Manual de configuración web del conmutador Dahua de 16/24 puertos PoE

V1.0.5

TECNOLOGÍA CO., LTD DE LA VISIÓN DE ZHEJIANG DAHUA

Advertencias y medidas de seguridad importantes

Lea atentamente las siguientes medidas de seguridad y advertencias antes de utilizar el producto para evitar daños y pérdidas.

Atenciones:

- No exponga el dispositivo a negro de lámpara, vapor o polvo. De lo contrario, podría provocar un incendio o una descarga eléctrica. No
- instale el dispositivo en una posición expuesta a la luz solar o a altas temperaturas. El aumento de temperatura en el dispositivo puede provocar un incendio.
- No exponga el dispositivo a un ambiente húmedo. De lo contrario, podría provocar un incendio.
- El dispositivo debe instalarse en una superficie sólida y plana para garantizar la seguridad bajo carga y terremoto. De lo contrario, puede hacer que el dispositivo se caiga o se vuelque.
- No coloque el dispositivo sobre una alfombra o un edredón.
- No bloquee la ventilación del dispositivo ni la ventilación alrededor del dispositivo. De lo contrario, la temperatura en el dispositivo aumentará y podría provocar un incendio.
- No coloque ningún objeto sobre el dispositivo.
- No desmonte el dispositivo sin instrucción profesional.
- Para evitar lesiones personales o daños al dispositivo, apáguelo antes de quitar el cable. El estabilizador
- de voltaje y el pararrayos son opcionales según la fuente de alimentación del sitio y el entorno circundante.

Advertencia:

- Utilice la batería correctamente para evitar incendios, explosiones y otros
- peligros. Reemplace la batería usada por una del mismo tipo.
- No utilice una línea de alimentación que no sea la especificada. Úselo correctamente. De lo contrario, podría provocar un incendio o una descarga eléctrica.
- Asegúrese de conectar a tierra el dispositivo (sección transversal del cable de cobre:> 2,5 mm_2, resistencia a tierra: ⩽ 4 Ω).

Anuncio especial:

- Este manual es solo para referencia.
- Todos los diseños y el software aquí están sujetos a cambios sin previo aviso por escrito.
- Siga siempre las instrucciones enumeradas en el manual. No somos responsables de ningún problema causado por modificaciones no autorizadas o intentos de reparación.
- Todas las marcas comerciales y marcas comerciales registradas son propiedad de sus respectivos
- dueños. Si hay alguna duda o controversia, consulte nuestra explicación final. Por favor visite nuestro
- sitio web para más información.

Tabla de contenido

1. Información general

1.1 Introducción del producto

El producto es un tipo de conmutador administrado, proporciona un puerto Ethernet PoE de 16/24 * 10 / 100M y 2 puertos Combo 1000M de enlace ascendente, admite funciones de administración de red de capa 2 y administración de PoE basadas en Web, lo que ayuda a realizar el reenvío de datos de alta velocidad. Se puede aplicar ampliamente en lugares como vigilancia de seguridad, administración de redes, etc.

1.2 Características del producto

- Proporcionar administración de red de capa 2 basada en web.
- Admite transmisión de 250 metros de larga distancia. Admite
- puertos combinados de 2 * 1000 M.
- Admite puertos RJ45 autoadaptables de 16/24 * 10 / 100M.
- Admite un puerto de consola.
- Cumple con los estándares IEEE802.3, IEEE802.3u, IEEE802.3ab / zy IEEE802.3X.
- VLAN estándar 802.1Q (acceso / troncal / híbrida)
- Todos los puertos se adaptan automáticamente al modo MDI / MDIX.
- Aprendizaje automático y envejecimiento de MAC, la capacidad de la lista de direcciones MAC es de 4K. Control
- de flujo dúplex completo IEEE802.3X y control de flujo semidúplex de contrapresión. Admite fuente de
- alimentación AC 100 ~ 240V.
- Cumple con los estándares IEEE802.3af e IEEE802.3at, tanto el puerto 1 como el puerto 2 admiten Hi-PoE 60W.
- Admite la gestión del consumo de energía PoE.
- Admite la gestión de red SNMP V1 / V2 / V3. Admite la
- plataforma de gestión de red iLinksView. Admite el
- protocolo de red de anillo STP / RSTP.
- Admite agregación manual y LACP estático.
- Admite la duplicación de varios a uno.
- Soporte de enlace MAC de puerto.
- Excelente protección de circuito aislado.
- Protección contra rayos hasta el nivel 4.

2 Estructura del dispositivo

2.1 Estructura del conmutador PoE de 24 puertos

2.1.1 Panel frontal

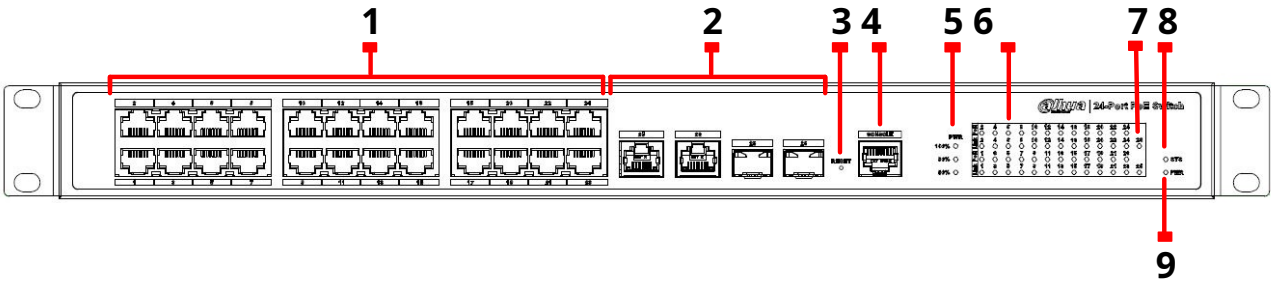


Figura 2-1

Consulte la tabla 2-1 para ver la descripción del panel frontal del conmutador PoE de 24 puertos.

SN	Parámetro	Nota
1	Puerto RJ45	Puerto Ethernet, admite autoadaptación 10 / 100M
2	Puerto combinado	Puerto Ethernet, admite autoadaptación 10/100 / 1000M, puerto de fibra compatible con 1000M.
3	Botón de reinicio	Mantenga presionado el botón para restablecer el dispositivo y recuperar la configuración predeterminada.
4	Puerto serie de la consola	Puerto de depuración del dispositivo
5	Uso de energía PoE indicador	Pantalla de consumo de energía actual
6	Luz indicadora de enlace descendente	Estado actual del enlace del puerto y estado de PoE.
7	Indicador de puerto combinado luz	El puerto combinado indica enlace / acto
8	Luz indicadora del sistema	Estado del sistema. - Cuando el dispositivo se inicia, la luz parpadea rápidamente. - Cuando el dispositivo funciona correctamente, la luz parpadea lentamente.
9	Luz indicadora de poder	Estado de energía actual del dispositivo.

Tabla 2-1

2.1.2 Panel trasero

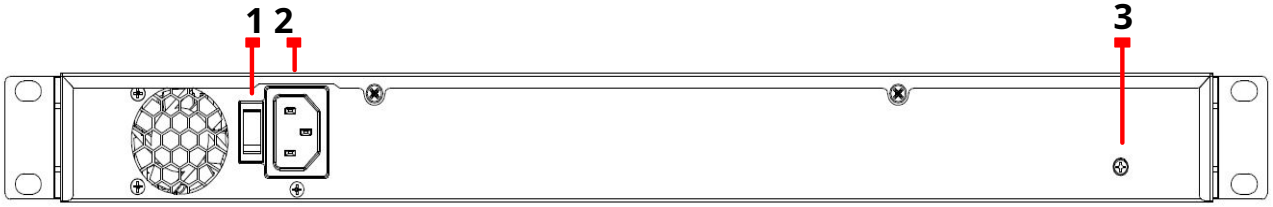


Figura 2-2

Consulte la tabla 2-2 para ver la descripción del panel trasero.

SN	Parámetro	Nota
1	Interruptor de alimentación	Control de encendido y apagado del dispositivo
2	Toma de corriente	Soporta AC 100～240 V
3	Terminal de tierra	Cable de tierra

Tabla 2-2

2.2 Panel frontal del conmutador PoE de 16 puertos

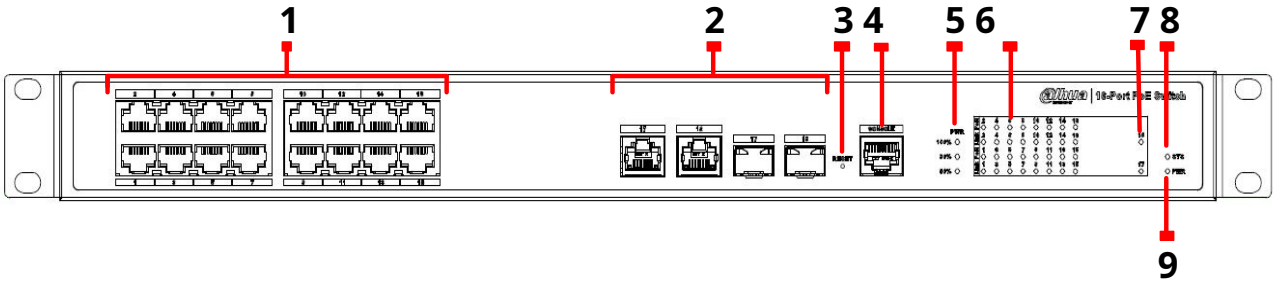


Figura 2-3

Consulte la tabla 2-3 para obtener más detalles.

SN	Parámetro	Nota
1	Puerto RJ45	Puerto Ethernet, admite autoadaptación 10 / 100M
2	Puerto combinado	Puerto Ethernet, admite autoadaptación 10/100 / 1000M, puerto de fibra compatible con 1000M.
3	Botón de reinicio	Mantenga presionado el botón para reiniciar el dispositivo.
4	Puerto serie de la consola	Puerto de depuración del dispositivo
5	Uso de energía PoE indicador	Pantalla de consumo de energía actual
6	Luz indicadora de enlace descendente	Estado actual del enlace del puerto y estado de PoE.
7	Indicador de puerto combinado luz	El puerto combinado indica enlace / acto
8	Luz indicadora del sistema	Estado del sistema. - Cuando el dispositivo se inicia, la luz parpadea rápidamente. - Cuando el dispositivo funciona correctamente, la luz parpadea lentamente.
9	Luz indicadora de poder	Estado de energía actual del dispositivo.

Tabla 2-3

3 Iniciar sesión en el interruptor

3.1 Cambiar inicio de sesión

Primero debe iniciar sesión en el conmutador antes de configurar el conmutador, los usuarios pueden administrar y mantener intuitivamente el conmutador Ethernet de la serie PFS42 a través de la administración de red web.

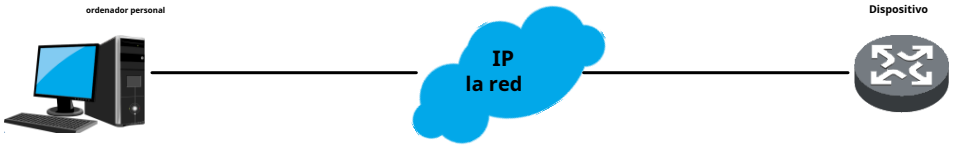


Figura 3-1

Puede acceder al conmutador a través del navegador web; asegúrese de que su computadora se haya conectado a la red donde se encuentra el conmutador. No necesita configuración adicional si es la primera vez que usa Switch, ahora puede usar Web para visitar.

1. Modifique la dirección IP y la máscara de subred del adaptador de red de su computadora a 192.168.1.50 y 255.255.255.0 respectivamente.
2. Abra el navegador web, ingrese 192.168.1.110 en la barra de direcciones y tenga en cuenta que 192.168.1.110 es la dirección de administración predeterminada del conmutador.
3. Establezca la contraseña del usuario administrador, que no debe tener menos de 8 caracteres, y luego haga clic en **Ahorrar**.

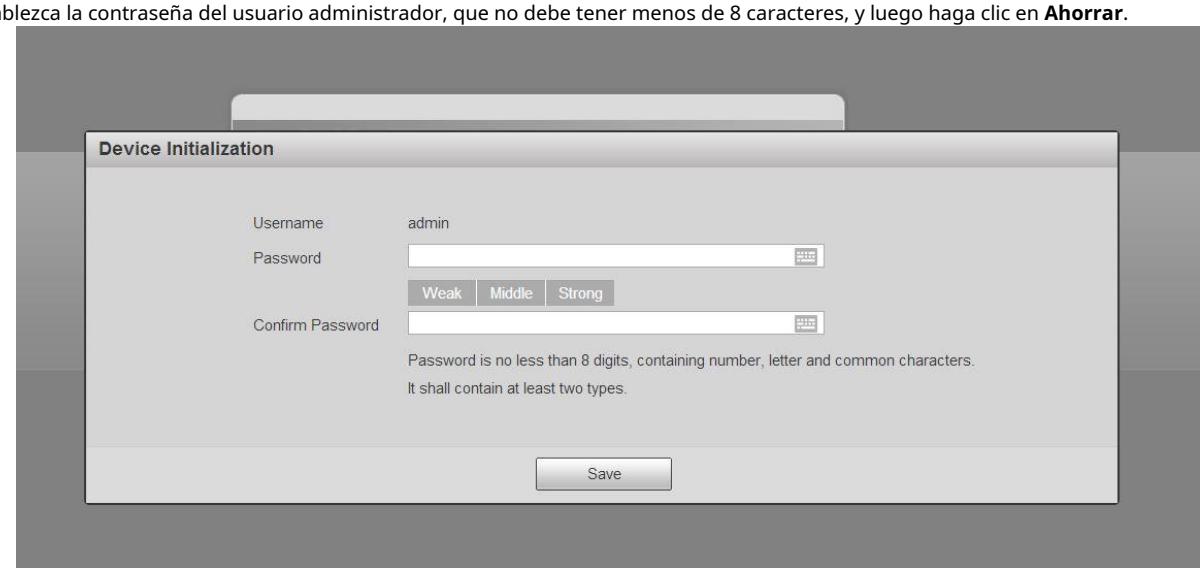


Figura 3-2

4. Ingrese la cuenta de usuario y la contraseña, y luego haga clic en **Acceso** para iniciar sesión en el dispositivo.

Figura 3-3

5. La interfaz de información del sistema del conmutador se mostrará si el nombre de usuario y la contraseña son correctos.

- iLinksView está habilitado de forma predeterminada y el nombre de usuario predeterminado es admin, la contraseña predeterminada es lt_91_il_02_nmp.
- Cuando utilice iLinksView para administrar el dispositivo, tenga en cuenta que el nombre de usuario y la contraseña deben ser los mismos que ha establecido en iLinksView; de lo contrario, iLinksView no puede descubrir el dispositivo.

3.2 Introducción a la interfaz WEB

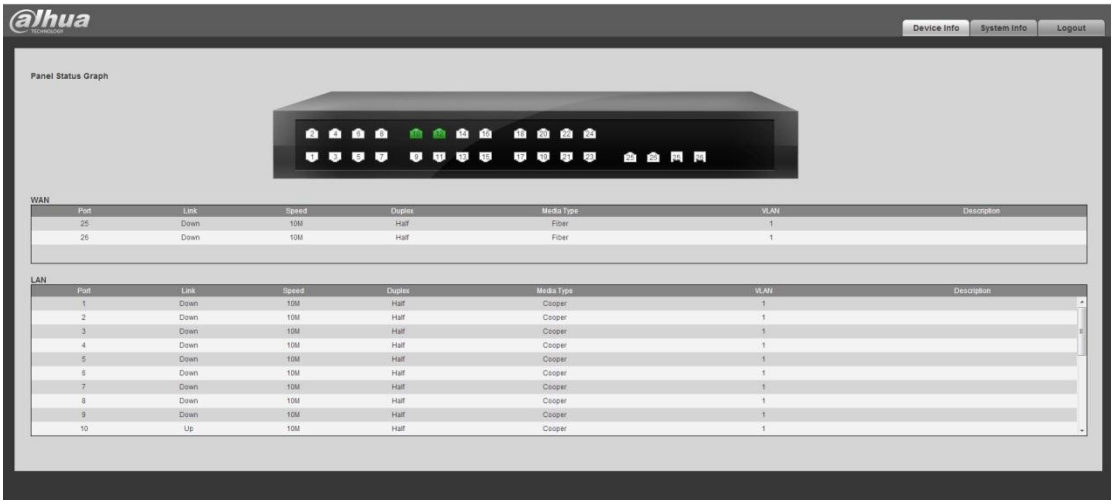


Figura 3-4

Como se muestra en la Figura 3-4, toda la interfaz de administración WEB se divide en varias partes que incluyen la sección de visualización de información del dispositivo, la barra de navegación y la sección de configuración, etc.

3.2.1 Sección de visualización de información del puerto

En la Figura 3-5 se muestra que la pantalla de información del puerto se divide en la pantalla del estado del puerto WAN y la pantalla del estado del puerto LAN. Puede mostrar el estado actual del enlace del puerto, la velocidad del puerto, el modo dúplex, etc.

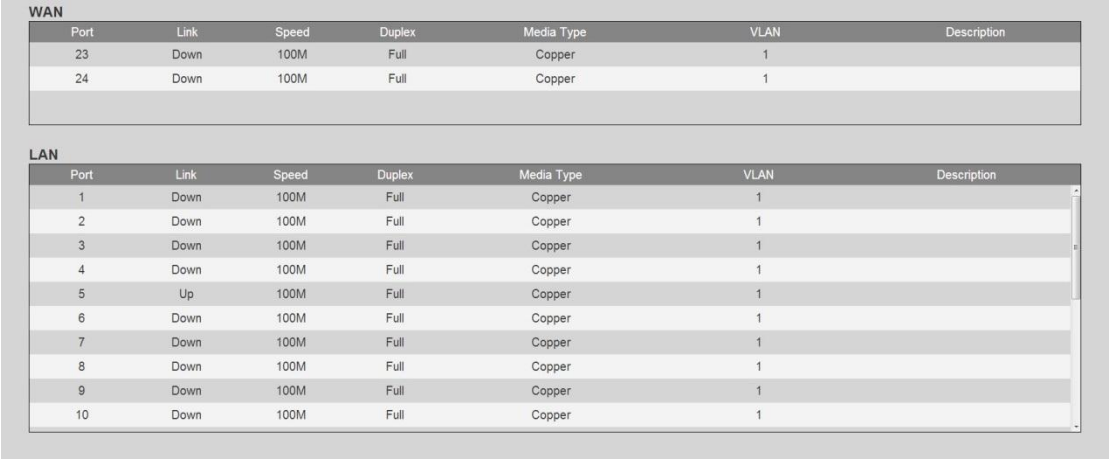


Figura 3-5

3.2.2 Barra de navegación

La barra de navegación controla lo que se muestra en la sección de configuración. El contenido de la barra de navegación se muestra en forma de lista y está dividido por categoría. Haga clic primero en el nombre del grupo si necesita configurar algún elemento, haga clic en los subelementos después de que se despliegue la lista. Por ejemplo, primero haga clic en Administración de puertos si necesita verificar el flujo del puerto actual y luego haga clic en Estadísticas del puerto; consulte la Figura 3-6 para obtener más detalles.

Figura 3-6

3.2.3 Sección de visualización de configuración

La sección de configuración mostrará los contenidos que se seleccionan en la barra de navegación, y se puede

comprobado y la configuración se puede modificar en la sección de configuración.

Se introducirán cuatro módulos de configuración a través de los siguientes cuatro capítulos, que son configuración del sistema, administración de puertos, administración de dispositivos y PoE.

4 Configuración del sistema

4.1 Descripción general de la configuración del sistema

Haga clic en información del sistema y podrá ver lo que se muestra en la Figura 4-1.

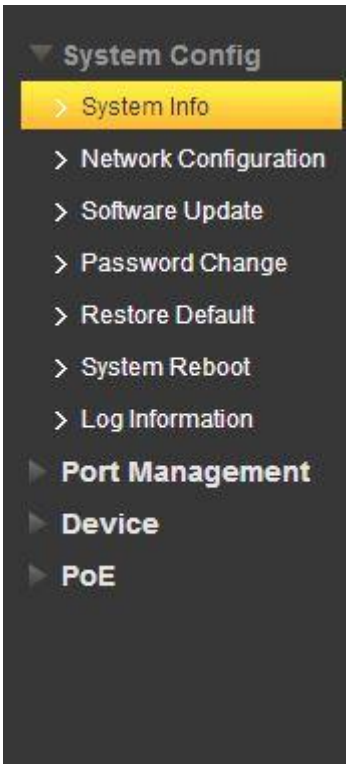


Figura 4-1

4.1.1 Información del sistema

Consulte la Figura 4-2 para ver la interfaz de visualización de información del sistema del conmutador, donde puede buscar el modelo del dispositivo, la dirección MAC y la versión del software.

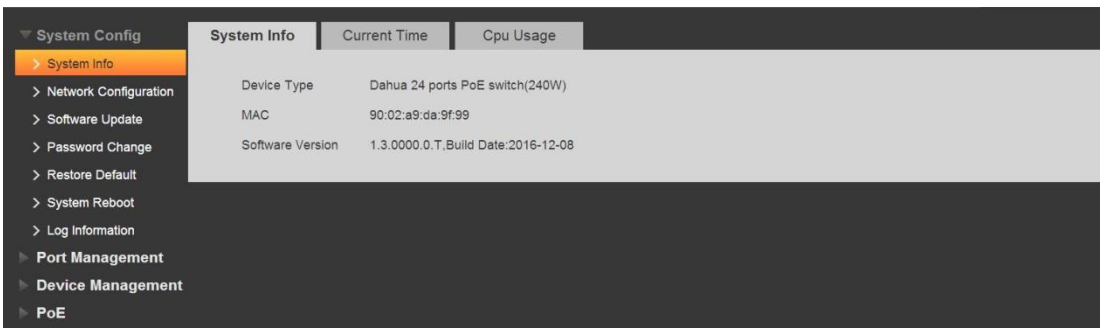


Figura 4-2

4.1.2 Hora actual

Consulte la Figura 4-3 para ver la interfaz de visualización de la hora del sistema de interruptores, donde puede configurar la hora y la zona horaria actuales del dispositivo.

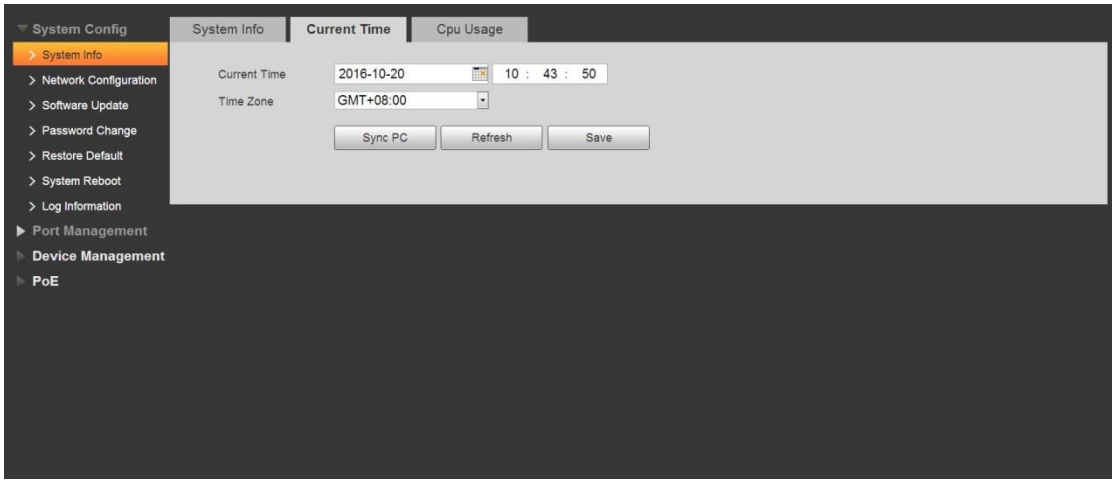


Figura 4-3

4.1.3 Uso de CPU

Consulte la Figura 4-4 para ver la interfaz de visualización del uso de la CPU del conmutador, donde puede buscar el uso de la CPU mientras el dispositivo está en funcionamiento.

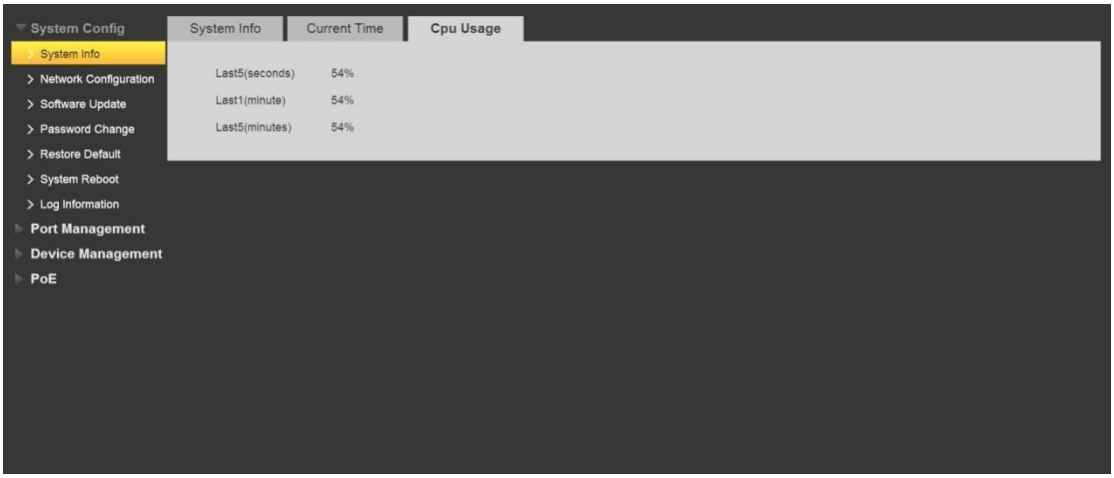


Figura 4-4

4.2 Configuración de red

Cada host necesita una dirección IP para la comunicación de red.
La dirección IP (Protocolo de Internet) es una dirección de 32 bits utilizada en Internet, es un tipo de formato de dirección uniforme proporcionado por el protocolo IP, que generalmente se muestra con 4 números decimales. La dirección IP es una dirección lógica distribuida para cada red y host en Internet, que se utiliza para identificar cada host y realizar la intercomunicación de la red.

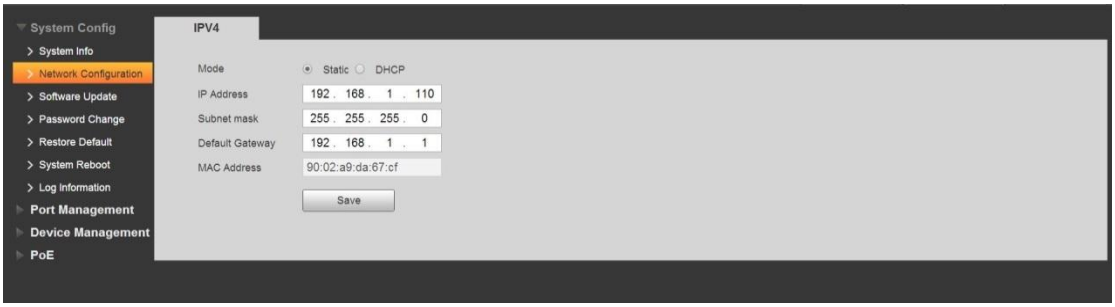


Figura 4-5

Consulte la Figura 4-5 para ver la interfaz de configuración de IP, donde puede verificar la dirección IP del dispositivo, la máscara de subred, la puerta de enlace predeterminada y la dirección MAC. La IP predeterminada del conmutador es 192.168.1.110, que se puede modificar en esta interfaz.

Consulte la tabla 4-1 para conocer la configuración de la dirección.

Parámetro	Nota
dirección IP	Dirección IP de gestión del conmutador, que puede modificar la IP de gestión del conmutador
Máscara de subred	Cambie la dirección de la máscara de subred, que puede modificar la configuración.
Puerta de enlace predeterminada	Cambiar ruta predeterminada
Dirección MAC	Dirección física del conmutador, que no se puede modificar.

Tabla 4-1

Nota

No modifique la máscara de subred del conmutador al azar. Es posible que no pueda iniciar sesión en el conmutador si se modifica incorrectamente.

4.3 DHCP

DHCP (Protocolo de configuración dinámica de host) se utiliza para asignar dinámicamente la dirección IP y otros parámetros de configuración de red para los dispositivos de red.

DHCP adopta el modo de comunicación cliente / servidor, el cliente realiza la aplicación de configuración al servidor y el servidor vuelve a la dirección IP y otra información de configuración correspondiente asignada por el cliente, que es para realizar la configuración dinámica de la dirección IP, etc.

En la aplicación típica de DHCP, generalmente incluye un servidor DHCP y varios clientes (como PC y computadora portátil), como se muestra en la Figura 4-6.

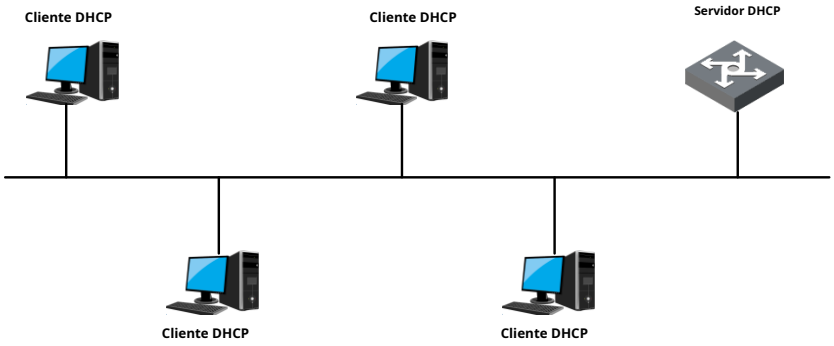


Figura 4-6

Ejemplos de configuración.

1. Requisito de trabajo en red

Configure el conmutador como cliente DHCP, adquiera automáticamente la dirección IP de gestión del conmutador.

2. Pasos de configuración

una. Marque "DHCP", que se muestra en la Figura 4-7.

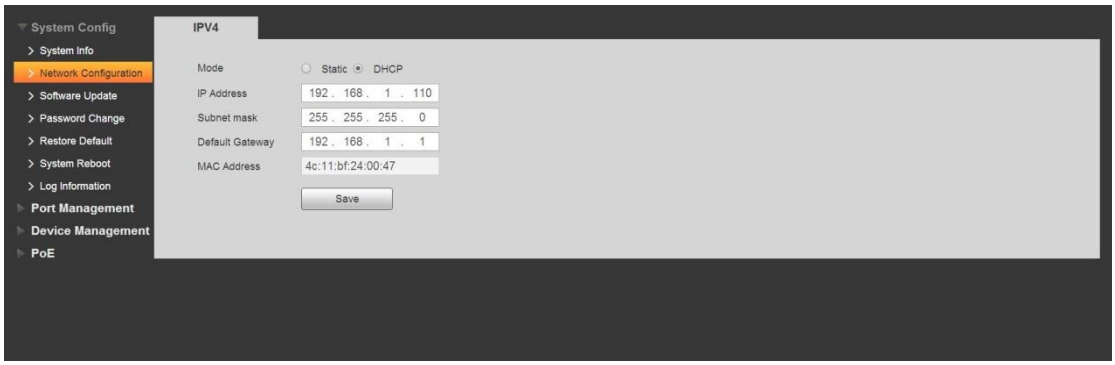


Figura 4-7

B. Clic en Guardar".

4.4 Actualización de software

En la siguiente interfaz, proporciona la función de actualización de archivos del sistema a través de WEB para el conmutador. Puede descargar la última versión del archivo del sistema en el sitio web de Dahua.

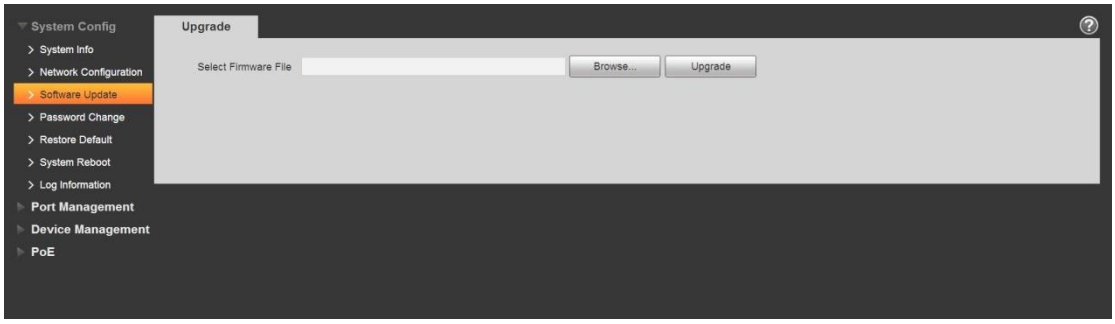


Figura 4-8

4.5 Cambio de contraseña

Puede modificar la contraseña de inicio de sesión del usuario en la siguiente interfaz; el nombre de usuario es admin, que no puede ser

modificado, y la contraseña predeterminada de fábrica es admin.

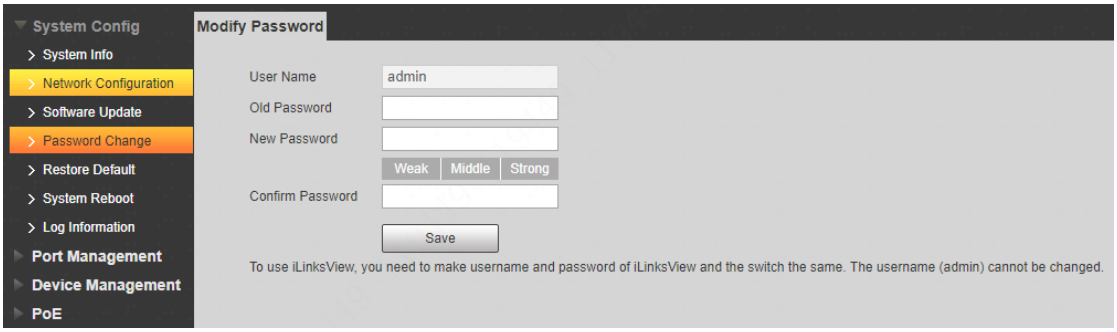


Figura 4-9

4.6 Restaurar valores predeterminados

Puede seleccionar la función predeterminada cuando necesite restaurar la configuración del conmutador a la configuración predeterminada del sistema inicial. Excepto la IP de administración y la contraseña de inicio de sesión, el resto de la información se restaurará a la configuración predeterminada de fábrica.

Nota

Cuando se restablece el interruptor presionando el botón de restablecimiento, todas las configuraciones se restablecerán a los valores predeterminados de fábrica, la dirección de administración se restablecerá a 192.168.1.110 y el usuario debe cambiar la contraseña para el primer inicio de sesión.

Figura 4-10

4.7 Reinicio del sistema

Necesita guardar la configuración antes de reiniciar el dispositivo. De lo contrario, todas las configuraciones se perderán después del reinicio. Debe iniciar sesión en la interfaz WEB del dispositivo nuevamente después de reiniciar el dispositivo.

Figura 4-11

4.8 Información de registro

Consulte la Figura 4-12 para ver la interfaz de visualización del registro del sistema, donde puede verificar parte de la información del registro del sistema durante el funcionamiento del dispositivo, lo que facilita que el personal de mantenimiento analice los problemas.

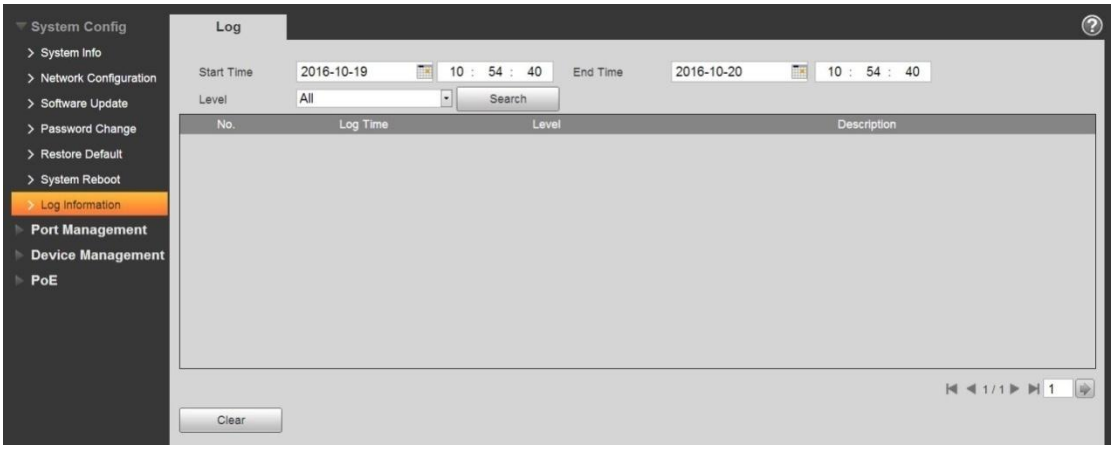


Figura 4-12

Ejemplo de configuración.

1. Configure "Hora de inicio" y "Hora de finalización", establezca el período que debe buscarse.
2. Seleccione el nivel de evento, incluidos Error, Advertencia e Información.
3. Haga clic en "Buscar".

5 Gestión de puertos

5.1 Configuración de puerto

La configuración del puerto se puede utilizar para configurar cada parámetro básico relacionado con el puerto del conmutador. El parámetro básico del puerto afectará directamente el modo de trabajo del puerto, realice la configuración de acuerdo con los requisitos prácticos.

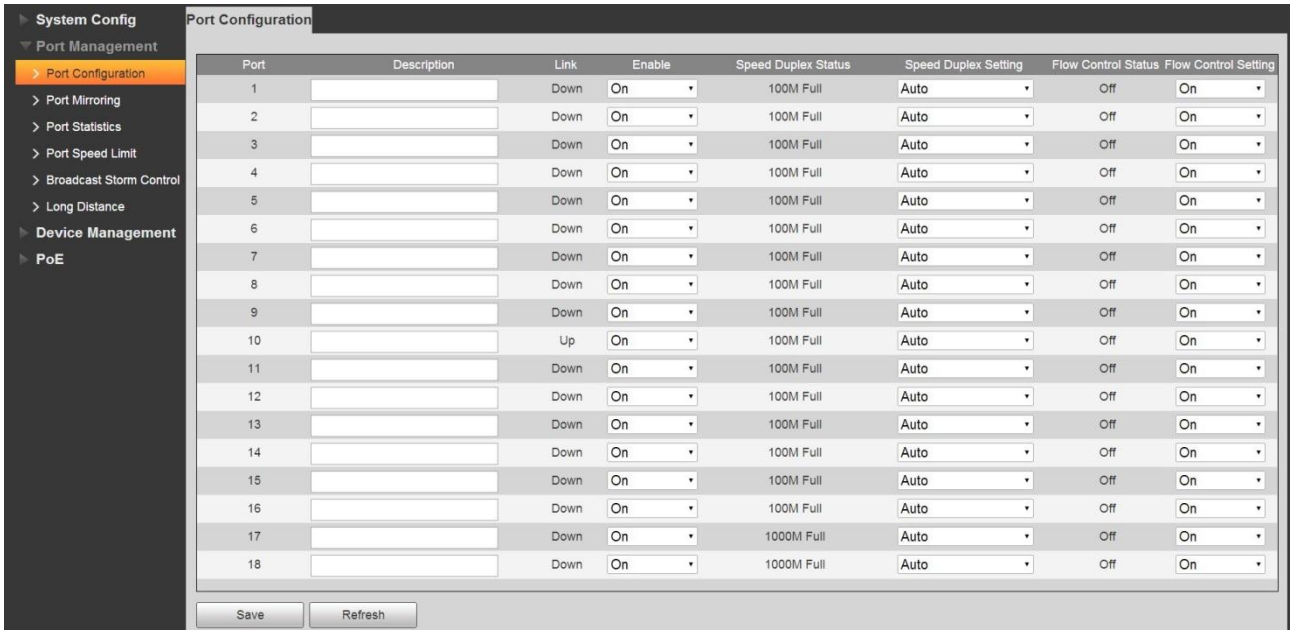


Figura 5-1

Consulte la Figura 5-1 para ver la interfaz de configuración del puerto del conmutador, en esta interfaz puede verificar la descripción, el estado del enlace, el estado del dúplex de velocidad, el estado del control de flujo de cada puerto, también puede agregar información de descripción del puerto, configurar el estado de habilitación y deshabilitación , velocidad, modo dúplex y función de control de flujo de cada puerto.

- Puerto: muestra el número de puerto del conmutador;
- Descripción del puerto: agrega información de descripción para el puerto; Habilitar: Sirve
- para configurar el puerto encendido / apagado.

Consulte la tabla 5-1 para conocer la configuración del estado del puerto.

Estado	Nota
Sobre	El enlace de configuración está habilitado.
Apagado	El enlace de configuración está en estado desactivado.

Tabla 5-1

- Enlace: muestra el estado del enlace del puerto.

Consulte la tabla 5-2 para ver la visualización del estado del puerto.

Estado	Nota
Hasta	Significa que el enlace está habilitado.
Abajo	Significa que el enlace está en estado desactivado.

Tabla 5-2

- Velocidad — actual: muestra el estado de velocidad actual del puerto.

Consulte la tabla 5-3 para ver la pantalla dúplex de la velocidad del puerto.

Puerto	Velocidad actual	Modo dúplex de velocidad
Puerto Ethernet	Auto (predeterminado)	Modo de negociación automática
	10M COMPLETO	Dúplex completo 10M
	10M MITAD	Medio dúplex de 10M
	100M COMPLETO	100 M dúplex completo
	100M MITAD	100M semidúplex
	1000M COMPLETO	1000M dúplex completo
Puerto de fibra	1000M-X	1000M dúplex completo

Tabla 5-3

- Speed –config: Sirve para configurar el modo dúplex de velocidad del puerto.

Nota

Afectará directamente la comunicación del puerto si cambia el modo dúplex de velocidad del puerto; así que modifíquelo con cuidado.

Consulte la tabla 5-4 para ver la configuración dúplex de la velocidad del puerto.

Puerto	Modo de velocidad	Definición
Puerto Ethernet	Auto（defecto）	Puerto velocidad dúplex modo autoadaptación
	10M COMPLETO	Velocidad del puerto modo dúplex 10 M dúplex completo
	10M MITAD	Velocidad del puerto modo dúplex medio dúplex de 10 M
	100M MITAD	Velocidad del puerto modo dúplex 100 M semidúplex
	100M COMPLETO	Velocidad del puerto modo dúplex 100 M dúplex completo
	1000M COMPLETO	Velocidad del puerto modo dúplex 1000M full duplex
Puerto de fibra	1000-X	El puerto de fibra está configurado como modo dúplex completo de 1000 M

Tabla 5-4

- Control de flujo: Sirve para configurar la función de control de flujo del interruptor (la configuración predeterminada está activada).

En la interfaz de control de flujo del puerto, **sobre** es habilitar la función de control de flujo del puerto y las tramas de pausa se pueden enviar o recibir normalmente, **apagado** es deshabilitar la función de control de flujo del puerto.

Nota

Para el puerto Ethernet, habilite la función de control de flujo del puerto para sincronizar la velocidad de entrada y la velocidad de salida en caso de que haya pérdidas de paquetes como resultado de las diferentes velocidades.

5.2 Duplicación de puertos

La duplicación de puertos (llamada monitor de puertos) es el proceso de copiar el paquete que pasa a través de un puerto o varios

puertos (llamado puerto de origen) a otro puerto (llamado puerto de destino) conectado con un dispositivo de monitoreo para el análisis de paquetes. Sirve para monitorear la red y resolver el mal funcionamiento de la red. Vea la Figura 5-2.

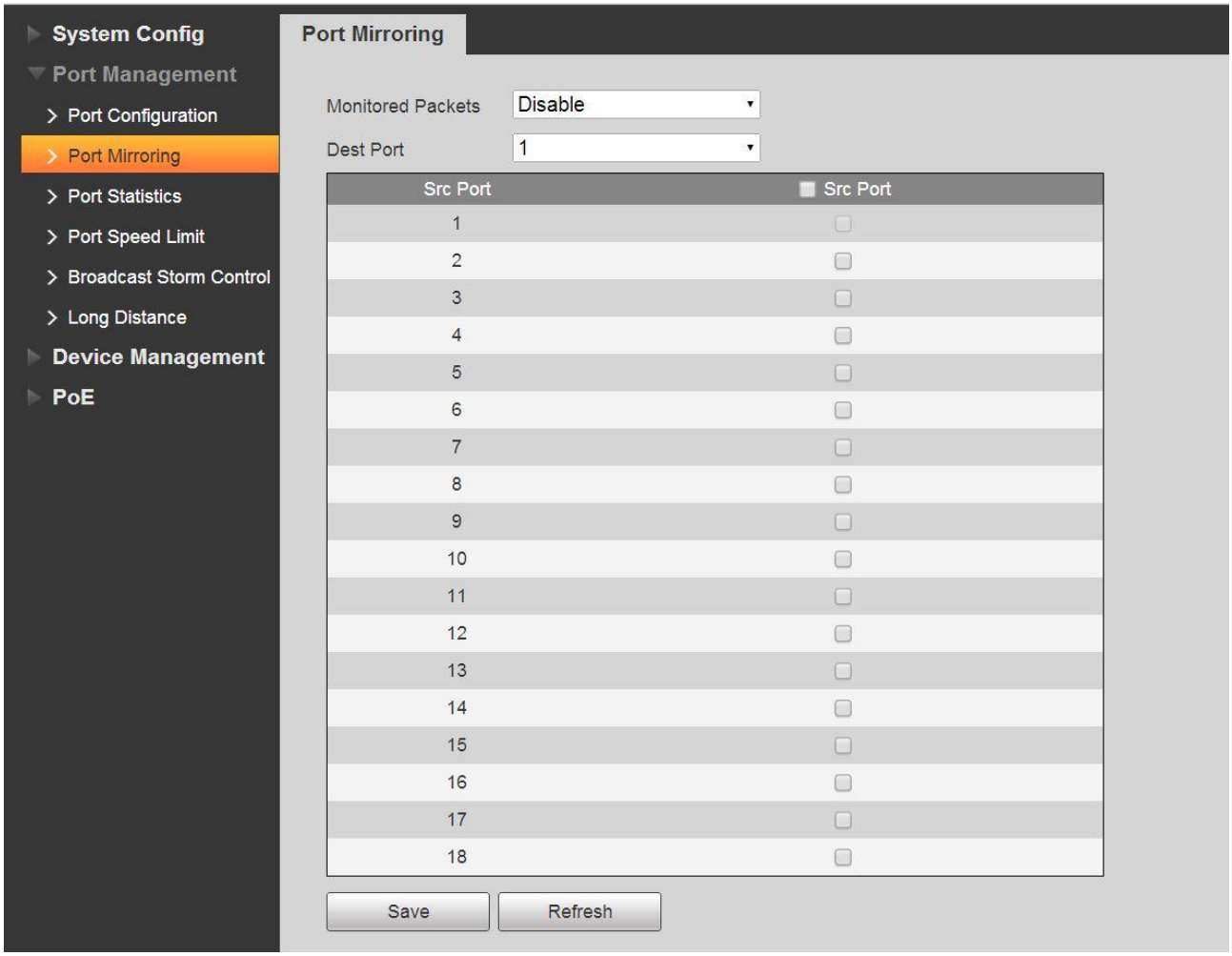


Figura 5-2

- Puerto de destino: el puerto del monitor. Seleccione solo un elemento. La configuración predeterminada está desactivada.
- Puerto de origen: el puerto que se está monitoreando. Seleccione uno o más artículos.
- Habilitar espejo: hay cuatro modos: Deshabilitar, solo Tx, solo Rx, habilitar.

Consulte la tabla 5-5 para obtener información sobre la configuración de la duplicación de puertos. •

Nombre	Nota	
Reflejado Paquetes	Desactivar（defecto）	Deshabilitar la función de monitor
	Tx solamente	Monitorear paquetes de salida
	Solo con receta	Monitorear paquetes de entrada
	Habilitar	Monitorear paquetes de entrada / salida
Puerto de destino	Puerto de monitorización. Seleccione solo un elemento. La configuración predeterminada está desactivada.	
Puerto de origen	El puerto que se está monitoreando. Seleccione uno o más artículos.	

Tabla 5-5

Ejemplo de configuración.

1. Conexión de red

Habilite la función de duplicación de puertos para que el puerto 1 pueda monitorear los paquetes del puerto 2 y el puerto 3. 2. Configuración

(1) Habilite la función de duplicación de puertos y seleccione los flujos de datos a monitorear.
(2) Seleccione el puerto de origen.
(3) Seleccione el puerto de destino. Ahora la interfaz se muestra como en la Figura 5-3.

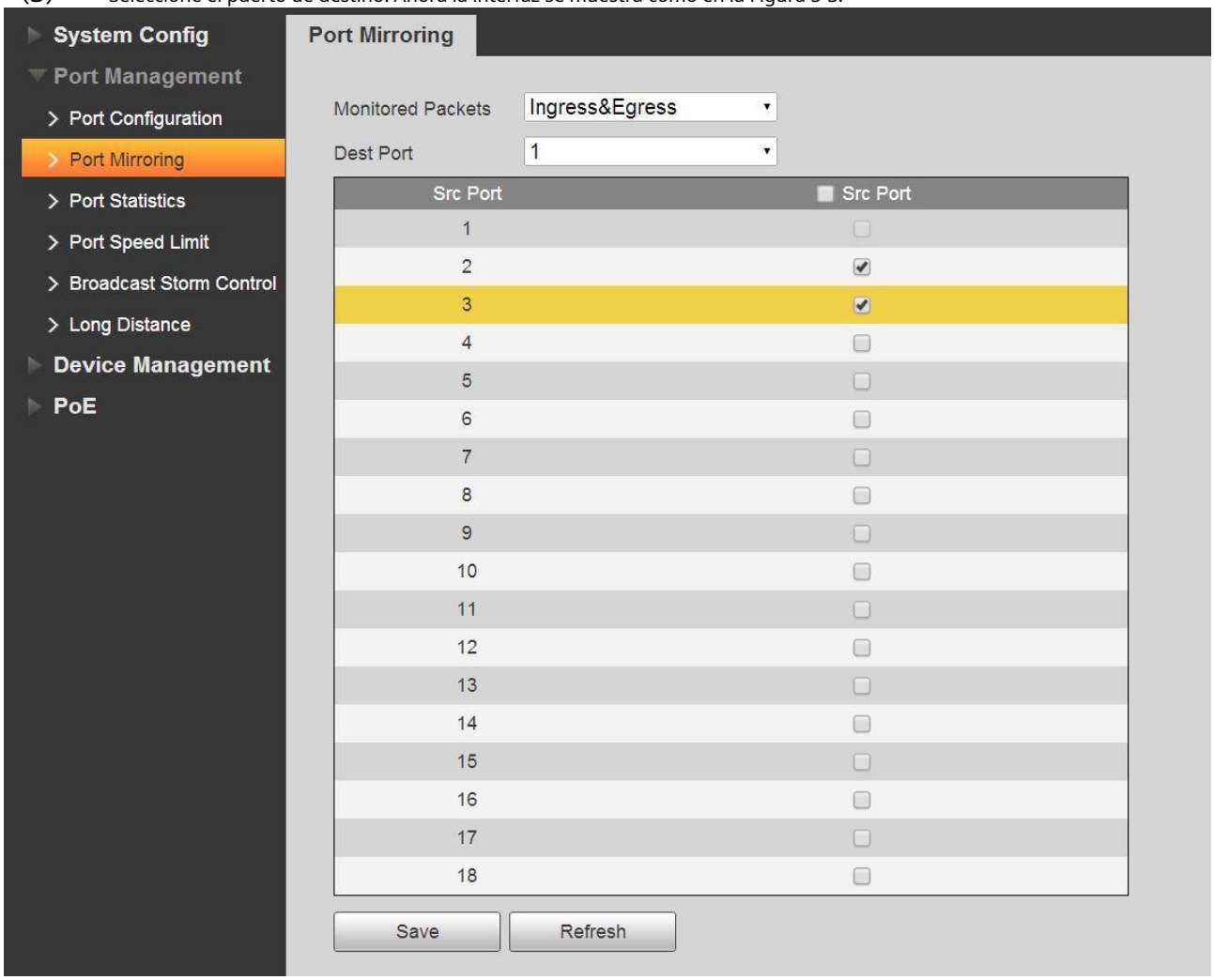


Figura 5-3

5.3 Estadísticas de puertos

La Figura 5-4 es la interfaz de estadísticas del puerto del conmutador. Aquí se muestra la cantidad de paquetes entrantes / salientes de cada puerto, estadísticas de conflicto, cantidad de pérdida de paquetes, paquete de error CRC, etc. El rendimiento de funcionamiento del puerto es bajo si la cantidad de paquetes de error es demasiado grande, verifique la conexión del cable del puerto o confirme El puerto opuesto correspondiente tiene un problema o no.

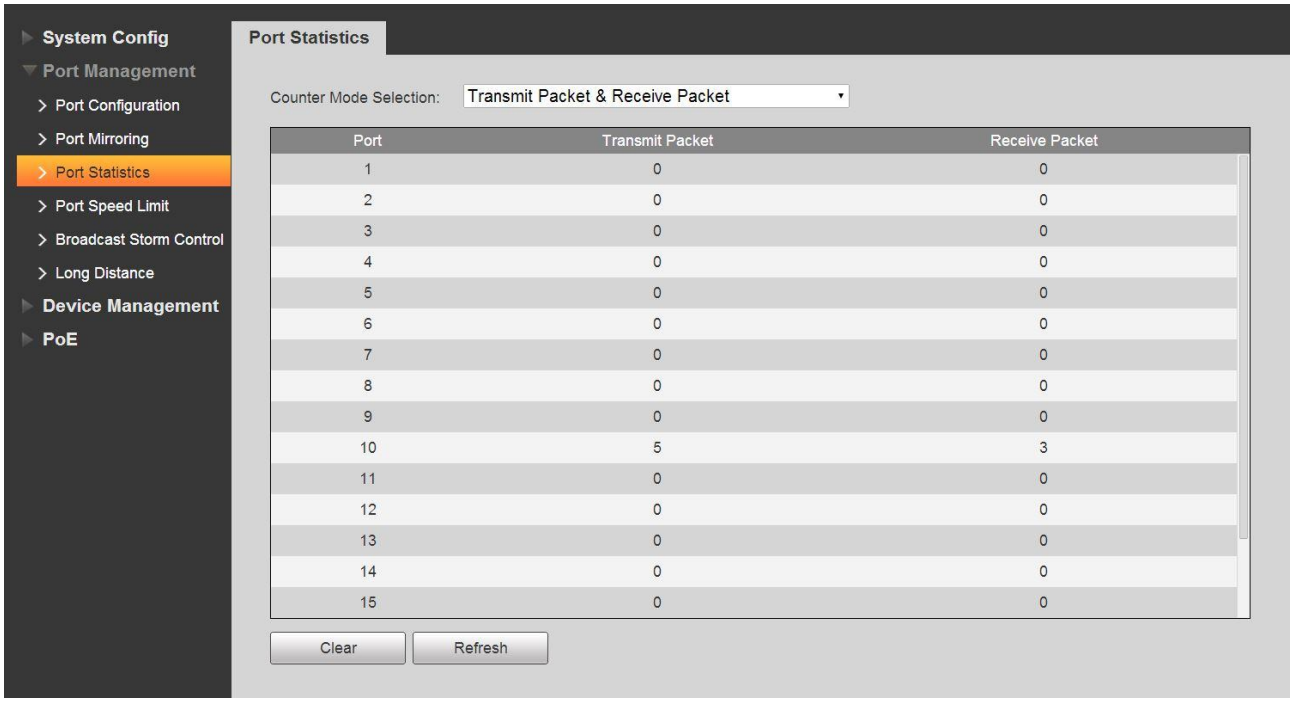


Figura 5-4

5.4 Límite de velocidad del puerto

Aquí se configuran los parámetros del límite de velocidad del puerto, se restringe la tasa de intercambio de paquetes de datos entrantes / salientes. Vea la Figura 5-5.

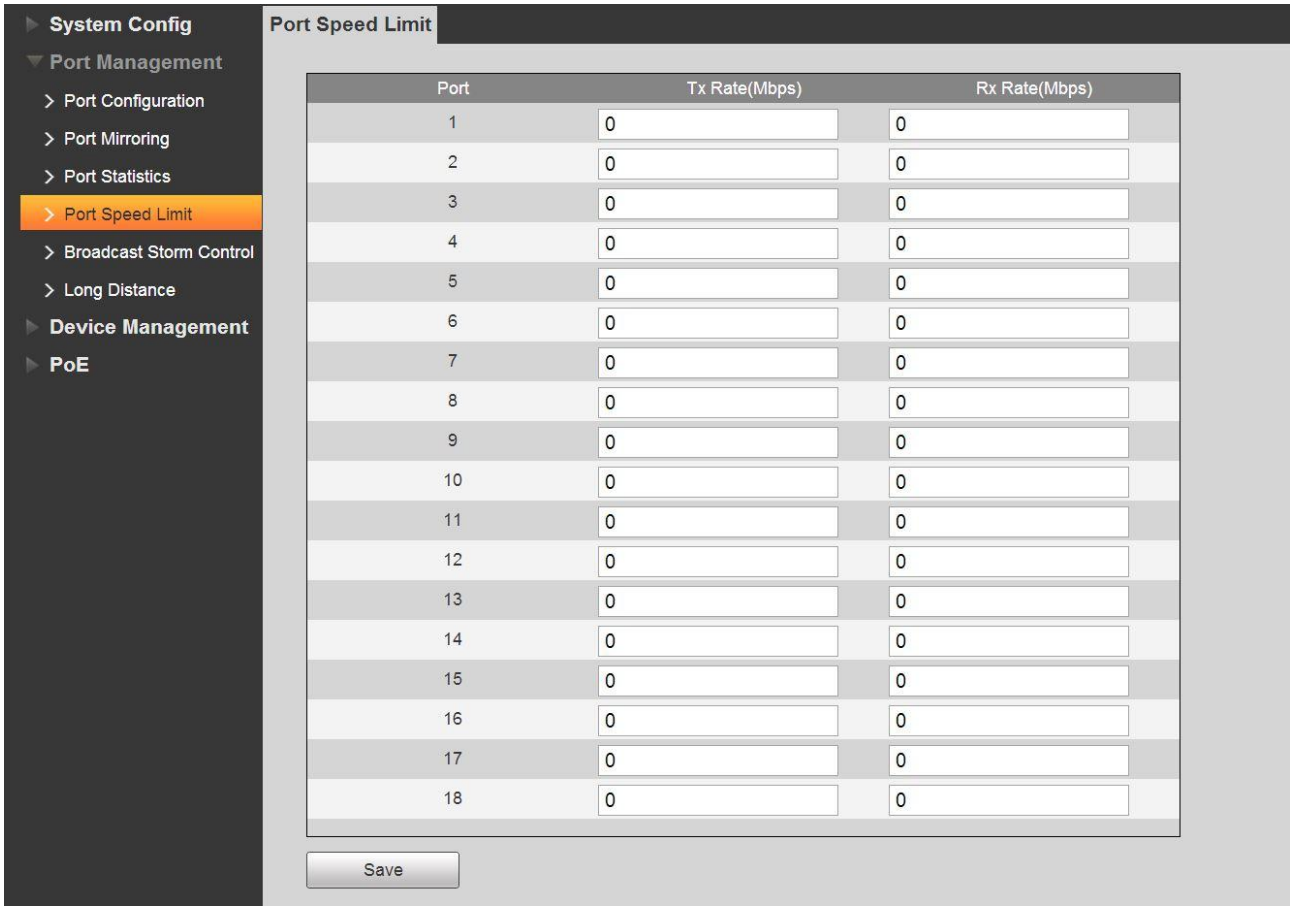


Figura 5-5

Consulte la Figura 5-5 para establecer la política de límite de velocidad de cada puerto. Consulte la Tabla 5-6 para conocer los parámetros de límite de velocidad del puerto.

Nombre	Nota
Puerto	Mostrar lista de puertos.
Velocidad Tx	Sirve para establecer la tasa de salida del puerto. El valor varía de 0 a 63 Mbps. La configuración predeterminada es 0, no hay límite de velocidad.
Velocidad Rx	Sirve para establecer la tasa de entrada del puerto. El valor varía de 0 a 63 Mbps. La configuración predeterminada es 0, no hay límite de velocidad.

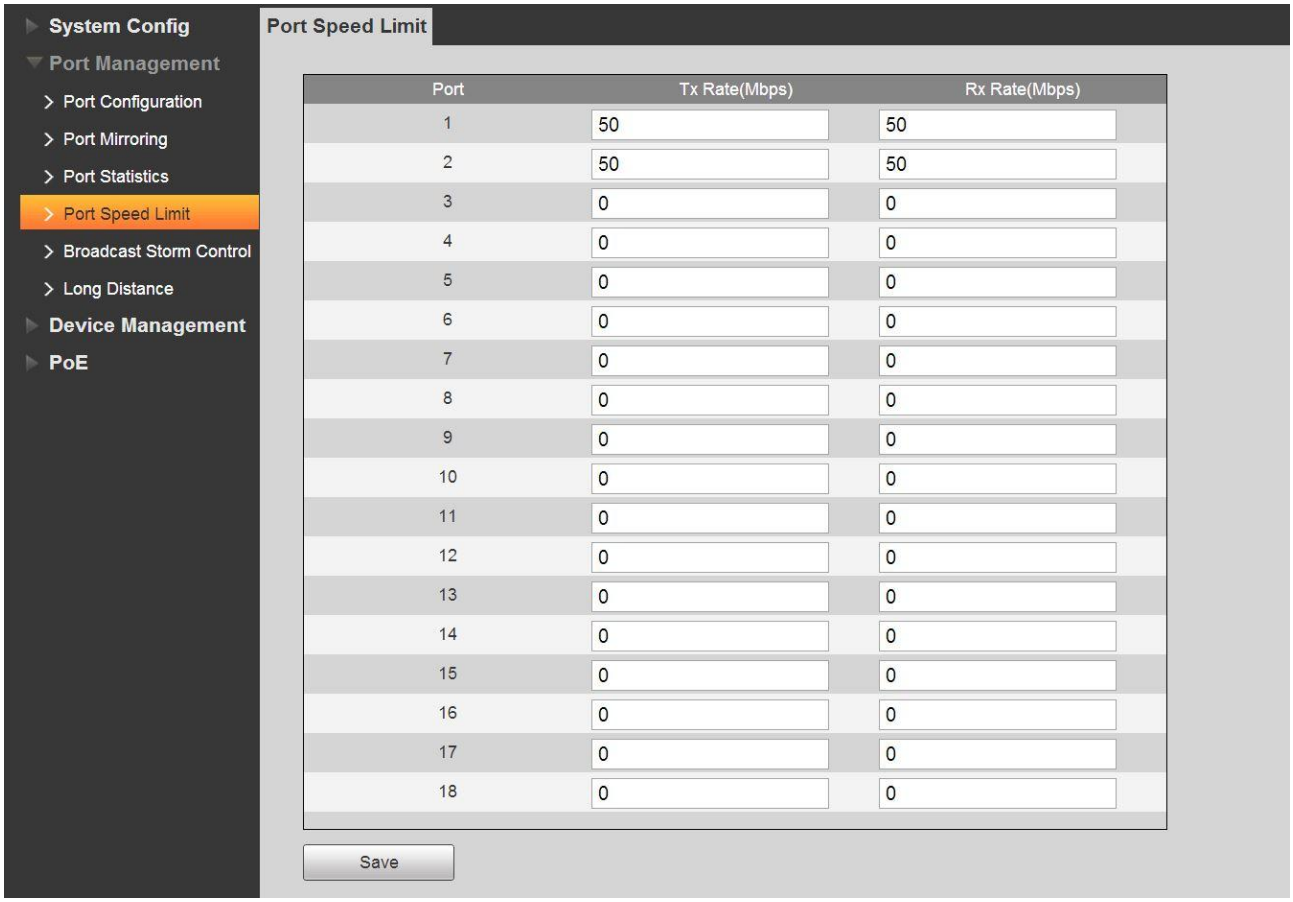
Tabla 5-6

Ejemplo de configuración.

1. Conexión de red

Establezca el límite de velocidad del puerto 1 y el puerto 2. La velocidad de cada puerto es inferior a 50 Mbps. 2. Configuración

（1） Configure la velocidad Tx / Rx del puerto. Vea la Figura 5-6.



.

Figura 5-6

(2) Haga clic en el botón Guardar.

5.5 Control de tormentas de difusión

La tormenta de transmisión se refiere a un fenómeno: las tramas de transmisión en la red se reenvían una y otra vez, lo que afecta las comunicaciones adecuadas. Reduce en gran medida el rendimiento de la red. El control de tormentas puede limitar los flujos de difusión del puerto y puede descartar las tramas de difusión una vez que el flujo ha superado el umbral especificado. Es para reducir el riesgo de tormenta de transmisión y garantizar el correcto funcionamiento de la red. Vea la Figura 5-7.

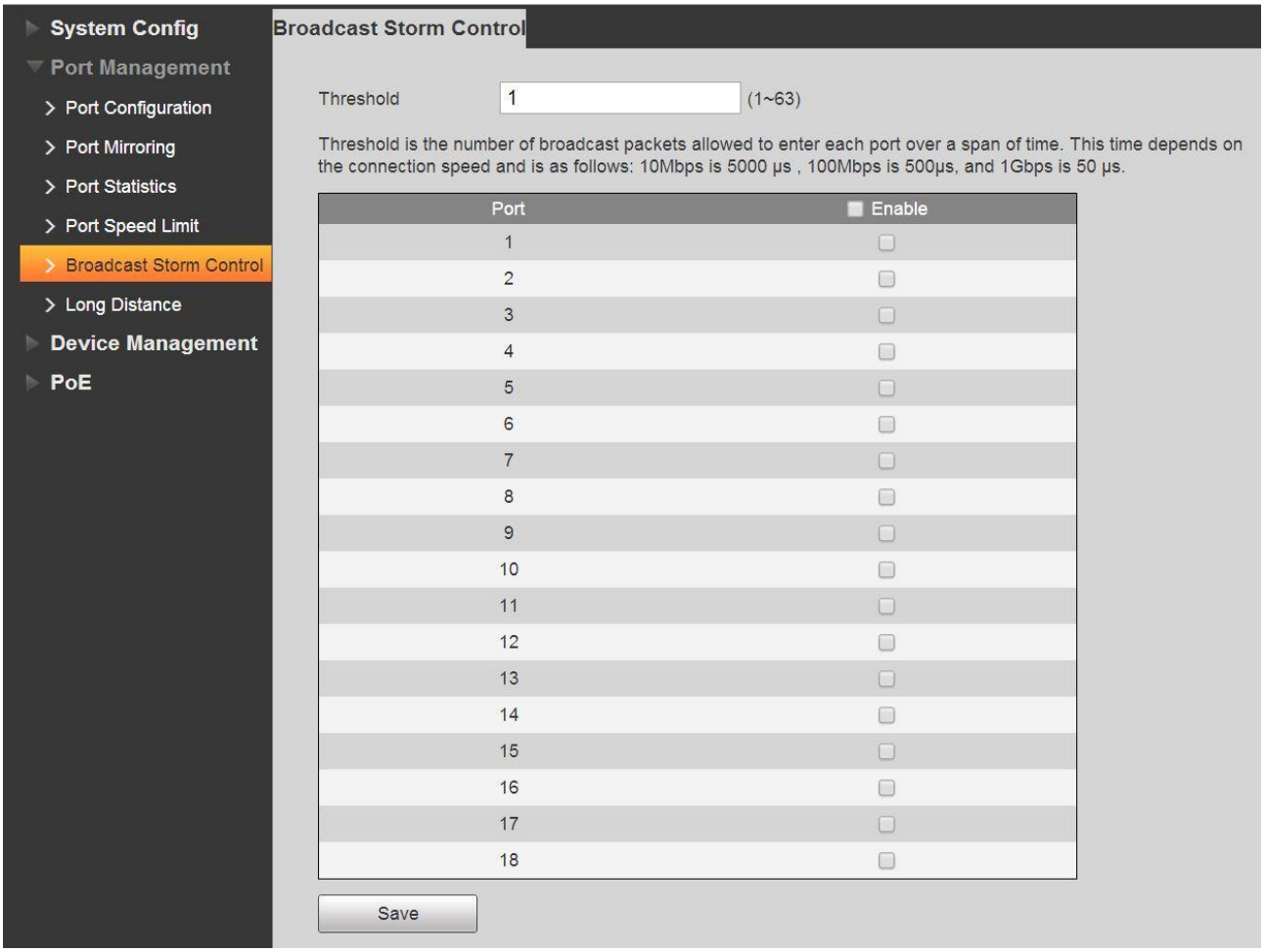


Figura 5-7

Consulte la Tabla 5-7 para conocer los parámetros de control de transmisión.

Nombre	Nota
Umbral	El límite de paquetes de difusión de un puerto durante el período especificado.
Puerto	Nombre del puerto.

Tabla 5-7

Ejemplo de configuración.

1. Conexión de red

Configure la función de control de tormentas de transmisión en todos los puertos. En caso de que el puerto funcione incorrectamente y el dispositivo no pueda transmitir correctamente los datos cuando hay tantos paquetes de transmisión.

2. Configuración

(1) Establecer valor de umbral. Es la cantidad de paquetes de difusión de un puerto.

(2) Seleccione un puerto para configurar.

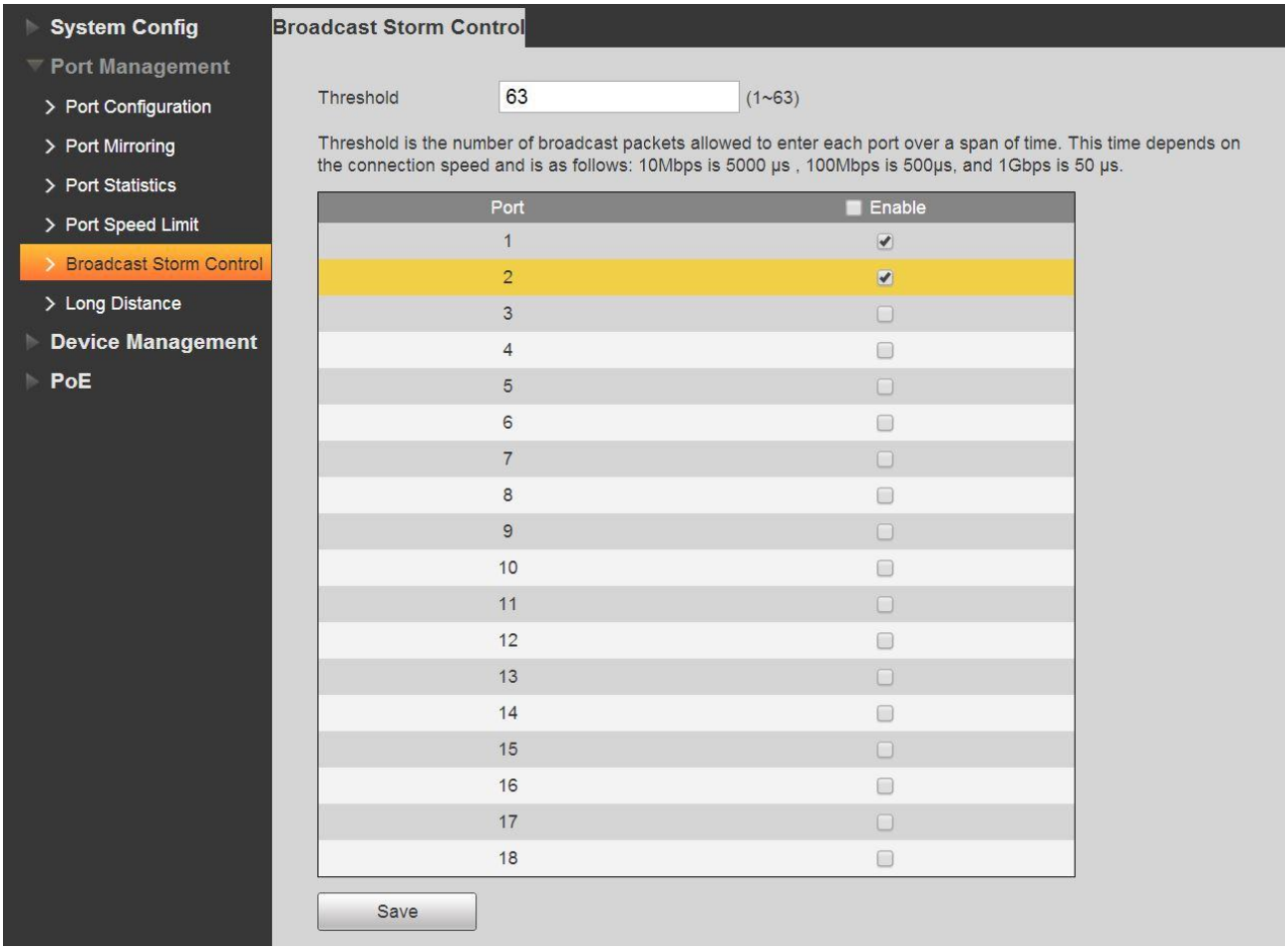


Figura 5-8

(3) Haga clic en el botón Guardar.

5.6 Transmisión de larga distancia

En esta interfaz, es para configurar el modo de transmisión de larga distancia del puerto. Para el modo Ethernet estándar, la velocidad de transmisión puede llegar a ser de 10 Mbps / 250 metros en lugar de 100 Mbps / 100 metros. Vea la Figura 5-9.

Figura 5-9

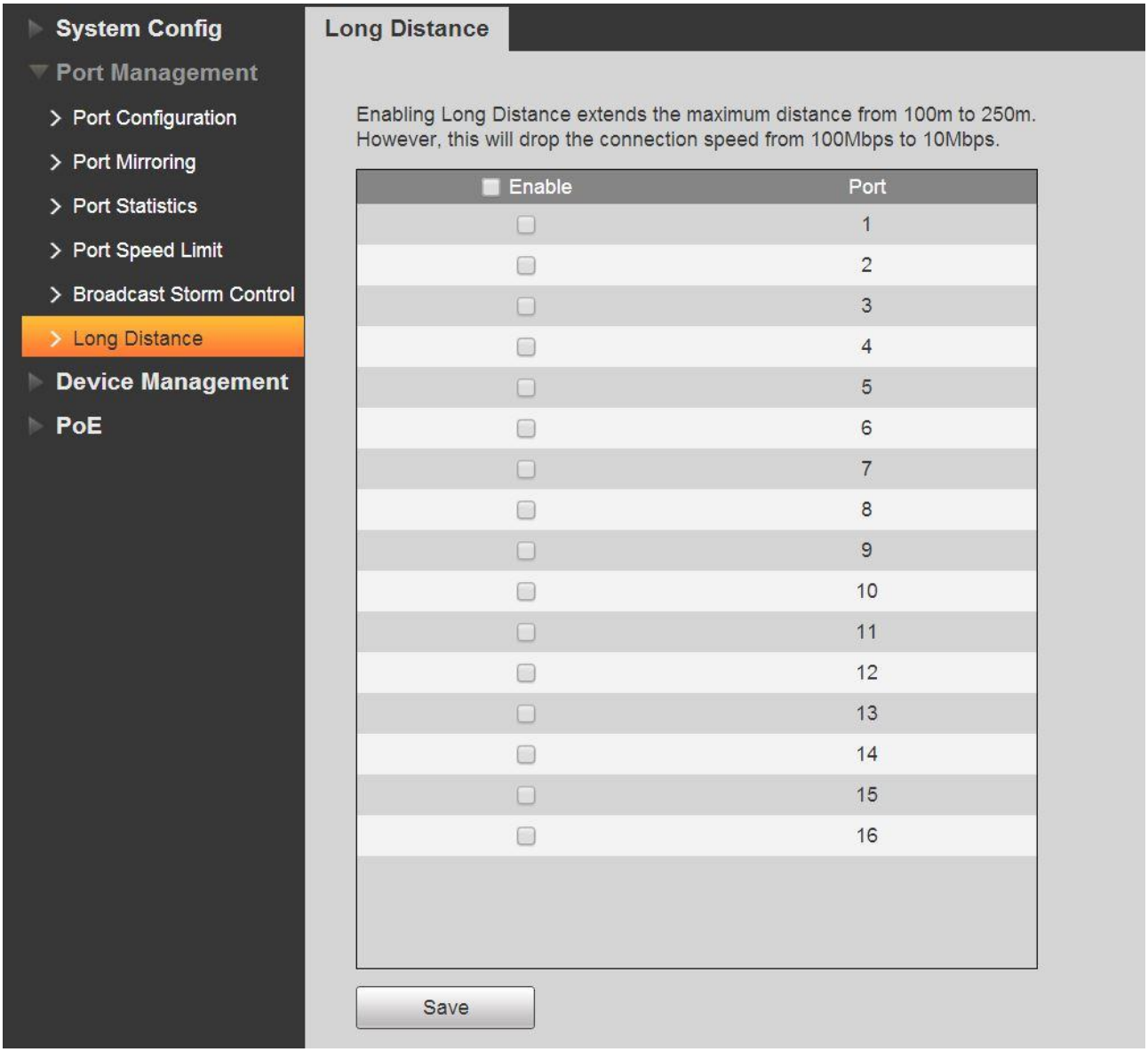


Figura 5-9

Ejemplo de configuración.

1. Conexión de red

Configure la función de transmisión de larga distancia de todos los puertos para que pueda admitir una transmisión adecuada de datos de 250 metros.

2. Configuración

(1) Compruebe un puerto para habilitar la función de transmisión de larga distancia.

(2) Haga clic en el botón Guardar. Vea la Figura 5-10.

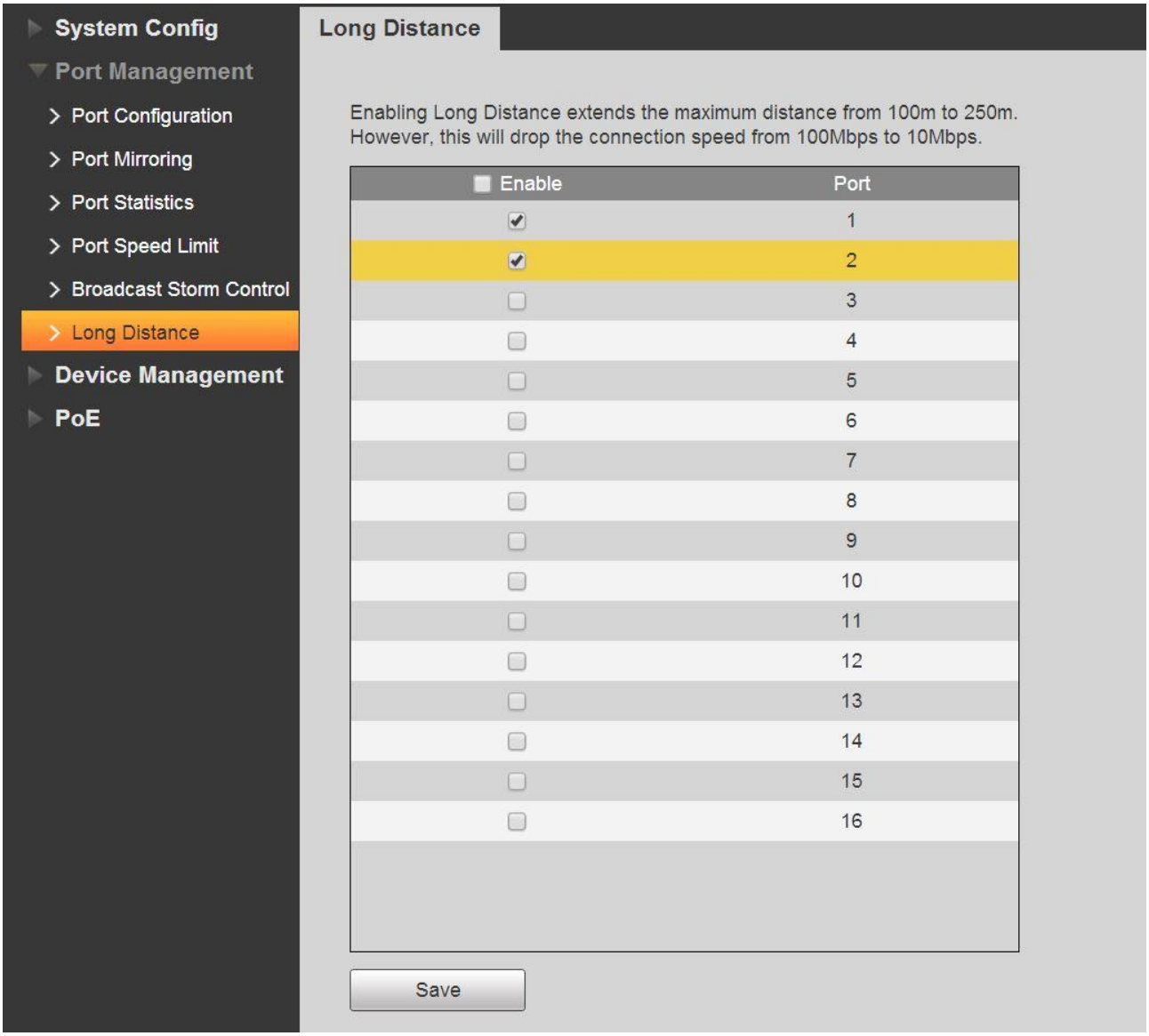


Figura 5-10

6 Gestión de dispositivos

6.1 Red de anillo

6.1.1 Definición de STP

La idea básica del protocolo STP es muy simple. Todos sabemos que los árboles que crecen en la naturaleza no generarán un circuito de bucle, por lo que no generará un circuito de bucle si la red crece como árboles en la naturaleza. Por lo tanto, define Root Bridge, Root Port, Designated Port, Path Cost y otros conceptos en el protocolo STP, que es realizar el propósito de recortar el circuito de bucle redundante mediante la estructuración de un árbol, y mientras tanto puede realizar la copia de seguridad del enlace y la optimización de la ruta. El algoritmo de estructuración del árbol se denomina algoritmo de árbol de expansión.

El paquete de protocolo adoptado por STP es BPDU (Bridge Protocol Data Unit), que también se denomina información de configuración. BPDU contiene suficiente información para garantizar el proceso de cálculo de completar el árbol de expansión. STP puede confirmar la estructura topológica de la red mediante la transmisión de BPDU entre dispositivos.
El formato BPDU y la descripción del campo pueden realizar las funciones del árbol de expansión, es para realizar la información

interacción mediante la transmisión de paquetes BPDU entre conmutadores. Todos los conmutadores que admiten el protocolo STP recibirán y tratarán el paquete recibido. El paquete contiene toda la información útil en el área de datos que se puede utilizar para el cálculo del árbol de expansión. El formato de trama BPDU y la descripción de campo del árbol de expansión estándar se muestran en la Figura 6-1.

2	1	1	1	8	4
Protocol Identifier	Version	Message Type	Flag	Root ID	Root Path Cost
Bridge ID	Port ID	Message Age	Max Age	Hello Time	Forward Delay
8	2	2	2	2	2

Figura 6-1

- Identificador de protocolo: la identificación del protocolo.
- Versión: la versión del protocolo.
- Tipo de mensaje: tipo BPDU.
- Bandera: Bandera bit.
- ID DE RAÍZ: ID de puente raíz, que se compone de 2 bytes de prioridad y 6 bytes de dirección MAC.
- Costo de la ruta raíz: el costo de la ruta raíz.
- Bridge ID: significa el ID del puente que envía BPDU, que se compone de 2 bytes de prioridad y 6 bytes de dirección MAC.
- Port ID: Identifica el puerto que envía BPDU. Edad del
- mensaje: tiempo de vida de BPDU.
- Edad máxima: tiempo de envejecimiento del BPDU actual, que es el tiempo más largo para que el puerto guarde
- BPDU. Hora de saludo: el ciclo de período de Bridge Root que envía BPDU.
- Retraso de reenvío: significa el tiempo de mantenimiento del estado de búsqueda y estudio antes de enviar el paquete de datos después de que se cambia la topología.

6.1.2 Conceptos básicos de STP

Identificador de puente: es el valor numérico completo de la prioridad del puente y su dirección MAC, y la prioridad del puente es un parámetro que se puede configurar. Cuanto menor sea el ID de puente, mayor será la prioridad del puente, lo que aumenta la posibilidad de convertirse en puente raíz.

Puente raíz: es el conmutador con ID de puente mínimo. Seleccione el mejor conmutador entre el circuito de bucle y configúrelo como el conmutador de puente raíz, que proporciona el mejor rendimiento y confiabilidad de la red.

Puente designado: en cada segmento de red, el puente con el costo de ruta más bajo hacia el puente raíz se convertirá en puente designado, a través del cual el paquete de datos se reenviará al segmento de red. El conmutador con el ID de puente más bajo se seleccionará como Puente designado cuando todos los conmutadores tengan el mismo costo de ruta raíz.

Costo de ruta raíz: es el total de todos los costos de ruta en la ruta entre dos puentes de red. El costo de la ruta raíz del puente raíz es cero.

Bridge Priority: es un parámetro que puede ser configurado por los usuarios, el rango numérico es de 0 a 61440. Cuanto menor sea el valor, mayor será la prioridad. Cuanto mayor sea la prioridad del puente, es más probable que se convierta en un puente raíz.

Puerto raíz: el puerto más cercano al puente raíz en el conmutador de puente no raíz, responsable de la comunicación con el puente raíz, el costo de la ruta desde este puerto al puente raíz es el más bajo. El puerto con la prioridad de puerto más alta se convertirá en el puerto raíz cuando varios puertos tengan el mismo costo de ruta hacia el puente raíz.

Puerto designado: es el puerto en el puente designado que implementa el reenvío de datos al conmutador.

Prioridad del puerto: el rango de valor numérico es de 0 a 240, y tiene que ser el múltiplo integral de 16. Cuanto menor sea la prioridad del puerto, mayor será la prioridad media y es más probable que se convierta en el puerto raíz.

Costo de ruta: el protocolo STP se utiliza para seleccionar el valor de referencia del enlace. El protocolo STP puede acortar la red a una estructura de red en forma de árbol sin circuito de bucle mediante el cálculo del costo de la ruta y el bloqueo de enlaces redundantes.

El diagrama de red del concepto básico del árbol de expansión se muestra en la Figura 6-2. Los conmutadores A, B y C están conectados secuencialmente, el conmutador A se selecciona como puente raíz después del cálculo por STP, el circuito entre el puerto 2 y el puerto 6 está bloqueado.

Puente: El conmutador A es el puente raíz de toda la red; El conmutador B es el puente designado del conmutador C. Puerto: el puerto 3 y el puerto 5 son los puertos raíz del conmutador B y el conmutador C, respectivamente; el puerto 1 y el puerto 4 son los puertos designados del conmutador A y del conmutador B, respectivamente; El puerto 6 es el puerto bloqueado del conmutador C.

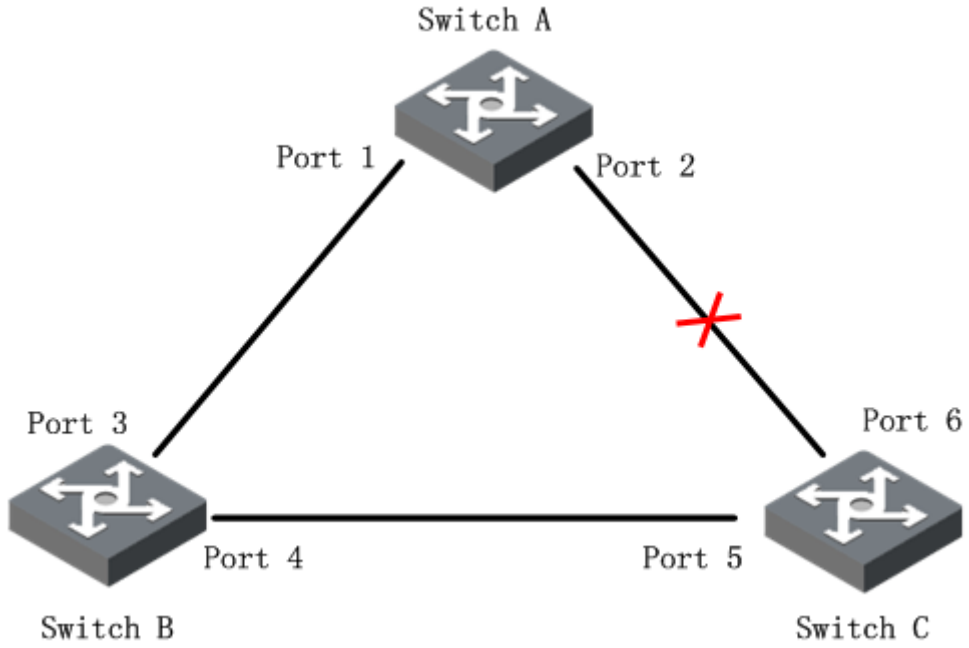


Figura 6-2

Temporizador STP

Hola tiempo

Varía de 1 a 10. Es el intervalo en el que el puente raíz envía el paquete de datos BPDU a todos los conmutadores, que se utiliza para comprobar si hay un mal funcionamiento del enlace de detección del conmutador.

Edad máx.

Varía de 6 a 40 segundos. El conmutador enviará el paquete de datos BPDU a todos los conmutadores y volverá a calcular el árbol de expansión si supera el tiempo de envejecimiento y no recibe el paquete de datos BPDU enviado por Root Bridge.

Retraso de reenvío:

Varía de 4 a 30 segundos. Es el tiempo que se emplea en la transición del estado del puerto del conmutador.

La estructura del árbol de expansión generará el cambio correspondiente cuando se vuelva a calcular el árbol de expansión, lo que se debe a un mal funcionamiento de la red. Sin embargo, el nuevo mensaje de configuración que se ha recalculado no se puede difundir por toda la red inmediatamente, causará un circuito de bucle temporal si el estado del puerto se transfiere inmediatamente. Por lo tanto, el protocolo de árbol de expansión adopta un mecanismo de transición de estado. Pasará por el doble de retraso de transmisión antes del reenvío de datos tanto para el nuevo puerto raíz como para el puerto designado, el retraso garantiza que el nuevo mensaje de configuración se ha extendido por toda la red.

Nota:
En la condición de estado topológico estable, solo el puerto raíz y el puerto designado realizan el reenvío de datos, los otros puertos están en estado de bloqueo, solo reciben paquetes BPDU pero no reenvían datos.

6.1.3 Configuración del puente STP

La interfaz de configuración del puente STP se muestra en la Figura 6-3.

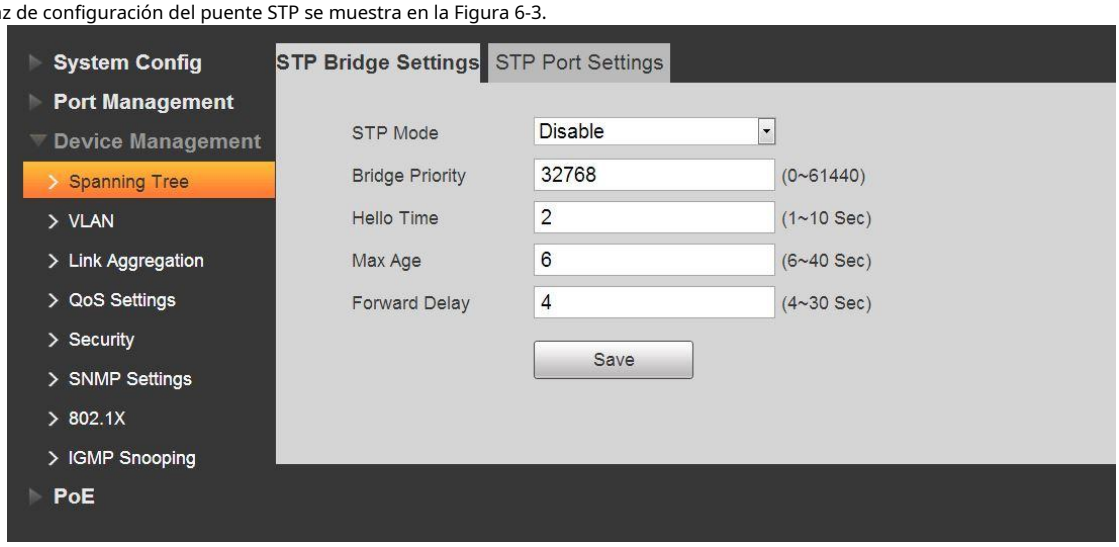


Figura 6-3

- Modo STP: habilita o deshabilita la función de red en anillo. Prioridad del
- puente: establezca la prioridad del puente, varía de 0 a 61440.
- Tiempo de saludo: establezca el período de envío de BPDU de Root Bridge, que varía de 1 a 10 s. Edad
- máxima: establezca el tiempo de envejecimiento de la BPDU actual, varía de 6 a 40 segundos.
- Retraso de reenvío: después de configurar el cambio topológico, el puente mantiene el tiempo de espionaje y el estado de estudio, que varía de 4 a 30 segundos.

6.1.4 Configuración del puerto STP

La interfaz de configuración del puerto STP se muestra en la Figura 6-4.

Figura 6-4

- No de puerto: seleccione el puerto que desea configurar.
- Prioridad: Configure la prioridad del puerto, varía de 0 a 240, tiene que ser el múltiplo integral de 16. RPC:
- Configure el costo de ruta desde el puerto actual al puente raíz, varía de 1-200000000, es el costo de ruta predeterminado cuando se establece en 0.

6.2 Configuración de VLAN

6.2.1 Definición de VLAN

Lógicamente, se trata de dividir una LAN en varios subconjuntos. Cada subconjunto tiene su propia área de transmisión, denominada LAN virtual (VLAN). Una VLAN se divide lógicamente sobre una base organizativa en lugar de una base física, de modo que se da cuenta del área de transmisión aislada en la VLAN.

6.2.2 Función VLAN

1) Mejore el rendimiento de la red. Los paquetes de transmisión están en la VLAN, puede controlar eficazmente la tormenta de transmisión de la red, reducir el ancho de banda de la red y mejorar la capacidad del proceso de la red.
2) Mejore la seguridad de la red. Los dispositivos en diferentes VLAN no pueden acceder entre sí y los hosts en diferentes VLAN no pueden comunicarse entre sí. Necesitan un enrutador o el conmutador de tres capas para reenviar el marco
3) Simplifique la gestión de la red. El anfitrión del mismo grupo de trabajo virtual no está limitado a un área física; simplifica la gestión de la red y es fácil establecer un grupo de trabajo para usuarios en diferentes áreas.

6.2.3 VLAN basada en el puerto

Los marcos del interruptor tienen marco de etiqueta y marco de desetiquetado. Consulte la siguiente figura para conocer la posición de la etiqueta.

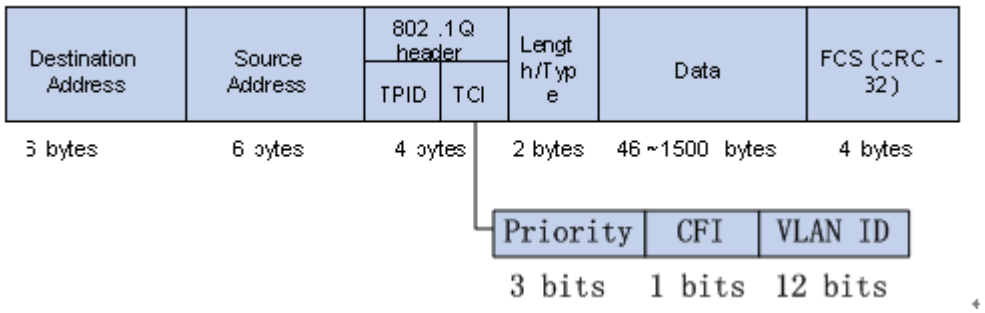


Figura 6-5

Untag es la trama de Ethernet general. El adaptador de red de la PC general puede reconocer el marco y luego comunicarse.

Para el marco de etiqueta, agrega la información de vlan de 4 bytes después de la dirección mac de origen y la dirección de destino. Es el panel azul (la cabeza de la etiqueta vlan) en la figura anterior. Por lo general, el adaptador de red de la PC general no puede reconocer este tipo de trama, el conmutador debe usar la etiqueta vlan para distinguir diferentes VLAN, de modo que las diferentes VLAN no puedan comunicarse entre sí. A veces, necesita comunicarse entre diferentes VLAN. Por lo tanto, existen diferentes tipos de puertos para permitir que las VLAN se comuniquen.

El puerto tiene tres tipos:

- El puerto de tipo de acceso pertenece a una VLAN. Por lo general, se conecta al puerto de la computadora.
- El puerto de tipo troncal permite el paso de varias VLAN y puede recibir o enviar la trama de varias

VLAN. Por lo general, es para los puertos del conmutador.

- El tipo híbrido puede permitir el paso de muchas VLAN y puede recibir o enviar la trama de varias VLAN. Es para conectar los interruptores y para las PC de los usuarios.

Al procesar los datos, el puerto híbrido y el puerto troncal son iguales. La única diferencia es cuando están enviando datos: el puerto híbrido puede enviar la trama de varias VLAN y sin una etiqueta, mientras que el puerto Trunk solo puede enviar la trama de la VLAN predeterminada sin una etiqueta.

Consulte la tabla 6-1 para conocer el tipo de enlace y los métodos de procesamiento de tramas para la VLAN predeterminada.

Puerto Escribe	Para marcos sin etiqueta	Para marcos con etiqueta	Para que los marcos se envíen
Acceso	Reciba la trama y coloque la etiqueta de la VLAN predeterminada.	Cuando la ID de VLAN es la misma que la ID de VLAN predeterminada, reciba marco actual. Cuando la ID de VLAN es diferente de los defecto VLAN IDENTIFICACIÓN, desechar el marco.	Eliminar etiqueta y enviar el marco.
Maletero	Coloque el ID de VLAN predeterminado, cuando el ID de VLAN predeterminado esté en la lista aceptada, reciba el marco y coloque el etiqueta de VLAN predeterminada.	Cuando la ID de VLAN esté en la lista aceptada, reciba la trama. Cuando la ID de VLAN esté en la lista de bloqueados, descarte la trama.	Cuando la ID de VLAN es la misma que la ID de VLAN predeterminada y está en la lista aceptada, quita la etiqueta y envía el marco.
Híbrido	Ponga la ID de VLAN predeterminada, cuando la ID de VLAN predeterminada está en la lista de bloqueados, descarte la trama.		Cuando el ID de VLAN está en la lista aceptada, enviar el marco. Utilice "puerto híbrido sin etiquetar / etiquetado vlan ”para configurar con etiqueta o no al enviar.

Tabla 6-1

Ejemplo de configuración.

1. Conexión de red

PC1 e IPC2 pertenecen a un departamento, PC2 e IPC1 pertenecen a un departamento, puede realizar intercomunicación dentro del departamento, pero no logra realizar la comunicación entre departamentos.

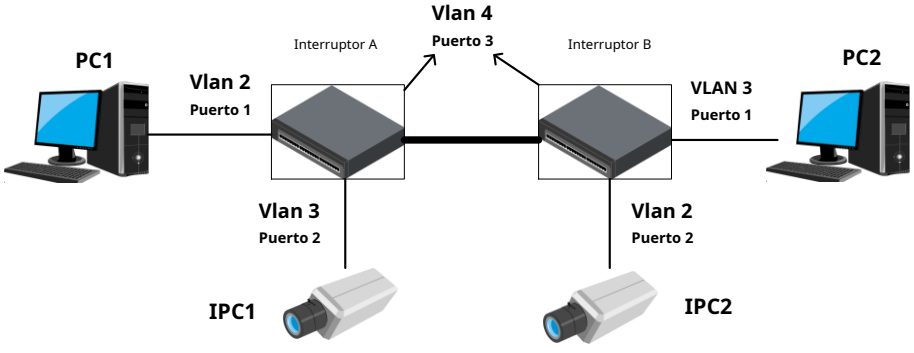


Figura 6-6

2. Conexión de hardware

(1) PC1 se conecta al puerto 1 del conmutador A y pertenece a vlan2，IPC1 se conecta al puerto 2 del conmutador A y pertenece a vlan3；

(2) PC2 se conecta al puerto 1 del conmutador B, y pertenece a vlan3, IPC2 se conecta al puerto 2 del conmutador B y pertenece a vlan2；

(3) El puerto 3 del conmutador A se conecta al puerto 3 del conmutador B y pertenece a vlan4.

3. Configuración

interruptor A：El puerto 1 pertenece a vlan2, configurado como puerto de acceso, el puerto 2 pertenece a vlan3, configurado como puerto de acceso, el puerto 3 configurado como puerto troncal y pertenece a vlan4, y permite que vlan2, 3 y 4 pasen.

Switch B: el puerto 1 pertenece a vlan2, configurado como puerto de acceso, el puerto 2 pertenece a vlan3, configurado como puerto de acceso, el puerto 3 está configurado como puerto troncal y pertenece a vlan4, y permite el paso de vlan2, 3 y 4.

Consulte la Figura 6-7.

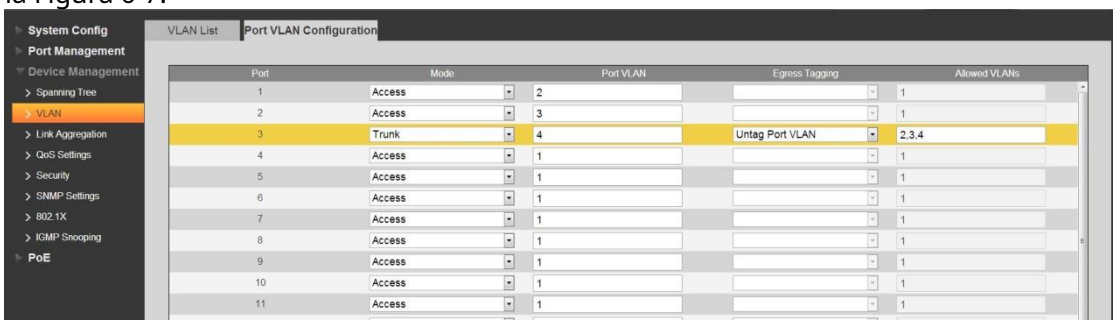


Figura 6-7

6.3 Agregación de enlaces

La agregación de enlaces consiste en formar varios puertos físicos del conmutador en un puerto lógico; varios enlaces que pertenecen al mismo grupo de agregación se pueden considerar como un enlace lógico con mayor ancho de banda.

La agregación de enlaces puede darse cuenta de que se comparte la responsabilidad del flujo de comunicación entre cada puerto miembro del grupo de agregación, que es para aumentar el ancho de banda. Mientras tanto, se puede realizar una copia de seguridad dinámica mutua entre cada puerto miembro en el mismo grupo de agregación, que es para mejorar la confiabilidad del enlace.

Tiene que haber cierta configuración para los puertos miembros que pertenecen al mismo grupo de agregación. Estas configuraciones incluyen STP, QoS, VLAN, propiedades de puerto, estudio de direcciones MAC, duplicación, filtrado de 802.1xy Mac, etc.

Nota:

No se recomienda implementar la configuración del puerto y las funciones avanzadas para los puertos que se utilizan para la agregación de enlaces.

La agregación de enlaces se puede dividir en agregación estática y LACP; por lo general, los dispositivos finales opuestos de la agregación de enlaces de conmutación son tarjetas de red y de conmutación.

6.3.1 Modo de agregación estática

El modo de agregación estática le permite agregar manualmente varios puertos miembros en el grupo de agregación, todos los puertos están en el estado de reenvío y comparten el flujo sobrecargado. Necesita crear un grupo de agregación y agregar puertos miembros a través de la configuración manual sin la participación del paquete de protocolo LACP (Link Aggregation Control Protocol).

- Modo de equilibrio de carga

Existen tres tipos de algoritmo de equilibrio de carga para el puerto, que se muestra en la siguiente tablami.

Modo de equilibrio de carga	Nota
MAC de origen	Cálculo de balance de carga basado en la dirección MAC de origen del paquete
MAC de destino	Cálculo de balance de carga basado en la dirección MAC de destino del paquete.
MAC Src y Dst	Cálculo de balance de carga basado en la dirección MAC de origen y destino del paquete.

Tabla 6-2

- Grupo de agregación

Es un conjunto de un grupo de puertos Ethernet. El número admitido de grupos de agregación es tres de forma predeterminada, que no se puede modificar. El estado predeterminado de todos los grupos de agregación es deshabilitado, el puerto miembro es nulo de manera predeterminada.

- Puerto miembro

El conmutador creó todos los grupos de agregación de forma predeterminada, los miembros del puerto son nulos. Primero debe habilitar el grupo de agregación si desea configurar los puertos miembros para el grupo de agregación y luego hacer clic en el grupo de agregación donde se encuentra el puerto para habilitar la función de agregación.

Consulte la Figura 6-8 para conocer la interfaz de configuración de agregación estática, que incluye el modo de equilibrio de carga, el grupo de agregación y los miembros del puerto.

Figura 6-8

6.3.2 Modo LACP

LACP (Protocolo de control de agregación de enlaces) se utiliza para realizar la convergencia dinámica de enlaces y la separación de convergencia que se basa en el estándar IEEE 802.3ad. Las dos partes de los dispositivos de convergencia hacen converger los enlaces coincidentes y reciben y envían datos a través de la información de convergencia de interacción de paquetes LACPDU. El protocolo puede agregar y eliminar automáticamente puertos en el grupo de convergencia, está equipado con una alta flexibilidad y proporciona la capacidad de equilibrio de carga.

Después de habilitar la función LACP del puerto, el puerto informará al extremo opuesto de la prioridad del sistema, MAC del sistema, número de puerto de prioridad del puerto y clave de operación (se decide por las propiedades físicas, la información del protocolo de capa superior y la clave de administración del puerto) .

El extremo con alta prioridad del dispositivo dominará la convergencia y la separación de convergencia, la prioridad del dispositivo se decide por la prioridad del sistema y el MAC del sistema, el dispositivo con un valor de prioridad del sistema más pequeño tiene una prioridad más alta, el dispositivo con un MAC del sistema más pequeño tiene una prioridad más alta cuando el sistema el valor de prioridad es el mismo. El extremo con mayor prioridad de dispositivo seleccionará el puerto de convergencia de acuerdo con la prioridad del puerto, el número de puerto y la clave de operación, los puertos con la misma clave de operación se pueden seleccionar en el

mismo grupo de convergencia, el puerto con menor valor de prioridad de puerto se seleccionará por prioridad en el mismo grupo de convergencia, el puerto con menor número se seleccionará cuando la prioridad de puerto sea la misma. Los puertos seleccionados convergerán para recibir y enviar datos después de que ambas partes interactúen con la información de convergencia.

El parámetro de configuración del protocolo LACP incluye principalmente la habilitación de la función LACP del puerto, el valor de la clave, la actividad (modo activo / pasivo) y la configuración del tiempo de espera.

Los puertos que solo habilitan el protocolo LACP pueden realizar la negociación LACP y luego pueden formar un enlace de convergencia. La clave secreta es la base de la negociación y los puertos con la misma clave secreta pueden negociar para formar un enlace de convergencia. El modo de negociación incluye "activo / pasivo". El dispositivo lanzará activamente el enlace de convergencia cuando seleccione "activo"; el dispositivo aceptará pasivamente la negociación de convergencia iniciada por otros dispositivos cuando seleccione "pasivo".

Hay al menos uno o dos extremos que deben configurarse como modo "activo" para lograr una negociación exitosa cuando dos dispositivos están interconectados.

- Valor clave: miembros en el mismo grupo de convergencia, necesita configurar la misma clave de operación, varía de 1 a 65535;
- Actividad: puede seleccionar Activo y pasivo por defecto, un extremo del dispositivo que está involucrado en la convergencia dinámica debe seleccionar el modo Activo y el otro extremo debe configurarse con el modo pasivo;
- Tiempo de espera: es un tiempo de espera largo de forma predeterminada, puede seleccionar un tiempo de espera largo y un tiempo de espera corto;

Ejemplo de configuración:

1. Requisito de red

Necesita realizar una copia de seguridad del enlace y un enlace ascendente de enlace de doble GB a través de la función de agregación de enlaces porque hay problemas ocultos en el enlace GN único.

2. Pasos de configuración

(1) Seleccione el grupo de agregación 3, haga clic en los puertos 25 y 26.

(2) Seleccione el modo de agregación de enlaces como LACP, configure Actividad como "Actividad".

(3) Haga clic en "Enviar" para aplicar la configuración.

(4) Seleccione el modo de agregación de enlaces como "MAC Src & Dst" y el resultado de la configuración se muestra en la Figura 6-10, los puertos correspondientes que se agregaron correctamente mostrarán "√".

Figura 6-9

6.4 Configuración de QoS

La calidad de servicio (QoS) refleja la capacidad de una red para satisfacer las necesidades del cliente. En Internet, QoS evalúa la capacidad de la red para reenviar paquetes de diferentes servicios.

La evaluación puede basarse en diferentes criterios porque la red puede proporcionar varios servicios. Generalmente, el rendimiento de QoS se mide con respecto al ancho de banda, el retardo, la fluctuación y la tasa de pérdida de paquetes durante el proceso de reenvío de paquetes.

En la red IP tradicional sin QoS, el dispositivo trata todos los paquetes como iguales y la política de proceso es la primera

primero en entrar (FIFO). Asigna los recursos necesarios según la hora a la que llegó el paquete. Todos los paquetes comparten la red y los recursos del dispositivo, y los recursos que puede obtener un paquete dependen de la hora a la que llega. Este tipo de servicio se denomina Mejor esfuerzo. Utiliza sus máximos esfuerzos para enviar el paquete a su destino, pero no hay garantía ni seguridad sobre el retraso, la fluctuación y la tasa de pérdida de paquetes durante el proceso de reenvío de paquetes.

La política tradicional de servicio Best-Effort es para la WWW, servicio de correo electrónico que no es sensible al ancho de banda ni a la demora. Pero ahora mismo, los nuevos negocios que surgen exigen un alto nivel de servicio de la red IP. El usuario no solo quiere enviar el paquete al destino, también quiere disfrutar de un mejor servicio durante el proceso de reenvío, como hay un ancho de banda de red especial, reducir la tasa de pérdida de paquetes, administrar o evitar la congestión de la red, ajustar los flujos de red. . Todos estos requieren que la red tenga una capacidad de servicio perfecta.

6.4.1 Congestión de la red

En entornos complicados de intercambio y agrupación de Internet, la congestión está en todas partes. Vea la Figura 6-10.

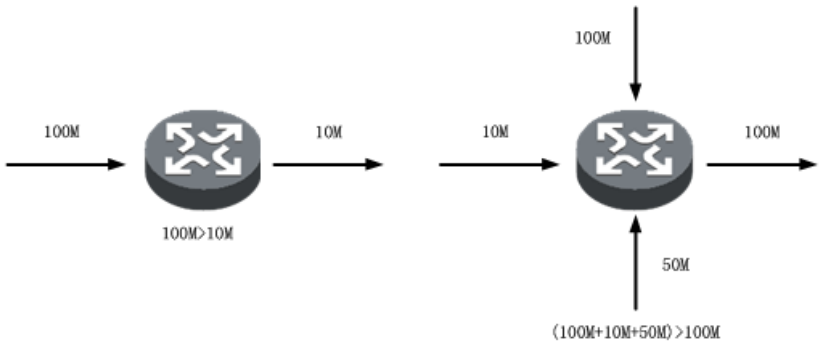


Figura 6-10

1) Las transmisiones grupales provienen del enlace de alta velocidad al dispositivo y se envían a través del enlace de baja velocidad,

2) Los flujos de grupo se conectan al dispositivo de red a través de varios puertos y luego se reenvían a través de un puerto (las velocidades de los puertos de entrada múltiples son mayores que la velocidad del puerto de salida).

Si la velocidad del flujo es demasiado grande, puede encontrar un umbral de recursos y provocar una congestión del flujo. No solo el ancho de banda de enlace tiene la congestión, cualquier recurso insuficiente del lugar de reenvío (como el tiempo de proceso disponible, el búfer, los recursos de memoria no son suficientes) puede resultar en congestión. Además, si el control de flujo está fuera del rango en algún momento y no hay suficientes recursos de red, también puede desencadenar una congestión en la red.

La congestión tiene una serie de efectos negativos:

- La congestión mejora el retardo y la fluctuación de la transmisión del paquete, la alta latencia puede resultar en el envío del paquete nuevamente.
- La congestión ralentiza los flujos entrantes y salientes de la red y reduce la tasa de uso de los recursos de la red.
- La congestión consume una gran cantidad de recursos de red (especialmente recursos de almacenamiento), la asignación incorrecta de recursos puede provocar que el sistema caiga.

Entonces, podemos ver que la congestión evita que los flujos obtengan los recursos a tiempo y es el original

fuente para reducir el rendimiento del servicio. En los entornos complicados donde hay intercambios grupales y negocios de múltiples usuarios, la congestión es inevitable. Así que habrá una forma adecuada de lidiar con la congestión.

6.4.2 Solución de congestión

El método directo para resolver la insuficiencia de recursos es agregar ancho de banda a la red. Pero el ancho de banda tiene su límite, no puede solucionar todos los problemas resultantes de la congestión de la red.

La forma más eficaz de resolver la congestión de la red es agregar la función de control de flujo y asignación de recursos en la red. Puede proporcionar diferentes servicios de acuerdo con los diferentes requisitos comerciales y asignar y utilizar los recursos de manera más razonable. Durante el proceso de asignación de recursos y control de flujo, intente controlar la dirección o los factores indirectos que pueden desencadenar la congestión de la red, que es para reducir la tasa de ocurrencia de la congestión. Cuando ocurre la congestión de la red, puede asignar los recursos según el tipo de negocio y los requisitos para reducir el efecto de la congestión al nivel mínimo.

6.4.3 Programación de colas

Por lo general, adoptamos la programación de colas para resolver la gestión de la congestión. Usar el algoritmo de línea para categorizar los flujos y usar el algoritmo de prioridad para enviar este tipo de flujos primero. Cada algoritmo de cola es para solucionar los problemas pendientes de flujo de la red; Tiene un gran efecto en la asignación de recursos de ancho de banda, el retraso, la fluctuación, etc.

Este producto de serie admite dos colas de prioridad: cola de alta prioridad y cola de baja prioridad. La prioridad de cada paquete se establece de acuerdo con los siguientes cuatro planes.

1. El puerto físico.
2. Etiqueta VLAN 802.1Q.
3. Cadena TOS / DS del paquete IP.
4. Puerto TCP / UDP.

Cuando hay varias configuraciones de QoS, una vez que un elemento de configuración de prioridad se convierte en la prioridad alta, el elemento se colocará en la línea de alta prioridad y luego se reenviará. Cuando hay varias prioridades altas, para el mismo nivel, adopta First In First Out (FIFO).

6.4.4 Modo de prioridad

Cada paquete recibido se asigna a una prioridad alta o baja. La configuración de la prioridad de paquetes tiene tres modos. Vea la Figura 6-11.

Figura 6-11

Referirse a Tabla 6-3 para prioriinformación del modo ty.

Nombre	Nota
Primero en llegar y primero en salir	El primer paquete recibido se reenviará primero. Cuando QoS

(FIFO)	La función está deshabilitada, el dispositivo adopta el modo FIFO para procesar los paquetes.
Todo alto antes bajo	El dispositivo reenvía los paquetes de acuerdo con el nivel de prioridad especificado.
Peso ronda Robin	Configure el nivel de peso para cambiar el porcentaje de reenvío de paquetes en prioridad alta y prioridad baja.

Tabla 6-3

6.4.5 QoS basada en el puerto / 802. 1p / DSCP

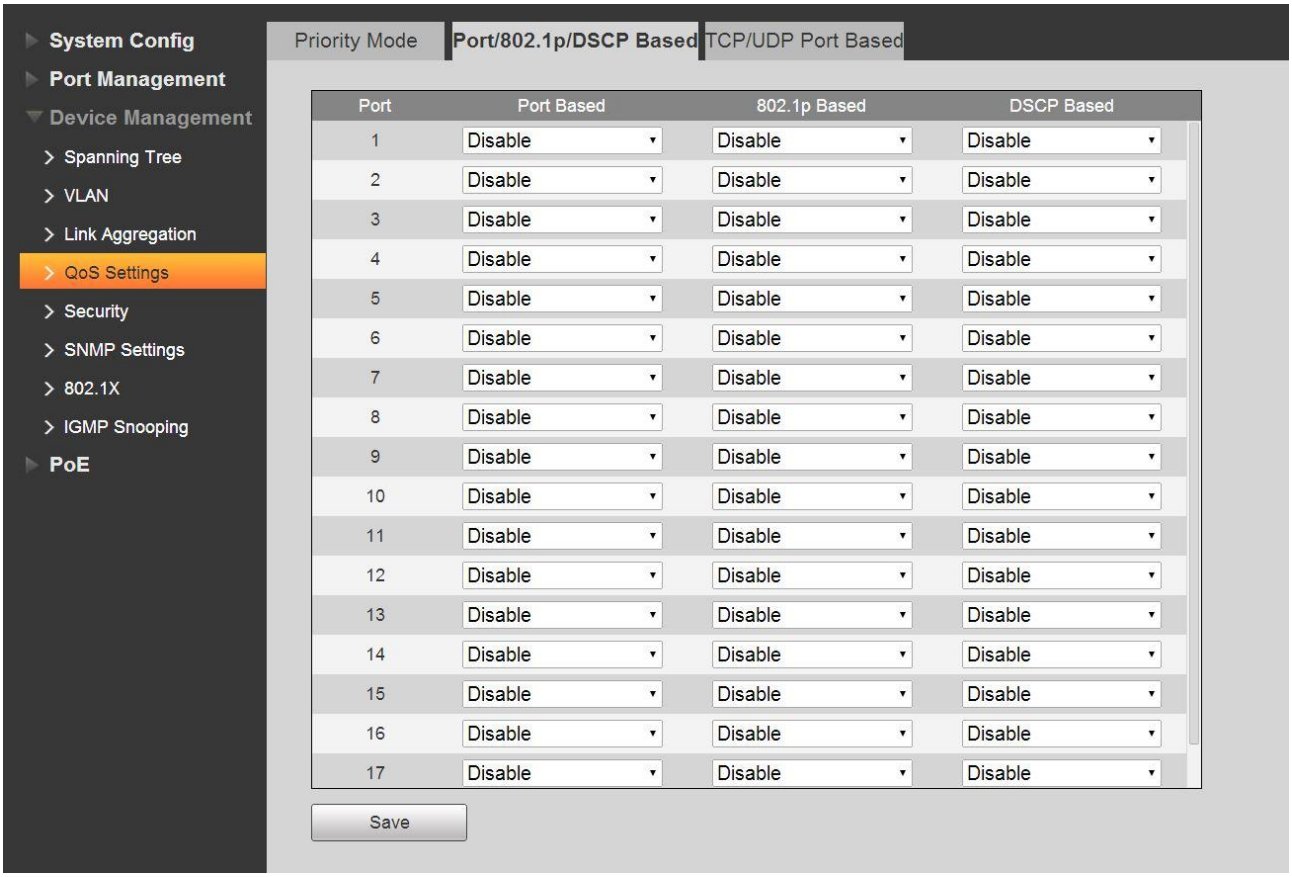


Figura 6-12

Basado en puerto

Cuando un puerto se establece como de alta prioridad, los paquetes recibidos se colocan en la cola de alta prioridad. Cada puerto puede establecerse como de alta prioridad.

Basado en 802.1p

La prioridad 802.1p está en el encabezado del paquete de 2 capas. Es para el entorno donde no hay necesidad de analizar el 3er cabezal y garantizará la QoS en el 2-layer.

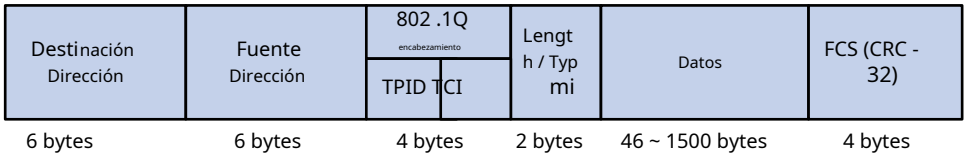


Figura 6-13

En la Figura 6-14, el cabezal de etiqueta 802.1Q de cuatro bytes incluye TPID de 2 bytes（Identificador de protocolo de etiqueta）y 2 bytes

TCI（Información de control de etiquetas）. El valor de TPID es 0x8100. En la Figura 6-9, muestra el contenido detallado del cabezal de etiqueta del 802.1Q, la cadena de prioridad es la prioridad 802.1p. La prioridad se llama 802.1p ya que la prioridad se define en las especificaciones 802.1p.

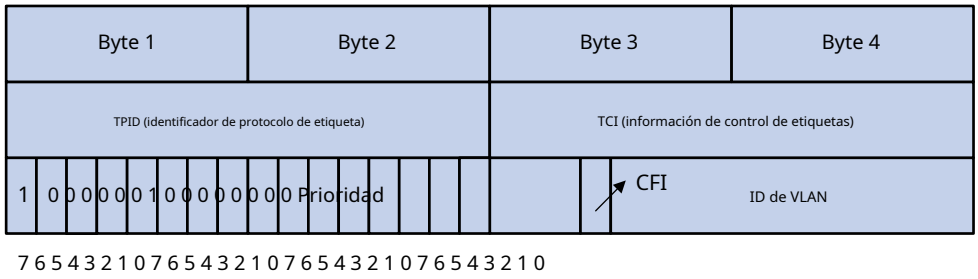


Figura 6-14

Consulte la Tabla 6-4 para conocer la prioridad de 802.1p.

Prioridad Cola	Prioridad 802.1p（Sistema decimal）	Prioridad 802.1p（Sistema binario）	Palabras clave
Baja prioridad cola	0	000	mejor esfuerzo
	1	001	antecedentes
	2	010	repuesto
	3	011	excelente esfuerzo
Alta prioridad cola	4	100	carga controlada
	5	101	video
	6	110	voz
	7	111	administrar la red ment

Tabla 6-4

Basado en la cadena TOS / DS del paquete IP

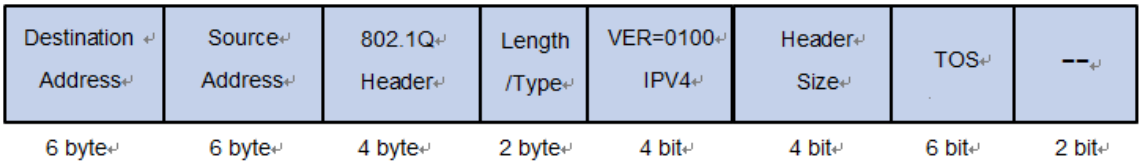


Figura 6-15

En la Figura 6-10, la cadena ToS del encabezado del paquete IP tiene 8 bits, RFC2474 redefine el dominio ToS del encabezado del paquete IP y se denomina (Servicios diferenciados). La prioridad DSCP utiliza los primeros 6 bits (0-5). El valor varía de 0 a 63 y los últimos 2 bits (6, 7) son el bit reservado.

Consulte la Tabla 6-5 para obtener información sobre la prioridad de IP.

Prioridad Cola	Prioridad de IP （Sistema decimal）	Prioridad de IP （Sistema binario）	Palabras clave
Alta prioridad l cola	46	101110	ef
	10	001010	af11
	18	010010	af21
	26	011010	af31
	34	100010	af41
	48	110000	cs6
	56	111000	cs7
Baja prioridad	Otros	xxxxxx	

cola			

Tabla 6-5

6.4.6 Puerto TCP / UDP

TCP y UDP adoptan un puerto de 16 bits para reconocer las aplicaciones. El servidor suele utilizar el puerto para reconocer. Por ejemplo, el puerto TCP del servidor FTP es el 21, el puerto TCP de cada servidor Telnet es el 23, el puerto UDP de cada servidor TFTP es el 69. Todos los servicios TCP / IP utilizan el conocido puerto 1-1023.

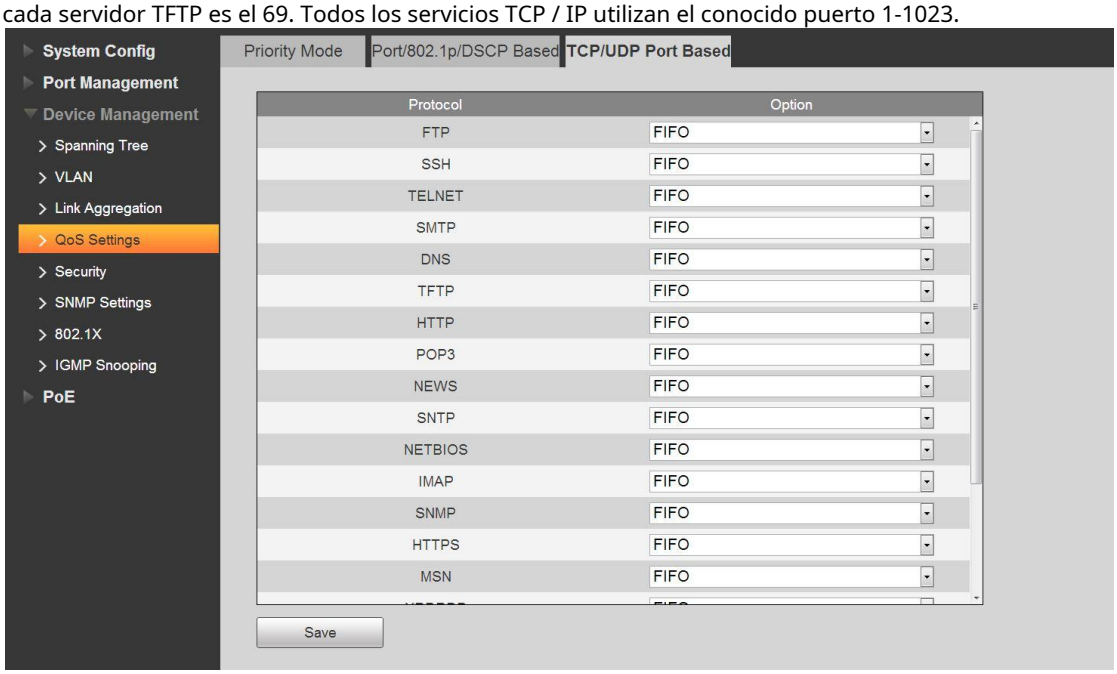


Figura 6-16

En la Figura 6-11, este producto de la serie puede procesar los paquetes recibidos según el puerto TCP / UDP, como FTP, SSH, TELNET, SMTP y DNS. Aquí se establece el paquete de alta prioridad, baja prioridad o descartar. La configuración predeterminada es FIFO.

Ejemplo de configuración.

1. Conexión de red

- En la Figura 6-12, conecte el dispositivo con el servidor FTP y use el puerto 1 y el puerto 2 para conectar el dispositivo.
- Con la función QoS configurada correctamente, el puerto 2 tiene mayor prioridad que el puerto 1 y está bloqueado para acceder al servidor FTP.

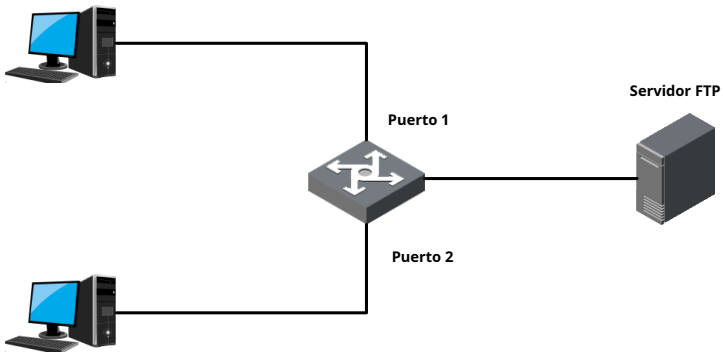


Figura 6-17

2. Configuración

(1) Configure el modo del dispositivo en modo todo alto antes que bajo

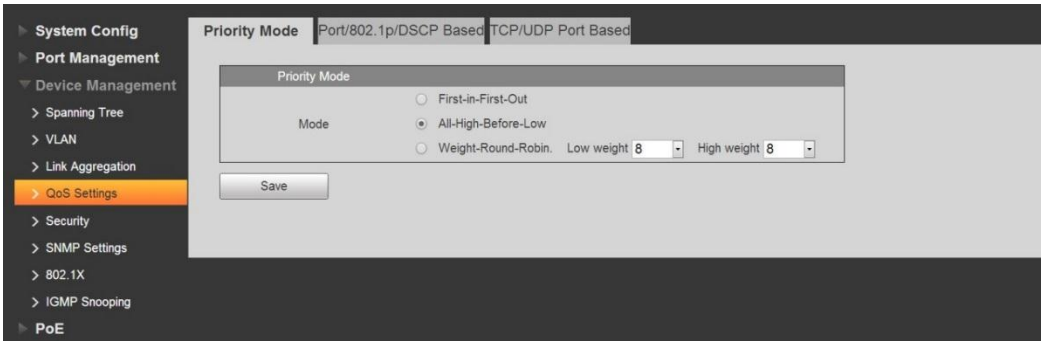


Figura 6-18

(2) Establezca el puerto 2 como de alta prioridad.

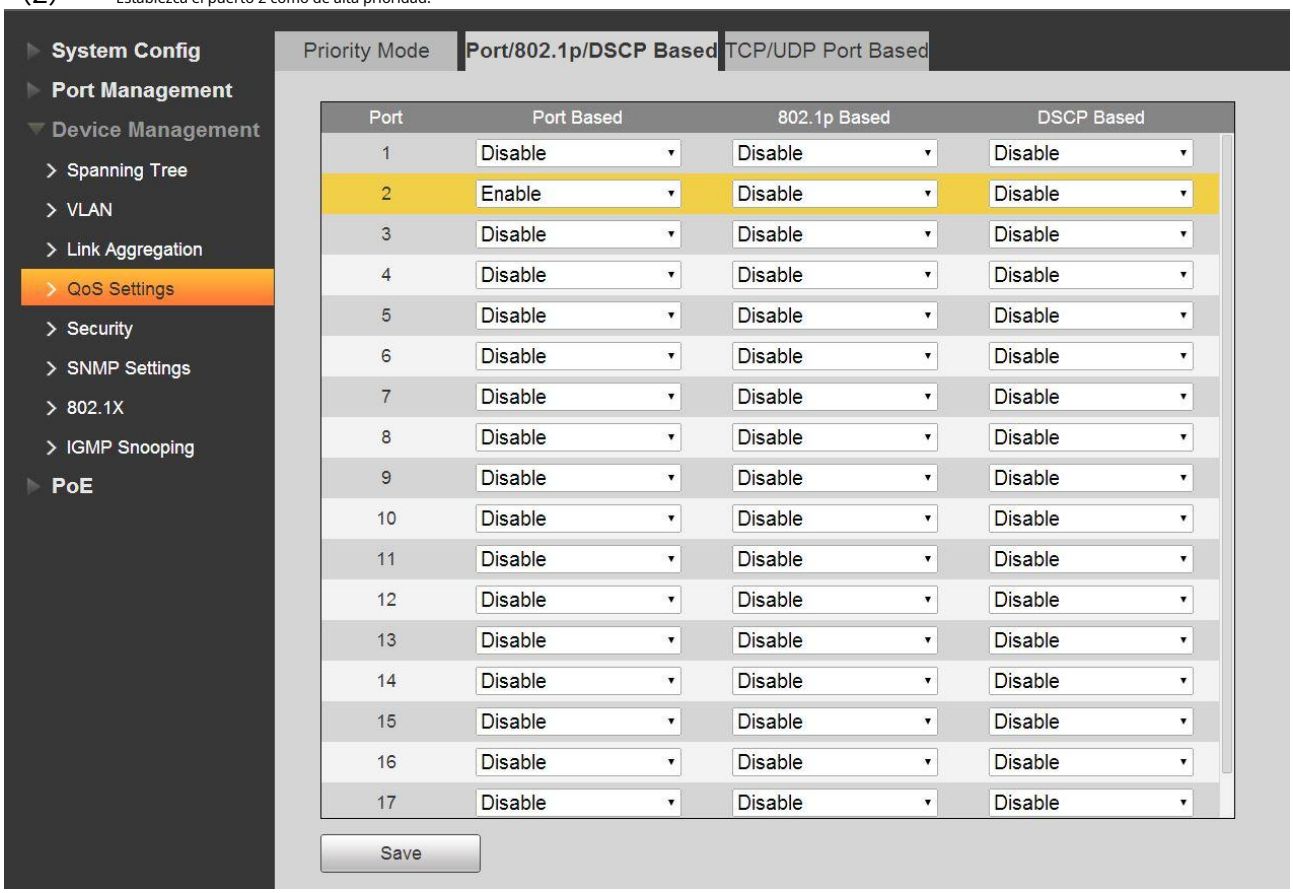


Figura 6-19

(3) Configure el dispositivo para que descarte el paquete de datos FTP, bloquee al usuario para que acceda al servidor FTP.

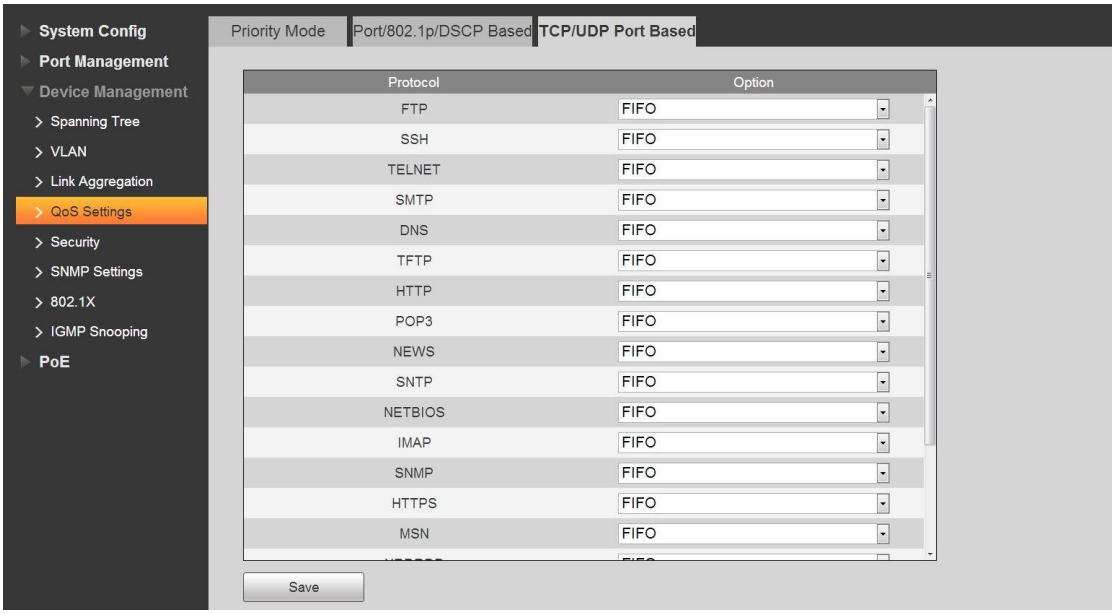


Figura 6-20

6.5 Seguridad

MAC (Media Access Control) registra la relación entre la dirección MAC y el puerto, y la información de VLAN del puerto que pertenece, etc.

6.5.1 Lista de direcciones MAC

Cuando el dispositivo reenvía el paquete, busca en la hoja de direcciones MAC de acuerdo con la dirección MAC de destino del paquete. Si la lista de direcciones MAC incluye un elemento que coincide con la dirección MAC de destino del paquete, utiliza el puerto de salida para reenviar el paquete. Si la dirección MAC no tiene ningún elemento que coincida con la dirección MAC de destino del paquete, el dispositivo adopta el modo de transmisión para reenviar el paquete a través de la VLAN correspondiente (excepto el puerto de entrada).

Consulte la siguiente figura para obtener información sobre la dirección MAC.

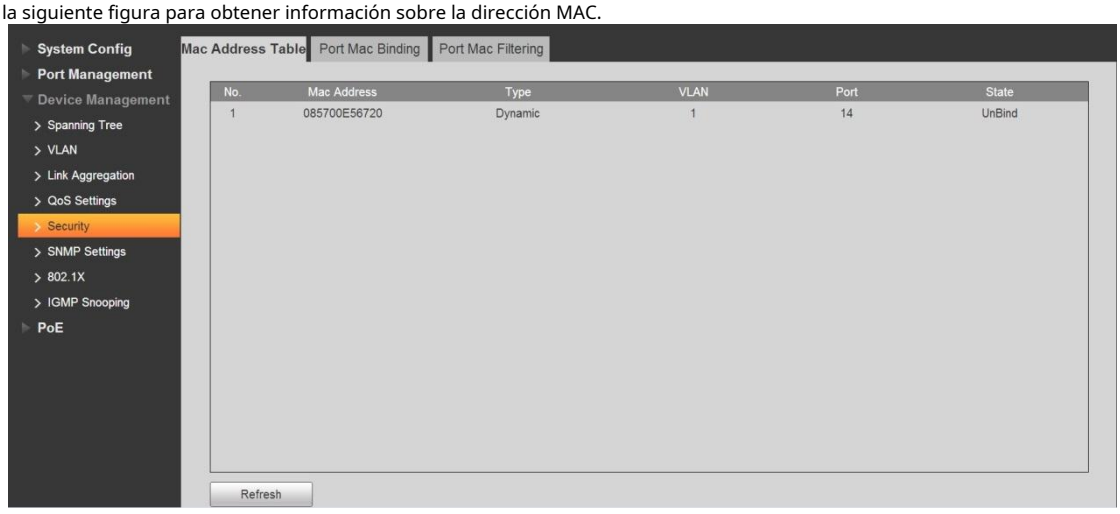


Figura 6-21

6.5.2 Enlace MAC de puerto

En la Figura 6-22, haga clic en el puerto conectado actual, configure la función de enlace MAC del puerto para que solo el puerto actual

reenviar la dirección MAC vinculante.

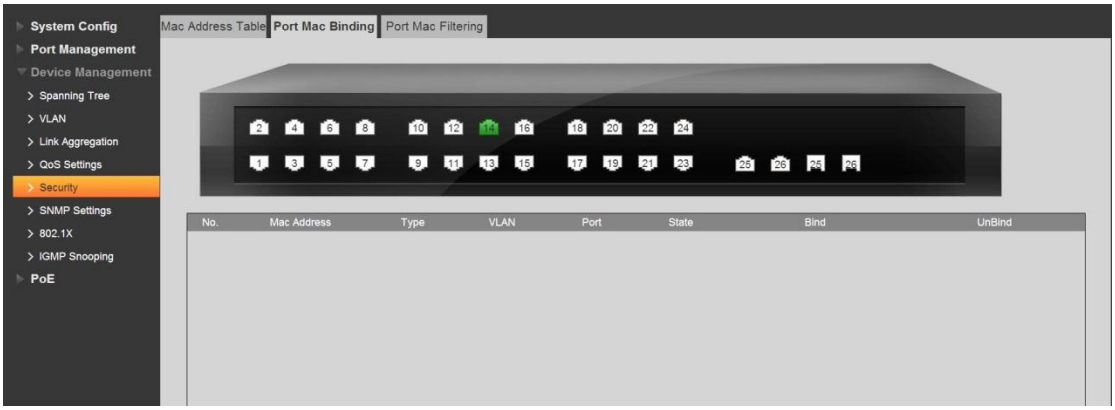


Figura 6-22

Ejemplo de configuración.

1. Conexión de red

El usuario usa WEB para configurar el enlace MAC del puerto de modo que el puerto solo pueda ser usado por el dispositivo actual. 2. Configuración

(1) De **Gestión de dispositivos**>**Seguridad**, ir a **Tabla de direcciones MAC** interfaz.

(2) Seleccione**Enlace de puerto MAC** interfaz.

(3) Seleccione el puerto cuyo estado de conexión es verde y luego haga clic en el botón Vincular. Vea la Figura 6-23.

Figura 6-23

6.5.3 Filtrado de puertos Mac

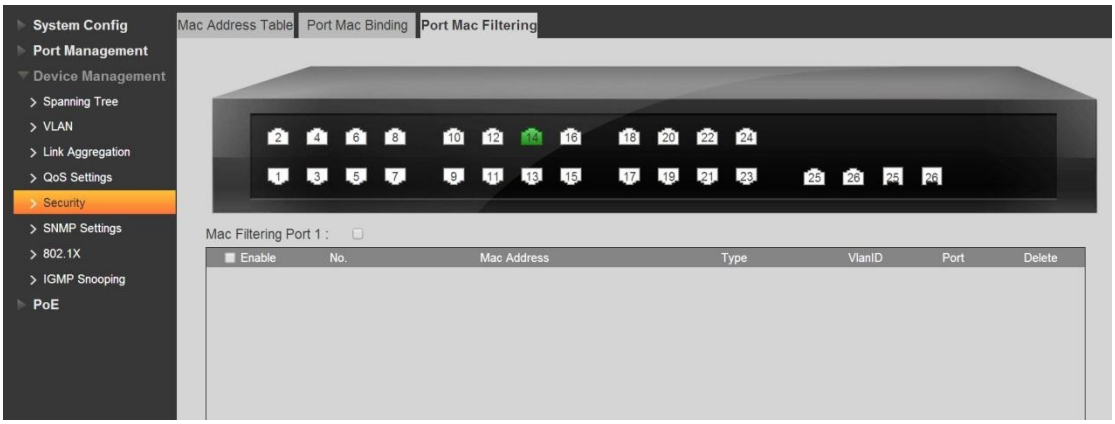


Figura 6-24

Como se muestra en la Figura 6-24, la función se utiliza para restringir los paquetes MAC permitidos en el puerto, lo que puede evitar un ataque de falsificaciones. Una vez que el puerto está configurado con la función, cuando el puerto recibe el paquete, verificará si la dirección MAC de origen del paquete es la misma que la dirección MAC permitida:

- Si es el mismo, entonces el paquete se considera legal y continuará implementando el procesamiento de seguimiento;
- Si es diferente, el paquete se considera ilegal y se descartará.

6.6 Configuración SNMP

La red SNMP incluye dos elementos: NMS y Agente.

- NMS（Sistema de gestión de red）es el administrador de la red SNMP. Proporciona una interfaz interactiva fácil de usar. Es adecuado para que el administrador de la red complete la mayor parte del trabajo de administración.

- El agente es el objeto a gestionar en la red SNMP. Es recibir, procesar el mensaje de consulta NMS. En alguna situación urgente, como que el estado del puerto haya cambiado, el agente puede enviar automáticamente la información de alarma al NMS.

Cuando NMS administra el dispositivo, presta gran atención a algunos parámetros, como el estado del puerto, la tasa de uso de la CPU, etc. Todos estos parámetros juntos se denominan Base de información de administración (MIB). Estos parámetros se denominan nodos en la MIB. MIB define las capas de estos nodos y las propiedades de estos objetos, como el nombre del objeto, los derechos de acceso, el tipo de datos, etc. Cada agente tiene su propia MIB. Todos los dispositivos administrados tienen su propio archivo MIB y la compilación de estos archivos MIB en el NMS puede generar la MIB de cada dispositivo. El NMS lee y escribe los nodos de la MIB de acuerdo con la configuración de los derechos de acceso para que pueda administrar el Agente. Consulte la siguiente figura para ver la relación entre NMS, Agent y MIB.

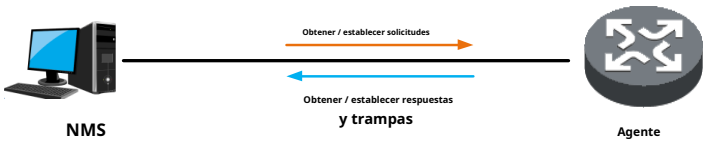


Figura 6-25

MIB adopta la organización de árbol, consta de muchos nodos. Cada nodo representa un objeto gestionado. El objeto gestionado puede utilizar un número único que represente la ruta que comienza desde la raíz. Este número se llama Identificador de objeto (OID). Consulte la siguiente figura para obtener información detallada. El objeto gestionado B puede utilizar un número de serie {1.2.1.1} para identificar. Este es el OID del objeto gestionado.

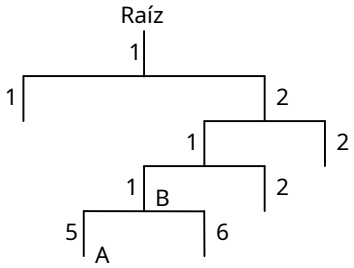


Figura 6-26

SNMP proporciona tres operaciones básicas para realizar la interacción entre el NMS y el Agente:

- Get: NMS lo usa para buscar el valor de uno o más nodos del Agent MIB. Establecer: NMS
- lo usa para establecer el valor de uno o más nodos de la MIB del agente.
- Trap: NMS lo usa para enviar información de Trap al NMS. El agente no requiere que el NMS envíe el mensaje de respuesta y el NMS no responde la información de la trampa. SNMPv1, SNMPv2 y SNMPv3 admiten la operación Trap.

Versión del protocolo SNMP

En este momento, el agente es compatible con SNMPv1, SNMPv2 y SNMPv3.

- SNMPv1 adopta el nombre de la comunidad para certificar. El nombre de la comunidad es como una contraseña, es para restringir la comunicación entre el NMS y el Agente. Si el nombre de la comunidad NMS y el nombre de la comunidad del dispositivo administrado no son el mismo, el NMS y el Agente no pueden establecer la conexión SNMP, lo que significa que el NMS no puede acceder al Agente y el NMS descarta el

información de advertencia del Agente.

- SNMPv2 adopta el nombre de la comunidad para certificar. SNMPv2c ha ampliado las funciones de SNMPv1. Proporciona más tipos de operaciones y admite más tipos de datos, proporciona abundantes códigos de error y puede distinguir los errores con precisión.
- SNMPv3 adopta el modelo de seguridad basado en el usuario (USM) para certificar. El administrador de la red puede configurar la función de autenticación y encriptación. La autenticación es para verificar la validez del remitente del mensaje para evitar el acceso ilegal. El cifrado sirve para cifrar los mensajes de comunicación entre el NMS y el Agente en caso de que se escuche a escondidas. La función de autenticación y encriptación puede mejorar el nivel de seguridad entre el NMS y el Agente.

Nota: Asegúrese de que el NMS y el agente estén usando la misma versión de SNMP; de lo contrario, la conexión del NMS y el agente puede fallar.

6.6.1 SNMP

Esta interfaz sirve para configurar el SNMP. V1 y V2 incluyen las siguientes configuraciones.

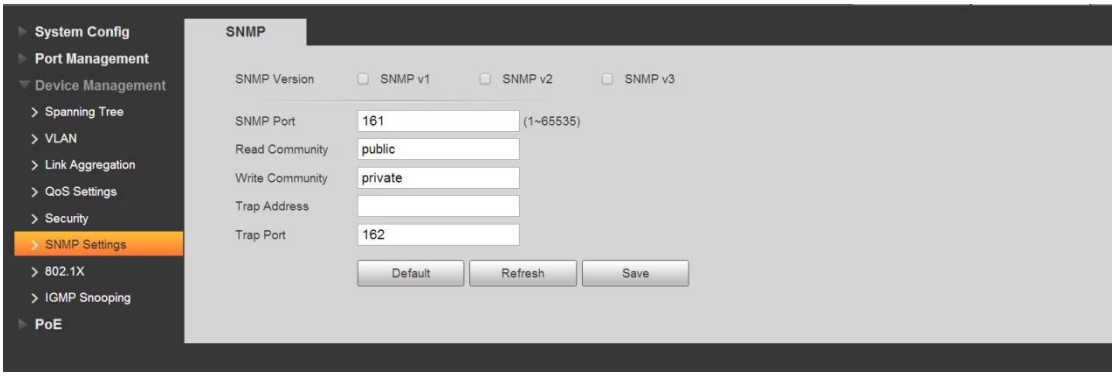


Figura 6-27

En la Figura 6-21, la interfaz de configuración SNMP V1 y V2 incluye el puerto SNMP, la versión, la comunidad de lectura, la comunidad de escritura, la dirección de captura y el puerto de captura.

La Figura 6-28 es la interfaz de configuración de SNMP V3.

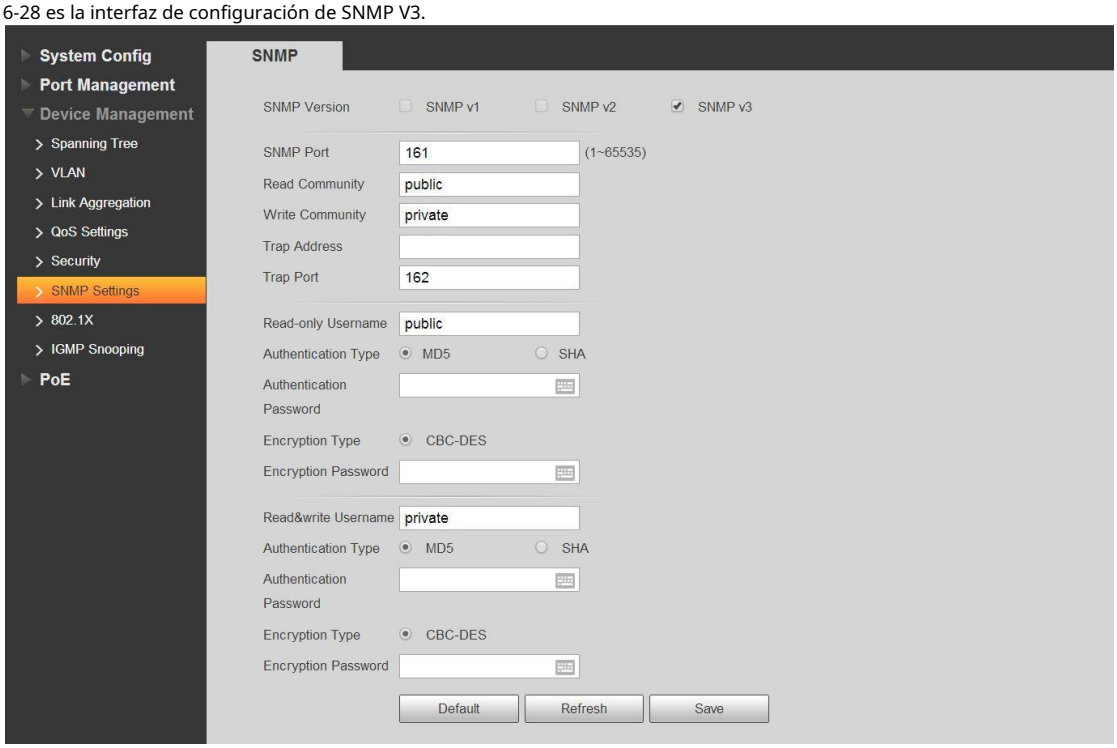


Figura 6-28

Referirse a Tabla 6-6 para dinformación detallada.

Nombre	Nota
Leer comunidad	El nombre de la comunidad para acceder al administrador de la red. Se lee la derecha. La configuración predeterminada es pública.
Escribir comunidad	El nombre de la comunidad para acceder al administrador de la red. El derecho es escribir. La configuración predeterminada es privada.
Dirección de trampa	Sirve para especificar la dirección IP del servidor.
Puerto de trampa	Sirve para configurar el puerto de destino de la trampa.
Solo lectura nombre de usuario	Establezca el nombre de usuario de solo lectura. Es solo para V3.
Autenticación modo n	Sirve para configurar el modo de autenticación cuando el nivel de seguridad es "Autenticación sin cifrado" o "Autenticación y cifrado". El modo de autenticación incluye MDS y SHA.
Autenticación n contraseña	Sirve para configurar la contraseña de autenticación.
Cifrado modo	Cuando el modo de autenticación es "autenticación y cifrado", es para configurar el modo de cifrado. Este producto de la serie solo es compatible con 3DES.
Cifrado contraseña	Cuando el modo de autenticación es "autenticación y cifrado", es para establecer la contraseña de cifrado.
Leer escribir contraseña	Sirve para configurar el usuario de lectura / escritura.

Tabla 6-6

Ejemplo de configuración.

SNMPv1 / v2

1. Conexión de red

Consulte la Figura 6-23, el NMS se conecta con el conmutador y cumplirá los siguientes requisitos. NMS monitorea y administra el Switch a través de SNMPv1 y SNMPv2c.

El interruptor puede enviar automáticamente un mensaje de trampa al NMS cuando hay un mal funcionamiento.

Figura 6-23

2. Configuración

1) En la barra de navegación, desde **Dispositivo**> **Configuración de SNMP**, el sistema va a la interfaz SNMPv1 de forma predeterminada.

2) Seleccione la versión de SNMP como v1 o v2.

3) El número de puerto SNMP es 161, configure “Comunidad de lectura”, “Comunidad de escritura”, “Dirección de captura” y “Puerto de captura”. Vea la Figura 6-29.

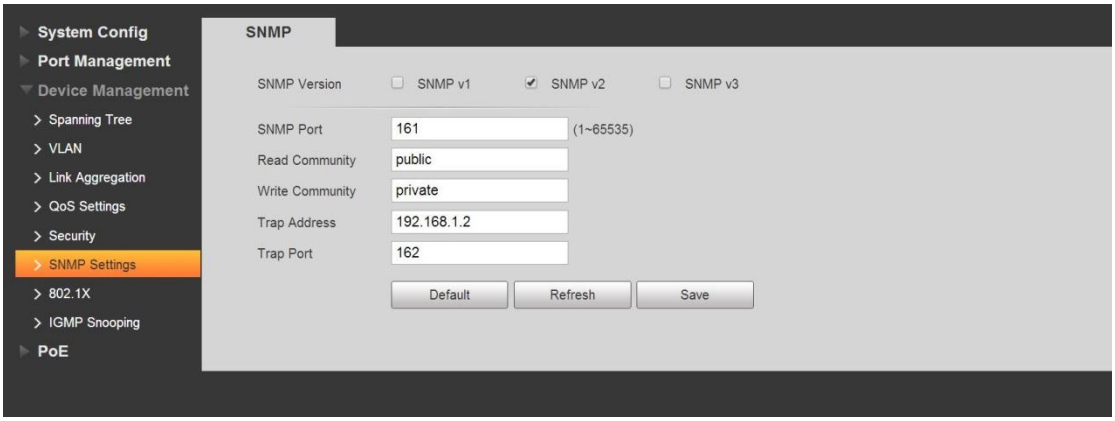


Figura 6-29

SNMPv3

1. Conexión de red

Consulte la Figura 6-31, el NMS se conecta con el conmutador y cumplirá los siguientes requisitos.

- NMS monitorea y administra el Switch a través de SNMPv3.
- El interruptor puede enviar automáticamente un mensaje de trampa al NMS cuando hay un mal funcionamiento.
- Cuando NMS conecta el Agente a través de SNMP, requiere autenticación. El modo de autenticación es MD5, la contraseña de autenticación es admin123.
- El mensaje SNMP entre el NMS y el Agente se cifrará, el modo de cifrado es DES56 y la contraseña de cifrado es admin123.

Figura 6-31

2. Configuración

(1) En la barra de navegación, desde **Dispositivo**>**Configuración de SNMP**, el sistema va a la interfaz SNMPv1 de forma predeterminada.

(2) Seleccione la versión de SNMP como v3.

(3) El número de puerto SNMP es 161, configure "Comunidad de lectura", "Comunidad de escritura", "Dirección de captura" y "Puerto trampa". El puerto de la trampa es 162.

(4) Ingrese el nombre de usuario de solo lectura como

(5) "usuario". El modo de autenticación es MD5.

(6) La contraseña de autenticación es

(7) "admin123". El modo de cifrado es "CBC-DES"

(8) La contraseña de cifrado y la contraseña de confirmación es "admin123". Introduzca el nombre

(9) de usuario de lectura / escritura como "usuario1".

(10) El modo de autenticación es "MD5". La

(11) contraseña de cifrado es "admin123". El

(12) modo de cifrado es "CBC-DES". La

(13) contraseña de cifrado es "admin123". Haga

(14) clic en el botón Guardar. Vea la Figura 6-32.

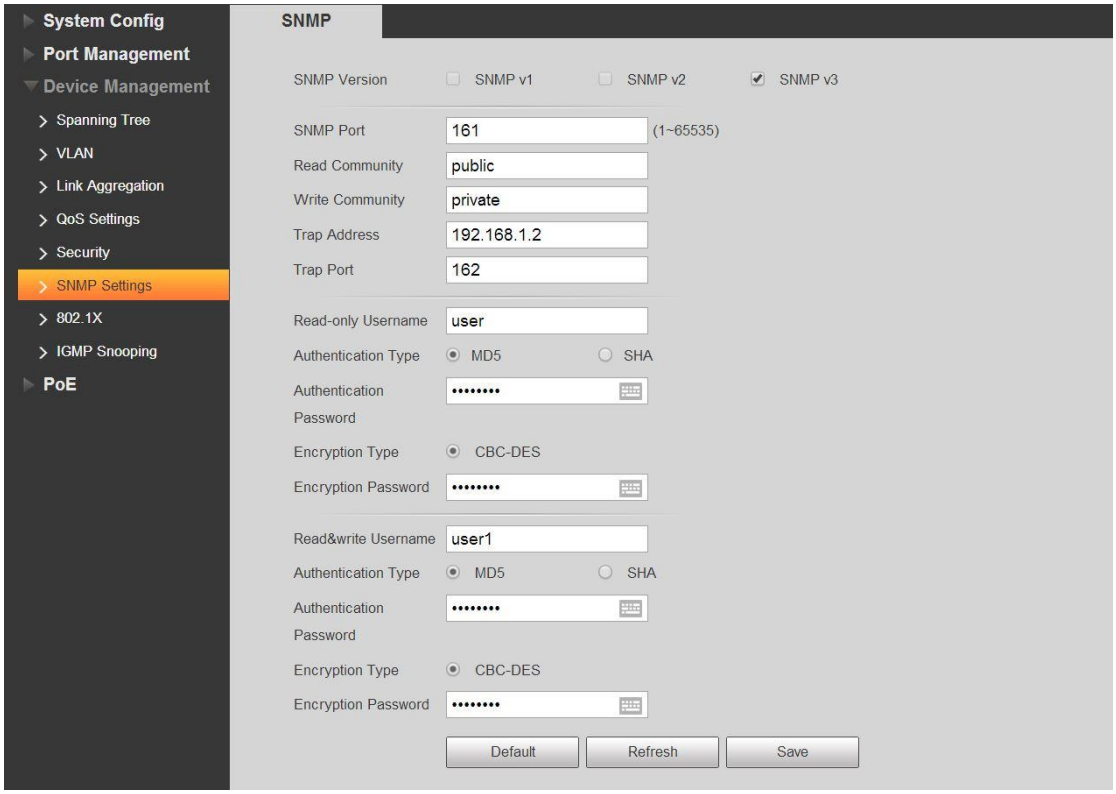


Figura 6-32

6,7 802.1x

IEEE 802.1x es el estándar de autenticación sobre el acceso a la red del usuario designado por IEEE, es un tipo de protocolo de control de acceso a la red basado en el puerto, por lo tanto, la función de autenticación 802.1x exacta debe configurarse en el puerto del dispositivo. En cuanto al dispositivo de usuario al que se accede al puerto, se debe controlar el acceso a la fuente de red mediante autenticación.

6.7.1 Estructura de red 802.1x

El sistema 802.1x incluye tres partes que son Cliente, Dispositivo y Servidor de autenticación, que se muestra en la Figura 6-33.

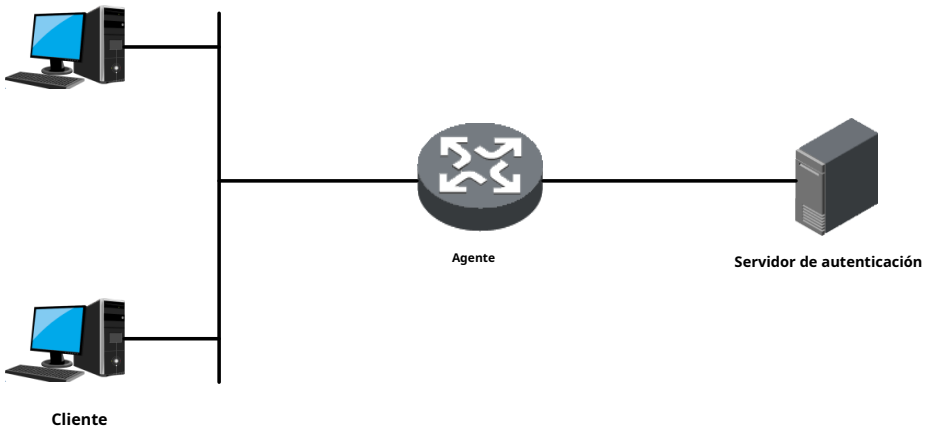


Figura 6-33

- El cliente es el dispositivo terminal de usuario que requiere acceso a la LAN, que es autenticado por el

extremo del dispositivo en la LAN. El cliente debe instalar un software de cliente que admita la
- autenticación 802.1x. El extremo del dispositivo es el dispositivo de red que controla el acceso del cliente en la LAN, está ubicado entre el cliente y el servidor de autenticación, que proporciona un puerto de acceso LAN para los clientes (puerto físico o puerto lógico) e implementa la
- autenticación en el cliente conectado a través de la interacción con el servidor. . El servidor de autenticación se utiliza para implementar autenticación, autorización y facturación, generalmente es un servidor RADIUS (Servicio de usuario de acceso telefónico de autenticación remota). El servidor de autenticación puede verificar la legalidad del cliente de acuerdo con la información de autenticación del cliente enviada por el extremo del dispositivo e informar al dispositivo de los resultados de la verificación; el extremo del dispositivo decide si permite el acceso del cliente o no.

6.7.2 Puerto controlado / no controlado de autenticación 802.1x

Los puertos de acceso LAN proporcionados por el dispositivo para el cliente se pueden dividir en dos puertos lógicos que son el puerto controlado y el puerto no controlado. Cualquier trama que llegue al puerto se puede mostrar tanto en el puerto controlado como en el puerto no controlado.

- El puerto no controlado está siempre en estado de conexión bidireccional, que se utiliza principalmente para transmitir paquetes de autenticación y asegurarse de que el cliente siempre pueda enviar o recibir paquetes de autenticación.
- El puerto controlado siempre está en el estado de conexión bidireccional bajo el estado de autorización, que se utiliza para transmitir paquetes comerciales; Está prohibido recibir cualquier paquete del cliente cuando se encuentra en estado no autorizado.

6.7.3 Modo de activación de la autenticación 802.1x

El proceso de autenticación de 802.1x es iniciado activamente por el cliente, también puede ser iniciado por el dispositivo. 1. Modo de activación activa del cliente

- Activador de multidifusión: el cliente envía activamente el paquete de solicitud de autenticación al dispositivo para activar la autenticación, la dirección de destino del paquete es la dirección MAC de multidifusión 01-80-C2-00-00-03.
- Activador de transmisión: el cliente envía activamente el paquete de solicitud de autenticación al dispositivo para activar la autenticación, la dirección de destino del paquete es la dirección MAC de transmisión. El modo puede resolver el problema de que el dispositivo no recibe la solicitud de autenticación del cliente porque algunos dispositivos no admiten el paquete de multidifusión anterior en la red.

2. Modo de disparo activo del dispositivo

El modo de activación activa del dispositivo se utiliza para ayudar al cliente que no puede enviar paquetes de solicitud de autenticación de forma activa, hay dos tipos de autenticación activa de activación del dispositivo:

- Activador de multidifusión: el dispositivo envía de forma activa un paquete de solicitud de tipo de identidad para activar la autenticación al cliente a intervalos regulares (es 30 segundos por defecto).
- Disparador de unidifusión: cuando el dispositivo recibe un paquete desconocido de la dirección MAC de origen, enviará activamente un paquete de solicitud con tipo de identidad a la dirección MAC unidifusión para activar la autenticación. Enviará el paquete nuevamente si el dispositivo no recibe la respuesta del cliente dentro del tiempo establecido.

6.7.4 Estado autorizado del puerto

Puede controlar si los usuarios accedidos al puerto necesitan visitar la fuente de la red a través de la autenticación configurando el estado autorizado para el puerto. El puerto admite los siguientes tres estados autorizados:

- Fuerza autorizada: Significa que el puerto siempre está en el estado autorizado, lo que permite a los usuarios visitar la fuente de la red sin autenticación.
- Fuerza no autorizada: significa que el puerto siempre está en estado no autorizado, lo que no permite la autenticación de los usuarios. El dispositivo no proporcionará un servicio de autenticación para el cliente al que se accede al puerto.
- 802.1x basado en puerto: significa que el estado inicial del puerto es un estado no autorizado, lo que no permite a los usuarios visitar la fuente de la red; El puerto cambiará al estado autorizado si los usuarios pasan

autenticación, y los usuarios visitarán la fuente de red.

Ejemplo de configuración:

1. Requisito de red

La IP del cliente es el segmento 192.168.1.1/24, la IP del servidor de autenticación es 192.168.1.100 y el servidor de autenticación debe autenticarla cuando se accede a todos los puertos del dispositivo.

2. Pasos de configuración

(1) Habilite la función de autenticación, todos los puertos están habilitados según la autenticación 802.1x, que se muestra en la Figura 6-34.

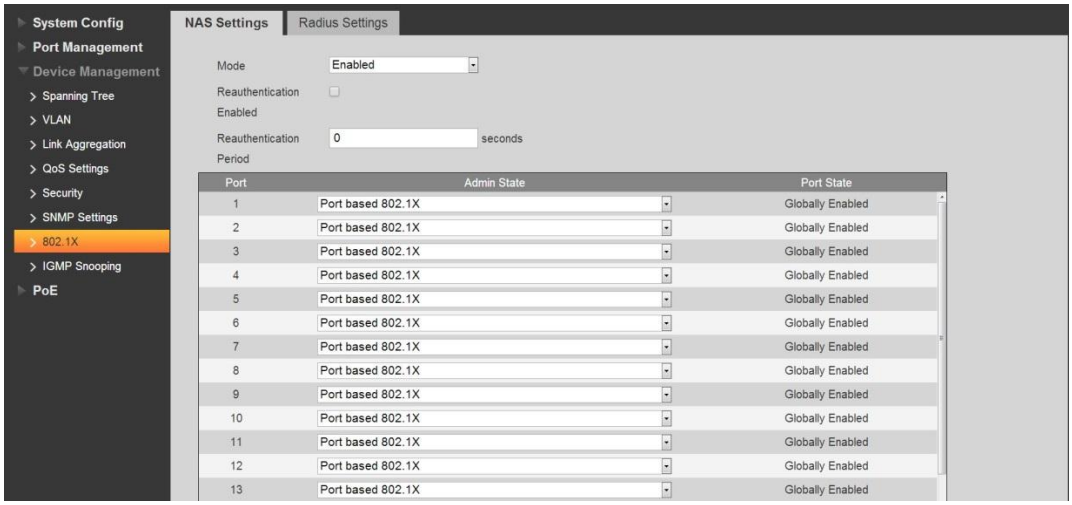


Figura 6-34

(2) Configure la dirección del servidor de autenticación, que se muestra en la Figura 6-35.

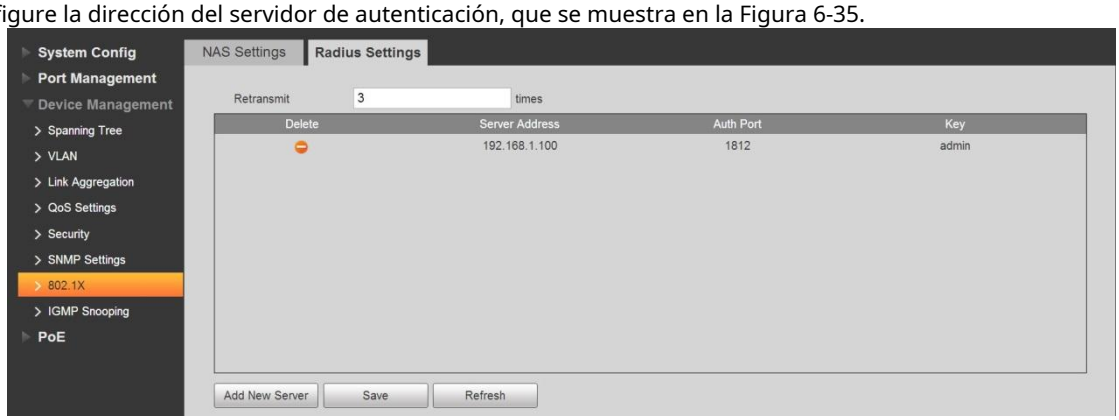


Figura 6-35

6.8 Inspección IGMP

IGMP Snooping (Internet Group Management Protocol Snooping) se opera en el dispositivo de capa dos, es para generar la tabla de reenvío de multidifusión de capa dos mediante la búsqueda del paquete IGMP entre el dispositivo de capa tres y el host, que es para administrar y controlar el reenvío de paquetes de datos de multidifusión y realizar la distribución requerida de la capa dos del paquete de datos de multidifusión.

6.8.1 Teoría de indagación IGMP

El dispositivo operativo de capa dos de IGMP Snooping puede establecer una relación de mapeo para el puerto y la dirección de multidifusión MAC a través del análisis sobre el paquete IGMP recibido, y es para reenviar datos de multidifusión de acuerdo con la relación de mapeo.

Los datos de multidifusión se transmitirán en la red de capa dos cuando el dispositivo de capa dos no opere IGMP Snooping; después de que el dispositivo de capa dos opera IGMP Snooping, los datos de multidifusión conocidos de

El grupo de multidifusión no se transmitirá en la red de capa dos, sino que se transmitirá a los receptores designados.

IGMP Snooping solo puede reenviar la información a los receptores necesarios a través de la multidifusión de capa dos, lo que puede traer las siguientes ventajas:

- Reduzca el paquete de difusión en la red de capa dos, ahorre ancho de banda de la red; Mejorar la
- seguridad de la información de multidifusión;
- Aporta comodidad para realizar la facturación individual para cada anfitrión.

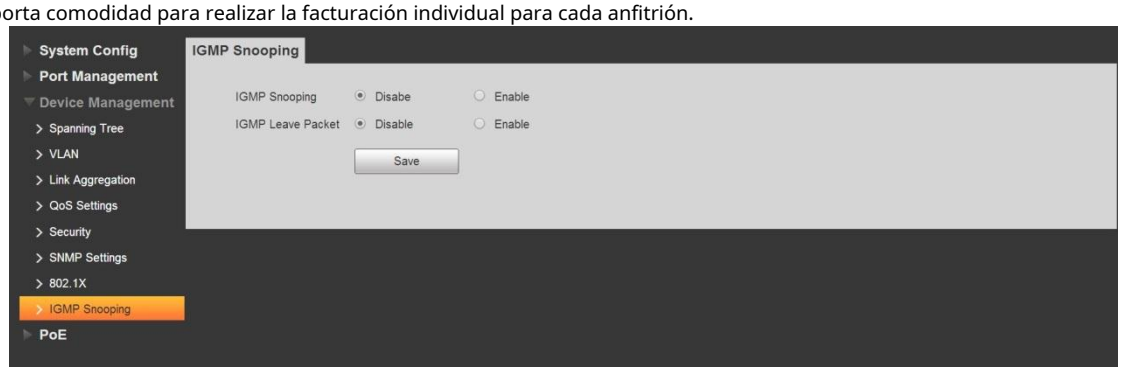


Figura 6-36

La interfaz de configuración de IGMP Snooping se muestra en la Figura 6-36.

- IGMP Snooping: habilita o deshabilita la función IGMP Snooping. Paquete de
- salida IGMP: habilita o deshabilita la función de salida rápida.

7 PoE

7.1 Configuración de PoE

Power over Ethernet (PoE) significa que el dispositivo usa el puerto Ethernet para proporcionar energía al dispositivo a través del cable de par trenzado de forma remota. La función PoE realiza el suministro de energía centralizado y es fácil de respaldar. El terminal de red solo usa un cable de red simple sin fuente de alimentación externa. Cumple con IEEE 802.3af e IEEE 802.3at y adopta el puerto de alimentación universal reconocido. Es para la cámara IP, teléfono IP, punto de acceso inalámbrico (AP inalámbrico), cargador de dispositivo portátil, POS, adquisición de datos, etc.

Consulte la Figura 7-1 para conocer el sistema PoE. Incluye alimentación PoE, equipo de suministro de energía (PSE), interfaz de alimentación (PI) y dispositivo alimentado (PD).

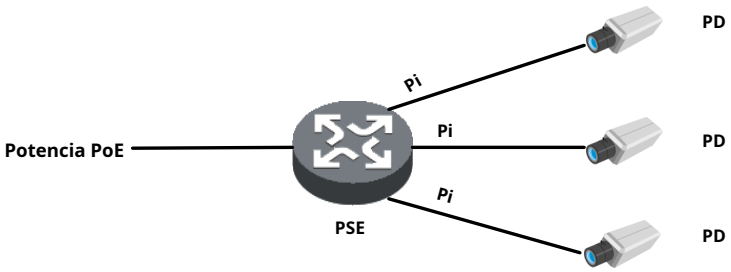


Figura 7-1

1. Energía PoE
PoE proporciona energía a todo el sistema.
2. PSE
El PSE debe proporcionar energía al PD directamente. El PSE admite funciones como buscar, detectar PD, categorizar PD y proporcionarle energía, realizar la gestión del consumo de energía, verificar la conexión de PD, etc.
3. PI
PI se refiere a la interfaz Ethernet que tiene la función PoE. Se llama puerto PoE. Incluye FE y GE.

El suministro de energía remoto PoE tiene dos modos:

- Sobre cables de señal: el PSE utiliza los pares (1, 2, 3, 6) para transmitir datos en un cable de par trenzado de categoría 3/5 para suministrar energía de CC mientras transmite datos a los PD.
- Sobre cables de repuesto: el PSE utiliza los pares (4, 5, 7, 8) que no transmiten datos en un cable de par trenzado de categoría 3/5 para suministrar alimentación de CC a los PD.

Nota: El modo de suministro de energía depende de las especificaciones de PD. El modo seleccionado debe admitir PSE y PD al mismo tiempo. Si el modo de suministro de energía PSE y PD no es el mismo (por ejemplo, el PSE no admite el suministro de energía del cable de repuesto o el PD solo admite el suministro de cable de repuesto), utilice el convertidor para proporcionar energía al PD.

4. PD

PD se refiere al dispositivo que recibe energía del PSE. Incluye teléfono IP, AP inalámbrico, cargador portátil, POS, cámara de red, etc.

Cuando el PD disfruta de la energía del dispositivo PoE, puede conectarse a otro dispositivo para hacer una copia de seguridad de la energía.

Referirse aTabla 7-1 para puerto información de configuración detallada.

Nombre	Nota
Puerto	En la figura del panel para seleccionar el puerto PoE. Los puertos seleccionados se mostrarán en la lista Puertos seleccionados en la parte inferior de la interfaz.
Estado de energía	Habilite o deshabilite PoE en los puertos seleccionados. - El sistema no suministra energía ni reserva energía para el PD conectado a un puerto PoE si el puerto PoE no está habilitado con la función PoE. - Se le permite habilitar PoE para un puerto PoE si el puerto PoE no da como resultado una sobrecarga de energía PoE; de lo contrario, no puede habilitar PoE para el puerto PoE. De forma predeterminada, PoE está deshabilitado en un puerto PoE. **Importante** Sobrecarga de energía de PSE: cuando la cantidad total de consumo de energía de todos los puertos excede la potencia máxima de PSE, el sistema considera que el PSE está sobrecargado.
Total poder consumo valor reservado	Sirve para establecer el valor reservado del consumo de energía total del puerto PoE. El valor de consumo de energía total de PoE se refiere al consumo de energía total para el PD desde todos los puertos PoE. Cuando el consumo de energía del PD conectado es mayor que el consumo de energía total de PoE, deja de suministrar energía al PD.

Tabla 7-1

Consulte la Figura 7-2 para ver la interfaz de configuración.

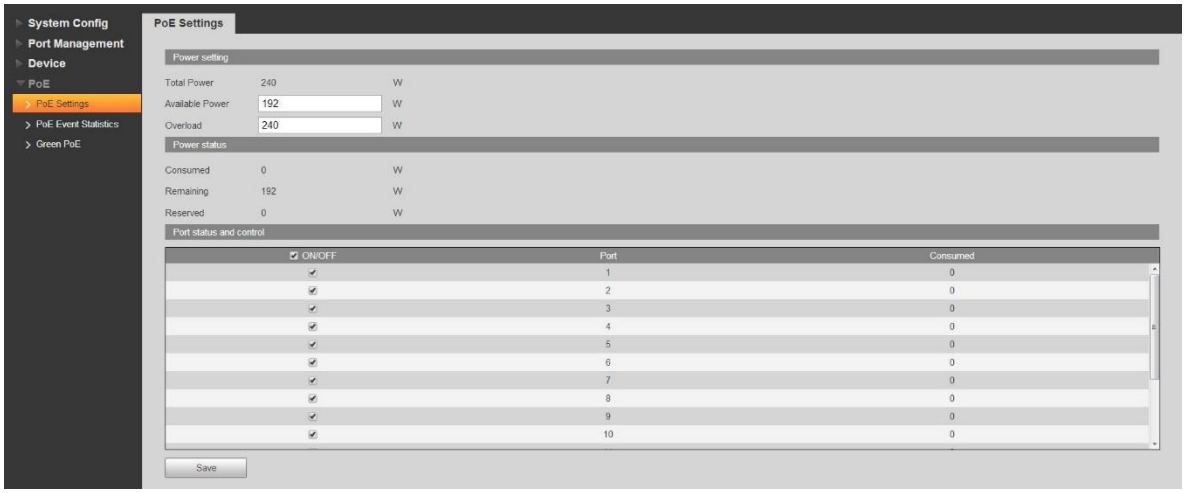


Figura 7-2

7.2 Eventos PoE

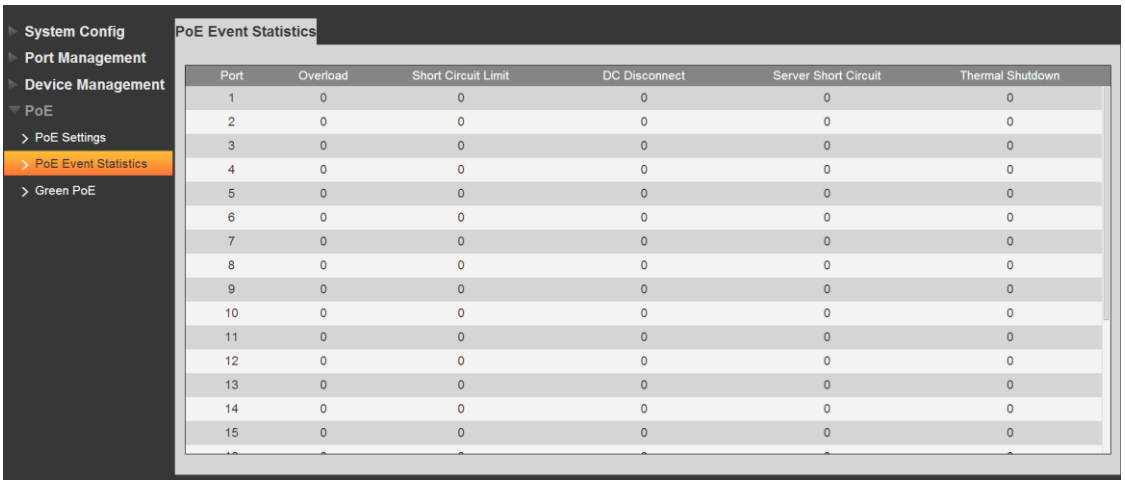


Figura 7-3

En la Figura 7-3, muestra las estadísticas de eventos de PoE de cada puerto. Incluye sobrecarga, límite de cortocircuito, desconexión de CC, cortocircuito del servidor y apagado térmico.

Consulte la Tabla 7-2 para conocer los parámetros de eventos de PoE.

Nombre	Nota
Sobrecarga	La corriente de alimentación de arranque de un solo puerto ha superado el umbral de corriente.
límite de cortocircuito	Cuando el chip de alimentación envía energía al puerto, se produce un cortocircuito.
Desconexión de CC	La alimentación de un solo puerto está apagada
Servidor cortocircuito	La energía es un cortocircuito cuando el chip de alimentación envía energía.
Térmico Apagar	La temperatura del chip de alimentación es demasiado alta debido a un cortocircuito u otra razón.

Tabla 7-2

7.3 PoE verde

En la Figura 7-4, se configuran los parámetros de ahorro de energía de PoE. La función PoE está apagada en el período especificado para ahorrar energía. Cuando termina el período, el puerto reanuda automáticamente el suministro de energía.

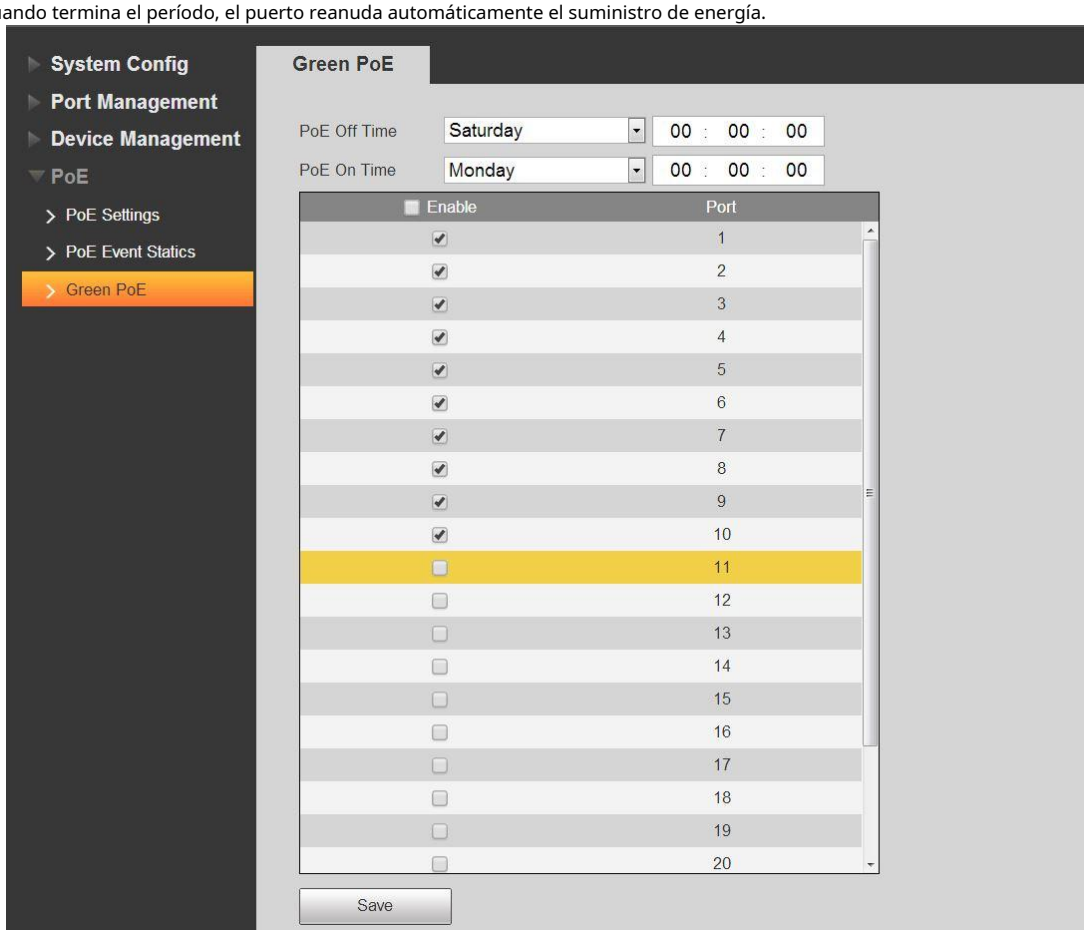


Figura 7-4

Consulte la Tabla 7-3 para obtener información detallada sobre la configuración de Green PoE.

Nombre	Nota
PoE fuera de tiempo	La corriente de entrada del puerto único ha superado su umbral de corriente del puerto de salida.
PoE a tiempo	El puerto de envío está en cortocircuito cuando el chip está probando energía al puerto.
Puerto	Los puertos que se seleccionarán.

Tabla 7-3

Ejemplo de configuración.

1. Conexión de red

El puerto del 1 al 10 se cerrará todos los sábados y domingos, y se reanudará automáticamente los lunes.

2. Configuración

(1) Configure el período de inactividad del puerto de sábado a domingo y reinicie automáticamente la energía el lunes. Establecer

(2) puertos.

(3) Clic en Guardar. Consulte la Figura 7-5 para obtener información detallada.

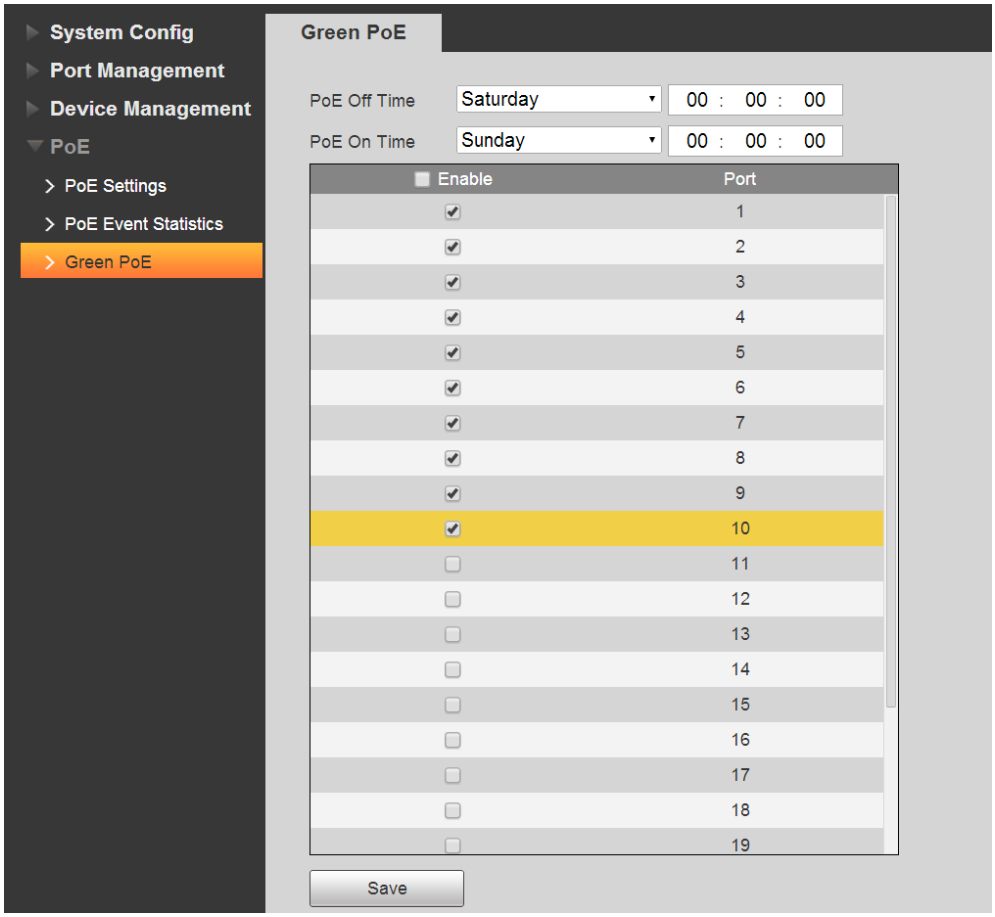

System Config
Port Management
Device Management
PoE
PoE Settings
PoE Event Statistics
Green PoE
Green PoE
PoE Off Time
Saturday
00 : 00 : 00
PoE On Time
Sunday
00 : 00 : 00
Enable
Port
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
Save

Figura 7-5

TECNOLOGÍA CO., LTD DE LA VISIÓN DE ZHEJIANG DAHUA

Dirección: No.1199, Bin'an Road, Binjiang District, Hangzhou, PR China Código postal: 310053

Tel: + 86-571-87688883

Envíe por fax: + 86-571-87688815

Correo electrónico: overseas@dahuatech.com

Sitio web: www.dahuasecurity.com