de reenvío sigue la especificación VLAN basada en puertos.

Comando CLI: l2 vlan vlanmode set <Modo VLAN (1: VLAN 802.1Q con etiquetas, 2: VLAN basada en puertos> <lista de puertos/*>

[Mostrar VLAN]

Muestra la información VLAN existente en el Switch.

Comando CLI: l2 vlan show <*identif*icador VLAN>

[Nombre]
[identificador VLAN]
[VLAN privada]

Permite configurar la VLAN. Puede crear una nueva VLAN proporcionando un único identificador de VLAN, un nombre descriptivo, y su lista de puertos miembro. Tenga en cuenta que los puertos miembro indicados deben tener etiquetas. Para especificar un puerto VLAN sin etiqueta, utilice el comando CLI **utportadd**. Puede usar los comandos CLI **add** (agregar) o **remove** (borrar) para agregar nuevos puertos miembro a una VLAN o excluir algunos puertos existentes de ésta. Escriba el comando CLI '**private**' y '**create**' para crear una VLAN privada.

Comando CLI: l2 vlan tagged create <identificador VLAN> <nombre VLAN> [<vlan type:private>][<lista de puertos: * para todos los puertos>

Comando CLI: l2 vlan tagged add <*identif*icador VLAN> <*lista de* puertos>

Comando CLI: l2 vlan tagged remove <*identif*icador VLAN> <*lista de* puertos>

Comando CLI: l2 vlan tagged utportadd <*identif*icador VLAN> <*lista de puertos sin etiqueta*>

[Borrar VLANs]

Permite la destrucción total de una VLAN existente.

Comando CLI: l2 vlan delete <identificador VLAN>

[Puerto Promiscuo]

Define el puerto promiscuo de una VLAN privada.

Comando CLI: l2 vlan tagged promisport <identificador VLAN> <identificador de puerto promiscuo>

[Anulación de prioridad]
[Prioridad]

Activa (Enable)/Desactiva (disable) la anulación de prioridad y asigna un valor de prioridad.

Comando CLI: l2 vlan tagged prioverride <identificador VLAN> <anulación de prioridad: enable/disable> <prioridad>

[Mostrar VLAN basada en puertos]

Muestra la información de VLAN basada en puertos en el Switch.

Comando CLI: l2 vlan portbased show <identificador de grupo: * para todos los grupos VLAN basados en puertos>

[Nombre]
[Identificador de grupo]

Permite configurar la VLAN basada en puertos. Puede crear un nuevo grupo proporcionando un único identificador de grupo, un nombre descriptivo, y su lista de puertos miembro. Puede usar los comandos CLI **add** (agregar) o **remove** (borrar) para agregar nuevos puertos miembro a un grupo o excluir algunos puertos existentes de éste.

Comando CLI: l2 vlan portbased create <id de grupo> <nombre de grupo> [<lista de puertos: * para todos los puertos>]

Comando CLI: l2 vlan portbased add <id de grupo> <lista de puertos: * para todos los puertos>

Comando CLI: l2 vlan portbased remove <id de grupo> <lista de puertos: * para todos los puertos>

[Borrar Grupo]

Permite la destrucción total de un grupo VLAN basado en puertos.

Comando CLI: delete <ide de grupo: * para todos los grupos VLAN basados en puertos>

[Recargar]

Restaura los ajustes previos desde un archivo de configuración.

Comando CLI: l2 vlan retrieve

[Mostrar Puerto]

Muestra la configuración del puerto.

Comando CLI: l2 port show <id del puerto o ** para todos los puertos*>

[PVID]

Muestra la VLAN por defecto de un puerto escribiendo el identificador de VLAN y su lista de puertos miembro asociados.

Comando CLI: l2 port vlan <id de vlan, 4095 para desactivar la VLAN basada en puertos> <lista de puertos>

[Valor CoS]

Define la clase de servicio para un puerto asignando una prioridad (con rango de 0 a 7) para paquetes sin etiquetas.

Comando CLI: l2 port priority <*CoS*> <*lista de* puertos>

[Recargar]

Restaura los ajustes previos desde un archivo de configuración.

Comando CLI: l2 port retrieve

5.3.4 SNMP

[Nombre de Comunidad] [Definir]

Una entrada de comunidad contiene una descripción y un grupo de privilegios. La función "**Get privilege**" (recibir privilegio) está activada por defecto. Es posible especificar privilegios ("**Set privilege**") durante la creación de una nueva entrada.

Comando CLI: snmp community add

New community string: <Nueva comunidad>

Get privileges: [y, siempre activado por defecto]

Set privileges? (y/n): [n] <definir privilegios*, y para 'si'; n para 'no'*>

Puede modificar una entrada de comunidad en la tabla reasignando sus caracteres y privilegios.

Comando CLI: snmp community set

Community entry (Índice de la tabla): <id de la entrada a configurar>

Community string (Comunidad anterior): <comunidad nueva>

Esta acción modificará todos los Hosts con de comunidad de 'comunidad anterior' a 'comunidad nueva'.

Are you sure? (y/n): [y] <y para 'si'; n para 'no'>

Get privileges: [y, siempre encendido por defecto]

Set privileges? (y/n): [n] <definir privilegios, y para 'si'; n para 'no'>

Para borrar una entrada de comunidad de la tabla:

Comando CLI: snmp community delete

Community entry (tabla index): <id de la entrada a borrar>

Esta acción borrará todos los Hosts de la comunidad con '***delete community***'.

Are you sure? (y/n): [y] <y para 'si'; n para 'no'>

[Recargar]

Restaura los ajustes previos desde un archivo de configuración.

Comando CLI: snmp community retrieve

[Dirección IP del Host] [Comunidad]

Una entrada de Host contiene una dirección IP, máscara de red y su comunidad dedicada.

Comando CLI: snmp host add

Host IP/Subnet: <*dirección IP*>

Netmask: <*máscara de red*>

Community: <comunidad>

Es posible modificar la entrada de Host en la tabla reasignando la dirección IP permitida, máscara de red y comunidad.

Comando CLI: snmp host set

Host tabla entry (Índice de la tabla): <id de la entrada a configurar>

Host IP/Subnet (Dirección IP anterior): <nueva dirección IP>

Netmask (Máscara de red anterior): <nueva máscara de red>

Community (Comunidad anterior): <nueva comunidad>

Para borrar una entrada de la tabla de Hosts:

Comando CLI: snmp host delete

Entry id (tabla index): <id de la entrada a borrar>

[Recargar]

Restaura los ajustes previos desde un archivo de configuración.

Comando CLI: snmp host retrieve

[Versión de Trampa] [v1/v2c]

[Destinación]

[Comunidad para la Trampa]

Una entrada de trampa esta formada por la versión SNMP (actualmente soporta la versión 1 y 2c), una dirección IP de destino y una comunidad remota.

Comando CLI: snmp trap add

SNMP version? (1/2c): [1, por defecto] <versión SNMP>

Destination IP: <*dirección IP*>

Community: <comunidad>

Es posible modificar una entrada de trampa en la tabla reasignando su versión SNMP, dirección IP de destino y comunidad.

Comando CLI: snmp trap set

Trap tabla entry (Índice de tabla): <id de la entrada a configurar>

SNMP version? (1/2c): [versión SNMP anterior] <nueva versión SNMP>

Destination IP (Dirección IP anterior): <nueva dirección IP>

Community (Comunidad anterior): <nueva comunidad>

Para borrar una entrada de trampa de su tabla:

Comando CLI: snmp trap delete

Trap tabla entry (tabla index): <id de la entrada a borrar>

[Recargar]

Restaura los ajustes previos desde un archivo de configuración.

Comando CLI: snmp trap retrieve

[Nombre de Grupo]

[Nombre de Vista para Lectura]

[Nombre de Vista para Escritura]

[Nombre de Vista para Notificación]

[Modelo de Seguridad]

[Nivel de Seguridad]

Una entrada de grupo VACM (Modelo de Control de Acceso Basado en Vistas) contiene el nombre del grupo, nombre de vista para lectura, nombre de vista para escritura, nombre de vista para notificación, modelo de seguridad, nivel de seguridad y paridad en contexto.

Comando CLI: snmp snmpv3 access add

Group Name: <nombre de grupo>

Security Model [0/1/2/3](any/v1/v2c/usm): <modelo de seguridad>

Security Level [1/2/3](noauth/authnopriv/authpriv): *<nivel de seguridad>*

Context Match [0/1](inexact/exact): *<paridad en contexto>*

Read View Name: <nombre de vista para lectura>

Write View Name: <nombre de vista para escritura>

Notify View Name: < nombre de vista para notificación>

Es posible modificar una entrada VACM en el grupo reasignando el nombre de grupo permitido, nombre de vista para lectura, nombre de vista para escritura, nombre de vista para notificación, modelo de seguridad, nivel de seguridad, y paridad en contexto.

Comando CLI: snmp snmpv3 access set

Group Name: (nombre de grupo anterior) <nueva grupo de nombre>

Security Model [0/1/2/3](any/v1/v2c/usm): (modelo de seguridad anterior) <nuevo modelo de seguridad>

Security Level [1/2/3](noauth/authnopriv/authpriv): (nivel de seguridad anterior) <nuevo nivel de seguridad>

Context Match [0/1](inexact/exact): (paridad de contexto anterior) <nueva paridad de contexto>

Read View Name: (nombre de vista para lectura anterior) <nueva nombre de vista para lectura>

Write View Name: (nombre de vista para escritura anterior) <nueva nombre de vista para escritura>

Notify View Name: (nombre de vista para notificación anterior) <nueva nombre de vista para notificación>

Para borrar una entrada VACM del grupo:

Comando CLI: snmp snmpv3 access delete

Access entry: <id de la entrada a borrar>

[Recargar]

Restaura los ajustes previos desde un archivo de configuración.

Comando CLI: snmp snmpv3 access retrieve

[Nombre de vista]

[Tipo de vista]

[Subárbol de vista]

[Máscara de vista]

VACM se utiliza para ver información del grupo VACM SNMPV3. Una entrada de vista VACM contiene un nombre, tipo, subárbol y máscara.

Comando CLI: snmp snmpv3 view add

View Name: < nombre de vista>

View Subtree [oid]: <subárbol de vista>

View Mask: <máscara de vista>

View Type[1/2](included/excluded): *<tipo de vista>*

Es posible modificar una entrada de vista VACM en la tabla reasignando su nombre de vista permitido, tipo, subárbol, y máscara.

Comando CLI: snmp snmpv3 view set

View Name: (nombre de vista anterior) <nueva nombre de vista>

View Subtree [oid]: (subárbol de vista anterior) <nuevo subárbol de vista>

View Mask: (máscara de vista anterior) <nueva máscara de vista>

View Type[1/2](included/excluded): (tipo de vista anterior) <nuevo tipo de vista>

Para borrar una entrada de vista VACM.

Comando CLI: snmp snmpv3 view delete

View entry: <id de la entrada a borrar>

[Recargar]

Restaura los ajustes previos desde un archivo de configuración.

Comando CLI: snmp snmpv3 view retrieve

[Id de motor]

[Nombre]

[Protocolo de Autentificación]

[Contraseña de Autentificación]

[Protocolo Privado]

[Contraseña Privada]

USM (Modelo de seguridad basado en usuarios) se utiliza para configurar la información de usuarios SNMPV3 USM. Una entrada de usuario USM contiene un identificador de motor, nombre, protocolo de autentificación, contraseña de autentificación, protocolo privado, y contraseña privada.

Comando CLI: snmp snmpv3 usmuser add

EngineId: < id de motor>

Name: < nombre de usuario>

AuthProtocol [oid]: < id de protocolo de autentificación>

AuthPassword: < contraseña de autentificación>

Priv Protocol [oid]: < id protocolo privado>

Priv Password: < contraseña privada>

Puede modificar una entrada de usuario USM reasignando su id de motor permitido, nombre, protocolo de autentificación, contraseña de autentificación, protocolo privado, y contraseña privada.

Comando CLI: snmp snmpv3 usmuser set

EngineId: (id de motor anterior) <nueva id de motor>

Name: (nombre de usuario anterior) <nueva nombre de usuario>

AuthProtocol [oid]: (id de protocolo de autentificación anterior) <nueva id de protocolo de autentificación>

AuthPassword: (contraseña de autentificación anterior) <nueva contraseña de autentificación>

Priv Protocol [oid]: (id protocolo privado anterior) <nueva id protocolo privado>

Priv Password: (contraseña privada anterior) <nueva contraseña privada>

Para borrar una entrada de usuario USM:

Comando CLI: snmp snmpv3 usmuser delete

USM user entry: <id de la entrada a borrar>

[Recargar]

Restaura los ajustes previos desde un archivo de configuración.

Comando CLI: snmp snmpv3 usmuser retrieve

5.3.5 Comandos de Seguridad

[Reautentificación]

Permite activar (enable) o desactivar (disable) la reautentificación periódica.

Comando CLI: security dot1x bridge reauth *<enable / disable>*

[Tiempo de Reautentificación]

Permite configurar el tiempo de reautentificación.

Comando CLI: security dot1x bridge reauthtime <tiempo de reautentificación *(1-4294967295 seg)*>

[Método de Autentificación]

Permite configurar el método de reautentificación (RADIUS o a base de datos local).

Comando CLI: security dot1x bridge authmeth <tipo (1:local 2:radius)>

[Periodo de Inactividad]

Permite configurar el periodo de inactividad.

Comando CLI: security dot1x bridge quietperiod <periodo de inactividad *(1-65535 seg)*>

[Tiempo de Retransmisión]

Permite configurar el tiempo de retransmisión.

Comando CLI: security dot1x bridge retxtime <tiempo de retransmisión *(1-65535 seg)*>

[Número Máximo de Intentos de Reautentificación]

Permite configurar el tiempo máximo de intentos de reautentificación.

Comando CLI: security dot1x bridge reauthmax <Número máximo de intentos de reautentificación *(1-10)*>

[Modo de Autentificación]

Permite seleccionar el modo de autentificación (Port_based/Mac_based).

Comando CLI: security dot1x port authmode <tipo (1: port_based 2: MAC_based)><lista de puertos/*>

[Multi-host]

Permite activar (enable) o desactivar (disable) Multi-host en puertos específicos.

Comando CLI: security dot1x port multihost *<enable/disable><lista de pu*ertos/*>

[Control de autentificación]

Permite configurar el control de autentificación en puertos específicos.

Comando CLI: security dot1x port authctrl <type (1: force_authorized 2: force_unauthorized 3: auto)><lista de puertos/*>

[Identificador de VLAN de invitado]

Permite configurar el identificador de VLAN de invitado en puertos especificos.

Comando CLI: security dot1x port guestvlan *<vlan id (0:no guest vlan)> <lista de pu*ertos/*>

[Inicialización de Puertos]

Permite la inicialización forzosa de un puerto. Puede descubrir nuevos Hosts conectados a un puerto a través de un hub, y solicitar la autentificación de nuevos Hosts.

Comando CLI: security dot1x port initialize <número de puerto: * para todos los puertos>

[Recargar]

Restaura los ajustes previos desde un archivo de configuración.

Comando CLI: security dot1x retrieve

[Nombre de Usuario]

[Contraseña]

[Confirmar Contraseña]

[VLAN Dinámica]

Crea usuarios en base de datos local para autentificación 802.1x del Switch. Una entrada de usuario contiene un nombre de usuario, contraseña, y una VLAN dinámica.

Comando CLI: security dialinuser create

User Name: <nombre de usuario>

Password: <contraseña>

Confirm Password: <confirmar contraseña>

Dynamic VLAN: <VLAN dinámica>

Comando CLI: security dialinuser remove <nombre de usuario/*>

Permite modificar una entrada de usuario de una base de datos local.

Comando CLI: security dialinuser modify <nombre de usuario/*>

User Name: <nuevo nombre de usuario>

Password: <nueva contraseña>

Confirm Password: <confirmar nueva contraseña>

Dynamic VLAN: <nueva VLAN dinámica>

[Recargar]

Restaura los ajustes previos desde un archivo de configuración.

Comando CLI: security dialinuser retrieve

[IP del Servidor de Autentificación]

[Puerto del Servidor de Autentificación]

[Clave del Servidor de Autentificación]

[Confirmación de Clave del Servidor de Autentificación]

Permite la configuración de la dirección IP, puerto del servidor y clave de servidor RADIUS.

Comando CLI: security radius set

authentication server ip <ip/none>: [dirección IP anterior del servidor]<nueva dirección IP del servidor>

authentication server port <port/default>: [puerto anterior del servidor]<nuevo puerto del servidor>

authentication server key <key/none>: <clave del servidor>

confirm authentication key <key/none>: <confirmar clave del servidor>

[Recargar]

Restaura los ajustes previos desde un archivo de configuración.

Comando CLI: security radius retrieve

[IP del Servidor de Autentificación]

[Puerto del Servidor de Autentificación]

[Puerto del Servidor de Autentificación]

[Confirmación de Clave del Servidor de Autentificación]

Permite la configuración de la dirección IP, puerto del servidor y clave de servidor TACACS+.

Comando CLI: security tacacs set

authentication server ip <ip/none>: [dirección IP anterior del servidor]<nueva dirección IP del servidor>

authentication server port <port/default>: [puerto anterior del servidor]<nuevo puerto del servidor>

authentication server key <key/none>: <clave del servidor>

confirm authentication key <key/none>: <confirmar clave del servidor>

[Recargar]

Restaura los ajustes previos desde un archivo de configuración.

Comando CLI: security tacacs retrieve

[Modo de Violación] [Protegido/Restringido/Apagado]

Permite la configuración del modo de violación en puertos (protegido - protect, restringido - restrict, apagado - shutdown).

Comando CLI: security portsecu violation violation <modo (1:protegido 2:restringido 3:apagado)> <lista de puertos/*>

[Número Máximo de Direcciones MAC]

Permite la configuración del número máximo de direcciones MAC seguras.

Comando CLI: security portsecu maxaddr <Número máximo de direcciones MAC seguras> <número de puerto>

[Tiempo de Envejecimiento]

Permite la configuración del tiempo de envejecimiento en puertos.

Comando CLI: security portsecu age <tiempo de envejecimiento> <lista de puertos/*>

[Tipo de envejecimiento] [Absoluto/Inactividad]

Permite configurar el tipo de envejecimiento en puertos.

Comando CLI: security portsecu agetype <type (1:absoluto 2: inactividad)> <lista de puertos/*>

[Reinicio]

Permite reiniciar un puerto si éste está en estado apagado (‘shutdown’).

Comando CLI: security portsecu restart <lista de puertos/*>

[Selección de Puertos]

[Petición]

Muestra las direcciones MAC en puertos.

Comando CLI: security portsecu mac display <lista de puertos/*>

[Dirección MAC]

[Selección de Puertos]

[Agregar]

Agrega una dirección MAC segura estática a un puerto.

Comando CLI: security portsecu mac add <dirección MAC> <número de puerto>

[Borrar]

Borra una dirección MAC segura estática a un puerto proporcionando una dirección MAC, VID, y el número de puerto, o borra todas las direcciones MAC seguras en puertos.

Comando CLI: security portsecu mac delete <direcciones MAC> <vid> <número de puerto>

Comando CLI: security portsecu mac clear <lista de puertos/*>

[Recargar]

Restaura los ajustes previos desde un archivo de configuración.

Comando CLI: security portsecu retrieve

[Generación de Claves SSH]

Permite la generación de claves SSH. SSH (Secure SHell) es un protocolo para el inicio de sesión remoto de una máquina a través de shell. Su funcionalidad es similar a telnet, con la diferencia de que todos los datos entre el cliente y el servidor están codificados. Esta codificación proporciona una protección contra varios riesgos en red. En la actualidad, este Switch soporta el protocolo SSH versión 2 y permite un solo inicio de sesión al mismo tiempo. Dos pares de claves SSH serán creadas en la unidad de almacenamiento Flash del sistema. Estos pares de claves son RSA y DSA públicas/privadas respectivamente.

Comando CLI: security sshkey start

[Reiniciar clave SSH]

Reinicia las claves SSH a su valor por defecto.

Comando CLI: security radius default

[Mostrar Estado de Generación]

Muestra el estado de generación de la clave SSH. Mostrará “success” si la creación ha sido realizada con éxito, o “SSH keys generated fail” si ha habido errores, o “system is generating keys ...” si el proceso de generación esta en curso.

Comando CLI: security sshkey show

5.3.6 Comandos QoS

[Estado] [CoS/DSCP]

Permite la configuración del estado de confianza en puertos.

Comando CLI: qos trust state <cos/dscp> <lista de puertos/*>

[Mapeo DSCP]

[A CoS]

Permite la configuración del mapeo desde DSCP a CoS.

Comando CLI: qos map dscpcos <dscp(0-63):inserte un solo valor DSCP o un rango de valores DSCP(e.j.:5-12)> <prioridad cos (0-7)>

[Anular Prioridad en Dirección MAC de Origen]

[Anular Prioridad en Dirección MAC de Destino]

Permite la activación o desactivación de la prioridad de direcciones MAC de origen y destino en QoS .

Comando CLI: qos prioverride set <SA priority override (0:desactivada 1: activada)><DA priority override (0:desactivada 1:activada)>

[Algoritmo de Programación] [Estricta/Basada en Peso(WRR)]

Permite la configuración de programación con prioridad estricta o basada en peso con forma circular.

Comando CLI: l2 cos sched <mode (1: stricta 2: basada en peso)>

[Prioridad]

[Cola CoS]

Permite mapear el prioridad CoS (con rango 0-7) para la cola buffer (total of 4, with queue ID of 1-4).

Comando CLI: l2 cos map <queue id (1-4)> <cos (0-7)>

[Recargar]

Restaura los ajustes previos desde un archivo de configuración.

Comando CLI: l2 cos retrieve

[Recargar]

Restaura los ajustes previos desde un archivo de configuración.

Comando CLI: security portsecu retrieve

[Recargar]

Restaura los ajustes previos desde un archivo de configuración.

Comando CLI: qos retrieve

5.3.7 Diagnóstico de Cable

[Puerto]

Permite realizar un diagnóstico de cable en un puerto determinado.

Comando CLI: cablediag port <número de puerto>

5.4 Comandos misceláneos

sys time uptime: Muestra el tiempo desde el inicio del sistema

sys time date: Muestra fecha y hora actual

sys time settime: configura la hora actual

sys files config backup: realiza una copia de seguridad de los archivos de configuración

sys files config default: restaura el archivo de configuración predeterminado en fábrica

sys monitor auto: activa (enable) o desactiva (disable) la auto comprobación de estado de los ventiladores

sys monitor set: Ajusta la velocidad del ventilador (1~255)

sys monitor show: Muestra el estado del sistema

net ping: hace “ping” a un Host remoto

net route show: Muestra entradas en la tabla de enrutamientos

6 Direcciones IP, Máscaras de red y Subredes

Esta sección está dedicada sólo a direcciones IP para IPv4 (versión 4 del Protocolo de Internet). Las direcciones IPv6 no son explicadas.

Esta sección asume que usted posee un conocimiento básico sobre números binarios, bits y bytes.

6.1 Direcciones IP

Las direcciones IP (la versión Internet de números telefónicos) son utilizadas para identificar nodos individuales (PCs o dispositivos) en Internet. Cada dirección IP contiene cuatro números, cada uno desde 0 a 255 y separados por puntos (periodos), p.e. 20.56.0.211. Estos números son llamados (de derecha a izquierda): Campo 1, Campo 2, Campo 3, y Campo 4.

Este estilo de escritura de direcciones IP como números decimales separados por puntos es llamado "notación decimal con punto". La dirección IP 20.56.0.211 es leída “veinte punto cincuenta y seis punto cero punto doscientos once”.

6.1.1 Estructura de una dirección IP

Las direcciones IP tienen un diseño jerárquico similar al de los números telefónicos. Por ejemplo, un número de teléfono de 7 dígitos comienza con un prefijo de 3 dígitos que identifica un grupos de miles de líneas telefónicas, y termina con cuatro dígitos que identifican una línea específica en éste grupo.

De manera similar, las direcciones IP contienen dos tipos de información.

- **Identificador de red**: Identifica una red particular en Internet o Intranet.
- **Identificador de Host**: Identifica un PC o dispositivo en la Red

La primera parte de cada dirección IP contiene el identificador de Red, y el resto de la dirección contiene el identificador de Host. La longitud del identificador de red depende de la clase de red (consulte la siguiente sección). La tabla 8 muestra la estructura de una dirección IP.

Tabla 8: Estructura de una dirección IP

	Campo1	**Campo2**	**Campo3**	**Campo4**
Clase **A**	Red ID	Host ID		
Clase **B**	Red ID		Host ID	
Clase **C**	Red ID			Host ID

Algunos ejemplos de direcciones IP válidas:

Clase A: 10.30.6.125 (red = 10, host = 30.6.125)

Clase B: 129.88.16.49 (red = 129.88, host = 16.49)

Clase C: 192.60.201.11 (red = 192.60.201, host = 11)

6.1.2 Clases de redes

Las tres clases usadas más comúnmente son las clases A, B, y C. (También hay una clase D pero tiene un uso especial que se haya fuera del alcance de esta discusión). Estas clases tienen diferentes usos y características.

Las redes de clase A son las mayores de Internet, cada una con más de 16 millones de Hosts. Sólo pueden existir un máximo de 126 de estas grandes redes, para un total de 2 billones de Hosts. Debido a su tamaño, estas redes son usadas para WANs y por organizaciones a nivel de Internet Infraestructura, tales como su ISP.

Las redes de clase B son más pequeñas pero aún así tienen un gran tamaño, cada una con capacidad para 65,000 Hosts. Pueden existir hasta 16,384 redes de clase B. Una red de clase B puede ser apropiada para una gran organización tal como una empresa u organización gubernamental.

Las redes de clase C son las más pequeñas, solamente con un máximo de 254 Hosts, pero con un posible número total de redes excediendo los 2 millones (2.097.152 para ser exactos). Las redes conectadas a Internet suelen ser de clase C.

La clase puede ser determinada fácilmente a través del campo 1:
campo 1 = 1-126: Clase A
campo 1 = 128-191: Clase B
campo 1 = 192-223: Clase C
(Los valores del campo 1 no mostrados están reservados para usos especiales)

Un identificador de host puede tener cualquier valor excepto 0 para todos los campos o 255 para todos los campos, ya que estos valores están reservados para usos especiales.

6.2 Máscaras de subredes

Una máscara es parecida a una dirección IP normal, pero contiene un patrón de bits que indica qué partes de una dirección IP son el identificador de red y qué partes forman parte del identificador de host: bits definidos como 1 significan "este bit es parte del identificador de red", bit definidos como 0 significan "este bit es parte del identificador de host".

Las máscaras de Subred son utilizadas para definir subredes (una subred es el resultado de dividir una red en varias partes). Un identificador de la subred de una red es creada "pidiendo prestada" uno o más bits de la porción del identificador de host de la dirección. La máscara de subred identifica estos bits del host.

Por ejemplo, considere una red de clase C 192.168.1. Para dividir ésta red en dos subredes, utilizaremos una máscara de subred:

255.255.255.128

Es más fácil ver lo ocurrido si escribimos la dirección en binario:

11111111. 11111111. 11111111.10000000

Tomando cualquier dirección de clase C, todos los bits del campo 1 al campo 3 son parte del identificador de red, pero vea como la máscara específica que el primer bit del Campo 4 también será incluido. Debido a que este bit extra puede tener dos valores (0 y 1), esto quiere decir que habrá dos subredes. Cada subred utilizará los siete bits restantes del campo 5 para su identificador de host, que tendrá un rango de 0 a 127 (en vez del rango usual de 0 a 255 para las direcciones de clase C).

De manera similar, para dividir una red de clase C en cuatro subredes, la máscara es:

255.255.255.192 o 11111111. 11111111. 11111111.11000000

Los dos bits extra del campo 4 tienen cuatro valores (00, 01, 10, 11), así que pueden ser creadas cuatro subredes. Cada subred utilizará los restantes 6 bits en el campo 4 para sus identificadores de Hosts, de rango 0 a 63.

A veces una máscara de subred no especifica bits para identificadores de red, no teniendo subredes. Esta máscara es llamada máscara de subred predeterminada. Estas máscaras son:
Clase A: 255.0.0.0
Clase B: 255.255.0.0
Clase C: 255.255.255.0
Éstas son llamadas "predeterminadas" porque se utilizan cuando una red es configurada inicialmente, momento en el cual no tiene subredes.

7 Solución de Problemas

Esta sección proporciona instrucciones para diagnosticar problemas usando utilidades IP. También se proporciona una lista de posibles problemas con soluciones sugeridas.

Todos los errores (bugs) conocidos están listados en las notas sobre la versión. Lea estas notas antes de instalar el switch. Contacte con el Servicio al Consumidor si estas sugerencias no resuelven su problema.

7.1 Diagnóstico de problemas con utilidades IP

7.1.1 ping

Ping es un comando que puede ser usado para comprobar si su PC puede reconocer otros PCs en red o Internet. Un comando ping envía un mensaje al PC que especifique. Si el PC recibe este mensaje, enviará un mensaje de respuesta. Para usar ping, es necesario conocer la dirección IP del PC con el que desee comunicar.

En PCs basados en Windows, es posible ejecutar el comando ping desde el menú de inicio. Haga clic en el botón de **inicio**, y luego haga clic en "**Ejecutar...**". En la ventana abierta, escriba lo siguiente:

ping 192.168.1.1

Pulse el botón <**Aceptar**>. Puede utilizar cualquier dirección IP privada de su red o pública en Internet, como la de un sitio web, si la conoce. Si

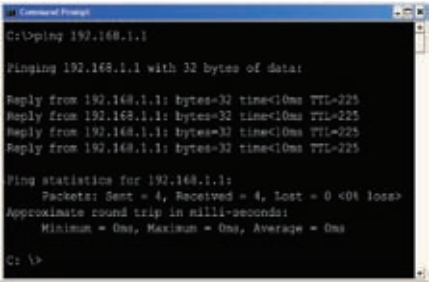


Figura 58. ***Utilizando la utilidad ping***

el PC de destino no puede ser localizado, recibirá un mensaje “Request timed out” (tiempo de petición expirado).

Con el comando ping puede comprobar si la ruta al dispositivo funciona correctamente (utilizando la dirección IP de red 192.168.1.1 preconfigurada por defecto) u otra dirección que haya asignado.

También puede comprobar el acceso a Internet escribiendo una dirección externa, como por ejemplo www.yahoo.com (216.115.108.243). Si no conoce la dirección IP de un sitio en Internet, utilice el comando nslookup, como se explica en la siguiente sección.

Es posible utilizar el mismo comando desde la mayoría de sistemas operativos preparados para soportar IP, a través de comandos o utilidades de administración de sistema.

7.1.2 nslookup

Puede utilizar el comando nslookup para determinar la dirección IP asociada con un nombre de sitio en Internet. Especificando u nombre común, nslookup buscará el nombre en el Servidor DNS (usualmente localizado en su ISP). Si este nombre no se encuentra en la tabla de entradas de su ISP, la petición será enviada a otro servidor de nivel superior, y así hasta que la entrada sea encontrada. Una vez encontrada el Servidor devolverá la dirección IP asociada.

En PCs basados en Windows, es posible ejecutar el comando nslookup desde el menú de inicio. Haga clic en el botón de inicio, y luego haga clic en "Ejecutar...". En la ventana abierta, escriba lo siguiente:

nslookup

Haga clic en **Aceptar**. Una ventana de comandos aparecerá con un símbolo "mayor que" (>). Escriba aquí el nombre de la dirección de Internet que desee, como por ejemplo www.absnews.com.

La ventana mostrará la dirección IP asociada, si ésta es conocida, tal y como se muestra en la figura 59.

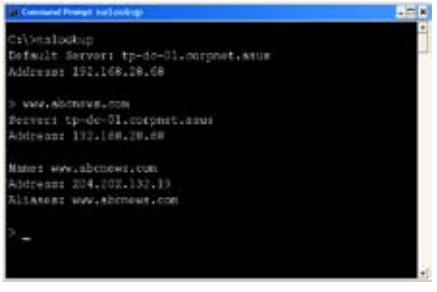


Figura 59. Utilizando la utilidad nslookup

Hay varias direcciones asociadas con un nombre de Internet. Ésto es común para sitios Web que reciben mucho tráfico; éstas utilizan servidores múltiples y redundantes que tienen la misma información

Para salir de la utilidad nslookup utility, escriba “exit” en el intérprete de comandos y pulse <Entrar>.

7.2 Reemplazando ventiladores defectuosos

Cuando cualquiera de los ventiladores del switch (en el panel trasero del switch) se estropea, éstos pueden ser reemplazados siguiendo estos pasos.

1. Afloje el tornillo del módulo de ventiladores que lo asegura al panel trasero.

Apague el switch antes de retirar el modulo de los ventiladores en la parte trasera del Switch.

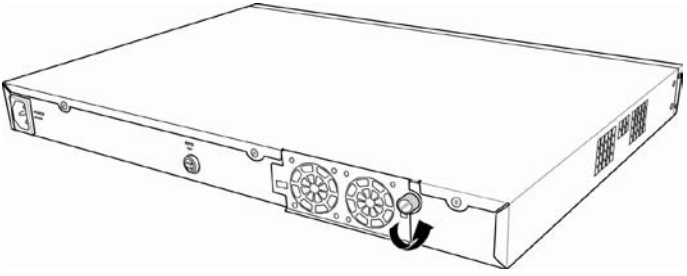


Figura 60. Aflojando el tornillo del panel trasero

2. Tire con cuidado del módulo como se muestra a continuación.

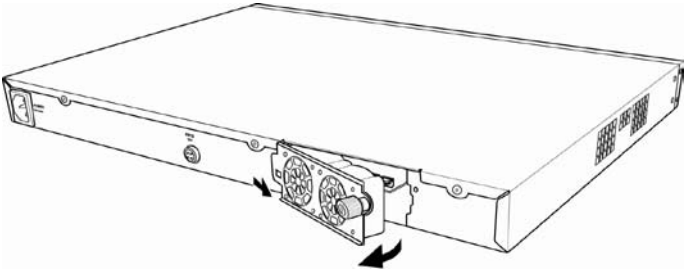


Figura 61. Retirando el módulo de ventiladores

3. Con cuidado tire de los dos cables de alimentación de los conectores de los ventiladores.
4. Afloje los tornillos que asegurar el ventilador al módulo. Retire el ventilador defectuoso.

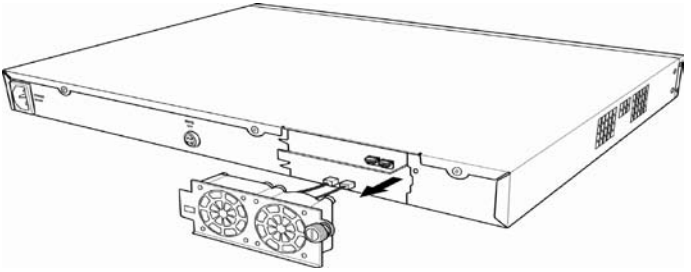


Figura 62. Desmontando el ventilador del módulo

Figura 62. Desmontando el ventilador del módulo

5. Ajuste el nuevo ventilador con los tornillos que retiró anteriormente. Asegúrese de que el cable del ventilador esta colocado cerca del fondo del módulo.

Siga estos pasos para reemplazar el otro ventilador.

6. Conecte los cables del ventilador al PCB. Asegúrese de que los cables del ventilador están conectados al conector del ventilador correcto. FAN 1 está en la parte izquierda cuando se encuentra frente a la parte trasera del panel.
7. Inserte el módulo de ventiladores al chasis del switch hasta que se ajuste a su sitio. Asegúrese de que los cables de alimentación no son apresados entre el módulo y el chasis.
8. Asegure el módulo de ventiladores al chasis apretando el tornillo. Compruebe de que el módulo de ventiladores para asegurarse de que ningún cable ha sido apresado entre el módulo y el chasis.

Especificaciones de los ventiladores

Dimensiones: 40 x 40 x 20 mm

Voltaje y Amperaje: 12VDC, 0.13A

Velocidad: 8200RPM

7.3 Soluciones para problemas simples

Tabla 9: Problemas y Soluciones sugeridas

Problema	Solución sugerida
LEDs	
El LED de encendido no se ilumina tras encender el producto.	Verifique que está utilizando el adaptador AC proporcionado con el dispositivo y que éste está correctamente conectado al switch y a un enchufe adecuado.
LED RPS no se ilumina cuando una unidad de alimentación redundante es conectada.	1.Verifique que el cable RPS ha sido conectado correctamente al conector RPS y al enchufe. 2.Asegúrese de que la unidad RPS se ajusta a los estándares proporcionados en la sección RPS del manual.
LED del ventilador es ámbar e intermitente	Compruebe el ventilador en la parte trasera del switch. Si alguno está defectuoso, consulte la sección 7.2 para reemplazarlo.
LED de enlace Gigabit Ethernet no se ilumina una vez que el cable Ethernet ha sido conectado	1.Verifique que el cable Ethernet haya sido conectado correctamente al switch/hub/PC de su red y al switch. Asegúrese de que el PC y/o hub/switch estén encendidos. 2.Verifique que el cable utilizado es el cualificado. Una red 1000 Mbps (1000BaseTx) debe utilizar cables de categoría 5. Redes a 10Mbit/seg podrían tolerar cables de inferior calidad
Acceso a red	
El PC no puede acceder a otro Host en la misma red	1.Compruebe el cableado Ethernet para asegurar una buena conexión y si el LED del puerto se ilumina en Verde. 2.Si el LED del puerto es ámbar, compruebe si el puerto ha sido desactivado. Podrá experimentar una desconexión de red en un periodo corto de tiempo (sobre un minuto) si acaba de encender el STP.

Problema	Solución sugerida
Acceso a red	
El PCs no puede mostrar las páginas Web de configuración.	1.Verifique que el switch tiene corriente y el puerto de conexión esta activado. La dirección IP de fábrica para el switch es 192.168.1.1. 2.Verifique su configuración de red en su PC para esta información. Si su PC no tiene una ruta valida para acceder al switch, cambie la dirección IP del switch a una apropiada que pueda ser accedida por su PC. 3. Haga ping al IP del switch desde el PC, y si esto falla, repita el paso 2. 4. Si el ping ha sido ejecutado con éxito pero la configuración Web aún falla, conecte el PC a través del puerto de consola utilizando un cable RS232, compruebe si hay una regla de filtrado o dirección MAC definida que bloquee el tráfico.
Interfaz de configuración Web	
Olvidó/Perdió el nombre de usuario o contraseña del Administrador de Configuración.	1.Si no cambió la clave por defecto, intente los valores "admin" como nombre de usuario (sin contraseña) 2.Inicie la sesión en modo consola a través del puerto RS232 o USB. Utilice "sys user show" para mostrar la información pérdida
Algunas páginas no son mostradas completamente	1.Verifique que esta utilizando Internet Explorer v5.5 o superior. Netscape no esta soportado. Es posible que necesite soporte para Javascript® que deberá ser activado en su navegador, así como soporte para Java®. 2.Haga ping a la dirección IP del switch para ver si es estable. Si algunos paquetes fallan, compruebe la configuración de red para asegurarse que los ajustes sean válidos.
Cambios en el Administrador de Configuración no son almacenados	Asegúrese de hace clic en el botón <**Save**> de la página **Save configuration** para guardar cambios.
Interfaz de la consola	
Textos no aparecen en el terminal emulador.	1.Los datos predeterminados de fábrica son: tasa de baudios como 9600, sin control de flujo, 8 bits de datos, sin comprobación de paridad, y bit de stop "1". 2.Cambie la configuración del emulador de terminal a estos números. Si utiliza USB para conectar el switch, instale el controlador USB primero. 3.Compruebe si el cable está en buenas condiciones.

7.4 Carga y descarga de archivos

7.4.1 Carga del módulo de inicio "boot" a través de TFTP

1. Pulse cualquier tecla en la consola para entrar en el modo "**Boot ROM Command**" durante el proceso de inicio (POST).
2. Utilice el comando "**c <Dirección IP> <Máscara de red>**" para definir la dirección IP de un cliente TFTP como la dirección IP del Switch. Ejemplo: "***c 192.192.1.100 255.255.255.0***".

Figura 63. Carga del módulo de inicio a través de TFTP

3. Utilice el comando "**s <Dirección IP> <Máscara de red>**" para definir la dirección IP del servidor TFTP donde el módulo de inicio esta localizado. Por ejemplo: "**s 192.192.1.121 255.255.255.0**".
4. Utilice el comando "**u <Nombre de archivo>**" para crear el módulo de inicio. El nombre de archivo es el mismo que el de su módulo local de inicio en el servidor TFTP. Por ejemplo: "**u armboot.img**".
5. Escriba "**Y**" para anular el cargador de inicio actual.
6. Power Cycle to activate the new boot module.

7.4.2 Upload firmware by TFTP

1. Pulse cualquier tecla en la consola para entrar en el modo "**Boot ROM Command**" durante el proceso de inicio (POST).
2. Utilice el comando "**c <Dirección IP> <Máscara de red>**" para definir la dirección IP de un cliente TFTP como la dirección IP del Switch. Por ejemplo: "**c 192.192.1.100 255.255.255.0**".

Figura 64. Carga de Firmware a través de TFTP

3. Utilice el comando "**s <Dirección IP> <Máscara de red>**" para definir la dirección IP del servidor TFTP donde el Firmware esta localizado. Por ejemplo: "**s 192.192.1.121 255.255.255.0**".
4. Utilice el comando "**u <Nombre de archivo>**" para cargar el Firmware. El nombre de archivo es el mismo que el de su módulo local de inicio en el servidor TFTP. Por ejemplo: "**u gx2024x_2.1.3.2_051026**"
5. Para cargar el Firmware, utilice el comando "**g**" para cargar y ejecutar éste.

7.4.3 Carga de Firmware a través de FTP

Asegúrese de que su PC y el Switch estan en la misma VLAN antes de usar la función FTP y otras herramientas de administración remota. La VLAN del Switch será mostrada en la página **System-->IP setup** de la página Web o utilice "**net interface show**" para mostrar el VID a través de CLI.

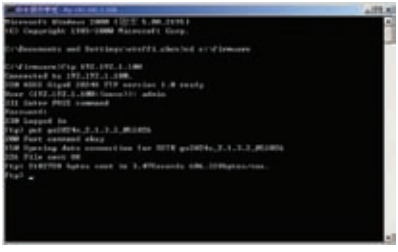


Figura 65. Carga de Firmware a través de FTP

1. Abra la ventana del interprete de comandos.
2. Vaya al directorio donde esté el Firmware.
3. Utilice el comando "**ftp <Dirección IP>**" para conectar al servidor FTP del Switch. La dirección IP es la del Switch. Por ejemplo: "**ftp 192.192.1.100**".
4. Escriba el nombre de usuario.
5. Escriba la contraseña del sistema.
6. Utilice el comando "**put <Nombre de archivo>**" para cargar el Firmware. El nombre del archivo es el nombre local del Firmware. Por ejemplo: "**put gx2024x_2.1.3.2_051026**".

7.4.4 Upload auto-config file by FTP

Asegúrese de que su PC y el Switch estan en la misma VLAN antes de usar la función FTP y otras herramientas de administración remota. La VLAN del Switch será mostrada en la página **System-->IP setup** de la página Web o utilice "**net interface show**" para mostrar el VID a través del intérprete de comandos.

El archivo de auto configuración consiste en comandos CLI en un archivo de texto. El Switch ejecutará los comandos una vez que el archivo sea cargado en el Switch.

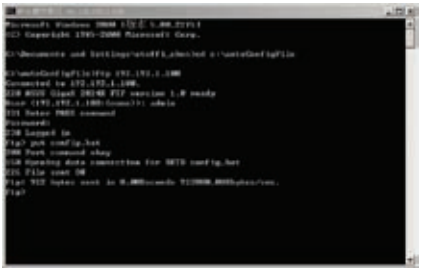


Figura 66. Carga de archivo de auto configuración a través de FTP

1. Abra la ventana del interprete de comandos.
2. Vaya al directorio donde esté el archivo de auto configuración.
3. Utilice el comando "**ftp <Dirección IP>**" para conectar al servidor FTP. Por ejemplo: "**ftp 192.192.1.100**".
4. Escriba el nombre de usuario.
5. Escriba la contraseña del sistema.
6. Utilice el comando "**put <Nombre de archivo>**" para cargar el archivo de auto configuración. "**#autoconfig**" debe ser incluido en la cabecera del archivo, y el nombre del archivo del archivo de auto configuración debe ser "**config.bat**". Por ejemplo: "**put config.bat**".

7.4.5 Configuración de sistema de copias de seguridad a través de FTP

Asegúrese de que su PC y el Switch estan en la misma VLAN antes de usar la función FTP y otras herramientas de administración remota. La VLAN del Switch será mostrada en la página **System-->IP setup** de la página Web o utilice "**net interface show**" para mostrar el VID a través del intérprete de comandos.

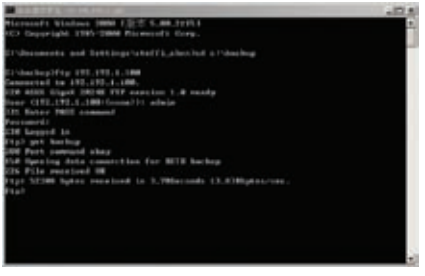


Figura 67. Configuración de sistema de copias de seguridad a través de FTP

1. Abra la ventana del interprete de comandos.
2. Vaya al directorio donde esté el archivo de configuración del sistema.
3. Utilice el comando "**ftp <Dirección IP>**" para conectar a dirección IP del Switch como la dirección IP de su servidor FTP. Por ejemplo: "**ftp 192.192.1.100**".

4. Escriba el nombre de usuario.
5. Escriba la contraseña del sistema.
6. El nombre por defecto de la configuración del sistema es "**backup**". Este nombre de archivo debe ser usado para hacer copias de seguridad de la configuración del sistema. El archivo puede ser renombrado tras la descarga.

7.4.6 Restauración de la configuración del sistema a través de FTP

Asegúrese de que su PC y el Switch estan en la misma VLAN antes de usar la función FTP y otras herramientas de administración remota. La VLAN del Switch será mostrada en la página **System-->IP setup** de la página Web o utilice "**net interface show**" para mostrar el VID a través del intérprete de comandos.

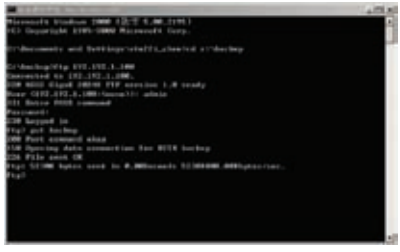


Figura 68. Restauración de la configuración del sistema a través de FTP

1. Abra la ventana del interprete de comandos.
2. Vaya al directorio donde esté el archivo de configuración del sistema.
3. Utilice el comando "**ftp <Dirección IP>**" para conectar a dirección IP del Switch como la dirección IP de su servidor FTP. Por ejemplo: "**ftp 192.192.1.100**".
4. Escriba el nombre de usuario.
5. Escriba la contraseña del sistema.
6. Utilice el comando "**put <Nombre de archivo>**" para restaurar la configuración del sistema. El archivo debe ser la copia de seguridad del mismo modelo de Switch. Por ejemplo: "**put backup**".

7.4.7 Copia de seguridad de la configuración del sistema a través de la Consola

1. Cambie la velocidad de su consola a 9600bps.
2. Ejecute el comando CLI "**sys files config backup**".
3. Recibirá la configuración del sistema a través del terminal con 1K Xmodem.

Figura 69. Copia de seguridad de la configuración del sistema a través de la consola

7.4.8 Restauración de la configuración del sistema a través de la Consola

1. Ejecute el comando CLI "**sys files config restore**". El archivo debe ser un archivo de copia de seguridad del mismo modelo de Switch.
2. Transfiera la configuración del sistema a través del terminal con 1K Xmodem .

Figura 70. Restauración de la configuración del sistema a través de la consola

8 Glosario

10BASE-T Designación para un tipo de cableado usado en redes Ethernet con una tasa de transferencia de datos de 10 Mbps. También conocida como cableado de Categoría 3 (CAT 3). Consulte tasa de datos, Ethernet.

100BASE-T Designación para un tipo de cableado usado en redes Ethernet con una tasa de transferencia de datos de 100 Mbps. También conocida como cableado de Categoría 5 (CAT 5). Consulte tasa de datos, Ethernet.

1000BASE-T Designación para un tipo de cableado usado en redes Ethernet con una tasa de transferencia de datos de 1000Mbps.

binario Sistema numérico en “base dos”, que utiliza solamente dos dígitos, 0 y 1, para representar todos los números. En binario, el número 1 esta escrito como 1, el 2 como 10, el 3 como 11, 4 como 100, etc. Aunque expresado como números decimales por conveniencia, las direcciones IP son realmente en binario. Por ejemplo, la dirección IP 209.191.4.240 es 11010001.10111111.00 000100.11110000 en binario. Consulte bit, dirección IP, máscara de red.

bit Quiere decir “dígito binario”, y es un número que tiene dos valores; 0 o 1. Consulte también binario.

bps bits por segundo.

CoS Clase de Servicio. Definido en 802.1Q, su rango de valores es desde 0 hasta 7.

DSCP Los seis bits más significantes del campo DiffServ en la cabecera IP es llamado DSCP. Los valores DSCP disponibles en GigaX son 0, 8, 10, 16, 18, 24, 26, 32, 34, 40, 46, 48, y 56.

broadcast (difusión) Envío de datos a todos los PCs de una red.

descargar Transferir datos hacia abajo. P.e. Desde Internet al usuario.

Ethernet La tecnología de red para computación usada más comúnmente, usualmente instalada sobre cableado par cruzado. Su tasa de transferencia es de 10 Mbps y 100 Mbps. Consulte también 10BASE-T, 100BASE-T, twisted pair (par cruzado).

filtrado Filtrar tipos de datos del tipo seleccionado, basados en reglas de filtrado. Filtrado puede ser aplicado en una dirección (entrada o salida), o en ambas direcciones.

regla de filtrado Una regla que especifica que tipos de datos un dispositivo de enrutado aceptará y/o rechazará. Las reglas de filtro están definidas para operar en un interfaz (o múltiples interfaces) y en una dirección particular (hacia arriba, hacia abajo, o en ambas direcciones).

FTP File Transfer Protocol. Protocolo de Transferencia de Archivos.

Un programa utilizado para transferir archivos entre PCs conectados a Internet. Usos comunes incluyen la carga de archivos a un servidor Web, y la descargas de archivos desde un servidor Web.

Host Un dispositivo (usualmente un Pc) conectado a una red.

HTTP Hyper-Text Transfer Protocol. Protocolo de transferencia de Hiper-Texto.

ICMP Protocolo de Control de Mensajes en Internet

Un protocolo de Internet usado para informar de errores u otra información de red. El comando ping utiliza ICMP.

IGMP Protocolo de Administración de Grupos en Internet

Un protocolo de Internet que permite a un PC compartir información sobre sus miembros en grupos de multidifusión con enrutadores adyacentes. Un grupo multidifusión de PCs en uno en el cual sus miembros han sido designados como interesados en recibir contenidos específicos de otros. Multicasting a un grupo IGMP puede ser usado para actualizar simultáneamente agendas en un grupo de usuarios móviles o para enviar cartas de empresa a una lista de distribución.

IGMP Snooping Snoop paquetes IGMP en cada puerto y asociarlos con el grupo multicast de nivel 2.

Internet Una colección global de redes interconectadas que se utilizan para comunicaciones públicas y privadas.

intranet Una red privada interna de una empresa que se parece mucho a Internet, pero que sólo puede ser accedida por sus empleados.

IP Consulte TCP/IP.

Dirección IP Dirección de protocolo de Internet

Dirección de un Host (PC) o Internet, con 4 números, cada uno entre 0 y 255, separados por comas, p.e. 209.191.4.240. Una dirección IP consiste en un identificador de red que identifica la red particular al cual el Host pertenece, y un identificador de Host que identifica éste de manera única en la red. Una máscara de red se utiliza para definir el identificador de red y el identificador de Host. Como las direcciones IP no son fáciles de recordar, éstas se asocian usualmente a un nombre de dominio que puede ser más específico. Consulte nombre de dominio, máscara de red.

ISP Internet Service Provider. Proveedor de servicios de internet.

Una empresa que proporciona acceso a internet para sus usuarios, usualmente por una cantidad de dinero.

LAN Local Area Network. Red de área local.

Una red limitada a una pequeña área demográfica, como por ejemplo una casa particular, oficina, o pequeño edificio.

LED Light Emitting Diode. Diodo emisor de luz.

Un dispositivo electrónico emisor de luz. Las luces indicadores frente al switch son LEDs.

MAC address Media Access Control address. Dirección de control de acceso al medio.

Dirección permanente del Hardware del equipo, asignada por su fabricante. Direcciones MAC son expresadas como seis pares de caracteres.

mask (máscara) Consulte máscara de red

Multicast Envío de datos un grupo de dispositivos de red.

Mbps Abreviación de Megabits por segundo, o un millón de bits por segundo. Tasa de datos en red suelen ser expresadas en Mbps.

Monitor También llamado “Roving Analysis”, permite insertar un analizador de red a un puerto para controlar el tráfico de otros puertos del switch.

network mask Una máscara de red es una secuencia de bits aplicados a una dirección IP para seleccionar el identificador de red mientras ignora el identificador de Host. Bits definidos como “1” significa “seleccionar éste bit” mientras que bits definidos como 0 significan “ignorar éste bit” Por ejemplo, si la máscara de red 255.255.255.0 es aplicada a la dirección IP 100.10.50.1, el identificador de red es 100.10.50, y el identificador de Host es 1. Consulte también binario, dirección IP, subred, sección “Explicación de direcciones IP”.

NIC **Tarjeta interfaz de red**

Una tarjeta adaptadora que es conectada a su PC y proporciona a interfaz física a su cableado de red, típicamente a través de un conector RJ-45. Consulte Ethernet, RJ-45.

paquete Los datos transmitidos en red están divididos en unidades llamadas paquetes. Cada paquete contienen “payload” (los datos), más información de cabecera como de donde vienen los datos (dirección de origen) y a donde va (dirección de destino).

ping **Packet Internet (o Inter-Network) Groper**

Un programa usado para verificar que el Host asociado a una dirección IP está online. También se utiliza para revelar la dirección IP de un dominio.

puerto Un punto de acceso físico a un dispositivo, como por ejemplo un PC o enrutador, a través del cual los datos fluyen desde y hasta éste dispositivo.

protocolo Un grupo de reglas que gobiernan la transmisión de datos. Para que una transmisión funciones, ambos extremos de la conexión deben seguir las reglas del protocolo.

PVLAN Private Virtual Local Area Network. Red de accceso de área local virtual privada.

QoS Quality of Service. Calidad del servicio.

Definido en 802.1Q, se utiliza para el rendimiento de red en comunicaciones de datos, las características QoS son ancho de banda, retraso, y confiabilidad.

remoto Un localización físicamente separada. Por ejemplo, un empleado que esté de viaje y se conecta a la intranet de su o empresa es un usuario remoto.

RJ-45 **Registered Jack Standard-45**

Un conector de 8 pínes usado en transmisiones de datos en líneas telefónicas. El cableado Ethernet utiliza usualmente éste tipo de conector.

RMON **Remote Monitoring**

Extensión de SNMP, proporciona capacidades para comprobación del estado de una red.

routing (enrutamiento) Envío de datos entre su red e internet usando la ruta más eficiente, basado en la dirección IP de destino y las condiciones actuales de red. Un dispositivo que realiza enrutamientos es conocido como enrutador.

SNMP **Protocolo Simple de Administración de Red**

Un protocolo TCP/IP usado para la administración de redes.

STP **Spanning Tree Protocol**

Un protocolo puente que evita que paquetes vayan en círculos en redes complicadas.

subnet (subred) Una subred es una porción de una red. La subred es distinguida de una red más grande con una máscara de subred que selecciona algunos de los PCs de la red y excluye el resto. Los PCs de la subred permanecen físicamente conectados al resto de la red, pero éstos son tratados como parte de una red separada. Consulte también máscara de red.

subred, máscara Una máscara que define una subred. Consulte también máscara de red

TCP Consulte TCP/IP.

TCP/IP **Transmission Control Protocol/Internet Protocol**

Uno de los protocolos básicos usados en Internet. TCP es responsable de la división de datos en paquetes para el envío y re-ensamblaje en destino, mientras que IP es responsable del envío de paquetes de origen a destino. Cuando TCP e IP trabajan juntos con aplicaciones superiores tales como HTTP, FTP, Telnet, etc., TCP/IP sirve para referir una suite de protocolos.

Telnet/SSH Un programa interactivo, basado en caracteres utilizado para acceder a un PC remoto. Mientras que HTTP (el protocolo Web) y FTP solo permiten la descargas desde un PC remoto, Telnet / SSH permite iniciar sesiones y utilizar PCs desde una localización remota.

TFTP **Trivial File Transfer Protocol**

Un protocolo para transferencia de archivos, TFTP es más fácil de usar que File Transfer Protocol (FTP) pero no tan capaz o seguro.

Trunk Dos o más puertos combinados en un puerto virtual, también llamado Adición de Enlaces.

TTL **Time To Live**

Un campo de un paquete IP que limita la vida del mismo. Originalmente significando duración, TTL esta representado usualmente en vez de número máximo de saltos; cada enrutador que recibe un paquete reduce este campo en una unidad. Cuando TTL es cero, el paquete es descartado.

twisted pair (par trenzado) Cableado de teléfono de cobre utilizado por compañías telefónicas. Contiene uno o más pares de cables cruzados juntos para reducir la inducción y ruido. Cada línea de teléfono utiliza un par. En casas, se suelen instalar dos pares. Para redes Ethernet, un grado superior llamado Categoría 3 (CAT 3) en usado en redes 10BASE-T, y un grado incluso superior llamado Categoría 5 (CAT 5) es usado en redes 100BASE-T. Consulte también 10BASE-T, 100BASE-T, Ethernet.

upstream La dirección de transmisión de datos desde un usuario a Internet.

VLAN Virtual Local Area Network

WAN Wide Area Network

Cualquier red que se extiende en una gran área geográfica, como por ejemplo un país o continente. Con respecto a SL-1000, WAN se refiere a Internet.

Web, navegador Un programa Software que utiliza el protocolo “Hyper-Text Transfer Protocol” (HTTP) para descargar o cargar información a sitios Web, y muestra ésta información, que puede consistir en texto, imágenes gráficas, sonido, o video, al usuario. Navegadores Web populares incluyen Netscape Navigator y Microsoft Internet Explorer. Consulte también página Web, sitio Web.

Web, página Archivo en sitio Web que contiene texto, gráficos y enlaces (referencias cruzadas) a otras páginas en el mismo sitio Web, o a páginas en sitios Web distintos. Cuando un usuario accede a un sitio Web, la primera página mostrada se llama página de inicio. Consulte también sitio web, navegador web.

Web, sitio Un PC en Internet que distribuye la información desde o hacia usuarios remotos a través de navegadores Web. Un sitio Web consiste típicamente en texto gráficos, y enlaces. Consulte también navegador Web, página Web.

WWW World Wide Web. Tela de araña mundial.

También llamada (la) Web. Término colectivo para todos los sitios Web en cualquier lugar en el mundo que pueden ser accedida a través de Internet.